राजस्थान पुलिस अकादमी, जयपुर

Volume – I

साइबर फोरेन्सिक एवं साइबर अपराध अनुसंधान

यतीन्द्र कुमार, पुलिस निरीक्षक

B.Sc. , M.A. , NET (UGC)

आभार

इस पुस्तक के लेखन के लिए मैं राजस्थान पुलिस अकादमी, जयपुर व इसके अतिरिक्त महानिदेशक पुलिस एवं निदेशक महोदय श्री राजीव शर्मा व अतिरिक्त निदेशक महोदय व महानिदेशक पुलिस श्री राघवेंद्र सुहास का आभारी हुॅ, जिनकी प्रेरणा व मार्गदर्शन से इस पुस्तक का लेखन सम्भव हो सका। इस पुस्तक के लेखन में मेरे द्वारा महत्त्वपूर्ण सामग्री अलग–अलग स्रोतो जैसे कि किताबों, लेखों, माननीय न्यायालयों के समय–समय पर दिये गये मार्गदर्शक निर्णयों, पुस्तकालय, वेबसाइट्स आदि से एकत्रित की गई जिनको मै धन्यवाद देना चाहता हुॅ। इस पुस्तक का उद्देश्य पुलिस कार्मिकों को साइबर अपराधों में मामलों में सामान्य भाषा में जानकारी देते हुए अनुसंधान के बारे में मार्गदर्शन प्रदान करना है। जो बिना किसी वित्तीय लाभ के निःशुल्क उपलब्ध कराई जावेगी। इस पुस्तक के लेखन में यदि किसी प्रकार की त्रृटी रहती है तो उनके सुधार हेतु सुझाव हमेशा आमंत्रित है। यह पुस्तक केवल मार्गदर्शन के लिए है। यदि इस पुस्तक में किसी भी प्रकार की त्रृटी रहती है तो लेखक इसके लिए उत्तरदायी नहीं होगा। इस पुस्तक की प्रति अकादमी के पुस्तकालय में भी उपलब्ध रहेगी। आशा करता हुॅ कि यह पुस्तक पुलिस कर्मियों के ज्ञानवर्धन करने में फलीभूत सिद्व होगी।

(यतींद्र कुमार खटाना)
पुलिस निरीक्षक
राजस्थान पुलिस अकादमी,
जयपुर
मोबाइल नंबर 7014158101
दिनांक 15.06.2022

अनुक्रमणिका

अध्याय–1

इलेक्ट्रोंनिक / डिजिटल साक्ष्य

- इलेक्ट्रोनिक साक्ष्य के सिद्वान्त
- अपराध स्थलो पर इलेक्ट्रोनिक साक्ष्य
- इलेक्ट्रोनिक उपकरणों, मोबाइल फोन, अन्य भण्डारण साधनों की जब्ती तथा संभाल व परिवहन
- साइबर अन्वेषण में इलेक्ट्रोनिक साक्ष्यों की भूमिका व चुनौतियॉ

साक्ष्य का परिचय

भारतीय साक्ष्य अधिनियम की धारा 3 में साक्ष्य को परिभाषित किया गया हैा साक्ष्य दो प्रकार के होते है जो निम्न प्रकार से है–

- मौखिक साक्ष्य– अदालत के सामने गवाहों द्वारा दिए गए बयान जो जॉच के तथ्यों से संबंधित है ऐसे बयानों को मौखिक साक्ष्य कहा जाता हैा
- दस्तावेजी साक्ष्य – न्यायालय के निरीक्षण के लिए पेश किए गए सभी दस्तावेज जिनमें इलेक्ट्रॉनिक रिकॉर्ड भी सम्मिलित है ऐसे दस्तावेजों को दस्तावेजी साक्ष्य कहा जाता है।

डिजिटल साक्ष्य को परिभाषित करनाः

डिजिटल साक्ष्य को आईटी संशोधन अधिनियम 2008 की धारा 79ए में परिभाषित किया गया हैा वह संभावित मूल्य जिसे इलेक्ट्रॉनिक रूप में संग्रहीत या प्रसारित किया जा सकता हैा उसे डिजिटल साक्ष्य कहते हैा कंप्यूटर, डिजिटल ऑडियो, डिजिटल वीडियो, सेल फोन, फैक्स मशीन, स्टोरेज डिवाइस आदि डिजिटल साक्ष्य हैा

डिजिटल साक्ष्य की विशेषताएंः–

डिजिटल साक्ष्य की कुछ प्रमुख विशेषताओं में शामिल हैंः–

- डिजिटल साक्ष्य की कई प्रतिया बनाई जा सकती हैा जिसके कारण जब कभी डिजिटल साक्ष्य में किसी भी प्रकार की कॉट छॉट हो या वह नष्ट हो जावे तो दूसरी प्रतियों के माध्यम से उनका विश्लेषण किया जा सके । ये विशाल और विभाजित रूप में होते है ।
- डिजिटल साक्ष्य के बारे में की गई समस्त कार्यवाही को प्रलेखित (डाक्यूमेंटेड) किया जाना अनिवार्य हैा ताकि अनुसंधान के दौरान किसी भी प्रकार की कॉटछॉट से बचा जा सको
- एकत्र, संग्रहीत या प्रेषित किए जाने के दौरान कोई सबूत नहीं बदला जाना चाहिए।

भारतीय साक्ष्य अधिनियम और आईटी अधिनियम में डिजिटल साक्ष्यः–

•प्राथमिक और द्वितीयक साक्ष्य

भारतीय साक्ष्य अधिनियम के तहत, दस्तावेजों की सामग्री को प्राथमिक या द्वितीयक साक्ष्य द्वारा साबित किया जा सकता है। अधिनियम की धारा 62 "प्राथमिक साक्ष्य को. स्वयं न्यायालय के निरीक्षण के लिए प्रस्तुत किए गए दस्तावेज' के रूप में परिभाा्ित करती है।

अधिनियम की धारा 63 (2) 'द्वितीयक साक्ष्य' को 'यांत्रिक प्रक्रियाओं द्वारा मूल से बनाई गई प्रमाणित प्रतियां' के रूप में परिभाषित करता है, जो अपने आप में प्रतिलिपि की सटीकता सुनिश्चित करता है।

द्वितीयक साक्ष्य से संबंधित कुछ महत्वपूर्ण धाराऍ निम्न प्रकार से है–

- धारा 65: ऐसे मामले जब इस तरह की मूल प्रकृति को न्यायालय के समक्ष ले जाए जाना आसान न हो जिनमें दस्तावेजों से संबंधित द्वितीयक साक्ष्य दिए जा सकते हैं ।
- धारा 65एः इलेक्ट्रॉनिक रिकॉर्ड से संबंधित साक्ष्य के बारे में विशेष प्रावधान – इलेक्ट्रॉनिक रिकॉर्ड की सामग्री को धारा 65बी के प्रावधानों के अनुसार द्वितीयक साक्ष्य द्वारा साबित किया जा सकता है।
- धारा 65बीः इलेक्ट्रॉनिक रिकॉर्ड की स्वीकार्यता के लिए शर्ते–

एक इलेक्ट्रॉनिक रिकॉर्ड में निहित कोई भी जानकारी जो एक कंप्यूटर द्वारा उत्पादित ऑप्टिकल या चुंबकीय मीडिया में एक कागज पर मुद्रित, संग्रहीत, रिकॉर्ड या कॉपी की गई है, को भी एक दस्तावेज माना जाएगा, यदि इस खंड में उल्लिखित शर्तों को संतुष्ठ करता है तो द्वितीयक साक्ष्य मान्य होगा।

.आईईए की धारा 65 बीः इलेक्ट्रॉनिक रिकॉर्ड की स्वीकार्यता के लिए शर्तें

साक्ष्य अधिनियम की धारा 65बी(4) के तहत, यदि इलेक्ट्रॉनिक रिकॉर्ड को द्वितीयक साक्ष्य के रूप में प्रस्तुत करना है तो उसे निम्न प्रकार की बशर्ते को संतुष्ठ करना आवश्यक है–

प्रमाण पत्र पेश किया जाना आवश्यक है जिसमें

- एक जो वाले इलेक्ट्रॉनिक रिकॉर्ड की पहचान का विवरण।
- इलेक्ट्रॉनिक रिकॉर्ड तैयार के तरीके का विवरण।
- जिस उपकरण की सहायता से इलेक्ट्रॉनिक रिकॉर्ड तैयार किया गया है उसका विवरण सम्मिलित होना आवश्यक है।
- एक जिम्मेदार आधिकारिक जिसकी अधिकारिता में डिवाइस हो द्वारा प्रमाण पत्र पर हस्ताक्षर किए जाने चाहिए।

आईईए की धारा 65 बीः इलेक्ट्रॉनिक साक्ष्य की प्रामाणिकता

यदि साक्ष्य अधिनियम की धारा 65बी के अनुसार इलेक्ट्रॉनिक रिकॉर्ड को विधिवत प्रस्तुत किया जाता है, तो इसकी वास्तविकता पर सवाल उठेगा और उस स्थिति में, धारा 45ए – इलेक्ट्रॉनिक साक्ष्य के परीक्षक की राय का सहारा लिया जा सकता है।

भारतीय साक्ष्य अधिनियम की धारा 45ए में कहा गया है किः–

जब एक कार्यवाही में, अदालत को किसी भी कंप्यूटर संसाधन या किसी अन्य इलेक्ट्रॉनिक या डिजिटल रूप में प्रेषित या संग्रहीत किसी भी जानकारी से संबंधित किसी भी मामले पर एक राय बनानी होती है, इलेक्ट्रॉनिक के परीक्षक की राय सूचना प्रौद्योगिकी अधिनियम, 2008 की धारा 79ए में संदर्भित साक्ष्य एक प्रासंगिक तथ्य है।

डिजिटल साक्ष्य के स्रोत

डिजिटल साक्ष्य के कुछ स्रोत इस प्रकार हैं:

कंप्यूटर, लैपटॉप और मोबाइल डिवाइस	कंप्यूटर/लैपटॉप/मोबाइल फोन फाइलों को स्टोर करते हैं जिनमें छवियों, वीडियो और हटाई गई फाइलों होती है।
ब्राउजर इतिहास	ब्राउजिंग इतिहास में वेबसाइटों का इतिहास होता है जिसमें उपयोगकर्ताओं द्वारा जिस समय व तिथि पर जो भी ब्राउजर में खोज की है उसके बारे में जानकारी होती हैा
जीपीएस जीपीएस	डिवाइस यात्रा लॉग प्रदान करता है जिसमें घर स्थान, पिछले गंतव्य, आदि के लॉग होते है।
सर्वर	सर्वर अंतिम लॉगिन, मेल एक्सचेंज, डाउनलोड की गई सामग्री, खोज और प्राप्त किए गए पेज की जानकारी होती है।
रिमूवेबल स्टोरेज मीडिया और	रिमूवेबल स्टोरेज मीडिया और डिवाइस में इमेज और वीडियो सहित फाइलों और फोल्डर होते है।

इलेक्ट्रॉनिक साक्ष्य के सिद्धांतः–

लोकार्ड का विनिमय सिद्धांत

लोकार्ड का विनिमय सिद्धांत एक दर्शक सिद्वान्त है जो बताता है कि अपराधी जब कोई अपराध करता है तो वह अपने अपराध के साक्ष्य अपराध स्थल पर अवश्य छोड कर जाता है साथ ही कुछ साक्ष्य वह अपने साथ ले जाता हैा

यह सिद्वान्त डिजिटल फोरेंसिक में भी लागू होता है। डिजिटल विधि विज्ञान के परिप्रेक्ष्य में इस सिद्वान्त के अनुसार कोई भी साइबर अपराधी अपने द्वारा इस्तेमाल की गई तकनीक व तरीके के साक्ष्य अपराध स्थल पर छोड कर अवश्यक जाता है साथ ही कुछ साक्ष्य अपने पास अवश्य ले जाता है जिसकी कॉपी अनुसंधान अधिकारी के लिए बहुत उपयोगी होती है।

ड्यूबर्ट का नियम

ड्यूबर्ट का नियम विशेषज्ञ गवाह गवाही की स्वीकार्यता के संबंध में साक्ष्य का नियम है। यह नियम बताता है कि न्यायालय में किसी की विशेषज्ञ गवाही स्वीकार्य होने के लिए कुछ शर्ते है– विशेषज्ञ उसे माना जाएगा जो

- संबंधित क्षेत्र में उचित शिक्षा प्राप्त किया हो।
- उसमें प्रशिक्षण प्राप्त किया हो साथ ही उसे अपने कार्य का अनुभव हो।
- जो वह न्यायालय में गवाही दे वह उस क्षेत्र में कार्य करने वाले अपने सहकर्मियों से समानता रखती हो।

- जिस अपराध के तथ्य के बारे में विशेषज्ञ के तौर पर गवाही दी जा रही हो उस तथ्य से संबंधित हो।
- वह अपने द्वारा जिन पद्वति और सिद्वान्तों को उपयोग कर अपनी गवाही दे रहा हो वे सब उस क्षेत्र के सामान्य सिद्वान्त हो।
- उसके निष्कर्ष के जो भी परिणाम आये वे आवश्यकता पडे तो उन्हे पुनः दौराया जा सके। दोहराव को समान परीक्षण वातावरण जैसे समान डिस्क, कंप्यूटर आदि पर समान परीक्षा परिणाम प्राप्त करने की क्षमता के रूप में परिभाषित किया गया है। ऐसी स्थितियां जहां एक ही प्रयोगशाला में समान परीक्षण मदों पर एक ही ऑपरेटर द्वारा एक ही उपकरण का उपयोग करके कम समय के भीतर स्वतंत्र परीक्षण के परिणाम एक ही विधि से प्राप्त किए जाते हैं।

अपराध स्थल पर डिजिटल साक्ष्यः–

डिजिटल साक्ष्य को उनकी उत्पत्ति के आधार पर निम्न प्रकार से विभाजित किया गया–

1.उपयोगकर्ता द्वारा सृजितः इन साक्ष्यों में उपयोग कर्ता द्वारा बनाई गई फाइलें होती हैं जैसे कि पाठ्य दस्तावेज, ईमेल, चौट, चित्र, वीडियो और सिस्टम पर उपयोक्ता द्वारा बनाए गए वेब पृष्ठ।

2.उपयोगकर्ता द्वारा सुरक्षितः इन साक्ष्यों में वे फाइल या डिवाइस है जो उपयोगकर्ता द्वारा पासवर्ड का उपयोग करके सुरक्षित किए जाते हैं। साक्ष्य प्राप्त करने या उसका विश्लेषण करने के लिए इन डिजिटल साक्ष्यों तक पहुच प्राप्त करने से पहले उपयोगकर्ता से प्रमाण पत्र प्राप्त करने की आवश्यकता होती है। उदाहरणों में उपयोगकर्ता द्वारा या सिस्टम द्वारा बनाई गई फाइलें या पासवर्ड का उपयोग करके उपयोगकर्ता द्वारा संरक्षित फाइलें शामिल हैं।

3. सिस्टम द्वारा उत्पन्नः ऑपरेटिंग सिस्टम द्वारा स्वत उपयोगकर्ता के बिना बनाए जाते हैं।

ये बहुत महत्वपूर्ण हैं और जांच के दृष्टिकोण से बहुत सारी महत्वपूर्ण जानकारी प्रदान कर सकते है। उदाहरण के लिए, उपयोगकर्ता गातिविधि लॉग, ब्राउजर कैश, कुकीज, ब्राउजर इतिहास, कुकीज और ऑपरेटिंग सिस्टम द्वारा बनाई गई रजिस्ट्री फाइलों को बिना किसी महत्वपूर्ण उपयोगकर्ता सहभागिता के सिस्टम द्वारा बनाई जाती है।

डिजिटल साक्ष्य को उनके स्थायित्व के आधार पर दो भागों में विभाजित किया जा सकता है:–

(1) अस्थिर और (2) स्थिर मेमोरी डिजिटल साक्ष्य

चूंकि अपराधी डाटा भण्डारण के लिए कई प्रकार के डिजिटल साधनों का उपयोग करते हैा जो स्थिर प्रकार के और अस्थिर प्रकार के होते है।

अस्थिर (वोलेटाइल)

यह अस्थिर प्रकार की कंप्यूटर स्मृति है जो केवल कम्प्यूटर के पावर ऑन होने पर ही जानकारी को भण्डारित रख सकती है। रैम अस्थिर स्मृति उदाहरण है। लेकिन जब कम्प्यूटर की बिजली बाधित होती है तो उसमें संगृहित डाटा नष्ठ हो जाता है। अस्थिर डिजिटल साक्ष्य की कुछ विशेषताएं निम्न प्रकार से हैः–

- ये सामग्री को अस्थायी रूप से संग्रहीत करते हैं।
- इनकी भण्डारण क्षमता कम होती है।
- ऐसे साक्ष्य में प्रोसेसर की डेटा तक सीधी पहुंच होती है।

अस्थिर डिजिटल साक्ष्य के उदाहरण हैः–नेटवर्क कनेक्शन, रनिंग प्रोसेस, ओपन फाइल्स, रैम और कैशे मेमोरी।

स्थिर (नॉन वोलेटाइल)

यह एक प्रकार की कंप्यूटर मेमोरी है जो कंप्यूटर के बंद होने के बाद भी संग्रहीत जानकारी को बरकरार रख सकती है। हार्ड ड्राइव, फ्लॉपी डिस्क, पेन ड्राइव और फ्लैश मेमोरी गैर–वाष्पशील मेमोरी के उदाहरण हैं।स्थिर (नॉन वोलेटाइल) साक्ष्य की विशेषताएं निम्न प्रकार से हैः–

- सामग्री स्थायी रूप से संग्रहीत है।
- अस्थिर साक्ष्य की तुलना में इनकी भंडारण क्षमता अधिक होती है।
- प्रोसेसर के पास डेटा तक कोई सीधी पहुंच नहीं है।

स्थिर (नॉन वोलेटाइल) डिजिटल साक्ष्य के उदाहरणों में शामिल हैं हार्ड डिस्क ड्राइव या एचडीडी, यूएसबी स्टोरेज डिवाइस, रॉम, सीडी, डीवीडी, ब्लू रे और फ्लॉपी डिस्क।

डिजिटल उपकरणों, मोबाइल फोन, अन्य भण्डारण साधनों की जब्ती तथा उनका संचालन व परिवहन

साइबर क्राइम से संबंधित प्रकरणों में मुख्य भौतिक साक्ष्यध्कंप्यूटर या संबंधी उपकरण जिनके अंदर संभावित साक्ष्य हो सकते हैं वह निम्न है दृ कंप्यूटर, लैपटॉप, मोबाइल फोन, स्टोरेज मीडिया (मेमोरी कार्ड, यूएसबी ड्राइव, सीडी, डीवीडी, डिजिटल कैमरा मेमोरी के साथ, स्मार्ट वॉचेस, डीवीआर इत्यादि है।

इन सभी प्रकार के उपकरणों में डिजिटल साक्ष्य किसी ना किसी फाइल के रूप में जैसे कि ऑडियो फाइल, वीडियो फाइल, डॉक्यूमेंट फाइल, पिक्चर फाइल इत्यादि के रूप में उपलब्ध हो सकते हैं. इन डिजिटल एविडेंसेस के कुछ अन्य स्वरूप भी हो सकते हैं जैसे कि किसी कंप्यूटर पर विशेष प्रकार के सॉफ्टवेयर का इंस्टॉल होना पाया जाना किसी साइबर अपराध को इंगित करता है, किसी साइबर अपराध के प्रतिपादित होने से संबंधित

लॉग फाइल्स, डिवाइस में कंफीग्रर किए गए आईपी ऐड्रेसेस या किसी विशेष प्रक्रिया के तकनीक का इस्तेमाल करके किसी वेबसाइट या संबंधित एप्लीकेशन को एक्सेस करना या डाटा के साथ छेड़छाड़ करने से संबंधित साक्ष्य डिजिटल एविडेंसेस की कैटेगरी में आते हैं. साइबर क्राइम से संबंधित सभी डिजिटल उपकरणों को निम्न पांच कैटेगरी में विभाजित कर दिया गया है यह कैटेगरी निम्नानुसार हैं–

1. कंप्यूटर
2. लैपटॉप
3. मोबाइल फोन या टैबलेट पीसी
4. डिजिटल वीडियो रिकॉर्डर (डीवीआर)
5. अकेले स्टोरेज मीडिया (सीडी, डीवीडी, मेमोरी कार्ड, यूएसबी डाइव आदि)

यह संभव हो सकता है कि एक कंप्यूटर सिस्टम, लैपटॉप, मोबाइल फोन और डीवीआर में अलग–अलग ऑपरेटिंग सिस्टम हो। भौतिक साक्ष्यों को जब्त करने की प्रक्रिया समान ही रहती है साथ ही इमेजिंग और क्लोनिंग की प्रक्रिया भी एक ही है। इन साक्ष्यों का विश्लेषण और महत्वपूर्ण साक्ष्यों का निष्कर्षण अलग हो सकता है। प्रत्येक ऑपरेटिंग सिस्टम में अलग–अलग फाइल हस्ताक्षर (signature) होते हैं, इसलिए इन ऑपरेटिंग सिस्टम और उसके फाइल सिस्टम के बारे में बुनियादी जानकारी होना जरूरी है। सबसे आम प्रकार ऑपरेटिंग सिस्टम इस प्रकार है –

s.no	डिवाइस के प्रकार	ऑपरेटिंग सिस्टम का नाम
1.	कंप्यूटर/लैपटॉप	विंडोज ऑपरेटिंग सिस्टम (विभिन्न वर्जन के साथ), लिनक्स ऑपरेटिंग सिस्टम (ubuntu, RedHat, Fedora, Centos, puppy, Mint, Gnome, chrome इत्यादि), मैक ऑपरेटिंग सिस्टम Mojave (released in 2018), High Sierra (2017), and Sierra (2016).)
2.	मोबाइल फोन	गूगल एंड्रॉयड, कस्टमराइज्ड एंड्रॉयड ऑस, ब्लैकबेरी, Apple iOS, KaiOS, विंडोज मोबाईल, सिमबीयन
3.	डीवीआर	विंडोज आधारित , लिनक्स आधारित DVR

उपरोक्त वर्णित उपकरणों के लिए जब्ती प्रक्रिया को निम्नलिखित प्रवाह चार्ट के अनुसार आगे वर्गीकृत किया जा सकता है और श्रेणी के अनुसार साक्ष्य के अनुसार अनुसरण किया जा सकता है:

(1) कंप्यूटर

- कंप्यूटर चालू स्थिति में बिना लॉक और नेटवर्क कनेक्टेड है
- कंप्यूटर बिना लॉक के चालू स्थिति में है लेकिन कोई नेटवर्क कनेक्ट नहीं है
- लॉक स्थिति के साथ और नेटवर्क कनेक्शन के साथ या बिना कंप्यूटर चालू स्थिति में
- कंप्यूटर बंद स्थिति में

(2) लैपटॉप

- बिना लॉक और नेटवर्क कनेक्टेड लैपटॉप ऑन कंडीशन में है
- लैपटॉप बिना लॉक के चालू स्थिति में है लेकिन कोई नेटवर्क कनेक्ट नहीं है
- लैपटॉप ऑन कंडीशन में लॉक कंडीशन के साथ और नेटवर्क कनेक्शन के साथ या बिना
- लैपटॉप बंद स्थिति में

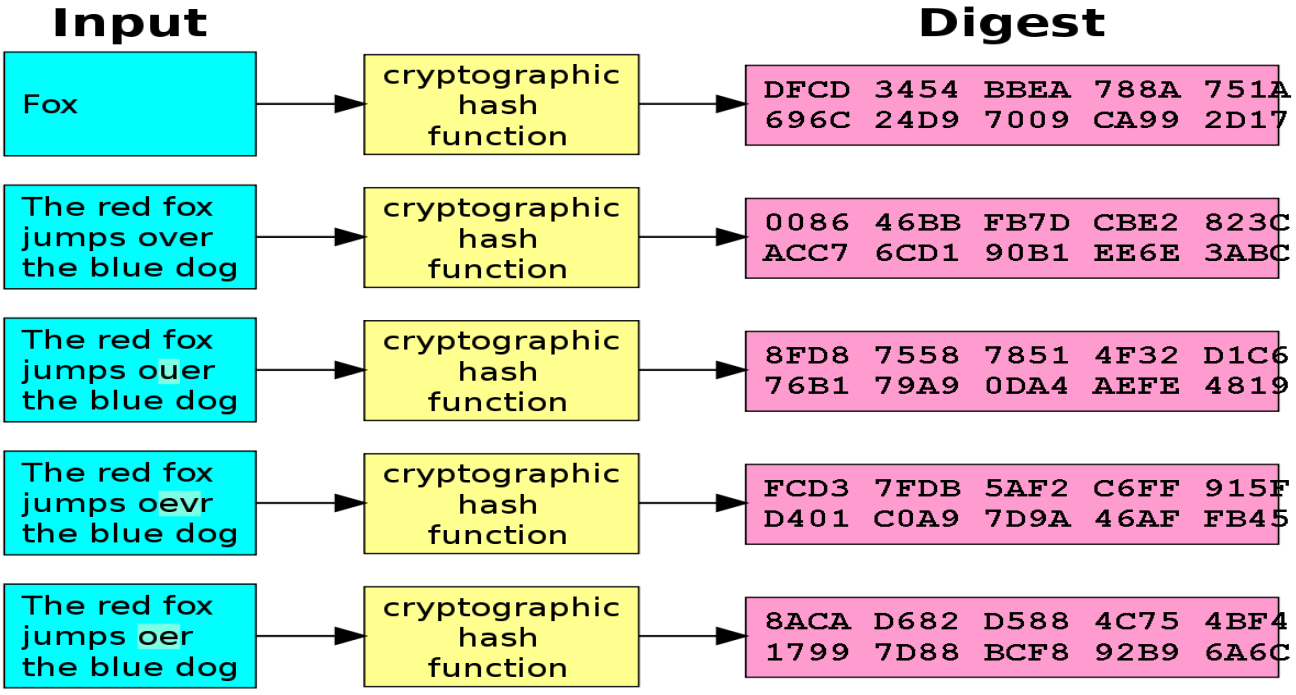
(3) मोबाइल फोन

- बिना मोबाइल फोन ऑन कंडीशन में और पासवर्ड
- मोबाइल फोन बंद हालत में

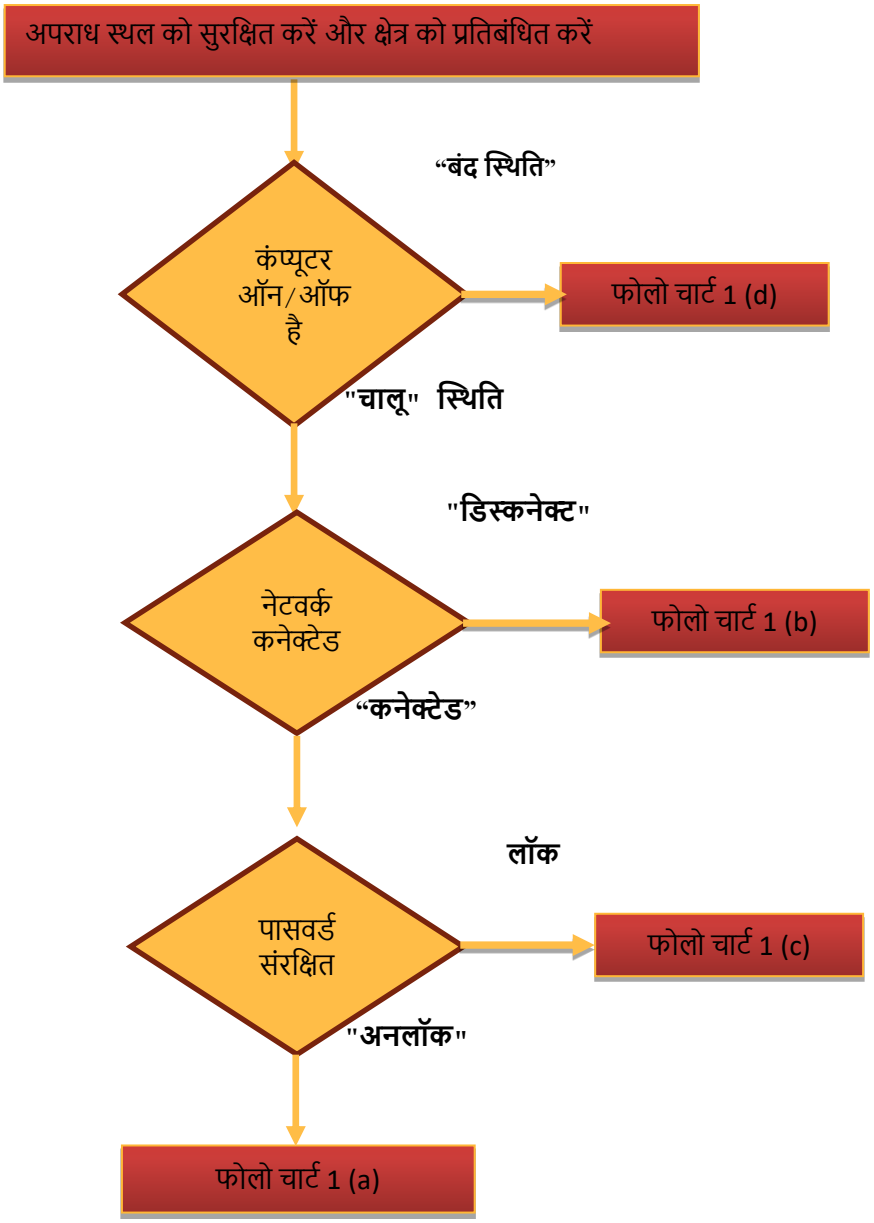
(4) **डीवीआर**

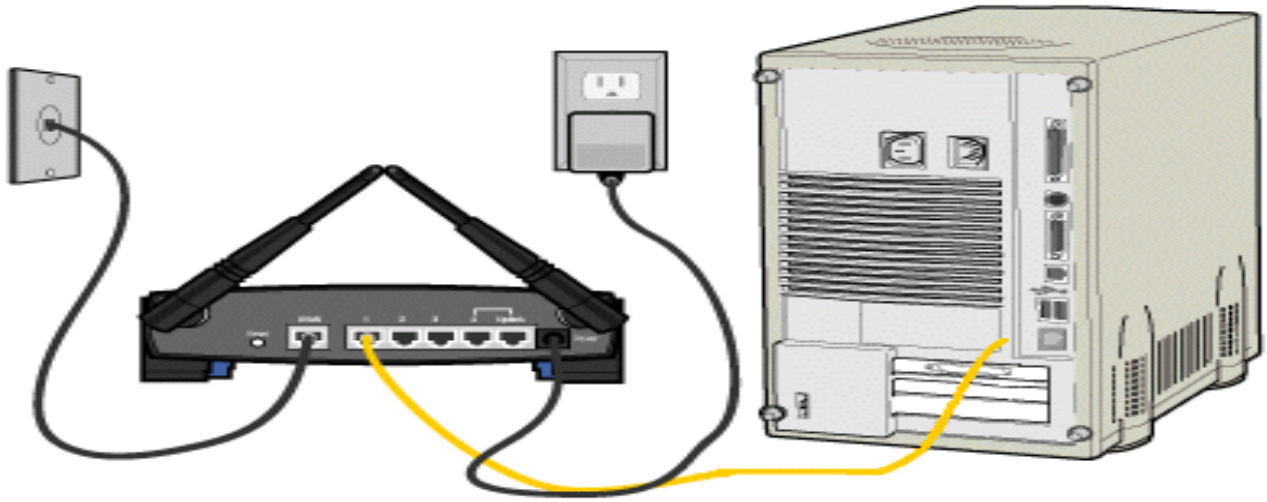
हैशिंग और हैश वैल्यू:–

हैशिंग करने से पूर्व यह जानना बहुत जरूरी है कि हैशिंग कब कि जानी चाहिए? इसलिए जब भी स्टॉरिज डिवाइस हो जिसमें हम दंसलेपे के लिए कुछ फाइल भेजनी है तो डेटा की पदजमहतपजल(कोई बदलाव नहे हुआ है) को साबित करने के लिए हैश मूल्य की गणना की जानी आवश्यक है। डेटा की `integrity` की गणना करने के लिए हैशिंग एक गणितीय `(mathematical)` ऑपरेशन है। इस प्रकार, हैश वैल्यू डिजिटल साक्ष्य की विशिष्ट पहचान बताता है। यह एक डिजिटल साक्ष्य की अखंडता (इंटीग्रिटी) का प्रतिनिधित्व करता है यद्यपि आज के समय में कई प्रकार की है एल्गोरिथ्म उपलब्ध हैं परंतु इन सभी से में से `md5` एवं `sha1` की सर्वाधिक लोकप्रिय एवं विश्वसनी एल्गोरिथ्म है।



साइबर क्राइम से संबंधित केस के सबूतों की अखंडता को सुनिश्चित करने के लिए डिजिटल एविडेंस के साथ इसकी संबंधित हैश वैल्यू की भेजी जानी चाहिए इससे यह साबित हो सकेगी चौन आफ कस्टडी को पूरी तरीके से मेंटेन रखा गया है एवं किसी भी प्रकार की कोई भी फेरबदल नहीं की गई है अब सुझाए गए क्रम के अनुसार कंप्यूटरों के संग्रह की प्रक्रिया का पालन करें:–





इंटरनेट के साथ कंप्यूटर कनेक्शन

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें। संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें। उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें। संबंधित व्यक्ति से कंप्यूटर के संबंधित विभिन्न पासवर्ड ले लें।

2-अपराध स्थल(घटनास्थल) की फोटोग्राफी और वीडियोग्राफी करें। घटनास्थल पर उपलब्ध संदिग्ध कंप्यूटर के सीपीयू के आगे के पैनल पिछले पैनल एवं सभी दृष्टिकोण से फोटो कैप्चर करें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3-तारीख, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें।

4-शिकायतकर्ता की शिकायत के आधार पर व एफ.आई.आर. रिपोर्ट में बताए गए संदिग्ध सबूतों को कंप्यूटर में खोजने का प्रयास करें। किसी भी परिस्थिति में किसी भी फाइल या नई प्रक्रिया (process or software) को न खोलें। यदि केस से संबंधित कुछ साक्ष्य प्राप्त होते हैं इसका उल्लेख रिपोर्ट में प्राप्त फाइल के नाम उसके लोकैशन, फोल्डर का नाम जिसमें यह फाइल उपलब्ध है, उसका साइज इत्यादि यूनिक जानकारी के साथ फर्द जब्ती रिपोर्ट में लिख दें ताकि फॉरेंसिक जांच करता के द्वारा यह फाइल आसानी से बहुत ही कम समय में पुनः प्राप्त की जा सके।

1-यदि आवश्यक हो तो Annexture – में सुझाए गए अनुसार रैम डम्प ले लें और साझा (Shared) स्टॉरेज की Annexture – II अनुसार की भी इमेज बना लें। कंप्यूटर को नेटवर्क (वाईफाई या लैन) से अलग करें।

1-यूएसबी कनेक्शन जैसी कोई अन्य प्रासंगिक जानकारी एकत्र करें। रजिस्ट्री डंप, फाइल में चल रही प्रक्रियाएं।

2-सभी कनेक्टेड केबल को सीधे हटा दें। सामान्य प्रक्रिया के साथ पीसी को बंद न करें। पावर केबल को सीधे खींचें या पावर स्विच बंद करें। सीपीयू केस से हार्ड डिस्क को निकालें (यदि संभव हो तो) और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली

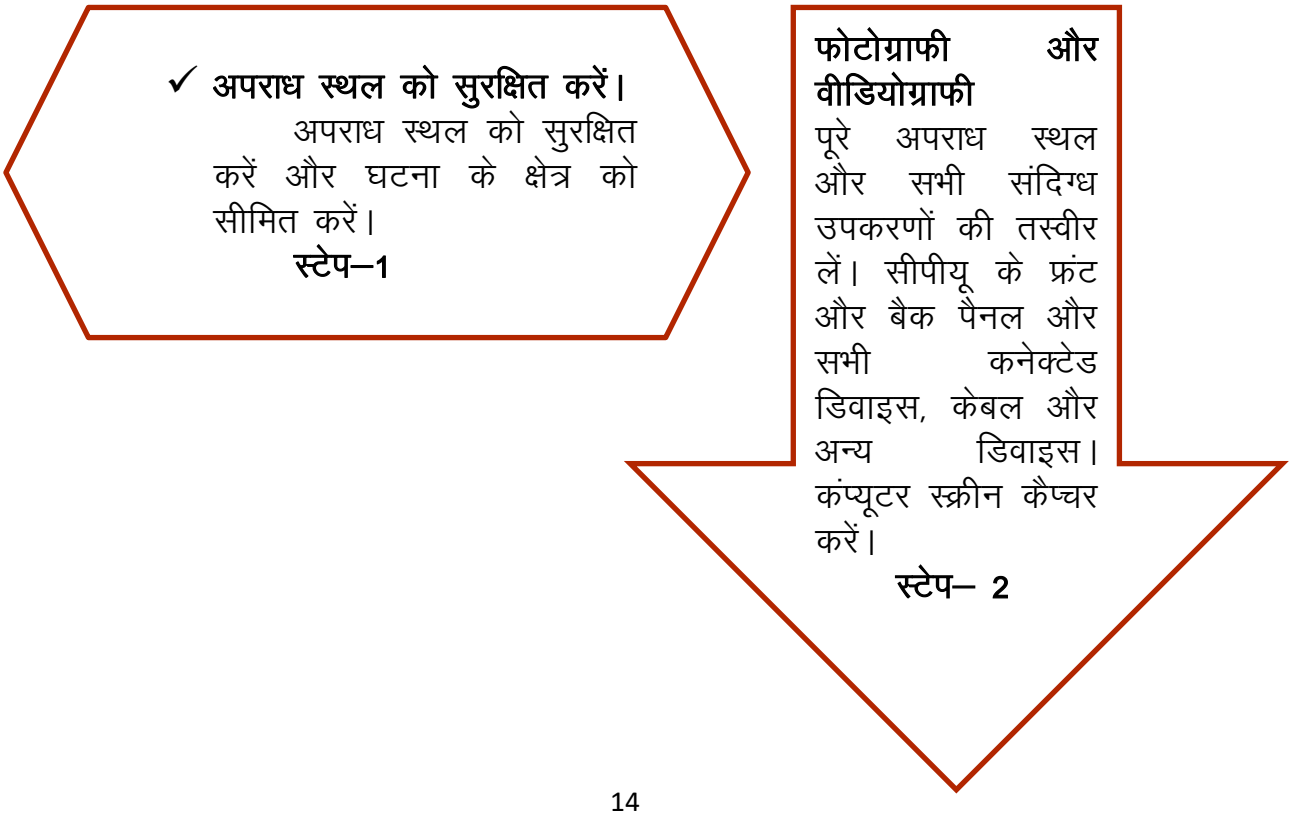
हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू ६ बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण हार्ड डिस्क, पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें।

3- जब्त किए गए डिवाइस को राइटब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्ती में विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-2/SHA-1 आदि) का भी उल्लेख करें।

1- हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके पूरे स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें. इमेजिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (जैसे संस्करण संख्या सहित) फर्द जब्ती में विवरण भरें और निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें।

2-फर्द जब्ती पर दो गवाहों के हस्ताक्षर करवाए जिसमें आरोपी ना हो। आरोपी के भी हस्ताक्षर करवावे तथा इन्वेस्टिगेटिंग ऑफीसर जो यह जब्ती करवा रहे हैं वह भी हस्ताक्षर करें। कंप्यूटर के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स कंप्यूटर से आसानी से अलग ना हो सके तो संपूर्ण सीपीयू को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

चार्ट 1 बिना लॉक और नेटवर्क कनेक्टेड कंप्यूटर चालू स्थिति में है



सिस्टम जानकारी एकत्र करें

दिनांक, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें। जब्ती ज्ञापन में उल्लिखित संभावित सबूत और सभी प्रासंगिक जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें।

स्टेप–3

रैम डंप वैकल्पिक– यदि आवश्यक हो तो

उपलब्ध सॉफ्टवेयर का उपयोग करके रैम डंप को कैप्चर करें, विश्लेषण करें और आवश्यक जानकारी निकालें। यदि उपलब्ध हो तो साझा संग्रहण (Storage) की छवि (Image) बनाएं। छवि का विश्लेषण करें और उपयोगी डेटा निकालें।

स्टेप– 4

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें। **स्टेप– 5**

नेटवर्क से कनेक्शन निकालें–

सभी कनेक्टेड केबल को सीधे हटा दें – नेटवर्क केबल, वाई–फाई, ब्लूटूथ या कोई अन्य कनेक्टिविटी । **स्टेप– 6**

पैकेजिंग और मार्किंग–

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 7**

1. घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से कंप्यूटर के संबंधित विभिन्न पासवर्ड ले।
2. अपराध स्थल(घटनास्थल) की फोटोग्राफी और वीडियोग्राफी करें। घटनास्थल पर उपलब्ध संदिग्ध कंप्यूटर के सीपीयू के आगे के पैनल पिछले पैनल एवं सभी दृष्टिकोण से फोटो कैप्चर करें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें। तारीख, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें।
3. शिकायतकर्ता की शिकायत के आधार पर एफ आई आर रिपोर्ट में बताए गए संदिग्ध सबूतों को कंप्यूटर में खोजने का प्रयास करें। किसी भी परिस्थिति में किसी भी फाइल या नई प्रक्रिया (process or software) को न खोलें। यदि केस से संबंधित कुछ साक्ष्य प्राप्त होते हैं इसका उल्लेख रिपोर्ट में उस फाइल के नाम उसके पते फोल्डर का नाम जिसमें यह फाइल उपलब्ध है उसका साइज इत्यादि यूनिक जानकारी के साथ फर्द जब्ती रिपोर्ट में लिख दें ताकि फॉरेंसिक जांच करता के द्वारा यह फाइल आसानी से बहुत ही कम समय में पुनः प्राप्त की जा सके।
4. यदि आवश्यक हो तो Annexture – I में सुझाए गए अनुसार रैम डम्प ले लें।
5. यूएसबी कनेक्शन जैसी कोई अन्य प्रासंगिक जानकारी एकत्र करें। रजिस्ट्री डंप, फाइल में चल रही प्रक्रियाएं (Process) इत्यादि।
6. सीपीयू केस से पावर प्लग निकालें और मदरबोर्ड से उपकरणों की आंतरिक कनेक्टिविटी' की तस्वीरें लें और फिर मदरबोर्ड से हार्डडिस्क कनेक्टिविटी (पावर और डेटा केबल्स) को हटा दें। सामान्य प्रक्रिया के साथ पीसी को बंद न करें। यदि संभव हो तो सीपीयू केस से हार्ड डिस्क को निकालें और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख, समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू/बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें।
7. जब्त किए गए डिवाइस को राइटब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

8. हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके पूरे स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें और इमेजिंग (यदि आवश्यकता हो तो) के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (जैसे संस्करण संख्या सहित) फर्द जब्ती में विवरण भरें और निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें।
9. फर्द जब्ती पर दो गवाहों के हस्ताक्षर करवाए जिसमें आरोपी ना हो। आरोपी के भी हस्ताक्षर करवावे तथा इन्वेस्टिगेटिंग ऑफीसर जो यह जब्ती करवा रहे हैं वह भी हस्ताक्षर करें। कंप्यूटर के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स कंप्यूटर से आसानी से अलग ना हो सके तो संपूर्ण सीपीयू को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

✓ **अपराध स्थल को सुरक्षित करें।**

अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।

स्टेप–1

फोटोग्राफी और वीडियोग्राफी

पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।

स्टेप– 2

सिस्टम जानकारी एकत्र करें

दिनांक, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें। जब्ती ज्ञापन में उल्लिखित संभावित सबूत और सभी प्रासंगिक जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें।

स्टेप–3

रैम डंप वैकल्पिक– यदि आवश्यक हो तो

उपलब्ध सॉफ्टवेयर का उपयोग करके रैम डंप को कैप्चर करें, विश्लेषण करें और आवश्यक जानकारी निकालें। यदि उपलब्ध हो तो साझा संग्रहण (Storage) की छवि (Image) बनाएं। छवि का विश्लेषण करें और उपयोगी डेटा निकालें।

स्टेप– 4

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें। **स्टेप– 5**

नेटवर्क से कनेक्शन निकालें–

सभी कनेक्टेड केबल को सीधे हटा दें – नेटवर्क केबल, वाई–फाई, ब्लूटूथ या कोई अन्य कनेक्टिविटी । **स्टेप– 6**

पैकेजिंग और मार्किंग –

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 7**

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से कंप्यूटर के संबंधित विभिन्न पासवर्ड ले।

2-अपराध स्थल(घटनास्थल) की फोटोग्राफी और वीडियोग्राफी करें। घटनास्थल पर उपलब्ध संदिग्ध कंप्यूटर के सीपीयू के आगे के पैनल पिछले पैनल एवं सभी दृष्टिकोण से फोटो कैप्चर करें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें। यदि सिस्टम हाइबरनेट स्थिति में है, तो पासवर्ड क्रैकिंग टूल जैसे भ्पतमदेइववज.पेव या किसी अन्य उपलब्ध पासवर्ड क्रैकिंग टूल का उपयोग करें। सफल होने पर प्रासंगिक (relevant) डेटा एकत्र करें और ऑपरेटिंग सिस्टम से पासवर्ड भी हटा दें या पासवर्ड को फर्द जब्ती में लिखें।

3-यदि पासवर्ड पुनः प्राप्त हो जाता है, फर्द जब्ती में इसका उल्लेख करें यदि आवश्यक हो तो शेयर्ड फोल्डर की फॉरेंसिक इमेज बनावे और एनालिसिस कर आवश्यक सबूत जुटा ले।

4-सभी जुड़े केबलों को सीधे हटा दें। सामान्य प्रक्रिया के साथ पीसी को बंद न करें। पावर केबल को सीधे खींचें या पावर स्विच को बंद करें। हार्ड डिस्क को निकालें और हार्ड डिस्क की मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति कार्यशील और गैर–कामकाजी (functional or non functional), जब्त डिजिटल स्टोरेज डिवाइस जैसे कि हार्ड डिस्क, पेनड्राइव, एसडी कार्ड का मेक, मॉडल और क्षमता उल्लेख करें।

5-शिकायतकर्ता की शिकायत के आधार पर एफ आई आर रिपोर्ट में बताए गए संदिग्ध सबूतों को कंप्यूटर में खोजने का प्रयास करें। किसी भी परिस्थिति में किसी भी फाइल या नई प्रक्रिया(process or software) को न खोलें। यदि केस से संबंधित कुछ साक्ष्य प्राप्त होते हैं इसका उल्लेख रिपोर्ट में उस फाइल के नाम उसके पते फोल्डर का नाम जिसमें यह फाइल उपलब्ध है उसका साइज इत्यादि यूनिक जानकारी के साथ फर्द जब्ती रिपोर्ट में लिख दें ताकि फॉरेंसिक जांच करता के द्वारा यह फाइल आसानी से बहुत ही कम समय में पुनः प्राप्त की जा सके।

6-जब्त किए गए डिवाइस को राइटब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

7-हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके पूरे स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें और इमेजिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (जैसे संस्करण संख्या सहित) फर्द जब्ती में विवरण भरें और निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें।

8-फर्द जब्ती पर दो गवाहों के हस्ताक्षर करवाए जिसमें आरोपी ना हो। आरोपी के भी हस्ताक्षर करवावे तथा इन्वेस्टिगेटिंग ऑफीसर जो यह जब्ती करवा रहे हैं वह भी हस्ताक्षर करें। कंप्यूटर के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा

देवें यदि हार्ड डिक्स कंप्यूटर से आसानी से अलग ना हो सके तो संपूर्ण सीपीयू को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

चार्टः लॉक के साथ चालू स्थिति में कंप्यूटर–

✓ **अपराध स्थल को सुरक्षित करें।**
अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।
स्टेप–1

फोटोग्राफी और वीडियोग्राफी
पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।
स्टेप– 2

सिस्टम जानकारी एकत्र करें
दिनांक, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें। जब्ती ज्ञापन में उल्लिखित संभावित सबूत और सभी प्रासंगिक जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें।

स्टेप–3

रैम डंप वैकल्पिक– यदि आवश्यक हो तो
उपलब्ध सॉफ्टवेयर का उपयोग करके रैम डंप को कैप्चर करें, विश्लेषण करें और आवश्यक जानकारी निकालें। यदि उपलब्ध हो तो साझा संग्रहण (Storage) की छवि (Image) बनाएं। छवि का विश्लेषण करें और उपयोगी डेटा निकालें।

स्टेप– 4

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें। **स्टेप– 5**

नेटवर्क से कनेक्शन निकालें–

सभी कनेक्टेड केबल को सीधे हटा दें – नेटवर्क केबल, वाई–फाई, ब्लूटूथ या कोई अन्य कनेक्टिविटी । **स्टेप– 6**

पैकेजिंग और मार्किंग–

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप–7**

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से कंप्यूटर के संबंधित विभिन्न पासवर्ड ले।

2-अपराध स्थल(घटनास्थल) की फोटोग्राफी और वीडियोग्राफी करें। घटनास्थल पर उपलब्ध संदिग्ध कंप्यूटर के सीपीयू के आगे के पैनल पिछले पैनल एवं सभी दृष्टिकोण से फोटो कैप्चर करें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3-सभी कनेक्टेड केबल को हटा दें। सीपीयू केस से हार्ड डिस्क को निकालें (यदि संभव हो तो) और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू/बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण हार्ड डिस्क, पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें।

4-जब्त किए गए डिवाइस को राइटब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

5-हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके पूरे स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें और इमेजिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (जैसे संस्करण संख्या सहित) फर्द जब्ती में विवरण भरें और निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें।

6–फर्द जब्ती जब्ती पर दो गवाहों के हस्ताक्षर करवाए जिसमें आरोपी ना हो। आरोपी के भी हस्ताक्षर करवावे तथा इन्वेस्टिगेटिंग ऑफीसर जो यह जब्ती करवा रहे हैं वह भी हस्ताक्षर करें। कंप्यूटर के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स कंप्यूटर से आसानी से अलग ना हो सके तो संपूर्ण सीपीयू को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

चार्ट कंप्यूटर बंद स्थिति में

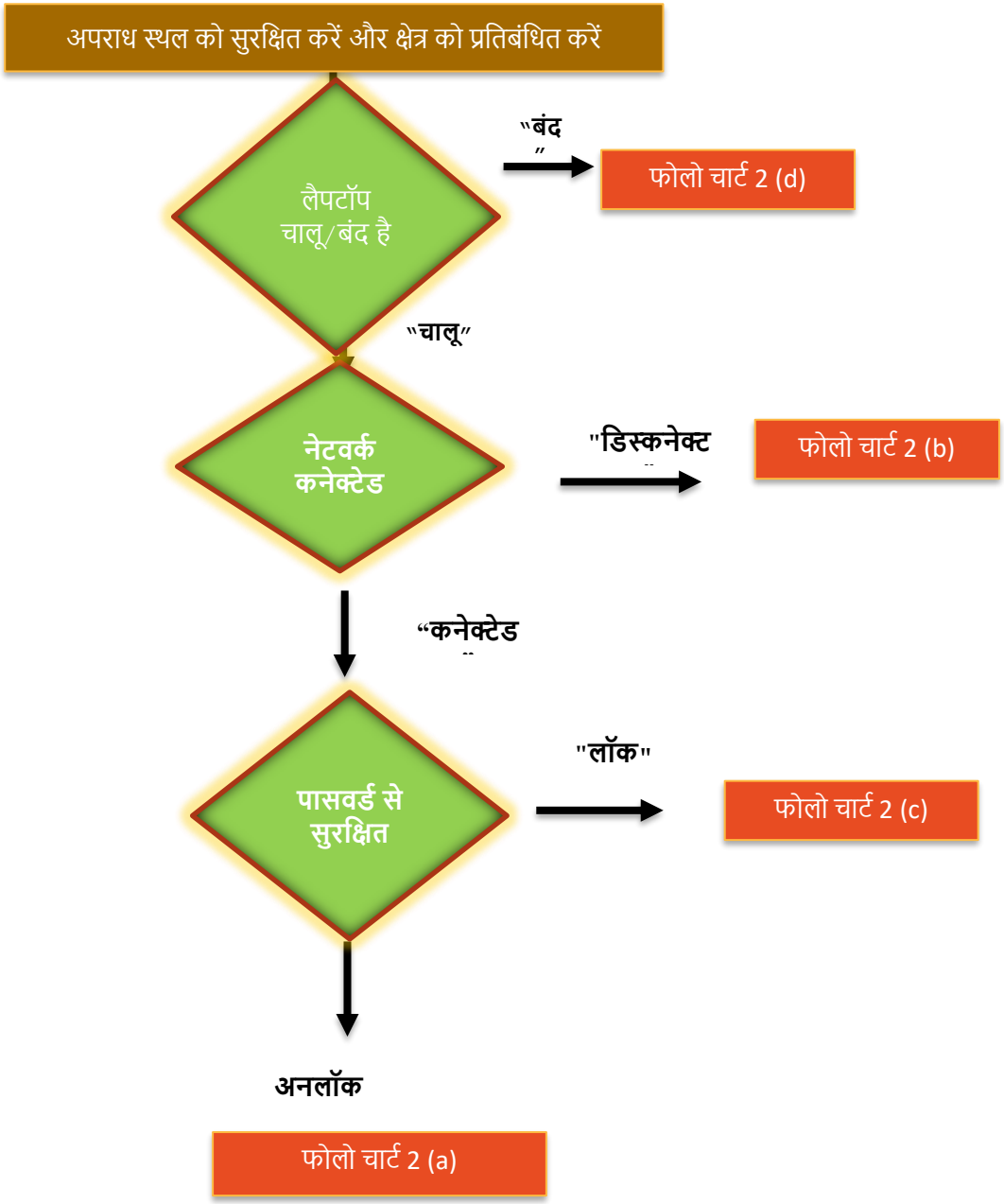
✓ **अपराध स्थल को सुरक्षित करें।**
अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।
स्टेप–1

फोटोग्राफी और वीडियोग्राफी
पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।
स्टेप– 2

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो
फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें। **स्टेप– 3**

पैकेजिंग और मार्किंग–
सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 4**

लैपटॉप की जब्ती का उसकी केटेगरी के अनुसार चार्ट



बिना लॉक और नेटवर्क कनेक्टेड लैपटॉप ऑन कंडीशन में है तो उसकी जब्ती परिवहन व सावधानियॉ

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से लैपटॉप के संबंधित विभिन्न पासवर्ड ले।

2-अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें। लैपटॉप के ऊपर, नीचे और सभी तरफ से लैपटॉप की तस्वीर लें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3-तारीख, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें।

4-शिकायतकर्ता की शिकायत के आधार पर एफ.आई.आर(FIR) रिपोर्ट में बताए गए संदिग्ध सबूतों को कंप्यूटर में खोजने का प्रयास करें। किसी भी परिस्थिति में किसी भी फाइल या नई प्रक्रिया (process or software) को न खोलें। यदि केस से संबंधित कुछ साक्ष्य प्राप्त होते हैं इसका उल्लेख रिपोर्ट में उस फाइल के नाम उसके पते, फोल्डर का नाम जिसमें यह फाइल उपलब्ध है, उसका साइज इत्यादि यूनिक जानकारी के साथ फर्द जब्ती रिपोर्ट में लिख दें ताकि फॉरेंसिक जांच करता के द्वारा यह फाइल आसानी से बहुत ही कम समय में पुनः प्राप्त की जा सके।

5-यदि आवश्यक हो तो Annexture – I में सुझाए गए अनुसार रैम डम्प ले लें और साझा (Shared) स्टॉरिज कि Annexture – II अनुसार की भी इमेज बना लें। कंप्यूटर को नेटवर्क (वाईफाई या लैन) से अलग करें।

6-यूएसबी कनेक्शन जैसी कोई अन्य प्रासंगिक जानकारी एकत्र करें। रजिस्ट्री डंप, फाइल में चल रही प्रक्रियाएं। अब कंप्यूटर को नेटवर्क (वाईफाई या लैन) से अलग करें।

7-जब्त किए गए डिवाइस को राइट ब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

8- हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके पूरे स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें और इमेजिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (जैसे संस्करण संख्या सहित) फर्द जब्ती में विवरण भरें और निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें।

9- कनेक्टेड केबल को सीधे हटा दें। हार्ड डिस्क को लैपटॉप से निकालें (यदि संभव हो तो) और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू/बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण हार्ड डिस्क, पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें। लैपटॉप के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स लैपटॉप से आसानी से अलग ना हो सके तो संपूर्ण लैपटॉप को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

2– लैपटॉप ऑन कंडीशन बिना लॉक और नेटवर्क कनेक्टेड

✓ **अपराध स्थल को सुरक्षित करें।**
अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।
स्टेप–1

फोटोग्राफी और वीडियोग्राफी
पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।
स्टेप– 2

सिस्टम जानकारी एकत्र करें

दिनांक, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें। जब्ती ज्ञापन में उल्लिखित संभावित सबूत और सभी प्रासंगिक जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें।

स्टेप–3

रैम डंप वैकल्पिक– यदि आवश्यक हो तो

उपलब्ध सॉफ्टवेयर का उपयोग करके रैम डंप को कैप्चर करें, विश्लेषण करें और आवश्यक जानकारी निकालें। यदि उपलब्ध हो तो साझा संग्रहण (Storage) की छवि (Image) बनाएं। छवि का विश्लेषण करें और उपयोगी डेटा निकालें।

स्टेप– 4

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें। **स्टेप– 5**

नेटवर्क से कनेक्शन निकालें–

सभी कनेक्टेड केबल को सीधे हटा दें – नेटवर्क केबल, वाई–फाई, ब्लूटूथ या कोई अन्य कनेक्टिविटी । **स्टेप– 6**

पैकेजिंग और मार्किंग–

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 7**

लॉक और नेटवर्क कनेक्टेड के साथ लैपटॉप चालू स्थिति में है तो उसकी जब्ती परिवहन व सावधानियॉ–

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से लैपटॉप के संबंधित विभिन्न पासवर्ड ले।

2-अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें। लैपटॉप के ऊपर, नीचे और सभी तरफ से लैपटॉप की तस्वीर लें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3-यदि सिस्टम हाइबरनेट स्थिति में है, तो पासवर्ड क्रैकिंग टूल जैसे Hirensboot-iso, Passware या किसी अन्य उपलब्ध पासवर्ड क्रैकिंग टूल का उपयोग करें। सफल होने पर, प्रासंगिक डेटा एकत्र करें और ऑपरेटिंग सिस्टम से पासवर्ड भी हटा दें या पासवर्ड को फर्द जब्तीमें लिखें।

4- यदि पासवर्ड पुनः प्राप्त हो जाता है, तो लैपटॉप के साथ साझा किए गए नेटवर्क फोल्डर(Shared Folder or Drive) की इमेज बनाएं

5- सभी कनेक्टेड केबल को सीधे हटा दें। पावर एडॉप्टर निकालें और लैपटॉप के पावर बटन से सीधे लैपटॉप को बंद कर दें। हार्ड डिस्क निकालें और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (कार्यशील और गैर–कामकाजी), जब्त डिजिटल स्टोरेज डिवाइस (उदाहरण– हार्ड डिस्क, पेन ड्राइव , एसडी कार्ड आदि ..), उनका मेक, मॉडल और क्षमता।

6- जब्त किए गए डिवाइस को राइट ब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

7- हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके पूरे स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें और इमेजिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (जैसे संस्करण संख्या सहित) फर्द जब्ती में विवरण भरें और निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें।

8- कनेक्टेड केबल को सीधे हटा दें। हार्ड डिस्क को लैपटॉप से निकालें (यदि संभव हो तो) और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू/बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण हार्ड डिस्क, पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें। लैपटॉप के हार्ड डिस्क अलग हो जाने की स्थिति में

हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स लैपटॉप से आसानी से अलग ना हो सके तो संपूर्ण लैपटॉप को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

2 लॉक और नेटवर्क कनेक्टेड के साथ लैपटॉप चालू स्थिति में है

✓ **अपराध स्थल को सुरक्षित करें।**
अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।
स्टेप–1

फोटोग्राफी और वीडियोग्राफी
पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।
स्टेप– 2

सिस्टम जानकारी एकत्र करें
दिनांक, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें। जब्ती ज्ञापन में उल्लिखित संभावित सबूत और सभी प्रासंगिक जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें।
स्टेप–3

रैम डंप वैकल्पिक– यदि आवश्यक हो तो
उपलब्ध सॉफ्टवेयर का उपयोग करके रैम डंप को कैप्चर करें, विश्लेषण करें और आवश्यक जानकारी निकालें। यदि उपलब्ध हो तो साझा संग्रहण (Storage) की छवि (Image) बनाएं। छवि का विश्लेषण करें और उपयोगी डेटा निकालें।
स्टेप– 4

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें।

स्टेप– 5

नेटवर्क से कनेक्शन निकालें–

सभी कनेक्टेड केबल को सीधे हटा दें – नेटवर्क केबल, वाई–फाई, ब्लूटूथ या कोई अन्य कनेक्टिविटी । **स्टेप– 6**

पैकेजिंग और मार्किंग–

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 7**

लैपटॉप ऑन कंडीशन में लॉक के साथ और बिना नेटवर्क कनेक्टेड है तो उसकी जब्ती परिवहन व सावधानियॉ–

1-अपराधस्थल (घटनास्थल) को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें। उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें। संबंधित व्यक्ति से लैपटॉप के संबंधित विभिन्न पासवर्ड ले

2-अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें। लैपटॉप के ऊपर, नीचे और सभी तरफ से लैपटॉप की तस्वीर लें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे

सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3-यदि सिस्टम हाइबरनेट स्थिति में है, तो पासवर्ड क्रैकिंग टूल जैसे Hirensboot-iso, Passware या किसी अन्य उपलब्ध पासवर्ड क्रैकिंग टूल का उपयोग करें। सफल होने पर, प्रासंगिक डेटा एकत्र करें और ऑपरेटिंग सिस्टम से पासवर्ड भी हटा दें या पासवर्ड को फर्द जब्ती में लिखें। तारीख, समय, सिस्टम की जानकारी को नोट करें और फर्द जब्ती में इसका उल्लेख करें।

4-सभी जुड़े केबलों को सीधे हटा दें। पावर एडॉप्टर निकालें और लैपटॉप के पावर बटन से सीधे लैपटॉप को बंद कर दें। हार्ड डिस्क निकालें और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (कार्यशील और गैर–कामकाजी), जब्त डिजिटल स्टोरेज डिवाइस (उदा हार्ड डिस्क, पेनड्राइव, एसडी कार्ड आदि..), उनका मेक, मॉडल और क्षमता।

5-जब्त किए गए डिवाइस को राइटब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें, निकाली गई इमेज फाइल को स्टेरलाइज्ड एक्सटर्नल हार्ड डिस्क (वाइप्ड) में स्टोर करें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

6-कनेक्टेड केबल को सीधे हटा दें। हार्ड डिस्क को लैपटॉप से निकालें (यदि संभव हो तो) और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू/बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण हार्ड डिस्क, पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें। लैपटॉप के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स लैपटॉप से आसानी से अलग ना हो सके तो संपूर्ण लैपटॉप को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

चार्टः लैपटॉप ऑन कंडीशन में लॉक के साथ और बिना नेटवर्क कनेक्टेड

✓ **अपराध स्थल को सुरक्षित करें।**

अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।

स्टेप–1

फोटोग्राफी और वीडियोग्राफी

पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।

स्टेप– 2

सिस्टम जानकारी एकत्र करें

दिनांक, समय, सिस्टम की जानकारी और चल रहे सॉफ्टवेयर आदि को नोट करें और फर्द जब्ती में इसका उल्लेख करें। जब्ती ज्ञापन में उल्लिखित संभावित सबूत और सभी प्रासंगिक जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें।

स्टेप–3

रैम डंप वैकल्पिक– यदि आवश्यक हो तो

उपलब्ध सॉफ्टवेयर का उपयोग करके रैम डंप को कैप्चर करें, विश्लेषण करें और आवश्यक जानकारी निकालें। यदि उपलब्ध हो तो साझा संग्रहण (Storage) की छवि (Image) बनाएं। छवि का विश्लेषण करें और उपयोगी डेटा निकालें।

स्टेप– 4

इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें।

स्टेप– 5

नेटवर्क से कनेक्शन निकालें–

सभी कनेक्टेड केबल को सीधे हटा दें – नेटवर्क केबल, वाई–फाई, ब्लूटूथ या कोई अन्य कनेक्टिविटी । **स्टेप– 6**

पैकेजिंग और मार्किंग–

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 7**

लैपटॉप बंद स्थिति में है तो उसकी जब्ती परिवहन व सावधानियॉ–

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से लैपटॉप के संबंधित विभिन्न पासवर्ड ले। लैपटॉप को किसी भी हालत में ऑन न करें।

2-अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें। लैपटॉप के ऊपर, नीचे और सभी तरफ से लैपटॉप की तस्वीर लें। कीबोर्ड, माउस, बाहरी ब्लूटूथ, लैन केबल, बाहरी हार्ड ड्राइव जैसे सभी जुड़े उपकरणों की तस्वीर कैप्चर करें। साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3-सभी जुड़े केबलों को सीधे हटा दें। लैपटॉप हार्ड डिस्क निकालें और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (कार्यशील और गैर–कामकाजी), जब्त डिजिटल स्टोरेज डिवाइस (उदा हार्ड डिस्क, पेनड्राइव, एसडी कार्ड आदि..), उनका मेक, मॉडल और क्षमता।

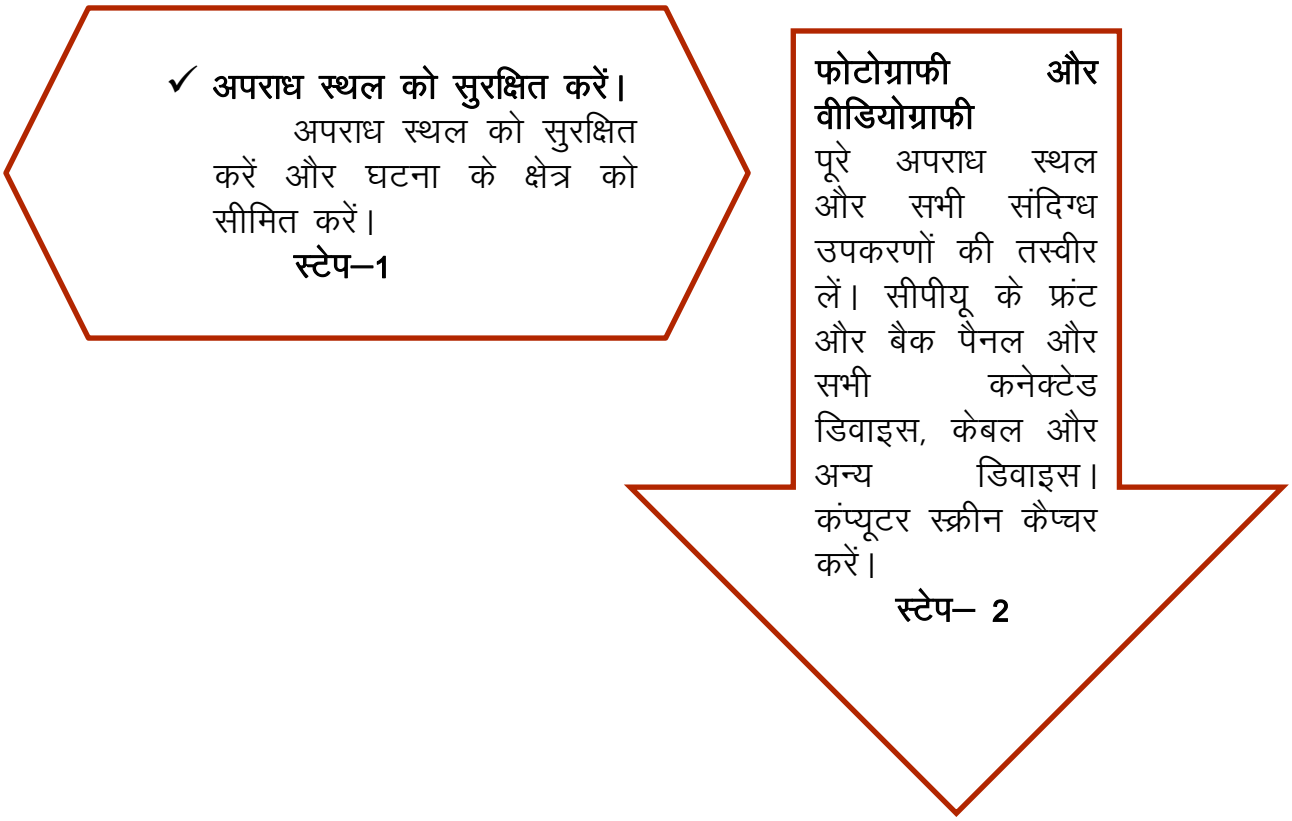
4-जब्त किए गए डिवाइस को राइटब्लॉकर के माध्यम से फोरेंसिक लैपटॉप से कनेक्ट करें और हैशिंग टूल का उपयोग करके पूरे जब्त स्टोरेज मीडिया के हैश वैल्यू की गणना करें। हैशिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और हैश मान और उपयोग किए गए हैशिंग एल्गोरिदम (SHA-1/SHA-2 आदि) का भी उल्लेख करें।

5-हैश मान की गणना करने के बाद, इमेजिंग टूल का उपयोग करके संपूर्ण स्टोरेज मीडिया की बिट स्ट्रीम इमेज लें और इमेजिंग के लिए उपयोग किए जाने वाले सॉफ्टवेयर या हार्डवेयर

टूल (संस्करण संख्या सहित) जैसे फर्द जब्तीमें विवरण भरें और निकाली गई इमेज फाइल को संग्रहीत करें बाहरी बॉझ मीडिया में।

6-कनेक्टेड केबल को सीधे हटा दें। हार्ड डिस्क को लैपटॉप से निकालें (यदि संभव हो तो) और हार्ड डिस्क के मेक, मॉडल और क्षमता स्पष्ट रूप से दिखाई देने वाली हार्ड डिस्क की तस्वीरें लें। फर्द जब्ती में सभी विवरण जैसे जब्ती की तारीख और समय, स्थान, पुलिस स्टेशन का अधिकार क्षेत्र, आईओ का नाम, सिस्टम की स्थिति (चालू/बंद), जब्त डिजिटल स्टोरेज डिवाइस उदाहरण हार्ड डिस्क, पेन ड्राइव, एसडी कार्ड आदि को नोट करें, उनका मेक, मॉडल और क्षमता को नोट करें। लैपटॉप के हार्ड डिस्क अलग हो जाने की स्थिति में हार्ड डिस्क को अकेले ही पैक करवा देवें यदि हार्ड डिक्स लैपटॉप से आसानी से अलग ना हो सके तो संपूर्ण लैपटॉप को ही पैक करवावे. हार्ड डिस्क अकेले की जब्ती की स्थिति में हार्ड डिस्क को पहले बबल पैकिंग में उसके पश्चात फैराडे बैग में पैक करें और मार्किंग करने के पश्चात सील भी लगावे मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

चार्टः लैपटॉप बंद हालत में



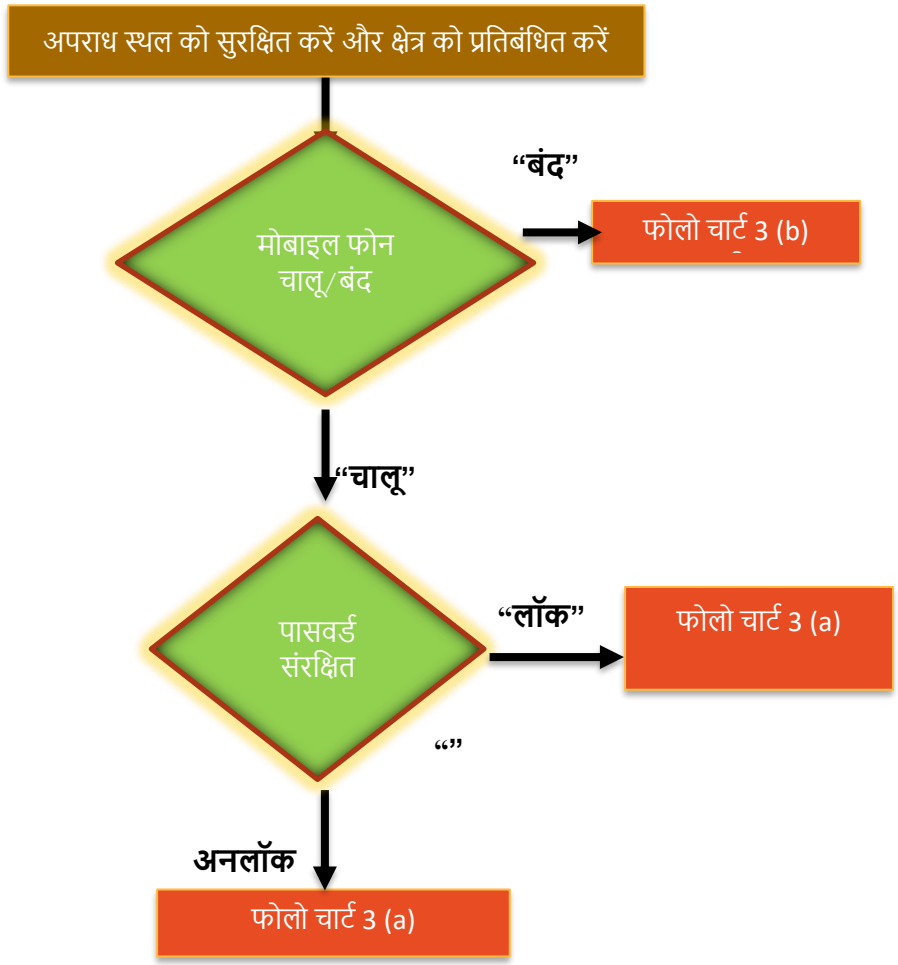
इमेजिंग और हैशिंग वैकल्पिक– यदि आवश्यक हो तो

फाल्कन नियो का उपयोग करके साझा भंडारण (Shared storage) की छवि (Image) तैयार करें, फोरेंसिक वर्कस्टेशन पर छवि का विश्लेषण करें और संभावित साक्ष्य निकालें। पीछे और आगे से हार्ड डिस्क (सेकेंडरी स्टोरेज मीडिया) का फोटोग्राफ लें। राइट ब्लॉकर का उपयोग करके हार्ड डिस्क की फोरेंसिक छवि तैयार करें और उत्पन्न हैश वैल्यू को सुरक्षित करें। छवि का विश्लेषण करें और छवि फाइल से आवश्यक साक्ष्य निकालें। **स्टेप– 3**

पैकेजिंग और मार्किंग–

सीपीयू, हार्ड डिस्क जैसे ब्रांड, मॉडल, सीरियल, आकार और अन्य सभी यूनिक (Unique) जानकारी के सभी विवरण लिखें। हार्ड डिस्क को बबल पैकिंग में पैक करें और फिर फैराडे बैग या होल सीपीयू अगर हार्ड डिस्क को हटाने में असमर्थ है, तो इसकी मार्किंग करें और सील करें। **स्टेप– 4**

मोबाइल फोन की जब्ती के बारे में उसकी केटेगरी के अनुसार चार्ट –



1- घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से मोबाइल के संबंधित विभिन्न पासवर्ड ले।

2- अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें। मोबाइल के ऊपर, नीचे और सभी तरफ से मोबाइल की तस्वीर लें और नोट करें कि यह कहां पाया गया था और ऑन–स्क्रीन जानकारी के साथ डिवाइस की स्थिति को रिकॉर्ड करें यानी डिस्प्ले की तारीख, समय, स्क्रीन की स्थिति और अन्य प्रासंगिक जानकारी। । साथ ही स्क्रीन को बहुत स्पष्ट रूप से चित्रित करें।

3- अगर डिवाइस "ON'मोड में है तो सबसे पहले उसे तुरंत फ्लाइट मोड (Flite mode – मोबाइल डिवाइस को इंटरनेट कनेक्टिविटी से बाहर करने के लिए) पर डाल दें। अब शिकायतकर्ता के अनुसार, अपराध के लिए रिपोर्ट किए गए सबूतों के निशान को मैन्युअल रूप से नेविगेट करें। कोई फाइल न खोलें। यदि कुछ प्रासंगिक पाया जाता है, तो फाइल/एप्लिकेशन (एपीपी) का नाम ठीक से लिखें और फर्द जब्ती में पथ लिखें। हैंडसेट से सोशल मीडिया से संबंधित किसी भी पोस्ट का स्क्रीन शॉट लें। फाइलों या मिले सबूतों

के attribute(name, size, duration, location or any other) नोट करें। अब इसे बंद कर दें। इसमें शामिल डेटा में किए जा रहे परिवर्तनों से बचने के लिए डिवाइस को नेटवर्क से सिग्नल प्राप्त करने से अलग करना महत्वपूर्ण है। सिम कार्ड और बैटरी (यदि हटाने योग्य हो) निकालें और एक बैग में पैक करें। मोबाइल के पीछे सिम लगाने के लिए पारदर्शी टेप का प्रयोग करें।

4- कनेक्टिंग केबल, चार्जर, पैकेजिंग मैनुअल, फोन बिल आदि को जब्त कर लें क्योंकि ये पूछताछ में सहायता कर सकते हैं और किसी भी परीक्षा में देरी को कम कर सकते हैं।

5- मोबाइल हैंडसेट से संबंधित बिल या अन्य कोई कागज यदि उपलब्ध हो तो संलग्न करें मोबाइल हैंडसेट से संबंधित पिनध्पीयूके जब्ती मेमो में बिना किसी अस्पष्टता संलग्न करें। मोबाइल के यूनिक नंबर यानी आईएमईआई नंबर और हैंडसेट के अन्य विवरण के साथ किसी भी पासकोड/पासवर्ड/लॉक पैटर्न आदि का स्पष्ट रूप से उल्लेख करें।

6- ध्यान रखें कि कुछ मोबाइल फोन हैंडसेट में स्वचालित हाउसकीपिंग फंक्शन हो सकते हैं जो कई दिनों के बाद डेटा साफ करते हैं। उदाहरण के लिए, कुछ सिम्बियन फोन 30 दिनों या किसी अन्य उपयोगकर्ता द्वारा निर्धारित अवधि के बाद कॉल/इवेंट लॉग को साफ करना शुरू करते हैं। जितनी जल्दी हो सके जांच के लिए आइटम जमा करें।

7- दो गवाहों के साथ फर्द जब्ती पर हस्ताक्षर करें जिसमें आरोपी या एक व्यक्ति भी शामिल है जिससे यह जब्ती की जा रही है। हैंडसेट की पैकेजिंग के लिए बबल पैकिंग और फिर फैराडे बैग का उपयोग करें। उदाहरण के लिए बड़े अक्षरों में अंग्रेजी वर्णमाला के साथ अलग से एकत्र किए गए प्रत्येक साक्ष्य को अलग से (प्रत्येक मोबाइल को अलग बैग में यदि अपराध के मामले में कई मोबाइल पाए जाते हैं) चिह्नित करें – मार्क ए

नोटः– कुछ उपकरणों को दूरस्थ रूप से वाइप/फैक्टरी रीसेट करना संभव है, इसलिए डिवाइस को बंद करके इसे रोका जा सकता है। मोबाइल डिवाइस को फ्लाइट मोड/एयरप्लेन मोड में रखना अनिवार्य है।

बिना किसी पासवर्ड या लॉक के मोबाइल फोन ऑन कंडीशन है तो उसकी जब्ती परिवहन व सावधानियों का चरण दर चरण चार्ट–

✓ **अपराध स्थल को सुरक्षित करें।**
अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें।
स्टेप–1

फोटोग्राफी और वीडियोग्राफी
पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। सीपीयू के फ्रंट और बैक पैनल और सभी कनेक्टेड डिवाइस, केबल और अन्य डिवाइस। कंप्यूटर स्क्रीन कैप्चर करें।
डिवाइस को तुरंत फ्लाइट मोड पर रखें और सिम कार्ड को सिम स्लॉट से हटा दें।
स्टेप–2

मोबाइल फोन की जानकारी एकत्र करें

हैंडसेट से संदिग्ध एप्प इंस्टॉलेशन की स्थिति, तारीख, समय, हैंडसेट की जानकारी को नोट करें और फर्द जब्ती में इसका उल्लेख करें। करें। शिकायत में उल्लिखित संभावित सबूत और सभी संबंधित जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें। सोशल मीडिया से संबंधित अपराधों के मामले में स्क्रीनशॉट लें।

स्टेप–3

पैकेजिंग और मार्किंग

हटाए गए सिम कार्ड को हैंडसेट के पीछे ट्रांसपेरेंट टाइप की सहायता से चिपका दें। मोबाइल डिवाइस के सभी विवरण जैसे ब्रांड, मॉडल, सीरियल नंबर, आईएमईआई नंबर अन्य सभी यूनिक (Unique) विवरण लिखें। यदि डिवाइस में कोई पासवर्ड/लॉकपैटर्न/पीयूके/पिन आदि है तो फर्द जब्ती में उसका उल्लेख करें। हैंडसेट, मेमोरी कार्ड और सिम कार्ड को एक ही बबल पैकिंग (प्रत्येक मोबाइल के लिए अलग) में पैक करें और फिर फैराडे बैग में, इसे मार्क करें और पैकेट को सील करें। **स्टेप–4**

बंद हालत में मोबाइल फोन तो उसकी जब्ती परिवहन व सावधानियॉ–

1-घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं एवं पूरे क्षेत्र का संरक्षण करें संदिग्ध व्यक्ति को किसी भी प्रकार के उपकरण को छूने ना दें उसे अन्य अनुसंधान टीम के व्यक्ति के साथ किसी अन्य कमरे या दूसरे स्थान पर बिठा दें संबंधित व्यक्ति से मोबाइल के संबंधित विभिन्न पासवर्ड ले।

2-अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें। मोबाइल के ऊपर, नीचे और सभी तरफ से मोबाइल की तस्वीर लें और नोट करें कि यह कहां पाया गया था और डिवाइस की स्थिति शारीरिक क्षतिग्रस्त या नहीं (Physically damaged) को रिकॉर्ड करें यानी तारीख, समय, स्क्रीन की स्थिति और अन्य प्रासंगिक जानकारी।

3-मोबाइल फोन को तुरंत फ्लाइट मोड पर डाल दें व इसमें में से सिम कार्ड को तुरंत हटा दें और उन्हें मोबाइल फोन के पिछले हिस्से में चिपका दें। अब डिवाइस को चालू करें (केवल जांच अधिकारी द्वारा)। अब शिकायतकर्ता के अनुसार, मैन्युअल रूप से उन तथ्यों की खोज करें जो साइबर अपराध में रिपोर्ट किए गए हैं। कोई फाइल न खोलें। यदि कुछ प्रासंगिक

पाया जाता है, तो फाइल/एप्लिकेशन (एपीपी) का नाम ठीक से लिखें और फर्द जब्ती में संदिग्ध फाइल की लोकेशन लिखें। हैंडसेट से सोशल मीडिया से संबंधित किसी भी पोस्ट का स्क्रीन शॉट लें। मिली फाइलों या सबूतों के हस्ताक्षर नोट करें और फर्द जब्ती में भी इसका उल्लेख करें ताकि फॉरेंसिक जांचकर्ता के द्वारा इन फाइलों को आसानी से बहुत ही कम समय में पुनः प्राप्त की जा सके। अब इसे बंद कर दें।

4-कनेक्टिंग केबल, चार्जर, पैकेजिंग मैनुअल, फोन बिल आदि को जब्त कर लें क्योंकि ये पूछताछ में सहायता कर सकते हैं और किसी भी परीक्षा में देरी को कम कर सकते हैं।

5-मोबाइल हैंडसेट से संबंधित बिल या अन्य कोई कागज यदि उपलब्ध हो तो संलग्न करें मोबाइल हैंडसेट से संबंधित पिनध्पीयूके जब्ती मेमो में बिना किसी अस्पष्टता संलग्न करें। मोबाइल के यूनिक नंबर यानी आईएमईआई नंबर और हैंडसेट के अन्य विवरण के साथ किसी भी पासकोड/पासवर्ड/लॉक पैटर्न आदि का स्पष्ट रूप से उल्लेख करें।

6-ध्यान रखें कि कुछ मोबाइल फोन हैंडसेट में स्वचालित हाउसकीपिंग फंक्शन हो सकते हैं जो कई दिनों के बाद डेटा साफ करते हैं। उदाहरण के लिए, कुछ सिम्बियन फोन 30 दिनों या किसी अन्य उपयोगकर्ता द्वारा निर्धारित अवधि के बाद कॉल/इवेंट लॉग को साफ करना शुरू करते हैं। जितनी जल्दी हो सके जांच के लिए आइटम जमा करें।

7-दो गवाहों के साथ फर्द जब्ती पर हस्ताक्षर करें जिसमें आरोपी या एक व्यक्ति भी शामिल है जिससे यह जब्ती की जा रही है। एक ही बैग में हैंडसेट, सिम कार्ड, बैटरी और मेमोरी कार्ड की पैकेजिंग के लिए बबल पैकिंग और फिर फैराडे बैग का उपयोग करें। यदि किसी साइबर क्राइम केस में एक से अधिक मोबाइल पाए जाते हैं तो सभी को अलग–अलग मार्किंग देकर अलग–अलग बैग में पैक करें। मार्किंग के लिए अंग्रेजी के बड़े अक्षरों का प्रयोग करें एवं दो अलग–अलग प्रदर्शनों की लिए एक ही अंग्रेजी वर्णमाला के अक्षर उपयोग में ना लावे. उदाहरण के लिए मार्क A, मार्क B

नोटः– कुछ उपकरणों को दूरस्थ रूप से वाइप/फैक्टरी रीसेट करना संभव है, इसलिए डिवाइस को बंद करके इसे रोका जा सकता है। मोबाइल डिवाइस को फ्लाइट मोड/एयरप्लेन मोड में रखना अनिवार्य है।

मोबाइल फोन बंद हालत में (पासवर्ड नहीं)

अपराध स्थल को सुरक्षित करें

अपराध स्थल को सुरक्षित करें और घटना के क्षेत्र को सीमित करें। डिवाइस को आरोपी या किसी अन्य व्यक्ति से तुरंत लें, जिसके पास संदिग्ध डिवाइस है। **स्टेप–1**

फोटोग्राफी और वीडियोग्राफी

पूरे अपराध स्थल और सभी संदिग्ध उपकरणों की तस्वीर लें। डिवाइस से संबंधित और कोई भी जानकारी उपलब्ध हो तो उसका फोटो खींच ले। **स्टेप–2**

मोबाइल फोन की जानकारी एकत्र करें

हैंडसेट से संदिग्ध एप्प इंस्टॉलेशन की स्थिति, तारीख, समय, हैंडसेट की जानकारी को नोट करें और फर्द जब्ती में इसका उल्लेख करें। करें। शिकायत में उल्लिखित संभावित सबूत और सभी संबंधित जानकारी की तलाश करें। कोई फाइल या दस्तावेज न खोलें। सोशल मीडिया से संबंधित अपराधों के मामले में स्क्रीनशॉट लें।

स्टेप–3

पैकेजिंग और मार्किंग

हटाए गए सिम कार्ड को हैंडसेट के पीछे ट्रांसपेरेंट टाइप की सहायता से चिपका दें। मोबाइल डिवाइस के सभी विवरण जैसे ब्रांड, मॉडल, सीरियल नंबर, आईएमईआई नंबर अन्य सभी यूनिक (Unique) विवरण लिखें। यदि डिवाइस में कोई पासवर्ड/लॉकपैटर्न/पीयूके/पिन आदि है तो फर्द जब्ती में उसका उल्लेख करें। हैंडसेट, मेमोरी कार्ड और सिम कार्ड को एक ही बबल पैकिंग (प्रत्येक मोबाइल के लिए अलग) में पैक करें और फिर फैराडे बैग में, इसे मार्क करें और पैकेट को सील करें।

स्टेप–4

डीवीआर (डिजिटल वीडियो रिकॉर्डर) की जब्ती तो उसकी जब्ती परिवहन व सावधानियॉ–

1- अपराध स्थल को सुरक्षित करें और उस क्षेत्र पर पूर्ण नियंत्रण रखें जहां डीवीआर स्थापित है। किसी अन्य व्यक्ति को डिवाइस के साथ इंटरैक्ट करने की अनुमति न दें। डिवाइस को आरोपी या किसी ऐसे व्यक्ति से लें जिसके पास यह है और जिस पर संदेह है।

2- अपराध स्थल की फोटोग्राफी और वीडियोग्राफी से शुरुआत करें। डिवाइस कनेक्टिविटी की पहचान करने के लिए ऊपर और नीचे के दृश्य से डीवीडीध्एनवीडीआर के फ्रंट और बैक पैनल की तस्वीरें लें।

3- डीवीआर की विस्तृत जानकारी और उसकी हार्ड डिस्क विवरण जैसे ब्रांड, मॉडलध्उत्पाद संख्या, सीरियल नंबर, फर्मवेयर नंबर और क्षमता को नोट करें और फर्द जब्ती में स्पष्ट रूप से उल्लेख करें।

4- हार्ड डिस्क को आरोपी, गवाह और जांच अधिकारी के हस्ताक्षर करने के बाद सील कर दें।

5- इसका क्लोन बनाने के लिए यह सलाह दी जाती है कि समान मेक, मॉडल और क्षमता या समान एल.बी.ए.(Logical block addressing) की एक खाली हार्ड डिस्क खरीदें।

6- सत्यापन के बाद रिकवरी मेमो में डीवीआर के लॉगिन और अन्य सिस्टम लॉक से संबंधित सभी पासवर्ड का स्पष्ट रूप से उल्लेख करें।

7- डीवीआर की हार्ड डिस्क को क्लोन करने के बाद विश्लेषण शुरू करें और लॉग और हैश वैल्यू के साथ एक अलग डीवीडीध्सीडी या पेन ड्राइव में पाए जाने पर आवश्यक वीडियो या इमेज निर्यात करें।

चार्ट डीवीआर (डिजिटल वीडियो रिकॉर्डर) की जब्ती–

अपराध स्थल को सुरक्षित करें

अपराध स्थल को सुरक्षित करें जहां डीवीआर स्थापित है, जहां डीवीआर इंस्टॉल है उस क्षेत्र को संरक्षित एवं सुरक्षित कर दें किसी भी बाहरी व्यक्ति का प्रवेश निषेध होना चाहिए। डिवाइस को आरोपी या किसी अन्य व्यक्ति के पास से तुरंत जांच अधिकारी के नियंत्रण में ले लें, जिसके पास संदिग्ध डिवाइस है। **स्टेप–1**

फोटोग्राफी और वीडियोग्राफी

पूरे अपराध स्थल और डीवीआर उपकरणों के सभी कनेक्शनों की तस्वीर लें। डीवीआर के बैक, फ्रंट और सभी साइड व्यू को कैप्चर करें। डिवाइस से संबंधित और कोई भी जानकारी उपलब्ध हो तो उसका फोटो खींच ले डीवीआर बॉक्स के अंदर कनेक्टेड हार्ड डिस्क के ऊपर और नीचे के दृश्य की तस्वीरें लें।

स्टेप–2

सिस्टम जानकारी एकत्र करें

डीवीआर में दिख रही तारीख(दिनांक), समय नोट करें। संभावित वीडियो क्लिप और सभी प्रासंगिक जानकारी खोजें एवं फर्द जब्ती में इसका उल्लेख करें। डीवीआर के कंफीग्रेशन सेटिंग्स में किसी भी प्रकार का कोई बदलाव ना करें।

स्टेप– 3

डिस्क की क्लोनिंग

हार्ड डिस्क की क्लोनिंग के लिए फाल्कन डुप्लीकेटर का प्रयोग करें। क्लोनिंग के दौरान उत्पन्न हैश को सुरक्षित करें। डिस्क का विश्लेषण करें। अगर कुछ प्रासंगिक पाया तो इसे एक्सपोर्ट(निर्यात) करें। हैशिंग को अलग से तैयार करें और पेन ड्राइव या किसी अन्य उपयुक्त स्टोरेज मीडिया में उपलब्ध कराएं। **स्टेप– 4**

पैकेजिंग और मार्किंग

डीवीआर डिवाइस के सभी विवरण जैसे ब्रांड, मॉडल, सीरियल नंबर, फर्मवेयर नंबर, मैक एड्रेस (MAC Address) या कोई अन्य यूनिक (Unique) जानकारी लिखें। पासवर्डध्लॉकपिन आदि लिखें। फर्द जब्ती में इसका उल्लेख करें। हार्ड डिस्क के सभी विवरण जैसे ब्रांड, मॉडल, सीरियल, स्टोरेज कैपेसिटी और अन्य सभी यूनिक (Unique) जानकारी क विवरण लिखें। पूरे क्टत कोध्हार्ड डिस्क को सफेद कपड़ा पैकिंग में पैक करें और इसे मार्क करें और सील करें। **स्टेप– 5**

स्टोरेज मीडिया की जब्ती (सीडी, डीवीडी, मेमोरी कार्ड, यूएसबी डाइव आदि तो उसकी जब्ती परिवहन व सावधानियॉ–

1- अपराध स्थल को सुरक्षित करें और उस क्षेत्र का पूरा नियंत्रण रखें जहां अकेले स्टोरेजण उपकरण मौजूद है। किसी अन्य व्यक्ति को डिवाइस के साथ इंटरैक्ट करने की अनुमति न दें। डिवाइस को आरोपी या किसी ऐसे व्यक्ति से लें जिसके पास यह है और जिस पर संदेह है।

2- अपराध स्थल की फोटोग्राफी और वीडियोग्राफी से शुरुआत करें। पहचानने के लिए ऊपर और नीचे के दृश्य से सीडी/डीवीडी/मेमोरी कार्ड या यूएसबी ड्राइव के फ्रंट और बैक की तस्वीरें लें।

3-सीडी/डीवीडी/मेमोरी कार्ड या यूएसबी ड्राइव की विस्तृत जानकारी और जैसे ब्रांड, मॉडलध्उत्पाद संख्या, सीरियल नंबर, क्षमता, रंग आदि को नोट करें और फर्द जब्ती में स्पष्ट रूप से उल्लेख करें।

4- आगे की जांच के लिए सीडी/डीवीडी/मेमोरी कार्ड या यूएसबी ड्राइव का क्लोन तैयार करें (मेमोरी कार्ड या यूएसबी ड्राइव को क्लोन करने के लिए राइट ब्लॉकर का उपयोग करें)। समान मेक, मॉडल और क्षमता या समान एल.बी.ए. की एक खाली हार्ड डिस्क खरीदने की सलाह दी जाती है। इसका क्लोन बनाने के लिए मूल्य। इसी तरह, क्लोनिंग के उद्देश्य से सीडी/डीवीडी और यूएसबी ड्राइव।

5- सत्यापन के बाद रिकवरी मेमो में डीवीआर के लॉगिन और अन्य सिस्टम लॉक से संबंधित सभी पासवर्ड का स्पष्ट रूप से उल्लेख किया जाना चाहिए।

6- हार्ड डिस्क/डीवीडी/मेमोरी कार्ड/यूएसबी ड्राइव को क्लोन करने के बाद, फर्द जब्तीपर हैश मान (क्लोनिंग के दौरान स्वचालित रूप से परिकलित) का उल्लेख करें। एफएसएल से त्वरित पुनर्प्राप्ति के लिए साक्ष्य के आसान पुनर्गठन के लिए फाइल का नाम, आकार और

अन्य विशेषता का उल्लेख करें। विश्लेषण शुरू करें और आवश्यक फाइलें (इमेज, चित्र, दस्तावेज या कोई अन्य) निर्यात करें यदि एक अलग डीवीडी ६ सीडी या पेन ड्राइव में लॉग और हैश मान के साथ पाया जाता है।

चार्टः स्टोरेज मीडिया की जब्ती (सीडी, डीवीडी, मेमोरी कार्ड, यूएसबी डाइव आदि)

अपराध स्थल को सुरक्षित करें

अपराध स्थल को सुरक्षित करें। आरोपी या किसी अन्य व्यक्ति जिसके पास संदिग्ध उपकरण है, से तुरंत जांच अधिकारी के नियंत्रण में स्टोरेज मीडिया लें।

स्टेप–1

फोटोग्राफी और वीडियोग्राफी

फोटोग्राफी और वीडियोग्राफी

पूरे क्राइम सीन पर मिले सभी स्टोरेज मीडिया(Hard disk/सीडी/डीवीडी/पेन ड्राइव/मेमोरी कार्ड) की तस्वीर लें। के बैक, फ्रंट और सभी साइड व्यू कैप्चर करें।

स्टेप– 2

सिस्टम जानकारी एकत्र करें

स्टोरेज मीडिया की विस्तृत जानकारी जैसे ब्रांड, क्षमता, रंग, सीरियल नंबर और सभी प्रासंगिक जानकारी नोट करें। फर्द जब्ती में इसका उल्लेख करें। **स्टेप– 3**

डिस्क की क्लोनिंग

आगे की जांच के लिए सीडी/डीवीडी/मेमोरी कार्ड/एचडीडी/यूएसबी ड्राइव या किसी अन्य स्टोरेज मीडिया (मेमोरी कार्ड या यूएसबी ड्राइव या हार्ड डिस्क को क्लोन करने के लिए राइट ब्लॉकर का उपयोग करें) का क्लोन तैयार करें। क्लोनिंग के लिए समान आकार की डिस्क का उपयोग करें। हार्ड डिस्क के मामले में, क्लोन बनाने के लिए समान क्षमता, समान मेक मॉडल और समान स्ठ। (लॉजिकल ब्लॉक वैल्यू) का उपयोग करें। क्लोन से उपयोगी डेटा निकालें। **स्टेप– 4**

पैकेजिंग और मार्किंग

स्टोरेज मीडिया की विस्तृत जानकारी जैसे ब्रांड, क्षमता, रंग, सीरियल नंबर और सभी प्रासंगिक जानकारी नोट करें। फर्द जब्ती में इसका उल्लेख करें। हार्ड डिस्क/यूएसबी ड्राइव/मेमोरी कार्ड/सीडी/डीवीडी या किसी अन्य स्टोरेज मीडिया को पैक करने के लिए फैराडे बैग के बाद बबल पैकिंग का उपयोग करें। **स्टेप– 5**

साक्ष्य संचालन प्रक्रिया के दौरान सावधानियॉ

जांच के दौरान सबूतों को संभालते समय, आप आम तौर पर निम्नलिखित प्रक्रियाओं का पालन करेंगेः–

1.यदि वर्तमान में कंप्यूटर में रखी गई हार्ड ड्राइव की सामग्री की जांच कर रहे हैं, तो जांच के तहत कंप्यूटर सिस्टम के बारे में जानकारी रिकॉर्ड करें।
2. मूल प्रणाली औरध्या मीडिया की डिजिटल तस्वीरें लें जिनकी नकल की जा रही है।
3. मूल मीडिया के लिए या फोरेंसिक दोहराव के लिए एक सबूत टैग भरें (जो भी हार्ड ड्राइव आप सबसे अच्छे सबूत के रूप में रखेंगे और अपने साक्ष्य को सुरक्षित रखेंगे)।
4. सभी मीडिया को एक साक्ष्य लेबल के साथ उचित रूप से लेबल करें।
5. साक्ष्य मीडिया की सर्वोत्तम साक्ष्य प्रति को अपने साक्ष्य में सुरक्षित रखें।
6. एक साक्ष्य अभिरक्षक साक्ष्य लॉग में सर्वोत्तम साक्ष्य का रिकॉर्ड दर्ज करता है। सर्वोत्तम साक्ष्य के प्रत्येक भाग के लिए, साक्ष्य लॉग में एक संगत प्रविष्टि होगी।

7. सभी परीक्षाएं सर्वोत्तम साक्ष्य की फोरेंसिक कॉपी पर की जाती हैं, जिसे वर्किंग कॉपी कहा जाता है।
8. एक साक्ष्य संरक्षक यह सुनिश्चित करता है कि सर्वोत्तम साक्ष्य की बैकअप प्रतियां बनाई जाएं। एक बार मामले के प्रमुख अन्वेषक के यह कहने के बाद कि डेटा की अब शीघ्रता से आवश्यकता नहीं होगी, साक्ष्य अभिरक्षक टेप बैकअप तैयार करेगा।
9. एक साक्ष्य संरक्षक यह सुनिश्चित करता है कि सभी निपटान तिथियां पूरी हों। साक्ष्य निपटान की तिथियां प्रमुख अन्वेषक द्वारा निर्धारित की जाती हैं।
10. एक साक्ष्य संरक्षक यह सुनिश्चित करने के लिए मासिक ऑडिट करता है कि सभी बेहतरीन साक्ष्य मौजूद हैं, ठीक से संग्रहीत और लेबल किए गए हैं।

डिजिटल साक्ष्यों का परिवहन करने समय सावधानियॉ

उपकरणों को एक स्थान से दूसरे स्थान तक ले जाने में भी बहुत सावधानी की आवश्यकता होती है।

डिजिटल साक्ष्य को कभी भी चुंबकीय क्षेत्र या वाहनों में सीट वार्मर के पास नहीं रखा जाना चाहिए क्योंकि सिस्टम क्षतिग्रस्त हो सकते हैं। ट्रांसपोर्टरों को भी अत्यधिक परिस्थितियों में डिजिटल साक्ष्य छोड़ने के बारे में सतर्क रहना चाहिए, जैसे कि गर्म कार की डिक्की में या ठंड स्थान में। कंप्यूटर और अन्य उपकरणों को इस तरह से पैक और सुरक्षित किया जाना चाहिए कि वे परिवहन के दौरान झटके, कंपन या गिरने से नुकसान के अधीन न हों। उदाहरण के लिए, आप बिना पैकेजिंग के अपनी कार की आगे की सीट पर एक लैपटॉप ले जाना नहीं चाहेंगे, जहां यह फिसल कर फर्श पर गिर सकता है, यदि आपको अपने ब्रेक पर पटकना पड़े। डिजिटल साक्ष्य को हमेशा यह शामिल करने के लिए प्रलेखित किया जाना चाहिए कि हिरासत की श्रृंखला को संरक्षित करने में मदद करने के लिए इसे कौन ले जा रहा है, जो यह दर्शाता है कि उनकी उपस्थिति में सामग्री किसके पास थी और कब थी।

पुलिस विभाग की अभिरक्षा ट्रेकिंग फॉर्म की श्रृंखला

मुकदमा नंबर	**02 / 2022**	मुकदमा दिनांक	**1 अप्रैल, 2022**
अंतर्गत धारा	66सी, 66डी आईटीएए 2008 एवं 419, 420 आईपीसी	**पुलिस थाना व जिला**	साइबर क्राईम पुलिस स्टेशन जिला जयपुर
जॉच अधिकारी का नाम व पद	यतींद्र कुमार खटाना, पुलिस निरीक्षक	**अभियोगी का नाम व पता**	सोनू कुमार जिला जयपुर
आइटम की जब्ती की दिनांक व समय	2 अप्रैल, 2022 समय 12:30 पीएम	**जब्ती का स्थान**	आमेर, जयपुर
संदिग्ध का नाम	रवि, अमित, शरद व सुरेश		

साक्ष्य का विवरण		
आइटम का नाम	**मात्रा**	**आइटम का विवरण (मॉडल, सीरियल नंबर, मार्क्स स्क्रैचेज इत्यादि)**
मोबाइल फोन	2	आइटम से संबंधित यूनिक नंबर जैसे आईएमईआई नंबर, मैक पता, सीरियल नंबर, मॉडल इत्यादि का विवरण
कम्प्यूटर	1	
लैपटॉप	1	
डीवीआर	2	

हिरासत में लेने की कडी				
आइटम का नाम	**दिनांक व समय**	**जारीकर्ता के हस्तारक्षर व आईडी**	**प्राप्तकर्ता के हस्ताक्षर व आईडी**	**विशेष टिप्पणी / स्थान**

अपराध जांच में इलेक्ट्रॉनिक साक्ष्य की भूमिका

प्रौद्योगिकी में वृद्धि के साथ, डिजिटल अपराधों में वृद्धि अपरिहार्य है। वास्तविक जीवन की तरह ही, इलेक्ट्रॉनिक उपकरणों का उपयोग करने वाले लोग अपने पीछे अलग–अलग पदचिन्ह और निशान छोड़ जाते हैं। ये आभासी या डिजिटल निशान फाइल के टुकड़े, गातिविधि लॉग, टाइमस्टैम्प, मेटाडेटा, और इसी तरह के हो सकते हैं।

डिजिटल फोरेंसिक एक नया विज्ञान है जिसमें कंप्यूटर, मोबाइल फोन या नेटवर्क जैसे डिजिटल मीडिया से सबूत ढूंढना शामिल है। फोरेंसिक टीमें डिजिटल साक्ष्य का विश्लेषण, निरीक्षण, पहचान और संरक्षण करती हैं, और इसका उपयोग प्रौद्योगिकी से संबंधित अपराधों की जांच में मदद करने के लिए करती हैं। चाहे साइबर हमले रैंसमवेयर द्वारा एन्क्रिप्ट की गई फाइलें, डेटा फोरेंसिक विशेषज्ञ यह निर्धारित करने में मदद कर सकते हैं कि हमला कैसे हुआ, नुकसान क्या था?

डिजिटल फोरेंसिक क्यों महत्वपूर्ण है? डिजिटल फोरेंसिक बहुत कुछ कर सकता है, जिसमें शामिल हैं:–

- साइबर हमले के कारण और संभावित मंशा की पहचान करना।
- अप्रचलित होने से पहले हमले में उपयोग किए गए डिजिटल साक्ष्य की सुरक्षा करना।
- सुरक्षा स्वच्छता बढ़ाना, हैकर के चरणों का पता लगाना, और हैकर टूल ढूंढना।
- डेटा एक्सेस/एक्सफिल्टरेशन की खोज करना।
- नेटवर्क पर अनधिकृत पहुंच की अवधि की पहचान करना।
- लॉगिन को जियोलोकेट करना और उनकी मैपिंग करना।

ये सभी न केवल किसी हमले से निपटने में बल्कि उसके परिणाम और उसके परिणामों से निपटने में सहायक होते हैं।

साइबर अपराध जांच के लिए चुनौतियां

साइबर अपराध जांच की कुछ प्रमुख चुनौतियों में निम्नलिखित शामिल हैं:–

- साइबर अपराधी गुमनाम हो कर अपराध करता है क्योकि ऐसा करने में साइबर तकनीक उन्हे सक्षम बनाती है। यह गुमनामी अनुसंधान के लिए एक बडी चुनौती है।
- डिजिटल साक्ष्य अत्यंत नाजुक होते जिनसे आसानी से छेडछाडी की जा सकती हैा
- सुरक्षा कर्मियों के पर्याप्त ज्ञान और प्रशिक्षण का अभाव होता है। जिसके कारण सही अनुसंधान करने में चुनौतियों का सामना करना पडता है।
- सामंजस्यपूर्ण राष्ट्रीय साइबर–अपराध कानूनों और अंतर्राष्ट्रीय की कमी से पूर्ण सूचना समय पर न मिलने से अनुसंधान बाधित होता है।
- साक्ष्य आवश्यकताओं का मानकीकरण नहीं होना।
- तकनीक में तेजी से बदलाव होना।

इकाई–2

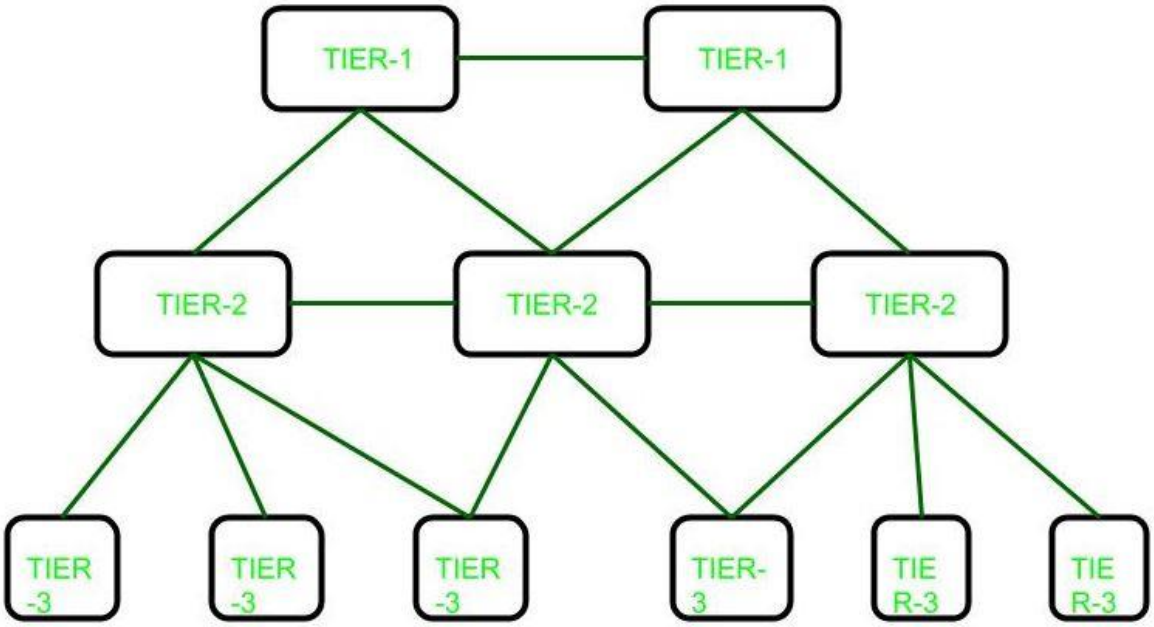
बाहरी अभिकरणों या कम्पनियों से सूचना संग्रहण

- इंटरनेट सेवा प्रदाताओं से सूचना और प्रारूप की उपलब्धता
- ईमेल सेवा प्रदाताओ से सूचना
- मोबाइल सेवा प्रदाताओ से सूचना
- सोशल नेटवक्रिग साइट्स जैसे फेसबुक, व्हाट्सअप, इन्स्टाग्राम, ट्यूटर आदि से सूचना
- वित्तीय संस्थानों से सूचना
- वेबसाइट्स डोमेन्स/हास्टिंग प्रदाताओ से सूचना
- इंटरनेट कॉल सेवा प्रदाताओ आदि से सूचना

इंटरनेट सेवा प्रदाता

इंटरनेट तक पहुँचने, उपयोग करने या इसमें भाग लेने के लिए सेवाएँ प्रदान करता है। इंटरनेट सेवा प्रदाताओं के विभिन्न रूप है जैसे वाणिज्यिक, समुदाय–स्वामित्व वाली, गैर–लाभकारी, या अन्यथा निजी स्वामित्व वाली। इनके द्वारा इंटनेट सेवा प्रदान करने के साथ इंटरनेट एक्सेस, इंटरनेट ट्रांजिट, डोमेन नाम पंजीकरण, वेब होस्टिंग, यूजनेट सेवा और कॉलोकेशन का कार्य भी किया जा सकता है।

इंटरनेट सेवा प्रदाता (ISP) एक ऐसी कंपनी है जो अंतिम उपयोगकर्ता को इंटरनेट कनेक्शन प्रदान करती है, लेकिन मूल रूप से ISP के तीन स्तर होते हैं। इंटरनेट सेवा प्रदाता (ISP) के 3 स्तर हैं। Tier-1 ISP, Tier-2 ISP और Tier-3 ISP।



टियर–1 आईएसपीः–

ये आईएसपी पदानुक्रम के शीर्ष पर हैं और उनकी वैश्विक पहुंच है। वे अपने नेटवर्क के माध्यम से किसी भी इंटरनेट ट्रैफिक के लिए भुगतान नहीं करते हैं। इसके बजाय निचले स्तर के आईएसपी को टियर–1 आईएसपी को अपने ट्रैफिक को एक भौगोलिक स्थान से दूसरे में स्थानांतरित करने के लिए एक लागत का भुगतान करना पड़ता है । आम तौर पर समान स्तर पर आईएसपी एक दूसरे से जुड़ते हैं और एक दूसरे को मुफ्त ट्रैफिक पास की अनुमति देते हैं। ऐसे ISP को पीयर कहा जाता है। इस वजह से लागत बच जाती है। वे अन्य सभी इंटरनेट सेवा प्रदाताओं को यातायात प्रदान करने के लिए अटलांटिक इंटरनेट समुद्री केबल जैसे बुनियादी ढांचे का निर्माण करते हैं।

उदाहरण

टियर 1 इंटरनेट प्रदाताओं के कुछ उदाहरणः–

टाटा कम्युनिकेशंस, भारती एयरटेल, रिलायंस जियो इन्फोकॉम लिमिटेड, ग्लोबल क्लाउड एक्सचेंज, सिफी टेक्नोलॉजीज, वोडाफोन

टियर–2 आईएसपीः–

ये आईएसपी सेवा प्रदाता हैं जो टियर 1 और टियर 3 आईएसपी के बीच जुड़ते हैं। उनकी क्षेत्रीय या देश तक पहुंच है और वे टियर –3 आईएसपी के लिए टियर –1 आईएसपी की तरह ही व्यवहार करते हैं।

टियर 2 ISP के उदाहरण

एयरटेल, रिलायंस जियो, वोडाफोन आइडिया, एसीटी फाइबरनेट, हेथवे, एपीएसएफएल, जीटीपीएल ब्रॉडबैंड प्रा0 लिमिटेड, वोडाफोन

टियर–3 आईएसपीः–

ये आईएसपी अंतिम उपयोगकर्ताओं के सबसे करीब हैं और कुछ पैसे चार्ज करके उन्हें इंटरनेट से जुड़ने में मदद करते हैं। ये आईएसपी परचेजिंग मॉडल पर काम करते हैं। इन ISP को उत्पन्न ट्रैफिक के आधार पर टियर –2 ISP को कुछ लागत का भुगतान करना पड़ता है।

भारत में कितने ISP हैं?

30 सितंबर 2021 तक भारत में 584 इंटरनेट सेवा प्रदाता (आईएसपी) ब्रॉडबैंड और नैरो बैंड इंटरनेट सेवाएं दे रहे थे।

ईमेल सेवा प्रदाता

एक ईमेल सेवा प्रदाता (ईएसपी) उपयोगकर्ताओं को ग्राहकों की सूची में ईमेल भेजने की अनुमति देता है। उदाहरणार्थ जीमेल, याहुमेल, रेडिफमेल इत्यादि।

ईमेल सेवा प्रदाता तकनीकी कंपनियां हैं जो लोगों के लिए ईमेल सूचियां बनाना और ईमेल भेजना आसान बनाती हैं। जैसा कि ईमेल मार्केटिंग एक अधिक लोकप्रिय मार्केटिंग स्थल बन गया है, अधिक ईमेल सेवा प्रदाता अलग–अलग सेवाएं प्रदान रहे हैं। सबसे बुनियादी स्तर पर, एक ईएसपी को दो काम करने की आवश्यकता होती हैः ईमेल पते संग्रहित करें और ईमेल भेजें।

एक अधिक उन्नत ईमेल सेवा प्रदाता अतिरिक्त सुविधाएँ प्रदान करता है, जिनमें शामिल हैंः

- ईमेल में गतिशील सामग्री
- ईमेल और मार्केटिंग ऑटोमेशन
- ईमेल विषय पंक्तियों और ईमेल सामग्री का परीक्षण
- वेबसाइट ट्रैकिंग, ग्राहकों के बारे में अधिक जानकारी एकत्र करने के लिए
- ग्राहकों की रुचि के आधार पर विभाजन

(1) ईमेल खाते का नाम, पता, टेलीफोन नंबर, पंजीकरण समय का आईपी पता, पंजीकरण की तिथि और समय।

(2) भारतीय मानक समय (आईएसटी) में सटीक तिथि और समय प्रारूप के साथ उपरोक्त ईमेल खाते का लॉगिन विवरण और मैक पते का विवरण।

(3) खाते से जुडी अन्य इंटरनेट सेवाओ का विवरण।

(4) लिंक ईमेल आईडी।

मोबाइल सेवा प्रदाता

एक टीएसपी या एमएसपी एक प्रकार का संचार सेवा प्रदाता है जो परंपरागत रूप से टेलीफोन और अन्य समान सेवाएं प्रदान करता है। इन दिनों दूरसंचार और मोबाइल सेवा प्रदाता न केवल दूरसंचार सेवाएं प्रदान कर रहे हैं बल्कि इंटरनेट सेवाएं भी प्रदान कर रहे हैं। भारत में मोबाइल सेवा प्रदाताओं की सूची भारत में कुछ प्रमुख मोबाइल सेवा प्रदाता और उनके संचालन के क्षेत्र का उल्लेख नीचे किया गया है:

S No.	सेवा प्रदाता का नाम	संचालन का क्षेत्र
(1)	टाटा टेलीसर्विसेज लिमिटेड	असम, NE और J&K को छोड़कर अखिल भारतीय
(2)	मेसर्स रिलायंस जियो इन्फोकॉम	अखिल भारतीय
(3)	मेसर्स रिलायंस टेलीकॉम लिमिटेड	कोलकाता,एमपी, डब्ल्यूबी, एचपी, बिहार, ओडिशा, असम और
(4)	मेसर्स रिलायंस कम्युनिकेशंस लिमिटेड	असम और पूर्वोत्तर को छोडकर अखिल भारतीय
(5)	मैसर्स महानगर टेलीफोन निगम लिमिटेड	दिल्ली और मुम्बई
(6)	वोडाफोन आइडिया लिमिटेड	अखिल भारतीय
(7)	भारत संचार निगम लिमिटेड	दिल्ली और मुम्बई को छोडकर अखिल भारतीय
(8)	भारती एयरटेल लिमिटेड	अखिल भारतीय

मोटे तौर पर भारत को विभिन्न सेल्युलर जोनों या सर्किलों में बांटा गया है, जिन्हें आगे 23 सर्किलों और 4 श्रेणियों में बांटा गया है। मेट्रो श्रेणी के तहत हमारे पास है–

1 दिल्ली
2 मुंबई
3 कोलकाता
4 चेन्नई

जबकि ए श्रेणी के शहरों में शामिल हैं:–आंध्र प्रदेश, तेलगना, कर्नाटक, केरल, तमिलनाडू, महाराष्ट्र, गुजरात
बी श्रेणी के शहरों में शामिल हैं:– हरियाणा, राजस्थान, मध्य प्रदेश, छत्तीसगढ़, पंजाब, उत्तर प्रदेश, उत्तराखंड, पश्चिम बगल और अंडमान।
सी श्रेणी के शहरों में शामिल हैं जम्मू और कश्मीर, हिमाचल प्रदेश, बिहार, झारखंड, असम, उत्तरपूर्व और ओडिशा।

कुछ राज्यों के लिए दूरसंचार सर्किल एक सर्कल के अंतर्गत आते हैं और कुछ राज्यों के लिए इसे कई सर्किलों में विभाजित किया जाता है।

एक सक्रिल में आने वाले संयुक्त राज्य हैंः–

1 महाराष्ट्र और गोवा

2 एमपी और छत्तीसगढ़

3 एपी और तेलगना

4 उत्तर पूर्व राज्य

दूसरी ओर दो सर्किलों में विभाजित राज्य हैं–

✓ यूपी पूर्व

✓ यूपी पश्चिम और उत्तराखंड

टीएसपी/एमएसपी की जिम्मेदारियांः नोडल पार्टियों के रूप में

नोडल पार्टियों के रूप में दूरसंचार और मोबाइल सेवा प्रदाताओं की जिम्मेदारियों में निम्नलिखित शामिल हैं–

- यह सुनिश्चित करना कि मांगी गई जानकारी उचित प्रारूप में है ठीक से भरी गई है, सही डेटा है और अप–टू–डेट है।
- कानून प्रवर्तन एजेंसियों के साथ समन्वय कानून प्रवर्तन ,जेंसियों या भारतीय क्षेत्रीय दूरसंचार नियामक प्राधिकरण ट्राई दूरसंचार प्रवर्तन और संसाधन निगरानी किसी भी निरीक्षण और लेखा परीक्षा सहित टर्म
- कॉर्पोरेट नियामक दिशानिर्देशों के अनुसार सीएएफ ऑडिट और नियामक अनुपालन कर समय पर व्यावसायिक सहायता और दर्शन प्रदान करना।
- सीएएफ, नेटवर्क और कानूनी मामलों से संबंधित मुद्दों के लिए अन्य कार्यों के साथ समन्वय करना और टर्म सेल के साथ बातचीत करना।
- दूरसंचार और मोबाइल सेवा प्रदाता पूर्व–निर्दिष्ट समय सीमा के अनुसार एक जांच एजेंसी को आवश्यक विवरण प्रदान करने के लिए भी जिम्मेदार हैं।

टीएसपी/एमएसपी के लिए सामान्य समयरेखा–

दूरसंचार नोडल एजेंसियों को यह सुनिश्चित करने की आवश्यकता है कि एक जांच अधिकारी द्वारा मांगी गई जानकारी उचित प्रारूप में प्रदान की जाती है और पूर्व–निर्दिष्ट समय सीमा के भीतर प्रदान की जाती है। ये समयरेखा है

टीएसपी/एमएसपी	समय
सब्सक्राईबर डेटा रिकॉर्ड (एसडीआर)	1 घंटा यदि ग्राहक का डाटा 15 दिनों से अधिक पूराना है। जिसे अपडेट कर लिया गया है। 24 धण्टे यदि ग्रहक का रिकोर्ड डाटा 15 दिनों के भीतर का है जिसे अपडेट नहीं किया गया है।
6 महिने तक की सीडीआर	6 घण्टे के अन्तर्गत
6 महिने से अधिक	12 घण्टे के अन्तर्गत

की सीडीआर	
कैफ की प्रतिलिपि	72 घण्टे के अन्तर्गत यदि नंबर पंजीकरण 3 महिने के भीतर का हो 48 घण्टे के अन्तर्गत यदि नंबर पंजीकर.ण 3 महिने से अधिक का हो।
बीटीएस स्थान की जानकारी	1 घण्टे से 6 घण्टे के भीतर

टीएसपी/एमएसपी के साथ ईमेल के माध्यम से संवाद करें–

जांच अधिकारी आधिकारिक ईमेल आईडी के माध्यम से दूरसंचार नोडल एजेंसियों के साथ संवाद कर सकता है। रॉ सीडीआर फाइल प्राप्त करने के लिए आप दूरसंचार एजेंसियों को जो कानूनी नोटिस भेजते हैं, वह त्रुटि रहित होना चाहिए। प्रमुख टीएसपी/एमएसपी के लिए ईमेल आईडी की सूची को 'दर्शनाने वाली तालिका यहां दी गई है:

टीएसपी/एमएसपी	ईमेल आईडी
एयरसेल	<XYZ.nodaldesk@aircel.co.in>
एयरटेल	<nodalofficerg 3.XYZ@in.airtel.com>
बीएसएनएल	<techcellone_hyd@bsnl.co.in>
आईडिया	<nodal.XYZ@idea.adityabirla.com>

एमएसपी से जानकारी

- CAF– ग्राहक आवेदन पत्र (हम लगभग 31 जानकारी प्राप्त कर सकते हैं)
- एसडीआर–सब्सक्राइबर विवरण रिपोर्ट
- सीडीआर– कॉल विवरण रिपोर्ट आईपीडीआर– इंटरनेट प्रोटोकॉल विवरण रिपोर्ट
- टीडीआर–टॉवर डंप रिकॉर्ड

वित्तीय संस्थान

बैंक एक वित्तीय संस्थान है जो जनता से जमा स्वीकार करता है और मांग जमा बनाता है। भारतीय रिजर्व बैंक (आरबीआई) इन सभी बैंकों को नियंत्रित करता है।

भारत में सर्वश्रेष्ठ बैंक निम्न प्रकार से हैः–

एचडीएफसी बैंक	बैंक ऑफ बड़ौदा
आईसीआईसीआई बैंक	केनरा बैंक
महिंद्रा बैंक	पंजाब नेशनल बैंक
भारतीय स्टेट बैंक	ऐक्सिस बैंक
आईडीबीआई बैंक	बैंक ऑफ इंडिया

डिजिटल वॉलेट

- मोबिक्विक
- Google पे
- एसबीआई द्वारा योनो
- PhonePe
- एयरटेल मनी
- धानी ऐप इंडियाबुल्स का हिस्सा है
- सिटी मास्टर पास
- आईसीआईसीआई पॉकेट्स
- भीम
- HDFC PayZapp
- पेटीएम
- अमेजन पे

बैंक से जानकारी

- खाता संख्या
- सीसीटीवी फुटेज
- नाम
- ईमेल आईडी
- पता
- डेबिट/क्रेडिट कार्ड नंबर
- फोटो
- मोबाइल नंबर
- ऑनलाइन ट्रांजेक्शन डिटेल
- निवास प्रमाण पत्र
- आधार कार्ड
- चल या अचल संपत्ति विवरण
- पैन नंबर

- इनकम टैक्स रिटर्न की कॉपी
- खाते का प्रकारः चालू या बचत या प्रकार
- फर्म का नाम, पता यदि फर्म के नाम से बैंक खाता खुला है।
- खाते के नोमिनी व गारंटर की डिटेल्स
- बैंक के अन्य खातों की जानकारी
- बैंक खाता धारक का हस्ताक्षर
- यदि खाता ऑनलाइन है तो खाते को लॉग–इन करने के आईपी लॉग्स

वॉलेट से सम्बंधित जानकारी–

- रजिस्ट्रेंट यूजर आईडी, नाम, फोन नंबर और ईमेल पता
- उपयोगकर्ता खाते का केवाईसी जो उपर्युक्त ट्रांजेक्शन में शामिल है।
- सभी ट्रांजेक्शन के जीपीएस निर्देशांक
- आईपी लॉग के साथ ट्रांजेक्शन इतिहास (दिनांक और समय)
- खाताधारक का पता
- बैंक खाता संख्या जो वालेट से जुडा हुआ है।
- कुल लेनदेन विवरण (अकाउण्ट स्टेटमेंट)
- वालेट के पंजीकरण की तारीख, आईपी लॉग
- डेबिट/क्रेडिट कार्ड विवरण
- ग्राहक/व्यापारी/पीओएस जो ट्रांजेक्शन में स्तेमाल की गई है।
- फोन नंबर/मोबाइल जो संदिग्ध लेनदेन का में स्तेमाल हुआ है।
- ईमेल आईडी
- वालेट को एक्सेस किया है वे सभी आईपी लॉग्स

सोशल मीडिया साइट्स

- सोशल मीडिया एनालिटिक्स टूल का उपयोग करके

सोशल मीडिया एनालिटिक्स टूल का उपयोग प्रवृत्ति की पहचान करने और विभिन्न प्रोफाइल के बीच लिंक खोजने के लिए किया जाता है। सही कीवर्ड का उपयोग करके किसी विशेष क्षेत्र की भावना प्रवृत्तियों की पहचान करना भी सहायक होता है। कुछ सोशल मीडिया एनालिटिक्स वेबसाइट जिनका आप उपयोग कर सकते हैंः **ट्रेंड 24, ट्रीटडेक और एक मिलियन ट्वीट मेप।** आप अपने स्थान या किसी अन्य स्थान के ट्रेडिंग टैग की पहचान करने के लिए Trends24.in का उपयोग कर सकते हैं। और यह जानने के लिए कि किसी विशेष स्थान से कौन क्या पोस्ट कर रहा है आप https://onemilliontweetmap.com वेबसाइट का उपयोग कर सकते हैं। यह एक बहुत शक्तिशाली उपकरण है। इसके माध्यम से हम किसी विशेष क्षेत्र का सेंटीमेंट एनालिसिस कर सकते हैं।

एक सोशल नेटवर्किंग सेवा (सोशल नेटवर्किंग साइट या सोशल मीडिया भी) एक ऑनलाइन प्लेटफॉर्म है जिसका उपयोग लोग अन्य लोगों के साथ सामाजिक नेटवर्क या सामाजिक संबंध बनाने के लिए करते हैं जो समान व्यक्तिगत या केरियर हितों, गातिविधियों, पृष्ठभूमि या वास्तविक जीवन कनेक्शन साझा करने के लिए करते हैं। सोशल मीडिया साइट हैः फेसबुक, व्हाट्सअप, टेलीग्राम, इंस्टाग्राम, ट्यूटर, यूट्यूब इत्यादि।

सोशल नेटवर्किंग साइट्स उपयोगकर्ताओं को अपने नेटवर्क में लोगों के साथ विचारों, डिजिटल फोटो और वीडियो, पोस्ट साझा करने और ऑनलाइन या वास्तविक दुनिया की गातिविधियों और घटनाओं के बारे में दूसरों को सूचित करने की अनुमति देती हैं।

सोशल नेटवर्किंग साइट्स के फायदे

- फंड जुटाने के लिए प्लेटफॉर्म
- सीमा के बिना नेटवर्किंग
- तत्काल समाचार और सूचना
- व्यापार के लिए बढ़िया मार्केटिंग चैनल
- जागरूकता और सक्रियता
- विचारों का आदान–प्रदान और सहयोग

सोशल मीडिया साइटों से जानकारी

- खाता उपयोगकर्ता का नाम
- पता
- जन्म की तारीख
- जीपीएस स्थान
- मोबाइल नंबर
- रजिस्ट्रेशन करते समय का आईपी पता
- खाते के पंजीकरण की तिथि और समय।
- सटीक तिथि और समय के साथ खाते का लॉगिन विवरण
- प्रारूप
- गातिविधियों का विवरण
- उपकरणों के मैक पते
- ईमेल नंबर
- आईपी लॉग
- खाता उपयोगकर्ता के अन्य ग्रुपों से संबंध
- रिश्तेदार व मित्रों के बारे में जानकारी
- संम्पति का विवरण
- देशी व विदेशी यात्राओं का विवरण

- फोटो खातेधारक की स्वयं, परिवार, मित्र व संबंधियों, सम्पति की
- व्यवसाय
- जीवन–वृत
- शिक्षा
- विभिन्न प्रकार की वे पोस्टे जो संदिग्ध ने शेयर या कमेंट या लाइक की है।
- डेबिट या क्रेडिट कार्ड या बैंक खातों की जानकारी।

व्हाट्सअप सोशल मीडिया

व्हाट्सअप द्वारा कानून प्रवर्तन एजेंसी को सूचना प्रदान करने के लिए एक पोर्टल बनाया हुआ है जिस पर अनुसंधान अधिकारी अपनी सरकारी ईमेल आईडी के माध्यम से रजिस्ट्रेशन करके चाहिए गई सूचना दण्ड प्रक्रिया संहिता की धारा 91 का नोटिस दे कर सूचना प्राप्त की जा सकती है उक्त पोर्टल पर तीन प्रकार से सूचना की सूचना की सुविधा दी गई है–

1. सामान्य प्रकार के मामलों में।
2. आपातकालीन मामलों में जिसमें किसी बालको की सुरक्षा के मामले बच्चे को नुकसानए मृत्यु व गभ्भीर शारीरिक चोट महिलाओ और किसी बच्चे को नुकसान या किसी भी व्यक्ति को मृत्यु या गंभीर शारीरिक चोट का जोखिम के "EMERGENCY' विषय में ।
3. किसी सूचना को संरक्षित कराने के बारे में जिसके बारे में अनुसंधान अधिकारी को यह विश्वास है कि निकट भविष्य में संरक्षित सूचना का उपयोग विशिष्ट मामले में किए जाने की संभावना है या व्हाट्सअप अकाउण्ट के डिलिट किए जाने की संभावना है। हम औपचारिक कानूनी प्रक्रिया प्राप्त होने तक 90 दिनों के लिए आपराधिक जांच के संबंध में खाता रिकॉर्ड को संरक्षित करा सकते है।

व्हाट्सअप निम्न प्रकार की सूचना देता हैः–

- खाता धारक का नाम
- मोबाइल नंबर
- रजिस्ट्रेशन की दिनांक व समय
- रजिस्ट्रेशन के समय की आईपी लॉग
- ईमेल एड्रेस
- उन व्हाट्सअप समूहो की सूचना जिनसे खाता धारक जुडा हुआ है।
- खाता धारक व व्हाट्स अप समूह की प्रोफाइल पर लगे फोटो
- खाता धारक जिन व्हाट्सअप नंबरों के साथ चैटिग करता है उन नंबरों के बारे में जानकारी
- खाता अंतिम बार कब लॉग–इन रहा वह दिनांक व समय
- अंतिम बार किस आईपी से लॉग–इन
- विशिष्ट मामलों में व प्रक्रिया से सम्पूर्ण आईपी लॉग मैसेज इमेज, ऑडियों व विडियो तथा कॉल का प्रकार व अवधि

- गुमशुदा व शोषित बच्चों का राष्ट्रीय केन्द्र (NCMEC) धारा व्हाट्स–अप खाते के बारे में कोई रिपोर्ट की हुई है अथवा नहीं

एंड–टू–एंड एन्क्रिप्शन का मतलब है कि संदेशों को व्हाट्सएप और तीसरे पक्ष को पढ़ने से बचाने के लिए कूट भाषा में बदला गया है।

वेबसाइट्स

एक वेबसाइट वेब पेजों और संबंधित सामग्री का एक संग्रह है जिसे एक सामान्य डोमेन नाम से पहचाना जाता है और कम से कम एक वेब सर्वर पर होता है जिस पर उसे चलाया जाता है। उल्लेखनीय उदाहरण हैं wikipedia-org, google.com और amazon.com

सभी सार्वजनिक रूप से सुलभ वेबसाइटें सामूहिक रूप से वाइड वेब का गठन करती हैं। वेबसाइटें आम तौर पर किसी विशेष विषय या उद्देश्य के लिए समर्पित होती हैं, जैसे समाचार, शिक्षा, वाणिज्य, मनोरंजन या सोशल नेटवर्किंग।

वेबसाइट के प्रकार–

वेवसाइट्स दो प्रकार की होती हैं

1. स्टेटिक वेबसाइट
2. गातिशील वेबसाइट

एक स्टेटिक अर्थात् स्थिर वेबसाइट वह है जिसमें वेब पेज सर्वर पर उस प्रारूप में संग्रहीत होते हैं जो क्लाइंट वेब ब्राउजर को भेजा जाता है। इस प्रकार की वेबसाइट्स उपयोग्कर्ता केवल उस वेबसाइट को केवल देख सकता है उस पर अपनी प्रतिक्रिया या वेबसाइट पर किसी भी प्रकार से संचार नहीं कर सकता है। अधिक जानकारी के लिए आप https://tihalt-com/eXamples-of-static&websites/ का अवलोकन कर सकते है। एक गातिशील वेबसाइट वह है जो खुद को बदलता या अनुकूलित कर सकती है जिसमें उपभोक्ता जो उस वेबसाइट को एक्सेस कर रहा है अर्थात उसका उपयोग कर रहा है उसमें अपनी ओर से बदलाव कर सकता है उसमें कण्टेण्ट को जोडने में अपना योग्ज्ञदान दे सकता है। अधिक जानकारी के लिए आप https://tihalt-com/eXamples-of-dynamic&websites/ का अवलोकन कर सकते है।

वेबसाइट से जानकारी

किसी वेबसाइट के बारे में जानकारी हमें दो प्रकार से मिलती है:–

1–यदि वेबसाइट स्वंय ही अपराध में शामिल हो– जिसके उपर लिखे गये या डाले गये विषय ही इस प्रकार के हो कि वह पूरी वेबसाइट ही उपराध में लिप्त हो तो ऐसी जानकारी सम्भावना है कि स्वयं के बारे में अपनी जानकारी न दे। ऐसी वेबसाइटों के बारे में जो जानकारी कानूनी तौर से ली जावेगी वह उस वेबसाइट के डोमेन नेम प्रदाता और उस वेब

को होस्ट करने वाले से ली जावेगी। इस प्रकार की वेबसाइट के बारे में डोमेन नाम प्रदाता से निम्न प्रकार की सूचना मॉगी जानी चाहिए–

- वेबसाइट के रजिस्ट्रेण्ट का नाम, पता और मोबाइल नंबर,
- वेबसाइट का डोमेन नेम कब रजिस्टर्ड कराया दिनांक व समय,
- रजिस्ट्रेशन के समय की आईपी एड्रेस,
- रजिस्ट्रेशन के लिए किये गये भुगतान के माध्यम का सम्पूर्ण विवरण इत्यादि सूचनाएँ मॉगी जानी जाएगी।

2–यदि कोई अपराध वेबसाइट के माध्यम से किया गया है जिसमें वेबसाइट धारक एक मध्यस्थ के रूप में सुविधा प्रदान कर रहा हो–

इस प्रकार की वेबसाइट स्वंय अपराध में लिप्त तो नहीं है लेकिन उस वेबसाइट को आधार बना कर उसके माध्यम से कोई अपराध किया जाता है जैसे फेसबुक पर कोई आपत्तिजनक पोस्ट या टिप्पणी का किया जाना। इस प्रकार की वेबसाइट से हमें संदिग्ध के बारे में सूचनाएँ ली जानी होती है। इस प्रकार की वेबसाइट्स से हम निम्न प्रकार की सूचनाएँ ले सकते हैः–

- संदिग्ध का नाम, पता और मोबाइल नंबर
- लॉग–इन आईपी विवरण
- ट्रांजेक्शन का सम्पूर्ण विवरण
- ईमेल आईडी
- बैंक खाता संख्या
- डेबिट/क्रेडिट कार्ड विवरण
- आईपी लॉग
- मैक पता

डोमेन होस्ट प्रदाता

वेब होस्टिंग एक ऐसी सेवा है जो संगठनों और व्यक्तियों को इंटरनेट पर वेबसाइट या वेब पेज पोस्ट करने की अनुमति देती है। यह किसी वेबसाइट को चलाने की सम्पर्ण सुविधा प्रदान करती है। एक वेब होस्ट, या वेब होस्टिंग सेवा प्रदाता, एक ऐसा व्यवसाय है जो वेबसाइट या वेबपेज को देखने के लिए आवश्यक तकनीकों और सेवाओं को प्रदान करता है। जिसमें डोमेन नाम प्रदान करना और उसकी होस्टिग करना दोना शामिल है। किसी वेबसाइट को इंटरनेट पर ले जाने के लिए उसे विशेष कंप्यूटरों पर संग्रहित किया जाता है जिन्हे सर्वर कहते है। ये सर्वर या तो स्वयं वेबसाइट धारक के होगे या वेब होस्टिंग की सुविधा प्रदान करने वाले वेब होस्टिंग की सुविधा प्रदान करने वाले डोमेन होस्ट प्रदाताओ के होगे। कुछ डोमेन होस्ट प्रदाता का नाम निम्न प्रकार से हैः–

सर्वश्रेष्ठ डोमेन होस्ट प्रदाता

☑ Domain.com

☑ ब्लूहोस्ट
☑ होस्टगेटर
☑ होवर
☑ Gandi.net
☑ ड्रीमहोस्ट
☑ Name.com

डोमेन होस्ट प्रदाता से जानकारी

यदि उस वेब साइट की होस्टिग किसी अन्य के धारा की जा रही है तो उस डोमेन होस्ट प्रदाता से हम निम्न प्रकार की सूचनाओ की मॉग दण्ड प्रक्रिया संहिता की धारा 91 का नोटिस दे कर प्राप्त कर सकते हैः–

- उस वेब साइट को एक्सेस करने वालों का विवरण जिसमें उनकी आईपी डिटेल्स, मैक संख्या, दिनांक व समय जब उसे एक्सेस किया गया।
- वेबसाइट के पंजीकरण की तिथि।
- वेबसाइट को होस्ट व डोमेन नाम प्रदान करने की तिथि।
- वह माध्यम जिसके धारा उस वेबसाइट का शुल्क का भुगतान समय समय पर किया गया उसका सम्पूर्ण विवरण।
- जिस समय उस वेब साइट को होस्ट किया गया उस पंजीकरण के समय की आईपी लॉग।
- संपर्क विवरण सहित कुलसचिव विवरण यानी नाम, पता, सभी फोन नंबर, उपरोक्त वेबसाइट के मालिक की ईमेल आईडी।
- डोमेन का डेटा बेस।

वीओआइपी (वॉयस ओवर इंटरनेट प्रोटोकॉल)

इसे आईपी टेलिफोनी, इंटरनेट टेलिफोनी भी करते है। वीओआइपी विडियों व ऑडियो कॉलिंग की आधुनिक इंटरनेट सेवा है जिसमें कॉल करने के लिए इंटरनेट का उपयोग किया जाता है। पहले जो हम वॉयस कॉलिंग करते थे वह केवल ओडियों कॉल ही होती थी जिसमें एनालॉग सिंग्नलों का उपयोग किया जाता था। जिसमें पैकेट स्विच्ड नेटवर्क पीएसटीएन का उपयोग किया जाता था। जिसमें जब कोई कॉल किया जाता था तो उस कॉल के लिए उसका मार्ग पहले ही निश्चित कर दिया जाता है। इस प्रकार की कॉल के कारण कॉल का एक निश्चित मार्ग अर्थात पथ या नेटवर्क हो जाने के कारण वह कॉल बहुत मेहॅगा होता है लेकिन वीओआइपी कॉल इंटरनेट आधारित होने के कारण उसका डाटा पैकिटों में विभाजित कर दिया जाता है। ये पेकिट विभिन्न पथ से हो कंर या़त्रा करते है जिसका कोई एक पथ निश्चित नहीं होता है तथा वह उस पथ का चुनाव करते है जो उन पैकिटों को सबसे कम समय में अपने गन्तव्य तक पहुॅचाए। इसलिए इस प्रकार के नेटवर्क में किसी निश्चित नेटवर्क को संरक्षित करने की आवश्यकता नहीं होती है। जिसके कारण इंटनेट पर होने वाली कॉल सुविधा बहुत सस्ती पडती है।

आजकल इंटनेट के माध्यम से होने वाले इस प्रकार के वीओआइपी कॉल के माध्यम से कई प्रकार के अपराध किये जा रहे है जिसके कई कारण हैः–

- सस्ती कॉल दर।
- देश में बैठे विदेशी वीओआइपी सेवा प्रदाता की सहायता से कॉल करने की सुविधा प्राप्त करना ताकि उनकी भारतीय कानूनों के आधार पर जो प्रतिबंध लगे है उनको दरकिनार किया जा सके।
- वचफ्रअल प्राईवेट नेटवर्क जिसे वीपीएन भी कहते है या प्राक्सी की मदद से उसके आईपी एड्रेस को छुपाया जा सके।
- कानून प्रवर्तन एजेंसियों को या तो उनके बारे में जानकारी प्राप्त ही न हो यदि प्राप्त हो भी तो बहुत समय में प्राप्त हो ताकि वे अपने आप को कानून प्रवर्तन एजेंसियों की पकड दूर बने रह कर अपराध करते जाए।
- देशों में विभिन्न प्रकार के कानून जो अपराधियों की निजता को बनाए रखते है उनका सहारा लिया जा सके।
- न्यायालय में प्रमाणित साक्ष्य न मिल पाने का फायदा उठाने के लिए। चूकि इस प्रकार की एजेंसी के द्वारा जो भी इलेक्ट्रोनिक साक्ष्य दिए जाते है उनके साथ धारा 65बी भारतीय साक्ष्य अधिनियम का प्रमाण पत्र नहीं दिया जाता है जिसके कारण कोर्ट में पेश किए गए साक्ष्य स्वीकार्य नहीं होते है।

व्हाट्सअप, फेसबुक, टेलिग्राम, स्काइप, फेसटाइम आदि द्वारा वीओआईपी कॉलिग की सुविधा प्रदान की जाती है। वीओआइपी सेवा प्रदाताओ से हमारे द्वारा निम्न प्रकार की जानकारी प्राप्त हो सकती है–

- पंजीकरण विवरण (खाता पंजीकरण के समय ली गई जानकारी)
- पंजीकरण के समय उपयोगकर्ता द्वारा प्रस्तुत विस्तृत जानकारी
- पंजीकरण खाता– नाम, पता, संपर्क नंबर, ई–मेल पता, बिलिंग पता (उपयोगकर्ता द्वारा प्रदत्त बिलिंग पता)
- भुगतान विधि/उपकरण डेटा आईपी लॉग्स (वीओआईपी सेवा में उपयोगकर्ता लॉगिन के समय कैप्चर किए गए आईपी पते)

•

इकाई–3
भारत से बाहर से सूचना संकलन हेतु कानूनी प्रावधान (एमएलएटी) पारस्परिक कानूनी सहायता संधि

पविदेशों से सूचना संकलन हेतु कानूनी प्रावधान

अनुसंधान करते समय यह हम जो प्रक्रिया अपनाते है वह दण्ड प्रक्रिया संहिता के प्रावधानों के तहत् अनुसंधान किया जाता है। दण्ड संहिता के प्रावधान भारतीय अधिकार क्षेत्र पर ही लागू होते है जिसके बारे में दण्ड प्रक्रिया संहिता के अध्याय 1 की धारा 1 में उसके अधिकारी क्षेत्र का वर्णन किया गया है। लेकिन कई बार ऐसा होता है किसी अपराध का अनुसंधान करते समय हमारी जानकारी में आता है कि अपराध के बारे में साक्ष्य देश की अधिकारिक सीमा से बाहर है, अपराधी विदेश में है या हमें जो जानकारी प्राप्त करनी है वह हमारे देश से बाहर है। इसलिए साक्ष्य प्राप्त करने, अपराधी की गिरफ्तारी, अपराधी व अपराध की जानकारी प्राप्त करने के लिए हमे विशेष प्रक्रियाओ का पालन करना पडता है। इस अध्याय के अन्तर्गत हम इन सब के बारे में विस्तार से चर्चा करेंगे।

भारतीय दण्ड प्रक्रिया संहिता के विदेश से अनुसंधान से संबंधित प्रावधान–

हालाकि भारतीय दण्ड प्रक्रिया का अधिकारिक क्षेत्र भारतीय अधिकारी क्षेत्र है जिसके बारे में हम पहले बता चुके है कि दण्ड प्रक्रिया संहिता की धारा 1 में अधिकार क्षेत्र में इसका वर्णन है। लेकिन दण्ड प्रक्रिया संहिता की धारा 166ए और 166बी दो ऐसी धाराएँ है जो हमें बताती है कि हमें विदेशों से अनुसंधान किस प्रकार से करना है और विदेशों को अपराध के संबंध में साक्ष्य प्रेषित करने समय क्या प्रक्रियाएँ अपनाई जानी है? इन दोनो धाराओ का वर्णन निम्न प्रकार से हैः–

धारा 166ए का विवरण–

दण्ड प्रक्रिया संहिता में धारा 166ए के अन्तर्गत यदि कोई पुलिस अधिकारी या भारसाधक अधिकारी, किसी मामले की जॉच हेतु भारत से बाहर किसी देश या स्थान में जॉच करने के लिए सक्षम अधिकारी को अनुरोध पत्र के आदेश जारी कर सकता है। यह धारा 166ए ऐसे मामलों में पुलिस अधिकारी द्वारा भारत से बाहर किसी देश या स्थान में अन्वेषण के लिए सक्षम प्राधिकारी को अनुरोध–पत्र जारी करने की प्रक्रिया को बतलाता है।

धारा 166बी का विवरण–

दण्ड प्रक्रिया संहिता में धारा 166बी के अन्तर्गत भारत से बाहर के किसी न्यायालय से या किसी विदेशी अधिकारिक संस्था से हमारे देश में कोई अनुरोध पत्र प्राप्त होता है तो उस पर उपलब्ध कराई जानी वाली सूचना के संबंध में क्या प्रक्रिया अपनाई जानी है उसके बारे में बताया किया गया है।

हमें किन मामलों में विदेश से सूचना प्राप्त करनी होती है?

- विदेश में खोजों का संचालन– जब विदेश में किसी व्यक्ति या कंपनी या संस्था से अपराध के संबंध में जानकारी प्राप्त होती है तो अनुसंधान अधिकारी विदेशी अधिकारिक कानूरी

एजेंसी से अनुरोध कर सकती है कि वह उस स्थान विशेष की तलाशी ले जहॉ अपराध से संबंधित साक्ष्य है।

- संदिग्धों से सवाल– संदिग्ध के बारे में जानकारी प्राप्त होती है वह अनुसंधान अधिकारी के मुकदमें में वांछित है जिससे अपराध के बारे में सवाल जबाव करना आवश्यक है तो अनुसंधान अधिकारी सवालों के जबाव प्राप्त करने के लिए इस प्रकार का अनुरोध पत्र जारी करवा कर सूचना प्राप्त कर सकता है।
- रिकॉर्ड बयान– यदि अपराध के बारे में गवाही देने वाला गवाह देश आने में सक्षम नहीं है या किसी अन्य कारण से यह उचित प्रतीत होता है कि गवाह द्वारा अपनी गवाही विदेश में स्थित सक्षम न्यायालय में ही रिकोर्ड की जाए तो अनुसंधान अधिकारी उसके बयान रिकोर्ड दर्ज किये जाने का अनुरोध कर सकता है।
- दस्तावेज प्राप्त करें– साइबर जैसे अपराधों में जब इंटरनेट ने पूरे विश्व को एक कर दिया है जिसमें कई विदेशी वेबसाइटों व संस्थाओं के माध्यम से अपराधों को अंजाम दिया जाता है तो उन दस्तावेजों को अनुसंधान हेतु प्राप्त करने के लिए अनुसंधान अधिकारी अनुरोध पत्र जारी करवा सकता है।
- अपराध की आय से अर्जित सम्पत्ति को जब्त करना– अपराध के माध्यम से जो सम्पत्ति प्राप्त की जाती है या अनुसंधान अधिकारी की राय है कि अपराधी द्वारा जो सम्पत्ति विदेशों में अर्जित की है उसे संलग्न किया जाये तो ऐसा अनुरोध किया जा सकता है।
- आरोपी को गिरफ्तार करना– यदि अपराध का आरोपी विदेश में है उसके खिलाफ अपराध को कारित किए जाने के पर्याप्त सबूत उपलब्ध है तो ऐसे अपराधी के प्रत्यर्पण की कार्यवाही अमल में लाई जा सकती है।

अब हम कुछ ऐसी सस्थाओं के बारे में जानकारी प्राप्त करेंगे जो विदेशों में अनुसंधान हेतु अनुसंधान अधिकारी के लिए मध्यस्थ का कार्य सम्पादित करती है। जो निम्न प्रकार से हैः–

इंटरपोल–

अंतर्राष्ट्रीय आपराधिक पुलिस संगठन (आईसीपीओ) इसका पूरा नाम है। इसमें कुल 194 सदस्य देश है। जिसका मुख्यालय –लिओंस, फ्रांस में स्थित है। इसके छह महत्वपूर्ण अंग हैं। जो निम्न प्रकार से हैः–

1. सामान्य सभा
2. कार्यकारी समिति
3. प्रधान सचिवालय
4. सलाहकार
5. इंटरपोल की फाइलों के नियंत्रण के लिए आयोग (सीसीएफ) और
6. राष्ट्रीय केंद्रीय ब्यूरो

इंटरपोल–इंडिया–

यह सीबीआई का हिस्सा है और 1966 में स्थापित, इंटरपोल दिल्ली भारत और विदेशों में कानून प्रवर्तन एजेंसियों के बीच इंटरफेस है अर्थात जब भी विदेश से संबंधित अनुसंधान व इंटरपोल से संबंधित सूचनाओ का आदान प्रदान करना हो या प्रक्रिया अपनाई जानी हो तो इन सब में भारत द्वारा केन्द्रीय अन्वेषण ब्यूरो, नई दिल्ली को नोडल बनाया गया है। सीबीआई द्वारा इंटरपोल की नोडल एजेंसी के रूप में निम्नलिखित कार्य सम्पादित किए जाते है–

- प्रत्यर्पण मामला।
- विदेश में जांच।
- भारत में विदेशी पत्र अनुरोध का निष्पादन।
- विभिन्न इंटरपोल नोटिस जारी करना।
- द्विपक्षीय बहुपक्षीय वार्ता।
- मदद के लिए लगातार एफआरआरओ (विदेशी क्षेत्रीय पंजीकरण अधिकारी), इमिग्रेशन चेक पोस्ट और राज्य पुलिस कानून प्रवर्तन एजेंसियों से सम्पर्क करते हैं।
- नई दिल्ली में दूतावासों, मिशनों के साथ लगातार सम्पर्क विदेश में भारतीय मिशन।

राष्ट्रीय केन्द्रीय ब्यूरो (एनसीबी)–

इंटरपोल का सभी देशों में अपना एक राष्ट्रीय केन्द्रीय ब्यूरो है जो इंटरपोल और देश के कानून प्रवर्तन एजेंसियों के साथ मिल कर मध्यस्थ का कार्य करना है। भारत में इंटरपोल की इस संस्था का नाम NCB India है जिसके लिए केन्द्रीय अन्वेषण ब्यूरो के अधीन अंतर्राष्ट्रीय पुलिस सहयोग इकाई (आईपीसीयू) को इस एजेंसी के तौर पर कार्य करने हेतु नामित किया हुआ है। सीबीआई के निदेशक इसके पदेन प्रमुख है। जो कार्य इंटरपोल के अधीन आईसीपीओ–इंटरपोल के द्वारा सम्पादित किए जाते है वह कार्य भारत में सीबीआई के अधीन अंतर्राष्ट्रीय पुलिस सहयोग इकाई (आईपीसीयू) द्वारा सम्पादित किए जाते है। इस प्रकार अंतर्राष्ट्रीय पुलिस सहयोग इकाई (आईपीसीयू) को NCB India के लिए नामित किया हुआ है। हालाँकि, NCB India से संबंधित सभी मामलों को गृह मंत्रालय, भारत सरकार द्वारा निपटाया जाता है। राज्यों के स्तर पर भी राज्य/संघ राज्य क्षेत्रों के इंटरपोल संपर्क अधिकारी (आईएलओ) बनाये हुए है। जो संघ और राज्यों के लिए इंटरपोल के सम्पक्र अधिकारी है। राजस्थान में इस हेतु सीआईडी सीबी को इसकी नोडल एजेंसी बनाया हुआ है। वर्तमान में DIGP, Crime Branch, Room No 334, Police HQ, Jaipur, Rajasthan इंटरपोल संपर्क अधिकारी (आईएलओ) और Superintendent of Police, Crime Branch, Jaipur, Rajasthan सहायक इंटरपोल संपर्क अधिकारी (आईएलओ) हैं।

हम इंटरपोल के माध्यम से अनौपचारिक सूचना प्राप्त करते है– आपराधिक मामलों की जांच में औपचारिक जानकारी एकत्र करने के लिए इंटरपोल के चैनल का उपयोग किया जा सकता है। अन्य देशों के एनसीबी के साथ अनौपचारिक पूछताछ करने के लिए एनसीबी–भारत के माध्यम से अनुरोधों को रूट करना। इंटरपोल भारत में अपने एनसीबी–भारत के माध्यम से निम्नलिखित सूचना प्राप्त करता हैः––

- गवाह–अभियुक्त के स्थान का पता लगाना
- किसी विशेष पते पर कुछ कंपनी की उपलब्धता का सत्यापन
- एक निश्चित बैंक में किसी विशेष व्यक्ति के नाम पर एक बैंक खाते की उपलब्धता का पता लगाना
- साक्ष्य देने के लिए किसी व्यक्ति की इच्छा
- पासपोर्ट विवरण का सत्यापन
- किसी निश्चित इकाई/व्यक्ति के नाम पर संपत्ति की उपलब्धता का सत्यापन
- साइबर/डिजिटल डेटा के संरक्षण के लिए अनुरोध
- दोहरी आपराधिकता का निर्धारण करने के लिए अनुरूप कानून

इंटरपोल चैनलों के माध्यम से अनौपचारिक जांच कराने के लिए आवश्यक विवरण के साथ एक अनुरोध निम्न पते पर भेजा जा सकता है–

सहायक निदेशक (एनसीबी),
सीबीआई मुख्यालय, 5–बी, छठी मंजिल, सीबीओ कॉम्प्लेक्स
लोधी रोड, नई दिल्ली – 110003.

यूके (एनसीए), यूएसए (एफबीआई), कनाडा (आरसीएमपी), फ्रांस, जर्मनी (बीकेए) और ऑस्ट्रेलिया (एएफपी) जैसे कई देशों ने भारत में अपने राजनयिक मिशनों में अपने एलईए/कानूनी प्रदाता स्थित किए हैं। उक्त सूचना के लिए इन पुलिस सम्पर्क अधिकारियों (पीएलओ) की सेवाएं IS-II/MHA □□ IPCU/CBI के माध्यम से प्राप्त की जा सकती हैं।

LRs/MLAT के माध्यम से विदेशों से साक्ष्यों का संग्रहण की प्रक्रिया व अंतर

इंटरपोल से जो हमें सूचना प्राप्त होती है वह अनौपचारिक रूप से होती है जिसका उपयोग न्यायालय में साक्ष्य के रूप में नहीं किया जा सकता है। वे जानकारी केवल पुलिस जॉच के लिए ही होती है न कि अदालतो के उपयोग के लिए होती है। इसलिए, औपचारिक मार्ग के माध्यम से पारस्परिक कानूनी अनुरोध/अनुरोध पत्र भेजकर अभियोजन उद्देश्यों के लिए स्वीकार्य साक्ष्य प्राप्त किया जा सकता है। गृह मंत्रालय (एमएचए), सरकार का आईएस–द्वितीय प्रभाग को भारत की पारस्परिक कानूनी सहायता के लिए केंद्रीय प्राधिकरण बनाया हुआ है। इसलिए अनुसंधान अधिकारी को यदि औपचारिक रूप से न्यायालय में प्रस्तुत करने के लिए साक्ष्य के रूप में सूचना प्राप्त करनी है तो उसे या तो एमएलईटी (पारस्परिक कानूनी सहायता संधि) या एलओआर (अनुरोध पत्र) के माध्यम से ही सूचना प्राप्त करनी होती है।

ये विदेशों में न्यायिक उद्देश्यक से सूचना प्राप्त करने के दो प्रकार है। आगे बढने से पहले हम इन दोनो के मध्य अंतर को समझेंगे।

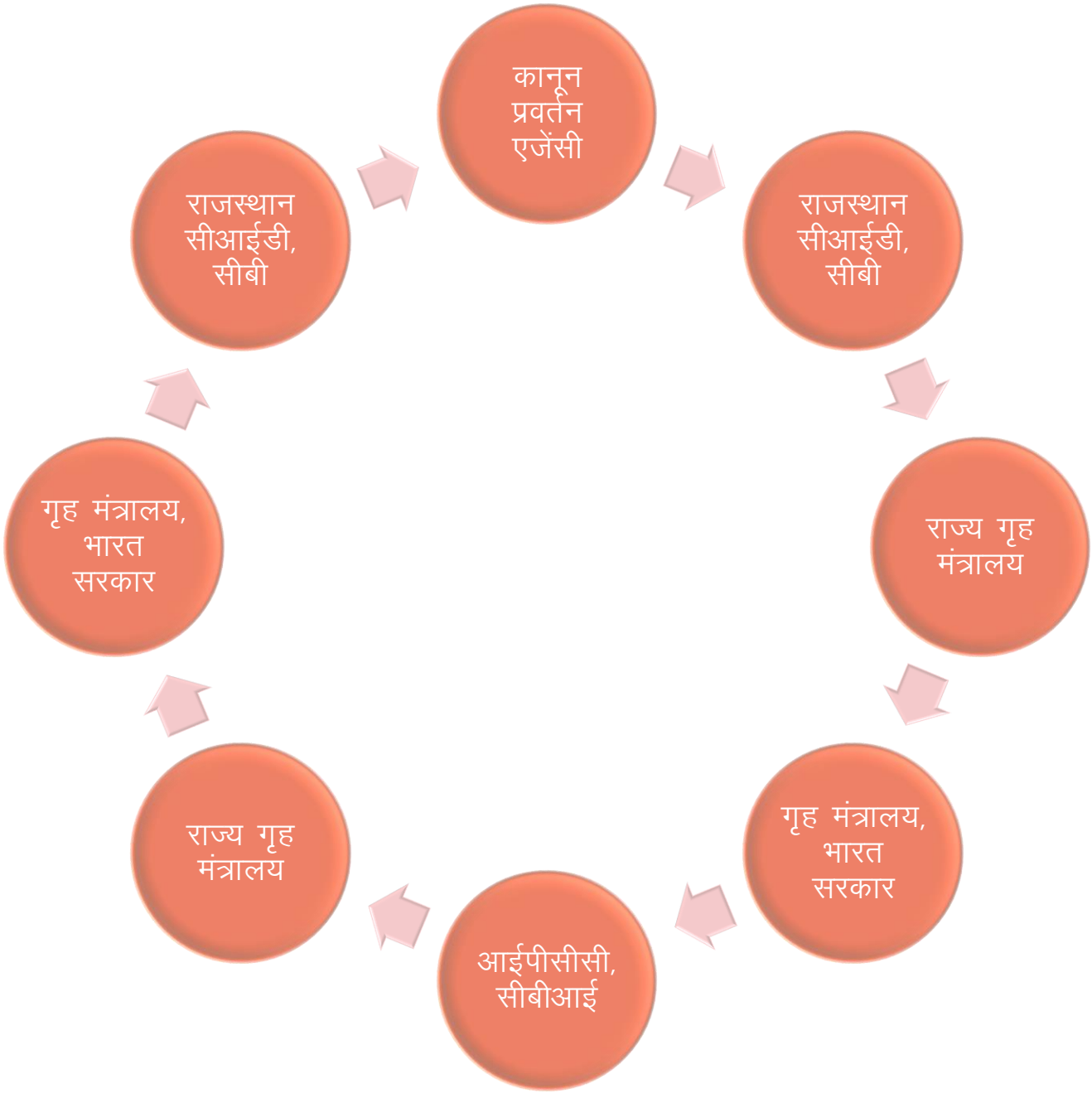
क्र स.	विषय	एलआर (अनुरोध पत्र)	पारस्परिक कानूनी सहायता अनुरोध (एमएलएटी)
1.	प्रकृति	भारतीय दण्ड प्रक्रिया संहिता की धारा 166ए के तहत् अनुसंधान अधिकारी या अनुसंधान एजेंसी के प्रार्थना पत्र पर न्यायालय द्वारा जारी किया जाता है।	यह अनुरोध पत्र अनुसंधान अधिकारी या अनुसंधान एजेंसी के प्रार्थना करने पर भारत की केंद्रीय एजेंसी द्वारा देश जिससे सूचना प्राप्त करनी है की केन्द्रीय एजेंसी को भेजी जाती है।
2.	क्षेत्र	यह किसी भी देश को भेजी जा सकती है। यदि दोनो देशों के मध्य आपसी विश्वास है।	यह केवल उन्ही देशों को भेजी जा सकती है जिनसे भारत सरकार ने द्विपक्षीय/बहुपक्षीय संधि या समझौता कर रखा हो या अन्तर्राष्ट्रीय सम्मेलन कर रखा हो

एमएलएटी भारतीय दण्ड प्रक्रिया संहिता की धारा 105(1)(ii) के तहत् जारी की गई है। जो निम्न प्रकार से है:–

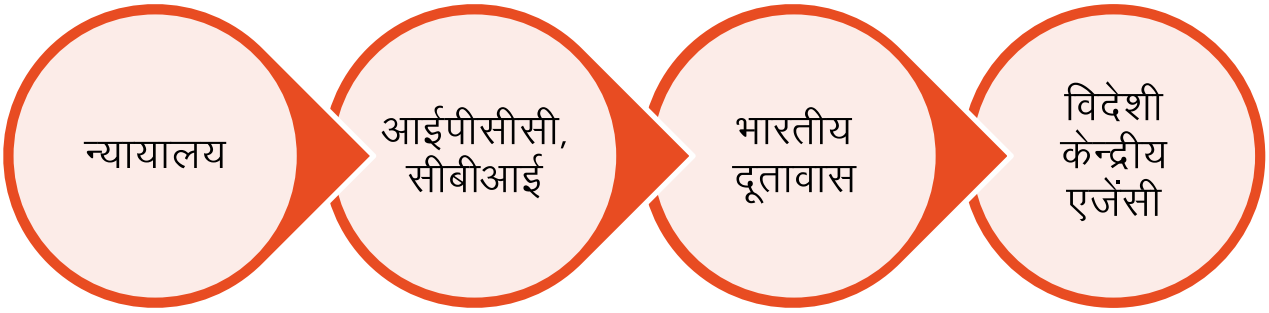
भारत के बाहर किसी ऐसे देश या स्थान में है, जिसकी बाबत केंद्रीय सरकार द्वारा, दांडिक मामलों के संबंध में समन या वारंट की तामील या निष्पादन के लिए ऐसे देश या स्थान की सरकार के (जिसे इस धारा में इसके पश्चात् संविदाकारी राज्य कहा गया है। साथ व्यवस्था की गई है, वहां वह ऐसे न्यायालय, न्यायाधीश या मजिस्ट्रेट को निर्दिष्ट ऐसे समन या वारंट को, दो प्रतियों में, ऐसे प्ररूप में और पारेषण के लिए ऐसे प्राधिकारी को भेजेगा, जो केंद्रीय सरकार, अधिसूचना द्वारा, इस निमित्त विनिर्दिष्ट करे।

अनुरोध पत्र की कार्यवाही भारतीय दण्ड प्रक्रिया संहिता की धारा 166A व 166B के तहत न्यायालय के माध्यम से जारी की जाती है। जिसके बारे में हम पूर्व में अध्ययन कर चुके है।

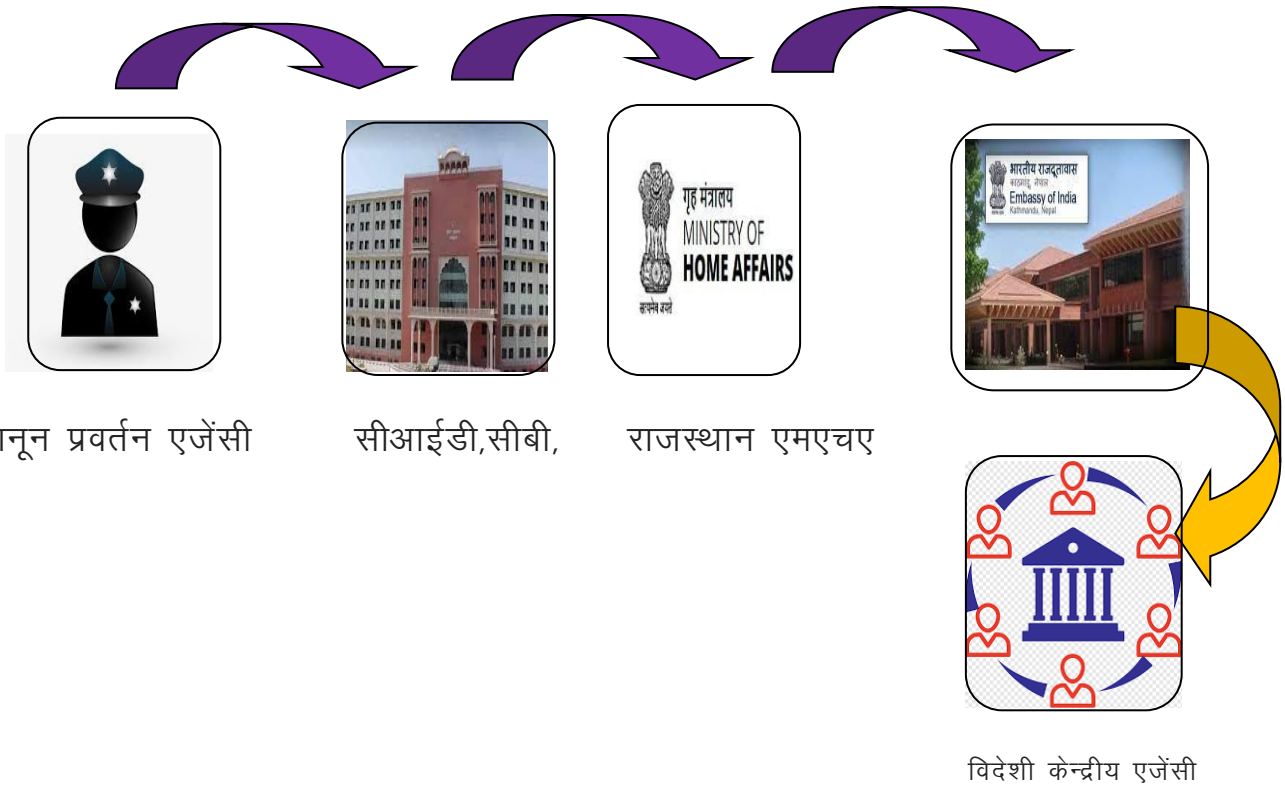
अनुरोध पत्र एलआर को जारी कराने की प्रक्रिया



प्रारूप के अप्रुवल के बाद



LAT आधारित प्रार्थना पत्र की प्रक्रिया–



कानून प्रवर्तन एजेंसी सीआईडी,सीबी, राजस्थान एमएचए

विदेशी केन्द्रीय एजेंसी

औपचारिक अनुसन्धान के लिए साक्ष्य एकत्रित करने हेतु, महत्त्वपूर्ण सबूत और दस्तावेज जुटाने हेतु दण्ड प्रक्रिया संहिता 1973 की धारा 166–ए अधिकृत न्यायालय द्वारा

अनुरोध पत्र जारी करने की प्रक्रिया निर्धारित की गई है, यह अनुरोध पत्र आपराधिक मामलों में आपसी कानूनी सहायता संधि (एम एल ए टी) के दायरे में अग्रेषित की जाती है अथवा समझौता ज्ञापन (एम ओ यू) और पारस्परिकता के आधार पर दोनों देशों के बीच मौजूदा मामले में ऐसी कोई समझौता सन्धि या ज्ञापन के आधार पर किया जाता है। कुछ मामलों में यह भी सम्भव हो सकता है कि इस तरह के परस्पर सहयोग के लिए एक अन्तर्राष्ट्रीय कन्वेन्शन (सम्मेलन) के प्रावधानों का प्रयोग कर सकते हैं जहां भारत एवं दूसरी तरफ दूसरा देश जिससे अनुरोध किया जा रहा हो, ऐसे कन्वेन्शन पर हस्ताक्षर करने वाला देश हो।

- जॉच एजेन्सी द्वारा केन्द्रीय (प्राधिकरण) अथोरिटी यानि गृह मंत्रालय द्वारा पूर्व स्वीकृति के बाद ही कोर्ट से अनुरोध पत्र जारी करवाये जाने का निवेदन किया जाना चाहिए।
- किसी सक्षम न्यायालय में अनुरोध पत्र जारी किये जाने का आवेदन प्रस्तुत करने से पहले ऐसे मामलों में जहां अनुरोध पत्र जारी कराया जाना आवश्यक हो वहां स्वतः स्पष्ट प्रस्ताव अपर सचिव (विधि) आन्तरिक सुरक्षा विभाग, गृह मंत्रालय, लोकनायक भवन, नई दिल्ली–110003 को सम्बन्धित राज्य के गृह विभाग द्वारा जहां प्रकरण राज्य पुलिस से सम्बन्धित हो और जहां प्रकरण सीबीआई का हो तो सीधे ही गृह मंत्रालय भारत सरकार के माध्यम से प्रकरण का भेजा जावे।
- गृह मंत्रालय को मामला देने से पहले अन्वेषण एजेन्सी मामले को विस्तार से जान लें कि क्या यह मामला पूरी तरह से अनवेषण योग्य है। एम एल ए टी. समझौता ज्ञापन व्यवस्था या अन्तर्राष्ट्रीय राधि के साथ ही अनुरोध दोहरी अपराधिकता के सिद्धान्त के रूप में देश के कानून की आवश्यकता को प्रावधानों तथा पारस्परिकता का आश्वासन इत्यादि को सुनिश्चित करने के लिए अध्ययन किया जाना चाहिए कि यह अनुरोध उस देश के मापदण्डों के अनुरूप होगा। यह महत्वपूर्ण है कि यह अनुरोध विशेष रूप में की गई संधि समझौता ज्ञापन व्यवस्था या अन्तर्राष्ट्रीय कन्वेशन के अनुरूप है यह अनुरोध पत्र में उल्लेख किया जाना चाहिए। जहाँ ऐसी कोई व्यवस्थायें द्विपक्षीय या बहुपक्षीय आधार पर उपलब्ध नहीं है। वहाँ पारस्परिकता के आश्वासन के आधार पर अनुरोध पत्र तैयार किया जा सकता है।

  गृह मंत्रालय की सहमति प्राप्त करने के लिए सम्बन्धित जाँच एजेन्सी को निम्नलिखित तथ्य तीन प्रतियों में भेजे जाने चाहिए

(1) एक सुस्पष्ट टिप्पणी जो सम्बन्धित मामले के संक्षिप्त तथ्यो तथा आरोप, आरोपियों के नाम व कारित अपराध के विवरण व कानून की धाराओं तथा प्रथम सूचना रिपोर्ट की एक प्रति शामिल हो प्रथम सूचना रिपोर्ट साफ सुथरे तरीके से टाईप (टंकित) की गई हो तथा यदि प्राथमिकी स्थानीय भाषा में हो तो (आंग्ल) अंग्रेजी अनुवाद आवश्यक है।

(2) विदेश में अनुसंधान किये जाने की आवश्यकता के सम्बन्ध में अभियोजन निदेशक या सबसे वरिष्ठ विधि अधिकारी की कानूनी राय जो अनुरोध पत्र की आवश्यकता को सुनिश्चित करे तथा यह भी स्पष्ट हो कि ऐसा अनुरोध एम एल ए टी., समझौता ज्ञापन अन्तर्राष्ट्रीय कानून व संधियों के दायरे में ही होगा अथवा दोहरी अपराधिकता के सिद्धान्तों के तहत होगा।

- गवाहों के बयानों की प्रासंगिकता जाँच करने के लिए।
- दस्तावेजों का संग्रह/सामग्री तथा इन्हें जब्त किया जाना है आदि के सम्बन्ध में भी टिप्पणी की जानी चाहिए।

(3) एमएलएटी या एमओयू या समझौता या सहमति व्यवस्था या अन्तर्राष्ट्रीय संधि जिसके तहत अनुरोध पत्र जारी किया जा रहा है आदि के संगत प्रावधानों को भी सलग्न किया जाना

चाहिए और यदि पारस्परिकता के आश्वासन पर अनुरोध पत्र भेजा जा रहा हो, तो इसका भी उल्लेख किया जायें।

(4) सक्षम न्यायालय में अनुरोध पत्र जारी करवाये जाने हेतु प्रस्तुत किये जाने वाले आवेदन का मसौदा भी सलग्न किया जाना चाहिए और ऐसे आवेदन में निम्न बिन्दु शामिल किये जाने चाहिए।

- प्रकरण के संक्षेप्ति तथ्यों व पृष्ठभूमि पर टिप्पणी आरोप व आरोपित व्यक्तियों के नाम तथा किये गये अपराध का विवरण तथा अपराध सम्बन्धी कानून की धारायें उद्धरित की जाये तथा सुस्पष्ट रूप से टंकित की गई प्रथम सूचना रिपोर्ट संलग्न की जाये।
- जो अनुसंधान दूसरे देश पर किया जाना है उसका पूर्ण विवरण यह ध्यान रखा जाना चाहिए कि अनुरोध सुस्पष्ट हो क्योंकि कोई भी देश सरसरी या अस्पष्ट जाँच या अन्वेषण की इजाजत नहीं देगा।
- जिन गवाहों का परीक्षण किया जाना है उसका विवरण, उनकी पहचान तथा यदि उपलब्ध हो तो उनके पते और प्रत्येक गवाह से पूछे जाने वाले विस्तृत प्रश्नों की प्रश्नावली।
- जो दस्तावेज या सामग्री जिनका संग्रह किया जाना है उनका विवरण व संग्रह की प्रक्रिया जिस देश से अनुरोध किया जा रहा हो उस देश के सब कानूनों की धाराओं का उद्धरण किया जाये जो भारत में जॉच किये जा रहे अपराध/अपराधों के समकक्ष आरोप हो।
- एमएलएटी या एमओयू या अन्तर्राष्ट्रीय संधि या व्यवस्थायें आदि उद्धरित की जाये जो अनुरोध किये जाने वाले देश से सहयोग प्राप्त करने में सहायक हो।
- इस आशय की घोषणा की प्रस्तावित अनुरोध पत्र अनुरोध किये जाने वाले देश की सभी अपेक्षाओं को पूरा करता है तथा अन्वेषण किया जाने वाला मामला राजनीतिक, मिलिट्री (सेना). नस्लीय, धार्मिक प्रकृति का नहीं है।
- ऐसे देश जिससे कोई एमएलएटी या एमओयू या आपसी अन्य व्यवस्था नहीं की गई हो और यह अनुरोध अन्तर्राष्ट्रीय संधि परिपेक्ष में नहीं आता हो वहाँ पारस्परिकता के आधार पर मसौदा संलग्न हो।
- अनुरोध पत्र को कार्यान्वित किये जाने हेतु अनुरोधित देश के अधिकारियों की सहायता के लिए क्या जाँच या अधिकारी की यात्रा प्रस्तावित है?

अनुरोध पत्र तैयार किये जाने के समय जाँच एजेन्सी द्वारा बरती जानी सावधानियाँ

- ☑ दस्तावेज प्रति चित्र (फोटो कॉपी) एवं वस्तु यदि अनुरोध पत्र के साथ संलग्न हो तो इन्हें स्पष्टतया अंकित करें एवं इनका विवरण पत्र में दिया जाये ताकि अनुरोध किये गये प्राधिकारी को यह समझाने में सहायक हो कि इस सामग्री का क्या उपयोग किया जाना है?
- ☑ सभी पत्र एवं दस्तावेजों की सलग्न की जाने वाली फोटो प्रतियाँ पठनीय एवं आवश्यक हो तो सम्बन्धित राष्ट्र भाषा में अनुवादित हो। अनुरोध पत्र सफाई से जिल्द किया जाये व प्रत्येक पृष्ठ पर पृष्ठांक हो। अधिकृत अनुवादित प्रतिया, अनुवादक द्वारा हस्ताक्षरित की जाकर मूल अनुरोध पत्र के साथ संलग्न की जाये और यदि आवश्यक हो तो ऐसी भाषा में भी प्रस्तुत एम एल ए टी एम ओ यु अन्य व्यवस्था आदि में वर्णित की गई हो।
- ☑ अनुरोध पत्र की कम से कम मूल सहित पाँच प्रतियों की जाये। तीन प्रतियाँ अनुवाद सहित (केन्द्रीय अन्वेषण अनुभाग) गृह मंत्रालय को भेजी जाये। साथ ही एक प्रति सी बी आई की
- ☑ अन्तर्राष्ट्रीय पुलिस सहयोग शाखा को भेजी जाये।

☑ गृह मंत्रालय जहाँ आवयश्क हो सी बी आई से परामर्श कर सकता है और प्रस्ताव पर अपनी स्वीकृति सक्षम न्यायालय में अनुरोध पत्र जारी कराये जाने वाले प्रस्ताव अनुज्ञापित करा सकता है । इस अनुशंसा की एक प्रति आई पी सी सी, सी बी आई, नई दिल्ली को भेजी जायेगी।

☑ गृह मंत्रालय की अनुशंसा प्राप्त करने के पश्चात् एक आवेदन सम्बन्धित क्षेत्राधिकार प्राप्त सक्षम न्यायालय में प्रस्तुत किया जायेगा जो सम्बन्धित देश के सक्षम प्राधिकारी को सम्बोधित अनुरोध पत्र जारी कर सके। सक्षम न्यायालय सम्बन्धित देश के सक्षम प्राधिकारी को सम्बोधित पत्र प्रार्थना के

☑ अनुसार जारी कर सकता है अथवा ऐसा करने से इन्कार भी कर सकता है। ऐसी स्थिति में जब आवेदन स्वीकार कर लिया जाये न्यायालय अपनी मुद्राक अधिकारिता अंकित करते हुये अनुरोच पत्र जारी करेगा एक प्रारूप अनुरोध पत्र के कथन इस मार्गदर्शिका के साथ अनुलगनक के रूप में संलग्न है।

सक्षम न्यायालय द्वारा अनुरोध पत्र जारी किये जाने के पश्चात अपनायी जाने वाली प्रक्रिया

(1) जाँच एजेंन्सी अनुरोध पत्र की तीन प्रतियां आई पी सी सी सी बी आई. नई दिल्ली व एक प्रति गृह मंत्रालय को भेजेगी। आई पी सी सी सी बी आई. नई दिल्ली इसे सम्बन्धित देश को भारतीय दूतावास के माध्यम से सक्षम अधिकारी को भेजेगी व इसकी सूचना गृह मंत्रालय को भेजी जायेगी।

(2) सम्बन्धित देश द्वारा स्पष्टीकरण अतिरिक्त सामग्री आदि की माग की जाये तो दूतावास इसे सीधे ही आई पी सी सी सी बी आई. नई दिल्ली को सूचित करेगा। जो इस पर गृह मंत्रालय व विदेश मंत्रालय को आगे सूचित करते हुये आवश्यक कार्यवाही करेगी।

(3) निष्पादन रिपोर्ट साध्य व सहायक सामग्री सहित जो अनुरोधित देश से प्राप्त हुई हो। विदेश स्थित दूतावास द्वारा सीधे ही आई पी सी सी सी सी आई नई दिल्ली को भेजा जायेगा जो इसके पश्चात इसे गृह मंत्रालय व विदेश मंत्रालय को सूचित करते हुये सम्बन्धित जाँच एजेन्सी को सी बी आई द्वारा भेज दिया जायेगा।

वे देश जिनके साथ भारत द्वारा एमएलएटी पर हस्ताक्षर किए हुए हैः–

Sl. No	Name of the Country	Year
1	Australia	2011
2	Azerbaijan	2013
3	Bahrain	2005
4	Bangladesh	2011
5	Belarus	2006
6	Bosnia and Herzegovina	2010
7	Bulgaria	2008
8	Canada	1998
9	Egypt	2009
10	France	2005
11	Hongkong	2009

Sl. No	Name of the Country	Year
12	Iran	2010
13	Indonesia	2011
14	Israel	2015
15	Kazakhstan	2000
16	Kyrgez Republic	2014
17	Kuwait	2007
18	Malaysia	2012
19	Maldives	2019
20	Maritius	2006
21	Mexico	2009
22	Mangolia	2004
23	Myanmar	2010
24	Russia	2000
25	Singapore	2005
26	South Africa	2005
27	South Korea	2005
28	Spain	2007
29	Sri Lanka	2010
30	Switzerland	1989
31	Sultanate of Oman	2015
32	Tajikistan	2003
33	Thailand	2004
34	Turkey	1993
35	Ukrain	2003
36	United Arab Emirates	2000
37	United Kingdom	1995
38	United States of America	2005
39	Uzbekistan	2001
40	Vietnam	2008

नोटः–अधिक व अद्यतन जानकारी के लिए MHA की वेबसाइट का अवलोकन करें।

इंटरपोल द्वारा जारी किए जाने वाले विभिन्न प्रकार के नोटिस

रेड नोटिस– वांछित/भगोड़े/वारंटी के लिए।

यह केवल एक प्रक्रिया है। इसके लिए निम्नलिखित चरणों को पूरा किया जाना चाहिए।

1) जिला पुलिस अधीक्षक में माध्यम से अनुसंधान अधिकारी रेड कॉर्नर नोटिस को प्रोफार्मा में भर कर राज्य के इंटरपोल सम्पक्र अधिकारी को भेजेगा।

2) ILO राज्य मामले की जांच करेगा और NCB को भेजेगा।
3) एनसीबी दिल्ली दस्तावेज की जांच करेगा और औपचारिकताएं पूरी करने के बाद इंटरपोल मुख्यालय को भेजेगा।
4) इंटरपोल मुख्यालय संतोष के बाद सभी देशों को आरसीएन जारी करेगा।
5) सभी एनसीबी – नोटिस की प्रति आव्रजन अधिकारियों को परिचालित करेंगे।
6) यदि आरोपी को गिरफ्तार किया जाता है / तलाशी ली जाती है तो सूचना अनुरोधकर्ता राज्य को भेजी जाएगी।

- येलो नोटिस– लापता व्यक्तियों, अक्सर नाबालिगों का पता लगाने में मदद करने के लिए, या उन लोगों की पहचान करने में मदद करने के लिए जो खुद को पहचानने में असमर्थ हैं।

- ब्लू नोटिस– किसी अपराध के संबंध में किसी व्यक्ति की पहचान, स्थान या गातिविधियों के बारे में अतिरिक्त जानकारी एकत्र करने के लिए।
- ब्लैक नोटिस– अज्ञात शवों के बारे में जानकारी लेने के लिए।
- ग्रीन नोटिस– किसी व्यक्ति की आपराधिक गातिविधियों के बारे में चेतावनी देने के लिए, जहां व्यक्ति को सार्वजनिक सुरक्षा के लिए संभावित खतरा माना जाता है।

- ऑरेंज नोटिस– सार्वजनिक सुरक्षा के लिए एक गंभीर और आसन्न खतरे का प्रतिनिधित्व करने वाली किसी घटना, व्यक्ति, वस्तु या प्रक्रिया की चेतावनी देने के लिए।

- बैंगनी नोटिस– अपराधियों द्वारा उपयोग किए जाने वाले तौर–तरीकों, वस्तुओं, उपकरणों और छिपाने के तरीकों के बारे में जानकारी प्राप्त करना या प्रदान करना।

रेड कॉर्नर नोटिस जारी कराने की आवश्यक शर्तेः–

- फरार लोगों के खिलाफ गैर जमानती वारंट
- भगोड़ा सशस्त्र बलों/राजनीतिक विषय का नहीं होना चाहिए।
- भगोड़े के खिलाफ केस ऐसा होना चाहिए जिसमें प्रत्यर्पण हो।
- रेड कॉर्नर नोटिस की अवधि– 5 वर्ष होगी। लेकिन एनसीबी की सिफारिश से समय सीमा बढ़ाई जा सकती है।

भारतपोल सिल्वर एलर्ट नोटिस–

अंतरराष्ट्रीय पुलिस सहयोग इकाई, सीबीआई के माध्यम से साइबर अपराध संबंधी सहायता प्राप्त करने के लिए हाल में इस नोटिस के प्राफार्मा को जारी किया है

जो साइबर अनुसंधान में तीव्र गाति से सूचना प्राप्त करने के लिए भारत सरकार की एक सुविधा है।

लुकआउट सर्कुलर एलओसीः–

लुकआउट सर्कुलर को डिप्टी डायरेक्टर, ब्यूरो ऑफ इमिग्रेशन ईस्ट ब्लॉक– 8वीं, लेवल– 2, सेक्टर –1, आर के पुरम, नई दिल्ली द्वारा जारी किया जाता है। इसके लिए एक आवेदन में निम्नलिखित विवरण लिखा जाना चाहिए।

☑ संदिग्ध/पीओ का नाम
☑ पिता का नाम
☑ जन्म की तारीख
☑ पासपोर्ट संख्या
☑ वारंट का विवरण और कारणों का विवरण

एनसीबी आगे की पहचान के लिए सभी आरसीएन को सभी इमिग्रेशन चेक पोस्ट पर परिचालित करता है। इसे किसी संदिग्ध व्यक्ति की विस्तृत गातिविधियों की जानकारी के लिए जारी किया जा सकता है।

समय–सीमा– जांच एजेंसी के अनुरोध पर इसे एक वर्ष के लिए बढ़ाया जा सकता है।

इकाई–4
बाहरी डेटा का विश्लेषण

समय क्षेत्र का रूपांतरण

आरोप और आरोपी के मध्य आरोप का संबंध सिद्व करने के लिए बहुत महत्वपूर्ण अवधारणा है। जिसका अनुसंधान अधिकारी को अपने अनुसंधान में बहुत सावधानी से उपयोग करना चाहिए। जैसा की हम जानते है। पृथ्वी अपनी धुरी पर परिक्रमण करती है। जिसके आधार पर पृथ्वी पर रात और दिन की घटना घटित होती है। पृथ्वी की गोलाई और अपने धुरी पर परिक्रमण के कारण सूर्य का ताप पृथ्वी पर सभी स्थानों पर एक साथ नहीं पडता है। जिससे भिन्न भिन्न स्थानों पर सूर्योदय और सूर्यास्त एक साथ नहीं होते है। जिसके कारण समय की गणना के लिए एक स्थान को मानक समय मानते हुए उसके स्थान के आधार पर पृथ्वी के अन्य स्थानों के समय की गणना की गई है। ग्रीनविच एक स्थान है जिसके आधार पर पृथ्वी के अन्य स्थानों की गणना की जाती है। ग्रीनविच के मानक समय को ग्रीनविच माध्य समय जीएमटी अथवा समन्वित वैश्विक समय Coordinated Universal Time UTC कहते है। इसी समय के आधार पर भिन्न देश अपने स्थानीय समय की गणना करते है। जिसे स्थानीय मानक समय कहते है। स्थानीय मानक समय की गणना हम ग्रीनविच माध्य समय जिसे यूटीसी समय भी कहते है के आधार पर की जाती है।

यदि भारत के मानक समय की बात की जाए तो भारत के मानक समय को आईएसटी अर्थात इण्डियन स्टैडड्र टाइम कहते है जो UTC से +05:30 घण्टे अधिक है। जब हमें अपने अनुसंधान में प्राप्त की गई सूचना में यदि समय के बारे में UTC लिखा मिलता है तो इसको हम हमारे IST समय में बदलने के लिए उस समय में 05:30 घण्टे जोडना होंगा। जिससे हमें हमारे भारतीय समय के अनुसार घटना को समझने में आसानी रहे। यदि हमें किसी भी अन्तर्राष्ट्रीय सस्था से जानकारी मॉगनी हो तो हमे आवश्यकता के अनुसार पहले समय को UTC में बदलना होगा और समय के बाद कोष्ठक में UTC अवश्य लिख देना चाहिए। जिस मानक के आधार पर समय को व्यक्त किया गया है उस मानक को कोष्ठक में लिख देना अनिवार्य है। इसको हम एक उदाहरण से समझ सकते है। यदि हमें सोशल

मीडिया वेबसाइट जैसे फेसबुक से कोई सूचना मॉगनी है तो हमें हमारे समय जिसे IST कहते है को पहले UTC में बदलना होगा और गणना किए हुए समय के बाद कोष्ठक में हमें UTC लिख देना चाहिए यदि हम भारतीय समय में सूचना मॉग रहे है तो हमें कोष्ठक में IST लिख देना चाहिए। यहॉ बताने का उद्देश्य यह है कि हम जिस किसी भी आधार पर समय की गणना करके सूचना मॉग रहे है उस समय के मानक के बारे में स्पष्टता रहे कि वह समय किस प्रकार का है। अधिकांशतः अन्तर्राष्ट्रीय संस्थाए हमें जो भी सूचनाए उपलब्ध कराते है वह में UTC होतीं है। यह भी हो सकता है कि कोई अन्तर्राष्ट्रीय संस्था हमें किसी अन्य मानक समय में सूचना उपलब्ध कराएँ जैसे कि PST (Pacific standard Time) या अन्य कोई समय मानक। जो भी समय मानक हो की सूचना के बारे में समय का मानक समय कौनसा है उसके बारे में अवश्य दिया होता है। जिसके बारे में हमें बडी सावधानी से गणना करनी चाहिए। जरा भी गलती हमारे पूरे केस पर विपरीत असर डाल सकती है और पूरा अनुसंधान ही दुषित हो सकता है। उदाहरण के लिए निम्नलिखित परिस्थितियों पर गौर करेः–

1. जैसे भारत में कोई अपराध किसी वेबसाइट के जरिए दिनांक 01.03.2022 को समय 1 एएम पर घटित हुआ। यदि उस घटना के बारे में हमने वेबसाइट को समय मानक की गणना स्पष्ट न बता कर साधारण रूप से ये लिखा जाता है कि दिनांक 01.03.2022 को समय 1 एएम पर घटना हुई जिसके बारे में जानकारी दे। इस संदर्भ में निम्न परिस्थितियॉ हो सकती हैः–

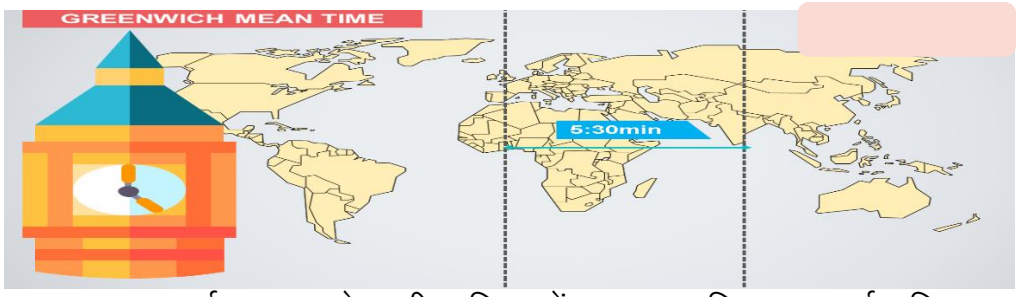
I. हो सकता है कि वह वेबसाइट जानकारी को समझ ही नहीं पाए कि किस समय मानक की सूचना मॉगी गई। इसलिए दे ही नहीं।

II. हो सकता है कि जो सूचना मॉगी गई वह वह चूकि भारतीय मानक समय के अनुसार थी लेकिन वेबसाइट द्वारा UTC के आधार पर सूचना दी जाए।

III. हो सकता है कि जानकारी वह अपने स्थानीय समय के अनुसार दे।

इन सब से स्पष्ट है कि हमे वेबसाइट द्वारा गलत जानकारी दी जाने की प्रबल संभावना है। उस जानकारी के आधार पर यदि हम आगे का अनुसंधान करे तो समय की तो बर्वादी तो होगी ही लेकिन साथ ही गलत व्यक्ति को अपराधी बना दिया जावे। इसलिए यह सब ध्यान में रखा जाना बेहद जरूरी है।

सही सूचना मॉगे जाने के लिए जरूरी था कि दिए गए समय में से 5:30 घण्टे कम करके उसे UTC समय में बदल कर उसे निम्न प्रकार से लिखा जाना चाहिए था। दिनांक 28.02.2022 समय 7:30 पीएम (UTC) लिखा जाना चाहिए। आवश्यक हो तो दिनांक में भी परिवर्तन किया जाना जरूरी होता है। 1 एएम में 5:30 घण्टे कम करने पर 7:30 पीएम होगा लेकिन दिनांक को एक दिवस पीछे करना होगा। चुकि फरवरी, 2022 का अंतिम दिन 28 फरवरी 2022 होता है इसलिए दिनांक 28.02.2022 होगी।



` वर्ल्ड वाइल्ड वेब की दुनिया में कम्प्यूटर सिस्टम/सर्वर विश्व भर में फैले हुए है जो अपने स्थानीय समय के अनुसार सेट किए जाते है। जब उनसे संबंधित सूचना हमारे द्वारा मॉगी जाती है तो वे अपने सिस्टम के स्थानीय समय के अनुसार हमे सूचना उपलब्ध कराते है। इसलिए हम जब भी सूचना प्राप्त हो तो स्पष्ट कर लेना चाहिए कि सूचना किस मानक समय के अनुसार ली गई है और सूचना प्रदाता ने किस मानक समय के अनुसार हमें सूचना प्रदान की है। तभी हम सही अपराधी तक पहुॅच पायेंगे। समय को भारतीय मानक समय आईएसटी को या अन्य इच्छित समय के अनुसार बदलने के लिए कई ऑनलाइन वेबसाइट और एप्लिकेशन उपलब्ध है जिसमें से

- http://www.timeanddate.com/worldclock/meeting.html
- https://www.woridtimebuddy.com है जिनका उपयोग करके हम आसानी से समय की गणना चाहे गए मानक समय के अनुसार कर सकते है।

ईमेल हेडर

ईमेल हेडर किसी ईमेल मेसेज का वह हिस्सा या क्षेत्र होता है जिसमें ईमेल के बारे मे बहुत महत्वपूर्ण जानकारी उपलब्ध होती है। ईमेल हेडर के माध्यम से हम ईमेल को प्राप्त करने वाले, भेजने वाले, दिनांक, समय, ईमेल के मेसेज की मेसेज आईडी, जिन सर्वर से हो कर प्राप्त हुआ है उनके आईपी एड्रेसेज, ईमेल के भेजने से ले कर प्राप्त होने तक का मार्ग अर्थात ईमेल का पथ होता है आदि सम्मिलित होते है।

ईमेल सेवा प्रदान करने के लिए वर्तमान में कई ईमेल सेवा प्रदाता कंपनियॉ है जिसमें जीमेल, याहु मेल, रेडिफ मेल, होटमेल आदि है। सभी ईमेल प्रदाता अपने उपभोक्ता अर्थात क्लाइंट को मेसेज भेजते है तो मेसेज के साथ उस मेसेज का ईमेल हेडर भी भेजते है जिसमें उस मेसेज से संबंधित सभी प्रकार की आवश्यक जानकारी होती है। जिसके आधार पर हम किसी मेल की प्रमाणिकता अर्थात ऑथेंटिसीटी भी जॉच सकते है। आज कल ईमेल के माध्यम से कई प्रकार के साइबर अपराध हो रहे है जिसमें कुछ साइबर अपराध निम्न प्रकार से अंजाम दिए जाते है:–

- ईमेल के अंतर्गत कोई फिसिंग लिंक भेज कर।
- किसी की नकली अर्थात फेक ईमेल आईडी से मेल भेज कर
- ईमेल स्पूफिंग ईमेल बना कर।
- ईमेल बोम्बिग।
- ईमेल के माध्यम से किसी को धमकी भेज कर।

इस प्रकार किसी भी साइबर अपराधी के लिए ईमेल एक महत्वपूर्ण हथियार है जिसके द्वारा वह अपने अपराध को आसानी से अंजाम दे सकता है। इसलिए एक पुलिस अधिकारी होने के नाते हमारे लिए यह जानना जरूरी है कि ईमेल के बारे जाने की यह कैसे काम करता है। इसी क्रम में ईमेल हेडर एक महत्त्वपूर्ण शब्द है। अगर ईमेल हेडर को हम ईमेल की जन्म कुण्डली कहे तो कोई अतिश्योक्ति नहीं होगी।

सबसे पहले हमे यह जानना आवश्यक है कि ईमेल हेडर आखिर होता कहॉ पर है? जीमेल में ईमेल हेडर को जानने के चरण निम्न प्रकार से हैः–

1. अपने ईमेल मेसेज को इनबॉक्स में जा कर खोले।
2. मेसेज के उपरी हिस्से में बायीं ओर स्थित तीन बिन्दुओ पर जा कर क्लिक करे।
3. जो मेनू लिस्ट निकल कर आये उसमें से "Show Original' टैब चुने।
4. जो पेज खुल कर आयेगा वह उस ईमेल का ईमेल हेडर है।

याहुमेल में ईमेल हेडर को जानने के चरण निम्न प्रकार से हैः–

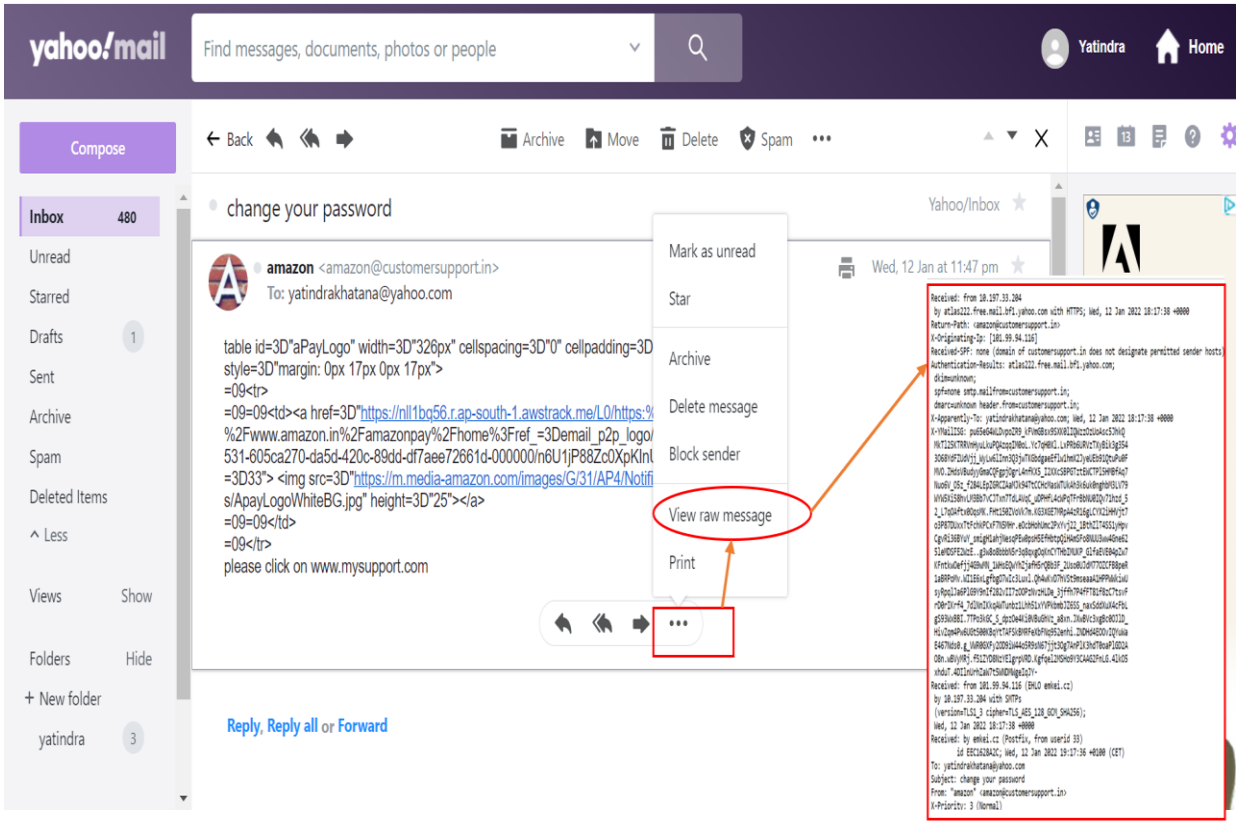
1. अपने ईमेल मेसेज को इनबॉक्स में जा कर खोले।
2. मेसेज के निचले हिस्से में बीच में स्थित तीन बिन्दुओ पर जा कर क्लिक करे।
3. जो मेनू लिस्ट निकल कर आये उसमें से ''View Raw message'' टैब चुने।
4. जो पेज खुल कर आयेगा वह उस ईमेल का ईमेल हेडर है।

होटमेल या आउटलुक में ईमेल हेडर को जानने के चरण निम्न प्रकार से हैः–

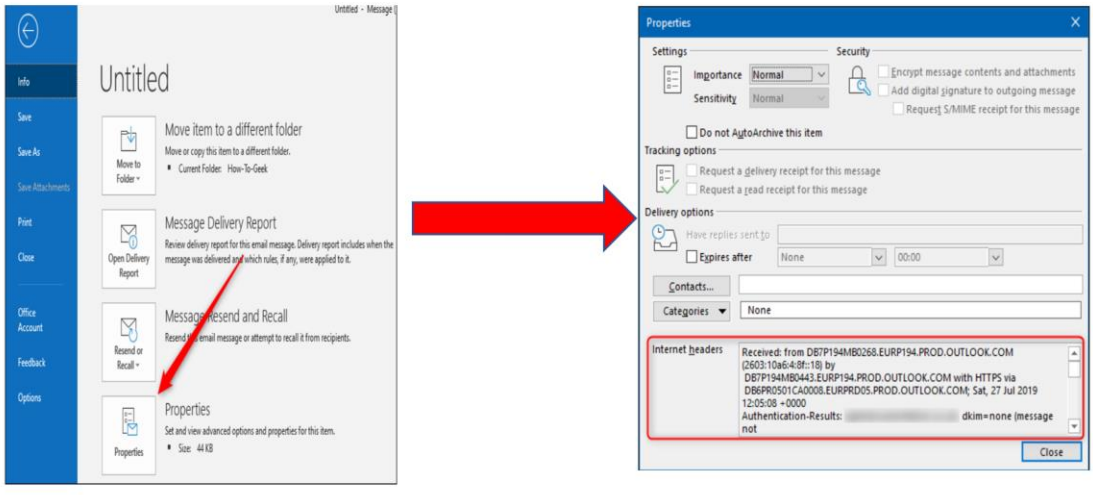
1. अपने ईमेल मेसेज को इनबॉक्स में जा कर खोले।
2. मेसेज में स्थित तीन बिन्दुओ पर जा कर क्लिक करे।
3. जो मेनू लिस्ट निकल कर आये उसमें से ''View message source'' टैब चुने।
4. जो पेज खुल कर आयेगा वह उस ईमेल का ईमेल हेडर है।

याहूमेल में ईमेल हेडर

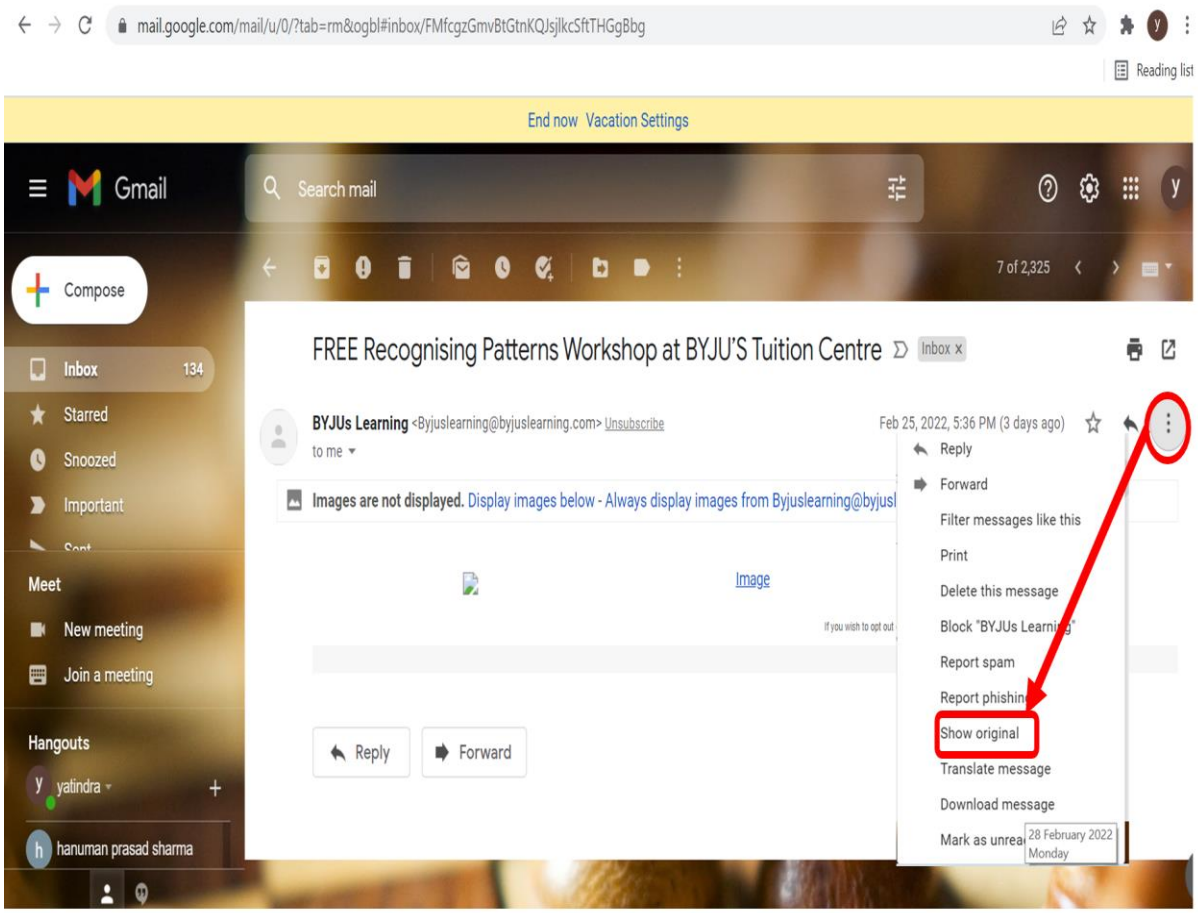
E-mail Header in Yahoo Mail



E-mail Header in Outlook



जीमेल में ईमेल हेडर



जीमेल में ईमेल हेडर का प्रारूप–

```
Delivered-To: yatindra79@gmail.com
Received:    by    2002:a17:522:b835:b0:432:e981:cefb    with    SMTP    id
   bt21csp700006pvb;
        Fri, 25 Feb 2022 04:06:46 -0800 (PST)
X-Google-Smtp-Source:
   ABdhPJxc+jo52/XLd5iTthMq9WH+xetuJVcyhJkEL/z1TM3xgBRZ4pCK3VX6LetOtIyUgVBm
   g/
X-Received:  by  2002:a05:620a:190a:b0:649:1cec:47de  with  SMTP  id  bj10-
   20020a05620a190a00b006491cec47demr4267585qkb.409.1645790806622;
        Fri, 25 Feb 2022 04:06:46 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1645790806; cv=none;
        d=google.com; s=arc-20160816;

   b=oHZf/uAwhBr26EGX/sjyv4JqxHINQ+b1eoPAmuXJN9clNZMQELqmyKL3g91ltBtoX5

   21P4uONW2gyrnE9oZXvVTh2v/NBiFfXR0TI3nUpku1tdE8Anu8iEp8su3pbaGGqu2MvI

   FDDJH31y+/NkAcXnTS9ZGRYjwFth+QOXYnGw5zkrVSTLyYzAHKiNDox9I/VHpNUQToDv

   jAR8YXl5E69pJxaZtGSIØuv5dwRiS7woXMCUSFhcEDgTXQmC4eJoGVa7WZZ7nZ5H3Fe
```

```
        z8rHl0Z4AXh89hP5SLCfbT5SQGwWmnRPxVÝIH/P4aKv/45vyVC8MªlYiYHcOh3KdÝ9
        pPGw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com;
   s=arc-20160816;
        h=to:subject:message-id:mime-version:from:date:dkim-signature
         :dkim-signature;
        bh=XE+lVvb+k/ypdpAULWNf7pGFCiJHFJKm9RLJc2BXpoo=;

   b=vtFajeJx5g/gFIkKYUHKmqsB0SMtK05ATr1MQXEup45CMgyElssqdkja+oHeKF4QwD

   10XXxtqxb7oH9A0S7Snl1LdRkZHKWSZ0T6Abu0Rddnhg9e+A6dcLlwpaqb1apc/ilt1G

   S9weY1u6uD7TNFdg7VS528bburm/c4R3pv8E90syQXabfmtvsiVFJkoD/1+Rcav9Pkeb

   xkrev4DJsv7NLT/3LMQgFHYu5s8dxS1TxOQ1eG0vH3bhnR41TXnfuBiAbdl21ZJgkXIS

   J49XKPe5Nu2KS/FrLYUTV6A641cj2JibpnuMpqRgt3C+IJeO8HdshmDoqyOoHQmx3Idy
        GMhw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass          header.i=@byjuslearning.com          header.s=002
   header.b=AXqxwVu0;
       dkim=pass          header.i=@sendgrid.info          header.s=smtpapi
   header.b="rFNa95/P";
       spf=pass     (google.com:     domain     of     bounces+15862634-d1a1-
   yatindra79=gmail.com@em3067.byjuslearning.com  designates  198.37.145.232
   as      permitted      sender)      smtp.mailfrom="bounces+15862634-d1a1-
   yatindra79=gmail.com@em3067.byjuslearning.com";
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=byjuslearning.com
Return-Path:                                          <bounces+15862634-d1a1-
   yatindra79=gmail.com@em3067.byjuslearning.com>
Received: from o58.email.byjus.com (o58.email.byjus.com. [198.37.145.232])
        by       mx.google.com       with       ESMTPS       id       t11-
   20020a0cef4b000000b0042dd0691ba8si1091513qvs.324.2022.02.25.04.06.46
        for <yatindra79@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Fri, 25 Feb 2022 04:06:46 -0800 (PST)
Received-SPF:   pass   (google.com:   domain   of   bounces+15862634-d1a1-
   yatindra79=gmail.com@em3067.byjuslearning.com  designates  198.37.145.232
   as permitted sender) client-ip=198.37.145.232;
Authentication-Results: mx.google.com;
       dkim=pass          header.i=@byjuslearning.com          header.s=002
   header.b=AXqxwVu0;
       dkim=pass          header.i=@sendgrid.info          header.s=smtpapi
   header.b="rFNa95/P";
       spf=pass     (google.com:     domain     of     bounces+15862634-d1a1-
   yatindra79=gmail.com@em3067.byjuslearning.com  designates  198.37.145.232
   as      permitted      sender)      smtp.mailfrom="bounces+15862634-d1a1-
   yatindra79=gmail.com@em3067.byjuslearning.com";
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=byjuslearning.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=byjuslearning.com;
   h=content-type:from:mime-version:subject:x-feedback-id:to;         s=002;
   bh=XE+lVvb+k/ypdpAULWNf7pGFCiJHFJKm9RLJc2BXpoo=;
   b=AXqxwVu0MvhX+6YnKz9I0CiyH35b+2ÝpVEXuP40AOoEWT4kTbXGqQiRFNK+BDPPy3pL
   EOcvUxctqUjqTEOxFoOhgjDaamPEBJOCnNoIQtzXR5OjgDgb2cA56bZtwVªN5P8GGau3eV
   o4GXVfoMquqsxOedMq9XEFQ5o0tggsHXR1MIRUOAxXYYvKetjj+WKzTp2xyyG5HECL1ZzE
```

```
   weXscNMULBWfIXpmmWVVs5oLE9tEUw2xSNsqoWjWD4/yRK+5Exobi2+5UQAP5wfHHGcnTl
   FQQ6UjWBlCzDw00g3YuBnvmm955AQUF/ik6y9a3hmd/KLxP7ebtIMHPGH2MiU2pg==
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.info;
   h=content-type:from:mime-version:subject:x-feedback-id:to;     s=smtpapi;
   bh=XE+lVvb+k/ypdpAULWNf7pGFCiJHFJKm9RLJc2BXpoo=;
   b=rFNa95/POyK9MBth2ofATrGDX+1pQpOMGsZVªizMueO7eJcNb0tzUSbVMPw4ze9XZZcl
   a2vsDBFWOFB5hlLUrkghh2IEgRKVFT6efolaLXdwNAX5geMKaMªNuytn4oV/JvUW7TKMUQ
   5LA28mBkSP32+/PlfEdFBaYhH6tvNIaxY=
Received: by filterdrecv-696dfd6446-khbvq with SMTP id filterdrecv-
   696dfd6446-khbvq-1-6218C654-72
        2022-02-25 12:06:44.652066035 +0000 UTC m=+15255967.154671145
Received: from MTU4NjI2MªQ (unknown) by geopod-ismtpd-canary-0 (SG) with
   HTTP id wTZOt6N8QUCZOleqSNh2lA Fri, 25 Feb 2022 12:06:44.430 +0000 (UTC)
Content-Type:                                          multipart/alternative;
   boundary=ecccc00a0009ead5fbfc3499f6e99ecc41ecb3af97ac3a06f2cfadbe5ec9
Date: Fri, 25 Feb 2022 12:06:45 +0000 (UTC)
From: BYJUs Learning <Byjuslearning@byjuslearning.com>
Mime-Version: 1.0
Message-ID: <wTZOt6N8QUCZOleqSNh2lA@geopod-ismtpd-canary-0>
Subject: FREE Recognising Patterns Workshop at BYJU'S Tuition Centre
```

नोटः— याहु मेल में ईमेल हेडर का विश्लेषण करने के लिए हमें उपर से नीचे की ओर देखना चाहिए जबकि जीमेल में नीचे से उपर की ओर देखते हुए विश्लेषण करना होगा।
ईमेल हेडर से हमें निम्न प्रकार की जानकारी प्राप्त होती हैः—

1. ईमेल को भेजने वाले की ईमेल आईडी
2. ईमेल के प्राप्त होने व भेजने की दिनांक व समय।
3. ईमेल के भेजने से प्राप्त होने तक का पथ अर्थात् वह ईमेल किन किन सर्वरों से हो कर प्राप्त हुआ है।
4. ईमेल की यूनिक मेसेज आईडी।
5. ईमेल ऑथेंटिक सोर्स अर्थात् वैद्य ईमेल सर्विस प्रदाता से प्राप्त हुआ है अथवा नहीं। इससे ईमेल के साथ स्पूफिंग का पता लगाया जा सकता है।
6. ईमेल के विभिन्न सर्टिफिकेटों जैसे एसएमपी, डीकेआईएम, डीएमएआरसी आदि की जानकारी प्राप्त होती है। जो किसी मेसेज की वैद्यता को सुनिश्चित करती है।
7. विभिन्न प्रकार की आईपी पते जिनसे हो कर मेसेज प्राप्त हुआ है।
8. मेसेज की ट्रेल का पता चलता है।

खोजी उपकरण के रूप में ई—मेल हेडर की सीमाएं

किसी ईमेल के मूल अर्थात ओरिजनल आईपी पते के बारे में सही जानकारी ईमेल हेडर से मिल सके ऐसा हर मामले में संभव नहीं है। जिसके निम्नलिखित कारण हो सकते हैः—

- Google जैसे मेल सेवा प्रदाता के मूल आईपी पते को छिपा देते हैं। इसलिए सरल हेडर विश्लेषण आईओ को ईमेल की उत्पत्ति के संबंध में कोई सुराग नहीं दे सकता है । इन

मामलों में, आईओ को मेल की उत्पत्ति का पता लगाने के लिए मेल सेवा प्रदाता द्वारा दी गई जानकारी भरोसा करना पड़ता है।

- आईपी स्पूफिंग और प्रॉक्सी सर्वर जांच अधिकारी को मेल स्थान के बारे में गलत बता कर गुमराह कर सकते हैं या कुछ मामलों में हेडर विश्लेषण से कोई उपयोगी निष्कर्ष नहीं निकाला जा सकता है।

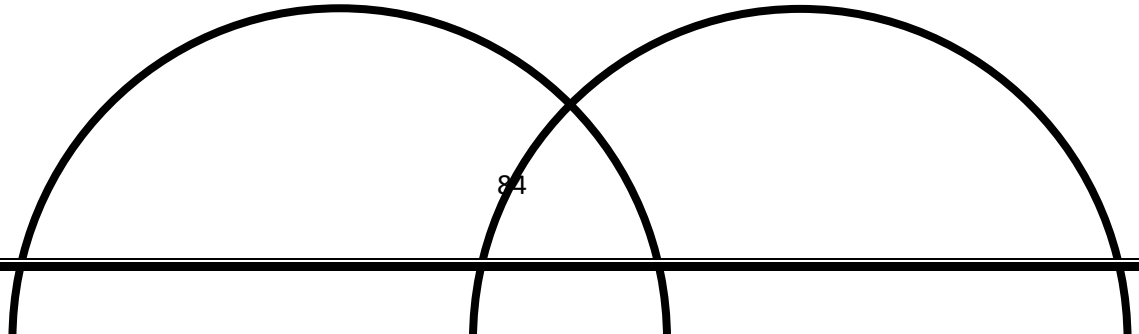
इन कारणों व ऐसी परिस्थितियों में, आईओ को जांच में आगे बढ़ने के लिए विशेषज्ञ की मदद लेनी चाहिए।

स्थान आधारित सेवाएँ (लोकेशन बेस्ड सर्विसेज)

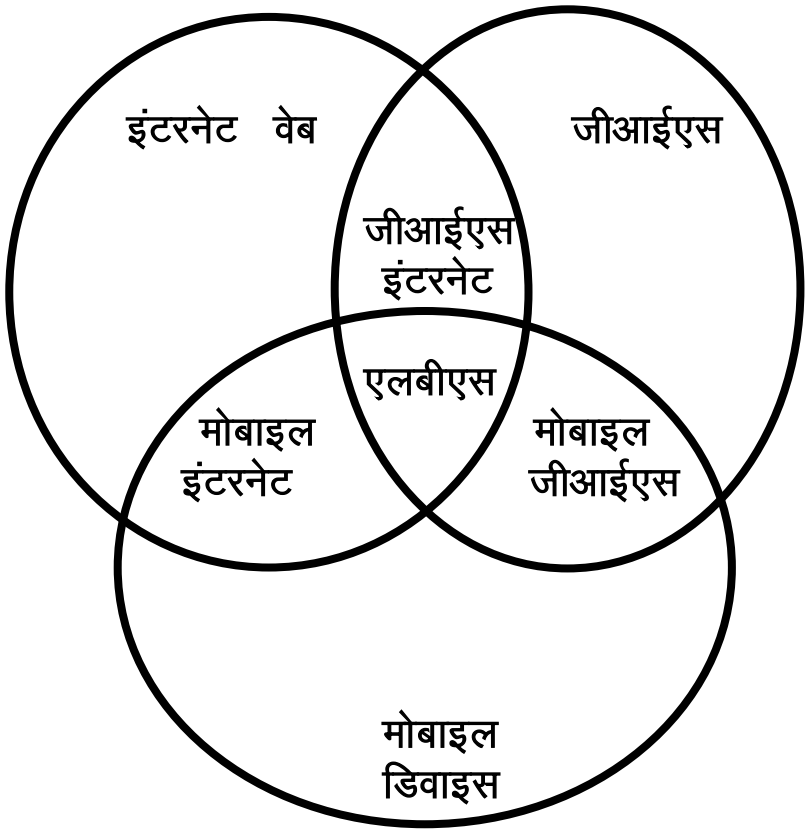
21वीं सदी में स्थान–आधारित सेवाओं (एलबीएस) का उपयोग आधुनिक कम्प्यूटरों और एप्लीकेशन के विकास के कारण व्यापक रूप से हो रहा है। कंप्यूटर सिस्टम और अनुप्रयोग। आधुनिक स्थान आधारित सेवाएं जैसे वल्ड्र वाइड वेब, ग्लोबल पोजिशनिंग सिस्टम और मोबाइल फोन जैसे तकनीकी विकास से संभव हो रहा है। स्थान आधारित सेवाएँ को उपग्रह, नेविगेशन सिस्टम, सेलुलर नेटवर्क और मोबाइल कंप्यूटिंग से प्राप्त डेटा को एकीकृत करके विकसित किया गया है। जब हम स्थान–आधारित सेवा (एलबीएस) की बात करते है तो हम कह सकते कि यह एक सॉफ्टवेयर आधारित सेवा है जो भौगोलिक डेटा का उपयोग करके उपयोगकर्ता को सूचना या सेवा उपलब्ध कराता है। स्थान आधारित सेवाओ का उपयोग विभिन्न क्षेत्रों में किया जा रहा है जैसे कि जैसे स्वास्थ्य, आंतरिक वस्तु खोज, मनोरंजन कार्य, व्यक्तिगत जीवन, नेविगेशन सॉफ्टवेयर, सोशल नेटवक्रिंग आदि। आपने कई बार अपने मोबाइल पर ऐसे मेसेज आते देखे होंगे जब आप बाजार में खरीदारी करने गए होंगे और जो मेसेज आपको प्राप्त हुआ वह आपके द्वारा खरीदे जाने वाले उत्पाद से संबंधित है। या फिर आपने अपने मोबाइल पर कोई डिस्काउंट कूपन देखा होगा जो उसी दुकान के बारे में है जिसके पास आप खडे है। हाल में जो कोरोना महामारी के समय भारत सरकार ने जो एप बना कर लोगों को ट्रेक किया या फिर आपके क्षेत्र में कोरोना महामारी से ग्रसित पीडित के पास में आ जाने पर चेतावनी मेसेज भेजा गया। भारत सरकार द्वारा अपने इमरजेंसी रेस्पोंस सपोर्ट सर्विस के बारे में आपने जरूर सुना होगा। जिसमें एक पेनिक बटन दिया है। जब किसी महिला को अपनी सुरक्षा का खतरा हो तो वह अपने द्वारा रजिस्टड्र कराये गए मोबाइल नंबरों पर इसकी सूचना भेज दी जाती है। साथ ही पुलिस को भी सूचना चली जाती है जिसके आधार पर पुलिस उसे ट्रेक करके सहायता उपलब्ध कराती है।

इस प्रकार आप देख चुके हो कि स्थान आधारित सेवाओं ने हमारे दैनिक जीवन में किस प्रकार से प्रवेश कर लिया है। आगे बढने से पहले हम इसकी तकनीक के बारे में जानकारी करते है।

स्थान आधारित सेवा तकनीक–



स्थान आधारित सेवा तकनीक–



स्थान आधारित सेवा कई तकनीकों का मिश्रण है। मोबाइल में स्थान आधारित सेवा प्राप्त करने के लिए निम्नलिखित अगें की आवश्यकता होती है:–

1. मोबाइल डिवाइस
1. इंटरनेट
2. भौगोलिक सूचना तंत्र का साफ्टवेयर

जब ये उपरोक्ता तीनों एक साथ कार्य करते है तो हमें स्थान आधारित सेवाओं की प्राप्ति होती है। यदि इनमें से एक भी काम नहीं करेगा तो स्थान आधारित सेवा संचालित नहीं होगी। मोबाइल डिवाइस में इंटरनेट की उपलब्धता होने पर और उसका जीपीआरएस सेवा चालू होने पर भौगोलिक सूचना तंत्र साफ्टवेयर प्राप्त हुई सूचना को प्रोसेस करके हमारी आवश्यकता के अनुसार सेवा उपलब्ध कराता है।

स्थान आधारित सेवा का महत्त्व–

मैपिंग, खोज और सूचना प्राप्ति में– आज किसी अज्ञात स्थान पर जाने से पहले हमें किसी से पूछने की आवश्यकता नहीं होती क्योंकि हमारे पास गुगल मैप जैसी सेवा है। इसी सेवा

के कारण पुलिस पीडित और अपराधियों की खोज करने में तथा साक्ष्य एकत्रित करने में इस तकनीक का उपयोग करती है।

2. ट्रेकिंग– किसी वाहन में यदि जीपीएस सिस्टम चालू है तो उसकी लाइव लोकेशन के आधार पर उसके होने के स्थान के बारे में जानकारी की जा सकती है।
3. विज्ञापन– बडी बडी कंपनियॉ अपने उत्पाद को जरूरतमंद ग्राहक को बेचने के लिए तरह तरह का प्रलोभन जैसे डिस्काउंट कूपन, उत्पाद की उपलब्धता, उत्पाद का फोटो देती है ताकि ग्राहक उस उत्पाद को खरिदने के लिए आकर्षित हो। पुरानी धारणा थी कि पुलिस का काम अब अपराध होने के बाद शुरू होता है। लेकिन अब ऐसा नहीं है पुलिस को अपराध होने से पहले उसकी जानकारी प्राप्त करके उसको होने से पहले ही रोकने की अपेक्षा की जाती है। इसलिए पुलिस को आम जनता के प्रति अपनी छवि सुधारना भी जरूरी हो गया है। इन सब के लिए विज्ञापन एक महत्तपूर्ण साधन है। इसलिए पुलिस विज्ञापन के माध्यम में लोगों के मध्य अपराधों के प्रति जागरूकता पैदा करने के लिए, अपनी छवि को संवेदनशील बनाने, कार्य में पारदर्शिता दिखाने के लिए आवश्यक हो गया है कि वह स्थान आधारित सेवाओं का उपयोग करे।
4. खेल– अब कई प्रकार के खेल है जो स्थान आधारित सेवा का उपयोग करके बनाये जाते है। जैसे–पोकेमोन।
5. आपातकालीन सेवा– इमरजेंसी रेस्पोंस सपोर्ट सर्विस की 112 सेवा बहुत महत्तपूर्ण है। जिसमें आपात स्थिति में आवश्यकता होने पर कोई भी महिला पुलिस की मदद पैनिक बटन दबाते ही ले सकती है। जिसकी सूचना तत्काल पुलिस और परिजनों को पहुंच जाती है।

स्थान आधारित सेवाओं के नुकसान–

1. निजता का उल्लंधन– इसके कारण हमारे निजी जीवन में कई प्रकार से बाधाऍ आती है। हम जहॉ भी हो हमें ट्रेक किया जा सकता है। हमारी गातिविधियों पर नजर रखी जा सकती है। अपराधी कई प्रकार से स्थान आधारित सेवा को हमारे मोबाइल में चालू करके हमें ट्रेक कर सकता है। जिसके कारण कई बार अपराधी को अपने अपराध को अंजाम देने में आसानी रहती है।
2. अपराध की तकनीकि जटिलता– कई बार अपराधी अपने अपराध का दायित्व किसी और पर डालने के लिए इस तकनीक का प्रयोग करके पुलिस को गुमराह करने की कौशिश करते है। जैसे अपराध स्थल पर मोबाइल को डालना, अपने मोबाइल को दूसरे स्थान पर छुपा कर अपनी उपस्थिति दूसरे स्थान पर बताने की कौशिश करना आदि।
3. मॅहगी तकनीक– आम नागरिक जो गरीब है उसके लिए इस सेवा का उपयोग करने में उसकी आर्थिक परिस्थिति एक बडा कारण सिद्व होती है। क्योंकि यह तकनीक इंटनेट व मोबाइल आधारित सेवा है जिसके लिए मॅहगे प्लान की आवश्यकता होती है।
4. तकनीक पर अधिक निर्भरता– कई बार देखा गया है कि लोग इस तकनीक पर जरूरत से ज्यादा भरोसा करते है जिसके कारण कई बार सडक दुर्घटना हो जाती है। लुभावने विज्ञापनों के कारण कई बार या तो अनचाहे या गैर–जरूरी या मॅहगे उत्पाद खरीदने के लिए मजबूर हो जाते है।

इकाई–5
कॉल डिटेल रिकोर्ड

कॉल डिटेल रिकोर्ड

मोबाइल पर कॉल करने के लिए निम्न तीन की महत्त्वपूर्ण भूमिका हैः–

- **मोबाइल फोन**
- **मोबाइल सिम**
- **मोबाइल सेवा प्रदाता कंपनी**

जब हम किसी व्यक्ति से उसके मोबाइल पर बात करना चाहते है तो आवश्यक है कि हमारे पास एक मोबाइल फोन हो। उस मोबाइल फोन में एक सिम लगी हुई हो जो या तो उसमें बाहर से ले कर लगाई जावेगी या उस मोबाइल के अंदर ही मोजूद हो जैसे–ई सिम। साथ ही सिम मोबाइल सेवा प्रदाता से जुडी हुई हो।

कॉल डिटेल का कानूनी प्रावधान–

भारतीय टेलीग्राफ अधिनियम (संशोधन) नियम, 2007 के नियम 419 (ए) के साथ पठित भारतीय टेलीग्राफ अधिनियम 1885 की धारा 5(2)के तहत तथा सीआरपीसी 1973 की धारा 91/92 में निहित प्रावधानों के तहत् अनुसंधान अधिकारी द्वारा जिला पुलिस अधीक्षक के माफ़त सीडीआर की मॉग मोबाइल सेवा प्रदाता से कर सकता है।

सीडीआर के प्रकार–

एक जॉच अधिकारी सीआरपीसी की धारा 92 के तहत् पुलिस अधीक्षक के माध्यम से अपराध के परिदृश्य के आधार पर सीडीआर प्राप्त करता है। सीडीआर पीडित या संदिग्ध में से किसी की भी ली जा सकती है। मोबाइल सेवा प्रदाता अपने ग्राहक के कॉल का रिकोर्ड कई आधारों पर संधारित करता है जिसके आधार पर सीडीआर की मॉग अनुसंधान अधिकारी द्वारा की जाती है। सीडीआर निम्न प्रकार की होती हैः–

1. **लक्ष्य मोबाइल नंबर सीडीआरः** लक्ष्य मोबाइल नंबर सीडीआर कॉल प्राप्त करने के लिए कानून प्रवर्तन एजेंसी द्वारा दूरसंचार सेवा प्रदाता से किसी विशिष्ट नंबर की कॉल डिटेल मॉगी जाती है। यह जानकारी व्यक्ति आधारित अपराधों के लिए मददगार हो सकती है।
2. टॉवर सीडीआरः टॉवर सीडीआर कानून प्रवर्तन एजेंसी द्वारा प्रदान की गई टावर सेल आईडी पर आधारित है। टावर सीडीआर में कई टारगेट नंबर और आईएमईआई हो सकते हैं। यह स्थान–आधारित अपराधों के लिए सुराग प्रदान कर सकता है।
3. IMEI CDR: IMEI CDR कानून प्रवर्तन एजेंसी द्वारा प्रदान किए गए एकल हैंडसेट पर आधारित है। यह आपको पीड़ित या संदिग्ध के इस्तेमाल किए गए उपकरण की पहचान करने में मदद कर सकता है।
4. इंटरनेशनल गेटवे सीडीआरः इंटरनेशनल गेटवे सीडीआर उस गेटवे के माध्यम से सभी अंतर्राष्ट्रीय कॉलों का विवरण प्रदान करता है।

5. आईपी एड्रेस सीडीआर–' आईपी एड्रेस सीडीआर सिंगल आईपी एड्रेस या सिंगल टारगेट नंबर पर आधारित होता है। यह जानकारी प्रदान करता है कि अपराध करने के लिए किस आईपी का उपयोग किया गया था।
6. जीपीआरएस सीडीआरः जीपीआरएस सीडीआर उस गेटवे या सेवा प्रदाता के माध्यम से संख्या से संबंधित नेटवर्क यातायात पर आधारित है। इसलिए, यदि कोई बैंडविड्थ चोरी–आधारित अपराध है, तो आप सीडीआर से सुराग ले सकते हैं।

प्रश्नः सीडीआर मांग प्रक्रिया बताइये।

संबंधित अधिकारियों को सीडीआर के लिए अनुरोध भेजने से पहले, यहां कुछ कदम दिए गए हैं जिन पर आपको विचार करने की आवश्यकता हैः

1. आवश्यक सीडीआर का प्रकार तय करें।
2. समयावधि सावधानी से तय करें।
3. मोबाइल नंबर की कंपनी और सक्रल चेक करें।
4. www.dot.gov.in देखें (नवीनतम मोबाइल कोड के लिए)
5. एमएनपी विवरण की जांच करें – नंबर की पोर्टिंग जानकारी।
6. सीडीआर के लिए मेल भेजने के लिए मोबाइल कंपनियों की पहचान करने के लिए इंट्रा–सक्रल रोमिंग समझौतों की जांच करें।

प्रश्नः जांच के लिए सीडीआर कॉलम क्या क्या है? उनके बारे में वर्णन करते हुए समझाइये।

सीडीआर में महत्वपूर्ण विवरण में शामिल हैं कॉलिंग नंबर या मोबाइल नंबर जिससे कॉल किया गया था या दूसरे व्यक्ति को भेजा गया एसएमएस, यहां कॉलिंग पार्टी के रूप में माना जाता है। जांच के लिए कुछ प्रमुख सीडीआर कॉलम नीचे दिए गए हैंः–

1 **कॉलिंग पाटी**– आमतौर पर जिस टेलीकॉम नंबर के लिए सीडीआर हासिल किया जाता है वह एक संदिग्ध आरोपी या लापता व्यक्ति का होता है । कॉलिंग पार्टी या कॉल/एसएमएस की उत्पत्ति के रूप में माना जाता है। जिस नंबर के द्वारा कॉल की गई है अर्थात वह नंबर जिसके द्वारा आउटगोइंग कॉल की गई है। मोबाइल स्टेशन इंटरनेशनल इंटीग्रेटेड सर्विसेज डिजिटल नेटवर्क (MSIDN) की सीडीआर में यदि MSIDN द्वारा कॉल किया जायेगा तो सीडीआर के प्रथम कॉलम में आयेगा। यदि पर कोई कॉल बाहर से आता है तो जो MSIDN नंबर होगा वह अगले अर्थात् सीडीआर के दूसरे कॉलम में होगा। MSIDN में दस अंक शामिल हैं जैसे 919440012345

जहां पहले दो कोड 2 अंकीय देश कोड का प्रतिनिधित्व करते हैं, अगले 5 राष्ट्रीय गंतव्य कोड जबकि अंतिम 5 अंक ग्राहक संख्या का प्रतिनिधित्व करते हैं।

कॉल्ड पार्टी	वह व्यक्ति जिसे कोलिंग पार्टी या कॉलिंग नंबर द्वारा कॉल किया गया था।
दिनांक	कॉल की तारीख
समय	कॉल का समय
समयांतराल	कुल कॉल अवधि

2 **ग्राहक आवेदन पत्र (सीएएफ)**

सीआरपीसी अनुभागों के तहत सीएएफ का अनुरोध करके संदिग्ध की संख्या से संबंधित विवरण प्राप्त कर सकते हैं। एक सीएएफ की सामग्री में शामिल हैं

- ✓ सब्सक्राइबर का फोटो,
- ✓ सब्सक्राइबर का नाम,
- ✓ पिता का नाम,
- ✓ पता,
- ✓ वैकल्पिक फोन नंबर,
- ✓ ईमेल आईडी,
- ✓ आईएमएसआई नंबर,
- ✓ जारी करने की तिथि,
- ✓ बिक्री एजेंट का नाम और पता,
- ✓ आईडी प्रूफ,
- ✓ कनेक्शन का प्रकार

3 लक्ष्य संख्या की पहचान

आप सीडीआर के दूसरे कॉलम में लक्ष्य संख्या और सम्पर्क नंबर पा सकते हैं। आम तौर पर वे संख्याएँ होती हैं जिन्हें पार्टी कहा जाता है। टाइमस्टेम्प या सहयोगी
उपकरणों को लागू करने के बाद कालिंग और कॉल किए गए पक्ष के संबंध का विश्लेषण करके आप उनके बीच एक लिंक स्थापित करने में सक्षम होंगे। लिंक निम्न में से कोई भी हो सकता है

–संदिग्ध–पीड़ित संबंध
–आरोपी संदिग्ध संबंध
–संदिग्ध–सह– संदिग्ध संबंध
–पीड़ित–सह–पीड़ित संबंध

4 सीडीआर में कॉल दिनांक स्वरूप को समझना

यहां तीसरा कॉलम तारीख और समय कॉलम है जो आपको अपराध की तारीख समय और उससे जुड़े लोगों के बीच संबंध बनाने में मदद करेगा। ये जांच के लिए फिल्टरिंग तकनीक हैं। संबंध स्थापित करने के लिए, एक पक्ष से दूसरे पक्ष में कॉल के प्रवाह की जांच करें। रॉ सीडीआर में दिनांक और समय अलग–अलग स्वरूपों में हो सकता है इसलिए आपको प्रारूप का उपयोग करना चाहिए।

5 सीडीआर में कॉल अवधि को समझनाः

सीडीआर स्प्रेडशीट में चौथा कॉलम कॉल अवधि कॉलम है। यह कॉलम संबंधित नंबरों के साथ कॉल की अवधि को समझने में आपकी सहायता करेगा।

6 सीडीआर में सेल आईडी को समझना

सीडीआर स्प्रेडशीट में पांचवां कॉलम सेल आईडी है जिसे टावर आईडी भी कहा जाता है। यह आपको यह पता लगाने में मदद करेगा कि किस टावर स्थान पर संदिग्ध को कॉल किया गया है या कॉल प्राप्त हुई है। यह एक अद्वितीय संख्या है जिसका उपयोग

स्थान क्षेत्र कोड (एलएसी) के भीतर प्रत्येक बीटीएस या बीटीएस के सेक्टर की पहचान करने के लिए किया जाता है। एलएसी एक सेलुलर रेडियो नेटवर्क के सेवा क्षेत्र को संदर्भित करता है और आमतौर पर इसे स्थान क्षेत्रों में विभाजित किया जाता है। प्रत्येक स्थान क्षेत्र को नेटवर्क के भीतर एक अद्वितीय संख्या दी जाती है। इस कोठ का उपयोग मोबाइल ग्राहक के स्थान के लिए एक अद्वितीय संदर्भ के रूप में किया जाता है और आने वाली कॉल के मामले में ग्राहक का पता जानना आवश्यक है।

7 बीटीएस टॉवर

बीटीएस टावर किसी संदिग्ध या लापता व्यक्ति की लाइव लोकेशन जानने में आपकी मदद कर सकता है। एक सेल टॉवर में तीन सेक्टर होते हैं जहां प्रत्येक सेक्टर 120 डिग्री क्षेत्र को कवर करता है और इसकी एक विशिष्ट आईडी होती है। ये क्षेत्र आपको सेल टॉवर का 360–डिग्री दृश्य प्रदान करने में मदद करते हैं।

8 अजीमुथ मूल्य को समझना

सिंगल दिशाओं या अजीमुथ वेल्यू को समझने से आपको संदिग्ध के लाइव स्थान की पहचान करने में मदद मिलती है। तो, एक सामान्य त्रिकोणीय एंटीना वाले टॉवर में तीन संभावित अजीमुध मान होते हैं जो 0 से 120, 120 से 240 और 240 से 360 डिग्री के अनुरूप होते है। मोबाइल सब्सक्राइबर की विशिष्ट कोणीय दिशा सेल साइट के भीतर या सरल शब्दों में उनके मोबाइल स्थान के भीतर उनके स्थान अनुमान को परिष्कृत करने में मदद करती है।

9 गूगल मानचित्र के माध्यम से स्थान की पहचान

बीटीएस टॉवर द्वारा पहचाने गए निर्देशांक प्रस्तुत किए जाएंगे। इन निर्देशांकों को गूगल मैप्स में दर्ज करके आप संदिग्ध व्यक्ति की लाइव लोकेशन का पता लगा सकते हैं। बेस स्टेशन या सेल आईडी में 4 पैरामीटर होते हैं एमसीसी, एमएनसी, एलएसी और सीआईडी सेल आईडी आपको लाइव लोकेशन या टावर लोकेशन का उपयोग करके मोबाइल डिवाइस का पता लगाने में मदद करेगी।

10 मोबाइल देश कोड की पहचान

मोबाइल कंट्री कोड–एमसीसी का उपयोग वायरलेस टेलीफोन नेटवर्क में उस देश की पहचान करने के लिए किया जाता है जिससे मोबाइल ग्राहक संबंधित है। एमसीसी कोड आपको कॉल के मूल देश को जानने में मदद करता है।

11 मोबाइल नेटवर्क कोड की पहचान–

एमएनसी देश के मोबाइल ऑपरेटर या दूरसंचार सेवा प्रदाता की पहचान करने में मदद करती है। आप सेवा प्रदाता से अपटूडेट सेल आईडी कोड ले सकते हैं।

12 सब्स्क्राईबर के स्थान क्षेत्र कोड की पहचानः

प्रत्येक स्थान क्षेत्र को नेटवर्क के भीतर एक अद्वितीय संख्या दी जाती है। इस कोड का उपयोग मोबाइल ग्राहक के स्थान के लिए एक अद्वितीय संदर्भ के रूप में किया जाता है। आने वाली कॉल के मामले में ग्राहक को संबोधित करने के लिए यह कोड आवश्यक है।

13 सेल फोन दिशा की पहचान

सीआइडी एक अद्वितीय संख्या को संदर्भित करता है जिसका उपयोग एलएसी के भीतर प्रत्येक बीटीएस या बीटीएस के सेक्टर की पहचान करने के लिए किया जाता है। सीआईडी आपको सेल फोन दिशा की पहचान करने में मदद करेगा।

14 सीजीआई की पहचान करना

एक बार जब आपके पास सभी 4 कोड की पहचान हो जाए जो हैं मोबाइल कंट्री कोड, मोबाइल नेटवर्क कोड, लोकेशन एरिया कोड और सैल आइडेंटिफिकेशन, सेल ग्लोबल आइडेंटिटी की पहचान कर सकते हैं। सेल ग्लोबल आइडेंटिटी सेल फोन नेटवर्क में बीटीएस के लिए विश्व स्तर पर विशिष्ट पहचानकर्ता है। अब संदिग्ध के स्थान की पहचान करने के करीब जा रहे हैं।

15 अंतिम टॉवर स्थान की पहचान–

छठा कॉलम सेल आईडी है, जिसे कॉल टर्मिनेटेड टावर आईडी भी कहा जाता है। यह आईडी आपको यह पहचानने में मदद करेगी कि संदिग्ध ने किस टावर तोकेशन पर कॉल को गिराया या समाप्त किया।

16 कॉल प्रकार का वर्णन–

सातवां कॉलम कॉल टाइप है, जो आपको इनकमिंग और आउटगोइंग कॉल और एसएमएस के बारे में जानकारी खोजने में मदद करता है सेवा प्रदाता के आधार पर, कॉल इन कॉल आउट, एसएमएस–इन, एसएमएस आउट कोड बदल जाएगा।

17 अंतर्राष्ट्रीय मोबाइल उपकरण पहचान (आईएमईआई) की पहचान करना

आठवां कॉलम है आईएमईआई आपको यह समझने में मदद करेगा कि लक्षित मोबाइल नंबर को संचालित करते समय संदिग्ध द्वारा कितने मोबाइल हैंडसेट का उपयोग किया गया था। जब आप चोरी हुए उपकरणों की जांच कर रहे हों तो आईएमईआई लुकअप महत्वपूर्ण है।

आईएमईआई एक 15–अंकीय संख्या है। यह आमतौर पर फोन के बैटरी डिब्बे के अंदर छपा हुआ पाया जाता है। इसे डायल पैड पर 'रु06रु दर्ज करके अधिकांश फोन पर ऑन–स्क्रीन भी प्रदर्शित किया जा सकता है।

आईएमईआई नंबर हर हैंडसेट के लिए यूनिक होता है। प्रत्येक आईएमईआई नंबर का अंतिम अंक एक चेक अंक होता है और बीएसएनएल को छोड़कर प्रत्येक सीडीआर इसे के रूप में दिखाएगा। एक सीडीआर से, जांच अधिकारी आईएमईआई नंबर कॉलम से

जांच कर सकता है कि हमारे लक्ष्य ने कितने हैंडसेट का इस्तेमाल किया है। जांच अधिकारी आईएमईआई नंबर से हैंडसेट के मेक और मॉडल की जांच के लिए www.numberingplans.com वेबसाइट का उपयोग कर सकते हैं। जांच अधिकारी हमारे लक्ष्य द्वारा उपयोग किए गए विभिन्न लक्ष्य संख्याओं की जांच करने के लिए आईएमईआई नंबरों का पता लगा सकते हैं। यदि आईएमईआई ट्रेस में कई लक्ष्य संख्याएँ पाई जाती है, तो इन नंबरों के स्थान की जाँच करके, हम चीनी हैंडसेट के उपयोग की संभावना की जाँच कर सकते हैं।

18. अंतर्राष्ट्रीय मोबाइल सब्सक्राइबर पहचान (आईएमएसआई) की पहचान करना

सीडीआर का नौवां कॉलम इंटरनेशनल मोबाइल सब्सक्राइबर आइडेंटिफायर आईएमएसआई है। इससे आपको यह समझने में मदद मिलेगी कि संदिग्ध ने एक ही नंबर पर कितने नए सिम कार्ड का इस्तेमाल किया है। आईएमएस आई लुकअप आपको सिम स्वैपिंग धोखाधड़ी की जांच करने में मदद करेगा। आईएमएसआई एक 14–15 अंकीय संख्या है जो एक मोबाइल ग्राहक की पहचान उसके सिम कार्ड से करती है। यह एक देश कोड, एक नेटवर्क कोड, और मोबाइल नेटवर्क के भीतर प्रत्येक कार्ड की पहचान करने वाले अंकों की एक व्यक्तिगत स्टिंग सहित कई भागों से बना है। प्रत्येक जीएसएम मोबाइल ग्राहक के सिम को प्रदाता द्वारा एक अद्वितीय 15 अंकीय आईएमएसआई दिया जाता है। उदाहरण के लिए यदि इसका आईएमएसआई नंबर 404–15––2800227727

- पहले 3 अंक मोबाइल देश कोड दर्शाते हैं।
- अगले 2 अंक मोबाइल नेटवर्क कोड दशति हैं।
- इसके बाद 10 अंक मोबाइल सब्सक्राइबर पहचान संख्या दर्शाते हैं। यह विभिन्न सिम में भिन्न होता है। इसके आधार पर हम पता लगा सकते है कि हमारे लक्ष्य ने कितने हैंडसेट का इस्तेमाल किया है।

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	Report : MSISDN No.: 8875279365 From Date 01/05/2011 To Date: 17/08/2011 Report Date: Thu Aug 18 17:34:01 IST 2011 Seq Id : Vodraj_20110818_89515														
6	A_Number	B_Number	Date	Time	Duration	FIRST_CELL_	LAST_CELL	Call_Type	IMEI	IMSI	PP_PO_IN	SMS_CEN	FIRST_ROAMING_NETWORK		
7	08875279365	08875279369	01-MAY-2011	19:53:27	542	404602001061	-	OUT	3527 01039	404 0474078	PP	-	-		
8	06596860379941	0887 79365	02-MAY-2011	12:51:09	1	404602001061	-	SMS_INC	3527 01039	404 0474078	PP	919888009	-		
9	08875279369	0887 79365	03-MAY-2011	08:28:25	129	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
10	08875279365	0887 79369	03-MAY-2011	13:43:23	65	404602001016	-	OUT	3527 01039	404 0474078	PP	-	-		
11	09649001608	0887 79365	04-MAY-2011	10:39:56	50	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
12	08875279365	0809 67287	04-MAY-2011	11:48:56	443	404602001016	-	OUT	3527 01039	404 0474078	PP	-	-		
13	0659666799999931	0887 79365	04-MAY-2011	11:58:20	1	404602001016	-	SMS_INC	3527 01039	404 0474078	PP	919888009	-		
14	0659666799999931	0887 79365	04-MAY-2011	11:58:28	1	404602001016	-	SMS_INC	3527 01039	404 0474078	PP	919888009	-		
15	08094567287	0887 79365	04-MAY-2011	12:33:21	561	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
16	08094567287	0887 79365	04-MAY-2011	12:43:02	172	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
17	08094567287	0887 79365	04-MAY-2011	21:56:43	919	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
18	08875279365	0998 00468	05-MAY-2011	09:14:38	2	404602001016	-	OUT	3527 01039	404 0474078	PP	-	-		
19	08094567287	0887 79365	05-MAY-2011	10:44:44	33	404602001036	-	INC	3527 01039	404 0474078	PP	-	-		
20	08875279365	0887 79369	05-MAY-2011	15:18:40	422	404601888821	-	OUT	3527 01039	404 0474078	PP	-	-		
21	09772064211	0887 79365	05-MAY-2011	15:35:57	3	404601888821	-	INC	3527 01039	404 0474078	PP	-	-		
22	08875279369	0887 79365	06-MAY-2011	08:07:15	82	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
23	012320	0887 79365	07-MAY-2011	02:43:35	1	404602001016	-	SMS_INC	3527 01039	404 0474078	PP	919839099	-		
24	012320	0887 79365	07-MAY-2011	02:43:45	1	404602001016	-	SMS_INC	3527 01039	404 0474078	PP	919839099	-		
25	0659666741288226l1	0887 79365	07-MAY-2011	10:01:01	1	404602001016	-	SMS_INC	3527 01039	404 0474078	PP	919828000	-		
26	09828722287	0887 79365	07-MAY-2011	10:13:45	5	404602001016	-	INC	3527 01039	404 0474078	PP	-	-		
27	06596645220860382	0887 79365	07-MAY-2011	14:35:46	1	404602001061	-	SMS_INC	3527 01039	404 0474078	PP	919828000	-		
28	09983000173	0887 79365	07-MAY-2011	18:39:05	3	404604000061	4046040000	INC	3527 01039	404 0474078	PP	-	-		
29	0659666741288226l1	0887 79365	08-MAY-2011	09:20:59	1	404602001016	-	SMS_INC	3527 01039	404 0474078	PP	919828000	-		
30	06596645220860382	0887 79365	08-MAY-2011	15:28:41	1	404601888821	-	SMS_INC	3527 01039	404 0474078	PP	919828000	-		

सीडीआर का प्रारूप

सीडीआर एनालाइसिस साफ्टवेयर

CDAMS & Cell Site Analyser ऐसे साफ्टवेयर है जिनके आधार पर सीडीआर का विश्लेषण किया जा सकता है। इनके द्वारा एक सीडीआर या अनेक सीडीआर का विश्लेषण एक साथ किया जा सकता है। उक्त साफ्वेयर द्वारा मोबाइल सेवा प्रदाता से हमे जो सीडीआर प्राप्त होती है वह एक सारणी के रूप में होती है। जिसमें टावर की सेल आईडी की केवल संख्या होती है। जिससे हमें जानने में परेशानी होती है कि उस सेल आईडी का पता क्या है। सबसे ज्यादा कॉल किस मोबाइल नंबर पर किए है। रात और दिन में मोबाइल धारक की लोकेशन क्या है? मोबाइल धारा रात में कहॉ रूकता है? अपराध स्थल पर उसकी उपस्थिति है या नहीं? विशिष्ट दिनांक व समय के मध्य उसका रूट चार्ट क्या रहा? सुबह और सोते समय प्रथम और अंतिम कॉल किसको करता है? उसके पास किस कंपनी के और कितने मोबाइल हैंडसेट है जो उस सिम पर उपयोग किये गये है? उसकी वर्तमान लोकेशन कहॉ पर है? किस किस मोबाइल को कितनी बार और कितनी अवधि तक कॉल किए गए है? इन सब की जानकारी हमें तुरंत इन सोफवेयर की मदद से हो सकती है।

सेल–साइट विश्लेषण एक फोरेंसिक तकनीक है, जो एक कॉल, एसएमएस संदेश या डाउनलोड प्राप्त या भेजे जाने पर मोबाइल फोन की भौगोलिक स्थिति को स्थापित करने में सक्षम होने के विज्ञान से संबंधित है।

इन सेवाओं का उपयोग आम तौर पर कानून प्रवर्तन एजेंसियों और रक्षा संगठनों द्वारा किया जाता है, यह सुनिश्चित करने के उद्देश्य से कि एक संदिग्ध आपराधिक गातिविधि के समय अपराध स्थल के आसपास के जिले में था या नहीं।

सेल–साइट विश्लेषण से उत्पन्न जानकारी आम तौर पर साक्ष्य उद्देश्यों के लिए उपयोग की जाती है और विशेषज्ञ गवाहों द्वारा अदालतों में समर्थित होती है। इसके द्वारा निम्नलिखित कार्य किए जाते हैः–

- सेल साइट विश्लेषण का करना
- कॉल डेटा रिकॉर्ड (सीडीआर) की जांच और व्याख्या
- स्थानीय सर्वेक्षण
- सेल कवरेज सर्वेक्षण
- मार्ग सर्वेक्षण
- कॉल डेटा विश्लेषण
- भौगोलिक मानचित्रण

व्यापक रिपोर्ट जिसमें सर्वेक्षण, मानचित्रण और कॉल शेड्यूल शामिल हैं

आईपीडीआर

एक आईपीडीआर जिसे इंटरनेट प्रोटोकॉल डेटा रिकॉर्ड के रूप में भी जाना जाता है, एक आईओ को उपयोगकर्ता की इंटरनेट गातिविधियों का पूरा विवरण प्राप्त करने में मदद करता है, जैसे कि विजिट की गई वेबसाइटें, एक्सेस किए गए ऐप्स और उपयोग

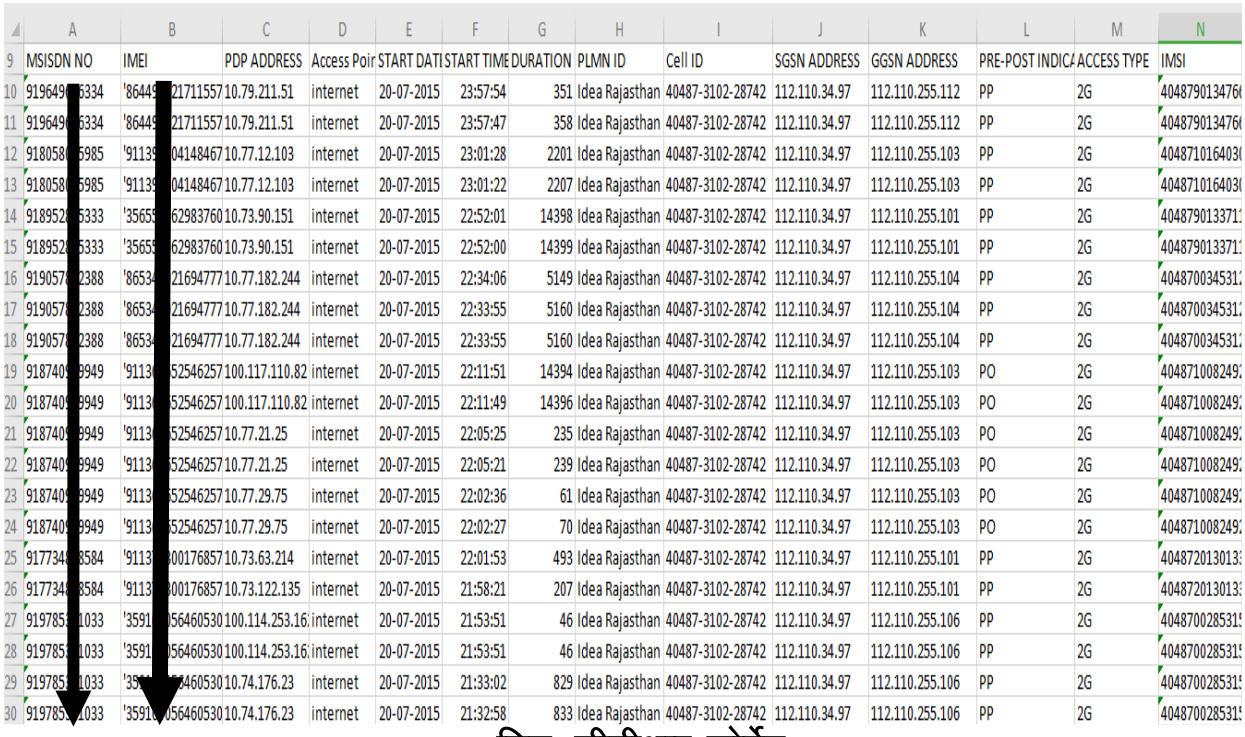
किए गए सोशल मीडिया एप्लिकेशन। जिस प्रकार मोबाइल से साधारण कॉल करने के लिए हमें मोबाइल नंबरों की आवश्यकता होती है। उसी प्रकार जब हम इंटरनेट के माध्यम से कोई डेटा को खोज रहे है या इंटरनेट सेवा का उपभोग कर रहे है तो इंटरनेट सेवा प्रदाता हमें एक गातिशील आईपी पता आबंटित करता है। जो इंटरनेट पर हमारी पहचान होता है। डेटा सत्र की जानकारी को कैप्चर करता है, जो आईपीडीआर में उपलब्ध कराया जाता है।

एक आईपीडीआर को मोटे तौर पर तीन प्रकारों में वर्गीकृत किया जाता है, मोबाइल नंबर आधारित आईपीडीआर, सार्वजनिक आईपी आधारित आईपीडीआर और टावर आईडी या कॉल आईडी आधारित आईपीडीआर।

1. मोबाइल नंबर आधारित आईपीडीआरः मोबाइल नंबर आधारित आईपीडीआर लक्ष्य मोबाइल नंबर से संबंधित इंटरनेट ब्राउजिंग जानकारी प्रदान करता है। आईओ यह जानकारी एक विशेष समय पर इंटरनेट सेवा प्रदाता से कानूनी नोटिस के माध्यम से प्राप्त कर सकता है। यह जानकारी आईओ को चरमपंथियों, आतंकवादियों और अन्य संगठित अपराधियों को ट्रैक करने में मदद करती है। इस प्रकार की आईपी को जीपीआरएस सीडीआर कहते है अर्थात् मोबाइल नंबरों के आधार पर इंटरनेट सेवा प्रदाता से जब उसके द्वारा एक्सेस किए गए इंटरनेट डेटा का रिकोर्ड मॉगा जाता है तो उसे जीपीआरएस सीडीआर कहते है।
2. सार्वजनिक आईपी आधारित आईपीडीआरः जब जांच अधिकारी वेब, ईमेल और ऐप सेवा प्रदाताओं से विभिन्न आईपी लॉग प्राप्त करता है, तो आईओ आईपी पते की पहचान के लिए आईएसपी से सार्वजनिक आईपी आधारित आईपीडीआर के लिए अनुरोध कर सकता है। यह जानकारी प्राप्त करने के लिए, आईओ आईपी पते के लिए दिनांक, समय और अनुरोध का उल्लेख करके आईएसपी को नोटिस देता है। टाइम स्टैंप के साथ आईपी का विश्लेषण करके, आईओ आरोपी के नंबर का पता लगा सकता है। सार्वजनिक आईपी आधारित आईपीडीआर आमतौर पर आईओ को अश्लीलता, मानहानि और अन्य सोशल मीडिया पोस्टिंग से संबंधित आरोपियों को ट्रैक करने में मदद करता है।
1. टॉवर आईडी या सेल आईडी आधारित आईपीडीआरः टॉवर आईडी या सेल आईडी आधारित आईपीडीआर का उपयोग स्थान–आधारित आईपीडीआर करने के लिए किया जाता है, और विशिष्ट स्थान आधारित इंटरनेट ट्रैफिक को ट्रैक करने के लिए आईओ द्वारा उपयोग किया जाता है। इस प्रकार की आईपीडीआर को चौरी, लूट, डकैती, हत्या जैसे अपराधों में गुमनाम अपराधी का पता लगाने के लिए ली जाती है।

क्र सं	विशिष्ट	विवरण
1.	**PRIVATEIP**	मोबाइल डिवाइस का प्राइवेट आईपी पता
2.	**PRIVATEPORT**	मोबाइल डिवाइस का प्राइवेट पोर्ट
3.	**PUBLICIP**	मोबाइल डिवाइस द्वारा प्रस्तुत सार्वजनिक आईपी पता
4.	**PUBLICPORT**	रिकॉर्ड गंतव्य का पोर्ट
5.	**DESTIP**	रिकॉर्ड गंतव्य का आईपी पता
6.	**DESTPORT**	रिकॉर्ड गंतव्य का पोर्ट
7.	**MSISDN**	मोबाइल स्टेशन इंटरनेशनल सब्सक्राइबर

		डायरेक्ट्री नंबर अंतरराष्ट्रीय स्तर पर मोबाइल फोन नंबर की पहचान करने के लिए इस्तेमाल किया जाने वाला नंबर है
8.	**IMSI**	अर्न्तराष्ट्रीय मोबाइल सिम आईडेंटिफिकेशन
9.	**START_DATE, START_TIME**	रिकॉर्ड प्रारंभ तिथि और समय
10.	**End_DATE, End_TIME**	रिकॉर्ड समाप्ति तिथि और समय
11.	**IMEI**	अंतर्राष्ट्रीय मोबाइल उपकरण पहचान संख्या जो विशिष्ट रूप से मोबाइल फोन की पहचान कर सकती है
12.	**CELL_ID**	सेल टॉवर की आईडी
13.	**UPLINK_VOLUME**	अपलोड किए गए डेटा की मात्रा
14.	**DOWNLINK_VOLUME**	डाउनलोड किए गए डेटा की मात्रा
15.	**TOTAL_VOLUME**	डेटा की कुल मात्रा
16.	**I_RATTYPE**	पहचानता है कि यह 2G डेटा है या 3G डेटा



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
9	MSISDN NO	IMEI	PDP ADDRESS	Access Poir	START DATI	START TIME	DURATION	PLMN ID	Cell ID	SGSN ADDRESS	GGSN ADDRESS	PRE-POST INDICA	ACCESS TYPE	IMSI
10	919649 6334	'8644 21711557	10.79.211.51	internet	20-07-2015	23:57:54	351	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.112	PP	2G	4048790134761
11	919649 6334	'8644 21711557	10.79.211.51	internet	20-07-2015	23:57:47	358	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.112	PP	2G	4048790134761
12	918058 5985	'9113 04148467	10.77.12.103	internet	20-07-2015	23:01:28	2201	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PP	2G	4048710164031
13	918058 5985	'9113 04148467	10.77.12.103	internet	20-07-2015	23:01:22	2207	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PP	2G	4048710164031
14	918952 5333	'3565 62983760	10.73.90.151	internet	20-07-2015	22:52:01	14398	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.101	PP	2G	4048790133711
15	918952 5333	'3565 62983760	10.73.90.151	internet	20-07-2015	22:52:00	14399	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.101	PP	2G	4048790133711
16	919057 2388	'8653 21694777	10.77.182.244	internet	20-07-2015	22:34:06	5149	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.104	PP	2G	4048700345317
17	919057 2388	'8653 21694777	10.77.182.244	internet	20-07-2015	22:33:55	5160	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.104	PP	2G	4048700345317
18	919057 2388	'8653 21694777	10.77.182.244	internet	20-07-2015	22:33:55	5160	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.104	PP	2G	4048700345317
19	918740 8949	'9113 52546257	100.117.110.82	internet	20-07-2015	22:11:51	14394	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PO	2G	4048710082497
20	918740 8949	'9113 52546257	100.117.110.82	internet	20-07-2015	22:11:49	14396	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PO	2G	4048710082497
21	918740 8949	'9113 52546257	10.77.21.25	internet	20-07-2015	22:05:25	235	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PO	2G	4048710082497
22	918740 8949	'9113 52546257	10.77.21.25	internet	20-07-2015	22:05:21	239	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PO	2G	4048710082497
23	918740 8949	'9113 52546257	10.77.29.75	internet	20-07-2015	22:02:36	61	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PO	2G	4048710082497
24	918740 8949	'9113 52546257	10.77.29.75	internet	20-07-2015	22:02:27	70	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.103	PO	2G	4048710082497
25	917734 8584	'9113 00176857	10.73.63.214	internet	20-07-2015	22:01:53	493	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.101	PP	2G	4048720130133
26	917734 8584	'9113 00176857	10.73.122.135	internet	20-07-2015	21:58:21	207	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.101	PP	2G	4048720130133
27	919785 1033	'3591 56460530	100.114.253.16	internet	20-07-2015	21:53:51	46	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.106	PP	2G	4048700285315
28	919785 1033	'3591 56460530	100.114.253.16	internet	20-07-2015	21:53:51	46	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.106	PP	2G	4048700285315
29	919785 1033	'359 56460530	10.74.176.23	internet	20-07-2015	21:33:02	829	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.106	PP	2G	4048700285315
30	919785 1033	'3591 56460530	10.74.176.23	internet	20-07-2015	21:32:58	833	Idea Rajasthan	40487-3102-28742	112.110.34.97	112.110.255.106	PP	2G	4048700285315

चित्रः सीडीआर फोर्मेट

टावर डम्प रिकोर्ड (TDR)

एक सेल टॉवर डंप आमतौर पर स्थान के आधार पर डेटा का संग्रह करता है। जब कोई मोबाइल या इंटरनेट उपकरण संचार स्थापित करता है तो उसका सबसे पहले किसी पास के मोबाइल टॉवर से जुडना आवश्यक होता है। प्रत्येक मोबाइल टावर की एक विशिष्ट पहचान होती है जो उसे पूरे विश्व में अद्वितीय बनाती है, उसे उस मोबाइल टॉवर की सेल आईडी कहते है। प्रत्येक मोबाइल टॉवर हर समय कई मोबाइल से जुडा रहता है। जिसके कारण वह एक ही दिनांक व समय पर कई मोबाइल नंबरों को एक साथ जोडे रखता है और उन मोबाइल नंबरों के बारे में समस्त जानकारी भी अपने पास रखता है। इसका उपयोग विभिन्न प्रकार के अपराधों में किया जाता है। जैसे की चौरी, लूट, डकैती या अन्य कोई ऐसा गम्भीर अपराध जिसके बारे में अपराधी के बारे में कोई सुराख हमारे पास नहीं होता है या फिर किसी प्रकार के विरोध प्रदर्शन में भाग लेने वाले लोगों की निगरानी करने के लिए। यह इस मान्यता पर आधारित है कि वर्तमान युग में प्रत्येक व्यक्ति मोबाइल का उपयोग अवश्य करता है। चाहे वह कॉलिंग के रूप में हो या इंटरनेट एक्सेस के रूप में हो। इसमें पहले विशिष्ट स्थान पर स्थित कंपनी के टॉवर की सेल आईडी पता करनी होती है। जिसके लिए कई प्रकार के हाड्रवेयर और साफ्टवेयर आते है जिनसे स्थान विशेष पर विभिन्न कंपनियों के मोबाइल टावरों की सेल आईडी का पता लगाना होता है। उन प्राप्त सेल आईडी के आधार पर उनकी कंपनियों से टॉवर डिटेल रिपोर्ट मॉगी जाती है। फिर सब टॉवर डिटेल रिपोर्ट का एक विश्लेषण करके अनुसंधान किया जाता है।

अंतर्राष्ट्रीय लंबी दूरी (ILD) सेवाएँ

अंतर्राष्ट्रीय सेवाओं का अर्थ है देश में उत्पन्न होने वाली और देश के बाहर समाप्त होने वाली और इसके विपरीत दूरसंचार सेवाएँ। वीओआईपी कॉल–आधारित अपराध करते समय इन सेवाओं का उपयोग अंतरराष्ट्रीय स्पूफिंग कॉल करने के लिए किया जाता है। ऐसे मामलों में, आईओ को आईएलडी गेटवे विवरण तक पहुंच की आवश्यकता होती है। कुछ प्रमुख कंपनियां हैं जो भारत में आईएलडी सेवाएं प्रदान करती हैं।

	H	I	J	K	L	M	N	O	P	Q	R
1											
2											
3											
4											
5	Outgoing OUT-Trunk ID	CALL_DIR (Voice-OUT/INC SMS-MOC/MTC)	Call Type(Voice/SMS)	IN Carrier Name	OUT Carrier Name	Call Status (Successful/Unsuccessful/Intermediate)	First Cell ID	Last Cell ID	Circle	Route Origin Carrier	Route Origin Carrier Name
6	JKLKTK2SWNM	INC	Voice			SUCCESSFUL			OR	SKCEUO3SW2V	Skype
7	JKLKTK1SWNM	INC	Voice			UNSUCCESSFUL			OR	SKCEUOASW2V	SKype
8	JKLKTK2SWNM	INC	Voice			SUCCESSFUL			OR	SKCEUO9SW2V	Skype
9	JKLKTK1SWNM	INC	Voice			SUCCESSFUL			OR	SKCEUO9SW2V	Skype
10	JKLKTK2SWNM	INC	Voice			UNSUCCESSFUL			OR	SKCEUO9SW2V	Skype
11											

वॉयस ओवर इंटरनेट प्रोटोकॉल–वीओआईपी

इसे इंटरनेट टेलीफोनी या आईपी टेलीफोनी भी कहते है। यह इंटरनेट पर आधारित ऐसी सेवा है जो वास्तविक समय अर्थात् रियल आइम आधार पर डेटा का स्थानांतरण करती है। वीओआईपी कॉल एक फोन से दूसरे फोन में, कंप्यूटर से फोन के मध्य किया जा सकता है। इसका अधिक उपयोग होने के कई कारण है इसमें हैः

- यह पुराने पीएसटीएन कॉल की तुलना में यह बहुत सस्ता होता है।
- इंटरनेट कॉल के उत्पन्न होने के स्थान को छुपा कर कॉलर की पहचान को गुप्त रखता है।
- किसी ज्ञात नंबर या अज्ञात नंबर के साथ कॉल करके धोखा देना आसान है।
- आईपी स्पूफिंग विधियों का उपयोग करके उनके स्थान को छुपाना।

वीओआईपी कॉल और पीएसटीएन कॉल में निम्न अंतर हैः–

हम बिना इंटरनेट के कॉल करते है वह पीएसटीएन अर्थात पब्लिक स्वीच्ड टेलिफोन नेटवर्क कहलाता है। जब हम इंटरनेट के माध्यम से कॉल करते है तो वह वीओआईपी कॉल होता है।

1. पीएसटीएन कॉल वॉयस नेटवर्क पर आधारित है और सक्रिट स्विचिंग का उपयोग करता है। हालांकि, वीओआईपी कॉल डेटा नेटवर्क पर आधारित है और पैकेट स्विचिंग का उपयोग करता है
2. पीएसटीएन में, कॉलिंग और कॉल की गई पार्टी के बीच एक समर्पित पथ बनता है। जबकि एक वीओआईपी कॉल में कोई समर्पित पथ नहीं बनता है।
3. पीएसटीएन में कॉल के लिए बैंडविड्थ अग्रिम रूप से आरक्षित होती है लेकिन वीओआईपी में कॉल्स आवश्यकतानुसार बैंडविड्थ प्राप्त कर लेती हैं और जारी कर देती हैं।
4. पीएसटीएन कॉल अधिक महंगी होती हैं क्योंकि दूरी और समय के साथ लागत बढ़ती है, जबकि वीओआईपी कॉल लागत कम होती है और दूरी और समय के आधार पर लागत भिन्न नहीं होती है।
5. पीएसटीएन में, ग्राहक डेटा, टावर डेटा और कॉल डेटा रिकॉर्ड का विश्लेषण करके एक आरोपी का पता लगाया जा सकता है। जबकि वीओआईपी कॉल में, ग्राहक डेटा, आईपी डेटा और आईएलडी सीडीआर डेटा रिकॉर्ड का विश्लेषण करके एक आरोपी का पता लगाया जा सकता है।

वीओआईपी कॉल प्रकार

वीओआईपी कॉल चार प्रकार से किया जा सकता हैः–

- ❖ वेब आधारित वीओआईपी कॉल– बहुत सी वेब है जो वीओआईपी कॉलिंग की सुविधा प्रदान करती है।
- ❖ अज्ञात ऐप–आधारित वीओआईपी कॉल– कई बारे हमारे पास ऐसे कॉल आते है जिनकी हमारे पास कोई ऐस नहीं होती है। तो ऐसे कॉल अज्ञात ऐप आधारित वीओआईपी कॉल कहलाते है।

- ज्ञात ऐप–आधारित वीओआईपी कॉल– जब हमारे मोबाइल में कोई ऐसा ऐस इंस्टाल हो जो वीओआईपी कॉलिंग सुविधा उपलब्ध कराता है तो ऐसे कॉल हमारे ऐप में दिखाई देंगे।
- स्पूफिंग–संचालित ज्ञात ऐप–आधारित वीओआईपी कॉल– कई ऐप ऐसे है जो मनचाहा नंबर चुनने का विकल्प देते है। जिससे अपराधी ऐसे नंबरों का चुनाव करता है जिससे की आसानी से धोखा दिया जा सके। ऐसे कॉल को स्पूफिंग कॉल कहते है।

इकाई– 6
मोबाइल फोरेंसिक

मोबाइल फोन उपकरण

मोबाइल फोन एक ऐसा वायरलेस हैंडहेल्ड उपकरण है, जिसके माध्यम से आप आसानी से एक दूसरे से बातचीत कर सकते है। यह एक लंबी दूरी का इलेक्ट्रॉनिक डिवाइस है। इस डिवाइस का उपयोग न सिर्फ बातचीत करने के लिए किया करते है बल्कि मोबाइल फोन का प्रयोग संदेश भेजने में, Email करने में, Internet आदि ऑनलाइन कार्यों में भी करते है। इसके साथ ही Bluetooth, गेमिंग, वीडियो रिकॉर्ड, ऑडियो रिकॉर्ड, MP3 Player, Radio, GPS इत्यादि के साथ–साथ तस्वीर खींचने में भी मोबाइल फोन का उपयोग किया जाता है।

मोबाइल फोन को Cell Phone, Cellular Phone, Wireless Phone जैसे अलग अलग नामों से भी जाना जाता है।

एक पोर्टेबल कंप्यूटिंग डिवाइस होती है जैसे कि एक स्मार्टफोन या टैबलेट कंप्यूटर या हाथ में पहनने योग्य उपकरण। ये हाथ द्वारा पकड़कर संचालित करने में आसान होते है।

मोबाइल उपकरण से संबन्धित तथ्य

- वर्तमान समय में अधिकतर लोगों के पास सेल फोन या फोन उपलब्ध हैं।
- सेल फोन बहुत ही छोटे कम्प्युटर है जो कि बहुत अधिक मात्र में डाटा स्टोर कर सकते हैं।
- अधिकतर लोग किसी अन्य व्यक्ति से बात करने के लिए सेल फोन का प्रयोग करते है।
- 96 % व्यापार वायर्लेस टेक्नालजी का प्रयोग करते है।
- यह किसी थी स्थान पर आसानी से उपलभ्ध हो जाता है।
- मोबाइल के माध्यम से तत्काल सूचना और डेटा का आदान–प्रदान और जानकारी साझा कि जा सकती है।

मोबाइल के मुख्य उत्पादक

जहां एक ओर भारतीय बाजार को बड़े पैमाने पर अंतरराष्ट्रीय कंपनियों ज्यादातर चीनी स्मार्टफोन निर्माता कंपनियों ने अपने कब्जे में लिया हुआ है। भारत में भी बहुत सी कम्पनियाँ ऐसी हैं जो प्रोडक्ट्स को निर्मित करती हैं, इनमें मोबाइल फोंस और टीवी के अलावा अन्य कई प्रोडक्ट्स भी शामिल हैं। अगर हम अंतरराष्ट्रीय ब्रांड्स की बात करें तो भारत में बड़े पैमाने पर Nokia, Panasonic, LG, Samsung आदि के मोबाइल फोंस को ज्यादा महत्त्व दिया जाता था, लेकिन पिछले कुछ सालों में इस चलन को चीनी स्मार्टफोन निर्माता कंपनियों ने बदला है, इस लिस्ट में हमने Xiaomi, Vivo, Oppo जैसे बड़े ब्रांड्स को देखा है, और इसी कड़ी में अभी हाल ही में Realme के तौर पर एक नया भी जुड़ा है।

कुछ मुख्य मोबाइल उत्पादक निम्न है :-

Xiaomi	Group Brands (Infinix, iTel and Tecno)	Celkon
Samsung	Micromax	YU
Vivo	Intex	XOLO
Oppo	Lava	Xiaomi
Apple	Karbonn	Honor
Realme	Iball	Google
OnePlus	Reliance	Nokia
Poco	Spice	Asus

Nokia	Swipe	LG
Transsion	Motorola	

अधिक जानकारी के लिए https://www.gizbot.com/mobile-brands-in-india/ यू.आर. एल. देखे।

मोबाइल फोन के ऑपरेटिंग सिस्टम

Mobile Operating System एक सॉफ्टवेयर है, जो कि मोबाइल फोन के अंदर इंस्टॉल किया जाता है, जिसकी मदद से यूजर मोबाइल फोन के सभी फीचर का उपयोग करने में सक्षम होता है जैसे कि किसी को कॉल लगाना या मैसेज करना इस प्रकार के सभी कार्य OS की मदद से किए जाते हैं, OS कई प्रकार के होते हैं।

कोई भी ऑपरेटिंग सिस्टम हार्डवेयर के साथ मिलकर कार्य करता है और प्रोग्राम को चलाने की अनुमति देता है।

Mobile Operating System के प्रकार

1- Apple iOS

2- Android OS

3- Windows 8 OS

4- BlackBerry OS

Mobile Operating System के प्रकार

क्रमांक	ऑपरेटिंग सिस्टम	प्रदाता कंपनी
1.	iOS	Apple
2.	Android	Google
3.	Windows	Microsoft
4.	BackBerry	Rim

1. Apple iOS

यह Apple द्वारा विकसित एक मोबाइल OS है, जिसे 2007 में iPhone और iPad के लिए बनाया गया था बाद में इसे एप्पल के टीवी में स्थापित किया गया। इसका इलेक्ट्रानिक डिजाइन बहुत ही आसानी से प्रयोग किया जाने वाला तथा तेज गाति से चलने से चलने वाला iOS है।

गुण–

1-iOS यूजर इंटरफेस किसी अन्य ऑपरेटिंग सिस्टम की तुलना में सबसे अच्छा और आसानी से एवं तेजी से अपडेट होता है.

2-Apple से डाउनलोड की गई Apps दूसरी एप्प की तुलना में सबसे बेहतर है.

3-एप्पल उपभोक्ता को अपने आईफोन और आईपोड का डाटा डेस्कटॉप कम्प्यूटर के साथ स्क्रिोनाइज करने में सहायता देता है। यह सुविधा एंड्राइड में उपलब्ध नहीं है।

दोष–

1-यह सख्त नियंत्रण रखता है और केवल उत्तम की एप्प को ही एप्प–स्टोर पर डालने की अनुमति देता है.

2-एप्पल और आईट्यून सॉफ्टवेयर के द्वारा ही उपभोक्ता को अपने आईफोन और आईपैड को डेस्कटॉप कम्प्यूटर के साथ सिंक्रोनाइज करने की अनुमति देता है.

3-आई.ओ.एस. प्रयोग करने वाले उपकरण अन्य स्मार्ट फोन या टैबलेट से महंगे होते हैं.

2- Android OS

Android एक लाइनेक्स सॉफ्टवेयर पर आधारित गूगल द्वारा विकसित मोबाइल Operating System है, यह ऑपरेटिंग सिस्टम ओपन सोर्स सॉफ्टवेयर है, यानि कि इस ऑपरेटिव सिस्टम का कोड मुफ्त में उपलब्ध होता है और कोई भी प्रोग्रामर इसका कोड लेकर अपने अनुसार कोड में बदलाव करके ला सकता है।

गुण–

1-एंड्राइड ओ.एस. के कोड में बदलाव लाकर कोई भी इसे अपने अनुकूल बना सकता है।

2-यह कई एप्प एक साथ चलाने की सुविधा देता है इसलिए अन्य ओ.एस. की तुलना में बेहतर है।

3-एंड्राइड ऑपरेटिंग सिस्टम ईमेल नोटिफिकेशन, एप्लीकेशन अपडेट, सोशल नेटवर्किंग, आदि से जुड़ी एप्प में बेहतर कार्य करता है।

4-एंड्राइड स्टोर (गूगल प्ले) पर असंख्य ऐप्प उपलब्ध हैं।

5-एंड्राइड ऑपरेटिंग सिस्टम के ओपन सोर्स होने के कारण यह कई प्रकार के हार्डवेयर उपकरणों के साथ आसानी से तालमेल कर पाता है.

दोष–

1-एंड्राइड ऑपरेटिंग सिस्टम बहुत ज्यादा बैटरी खाता है.

2-कुछ ही समय के अन्तराल में गूगल ने एंड्राइड ऑपरेटिंग सिस्टम के बहुत सारे संस्करण बाजार में उतार दिये हैं, जिसके कारण बाजार में एंड्राइड ऑपरेटिंग सिस्टम पर आधारित उपकरणों में उलझन बढ़ गयी है.

3-एंड्राइड आपरीटिंग सिस्टम को सही से इस्तेमाल करने के लिए ळववहसम के प्रकार लाग इन करना जरूरी होता है जोकि सविधाजनक नहीं है.

4-एंड्राइड उपकरणों तथा ब्वउचनजमत के बीच डाटा को सिंक करने के लिए कोई भी तरीका उपलब्ध नहीं है.

3- Windows 8 OS

Windows 8 ऑपरेटिंग सिस्टम को माइक्रोसॉफ्ट के डेस्कटॉप एवं लैपटॉप के लिए बनाया था, इसके अन्य प्रकार "विंडोज फोन 8'और "विंडोज आर.टी.'क्रमशः स्मार्टफोन और टैबलेट के लिए बनाये गए हैं।

.

गुण–

1-विंडोज 8 ऑपरेटिंग सिस्टम का यूजर इंटरफेस बहुत सुविधाजनक है, जिसमें हर एक एप्लीकेशन टाइल की तरह प्रदर्शित होती है।

2-कुछ एप्लीकेशन जैसे सोशल नेटवर्किंग, सर्च, माइक्रोसॉफ्ट ऑफिस, आदि तथा मैप (मानचित्र) से जुड़ी एप्प बहुत आसानी से चलती हैं।

दोष–

1-एक साथ कई कार्य करने के लिए उपभोक्ता को कई स्क्रीन खोलनी पड़ती हैं जोकि कभी–कभी बहुत परेशानी पैदा कर देता है।

2-गूगल प्ले स्टोर और एप्पल के ऐप्पस्टोर की तुलना में विंडोज स्ट्रोर में काफी कम ऐप्प हैं।

3-बहुत कम हार्डवेयर की कम्पनियाँ जैसे कि नोकिया और डेल विंडोज ओ.एस. को अपने फोन के साथ जोड़ती हैं क्योंकि यह इतना प्रचलित नहीं है।

4- BlackBerry OS

यह RIM (रिसर्च इन मोशन) कंपनी द्वारा विकसित ऑपरेटिंग सिस्टम है, जिसे BlackBerry अपने ही ब्राण्ड के स्मार्टफोन और टैबलेट उपकरणों के लिए बनाता है।

गुण–

1-ब्लैकबेरी उपकरण 'पुश ई–मेल' तकनीक के साथ आसानी से तालमेल बना लेता है, जिससे उपभोक्ता अपनी ई–मेल अपने उपकरण पर तुरन्त पढ़ सकते हैं जोकि कुछ सेकण्ड के अन्तराल पहले ही उन्हें भेजी गई है।

2-ब्लैकबेरी फोन डाटा को लगभग 50 प्रतिशत कॉम्प्रेस कर सकता है जिससे ई–मेल भेजने या डाटा Sharing के दौरान बैंडविड्थ कम खर्च होती है, इसके साथ–साथ यह एन्क्रिप्टेड फॉर्म में डाटा को ई–मेल करने की सुविधा देता है.

3-ब्लैकबेरी अन्य ओ.एस. की तुलना में सबसे अच्छा 'बैटरी मैनेजमेंट' उपलब्ध कराता है, जिससे यह फोन कम से कम बैटरी खर्च करता है.

दोष–

1-ब्लैकबेरी का एप्प स्टोर 'एप्लीकेशन प्रोग्रामरस' को आकर्षित करने में असमर्थ दिखाई पड़ता है, और इसमें उपलब्ध एप्प की संख्या अधिक नहीं है.

2-ब्लैकबेरी में दूसरे ओ.एस. की तुलना में इंटरनेट की गाति कम होती है.

3-ब्लैकबेरी उपकरण एक आम आदमी के प्रयोग हेतु फोन न लगाकर एक 'कॉर्पोरेट 100 प्रायोजित उपकरण' ज्यादा दिखाई पड़ता है.

जैसे कि हमने आपको बताया यह चार ऑपरेटिंग सिस्टम दुनियाभर में बहुत ही ज्यादा प्रचलित है जिसमें एंड्राइड और आईफोन के ऑपरेटिंग सिस्टम सबसे ऊपर आते हैं।

मोबाइल फोन उपकरण के अलावा मोबाइल के मुख्य हार्डवेयर पार्ट्स

मोबाइल फोन के अलावा मोबाइल के दो अन्य महत्त्वपूर्ण हिस्से है जो निम्न हैः–

1-SIM card
2-Memory card

SIM कार्ड का पूरा नाम Subscriber Identification Module होता है। SIM Card को सबसे पहले 1991 में बनाया गया था और यह सिर्फ ळैड मोबाइल्स के लिए उपलब्ध कराया गया था और यह सिम कार्ड 2G नेटवर्क पर काम करते थे GSM का फुल फॉर्म (Global System Of Mobile Communication) है।

सबसे पहले वायरलेस सिम कार्ड का आविष्कार 'Giesecke & Devrient' नामक कंपनी द्वारा 1991 में किया गया था. और इस कंपनी ने सिम आविष्कार के पहले ही साल में 300 सिम कार्ड बेचने में सफल रही और यहीं से शुरू हुआ मोबाइल और सिम कार्ड का अनोखा व्यवसाय जो आज के दिन में भी काफी तेजी से चल रहा है।

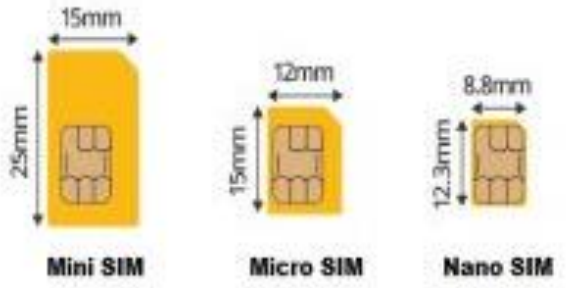
सिम कार्ड का फुल फॉर्म 'Subscriber Identity Module' है और हिंदी में Sim Card को "उपभोक्ता पहचान इकाई पता'कहा जाता है. और यह हमारे लिए मोबाइल नेटवर्क की दुनिया में हमारी आईडेंटिटी यह पहचान के रूप में भी काम करता है।

यानी कि एक ऐसा चिप जिसे Uniquely (आदित्य) एक टेलीकम्युनिकेशन कंपनी ग्राहक को आईडेंटिफाई कर सके और जिस तरह मेमोरी कार्ड 2GB, 4GB, 32GB के होते हैं। एक सिम कार्ड में कितना स्टोरेज रहता है क्या पता है आपको? सिर्फ और सिर्फ 64KB और इसी में आपकी सारी जानकारी मौजूद होती है।

कीपैड मोबाइल में यह सिम कार्ड को बैटरी के पीछे लगाया जाता है और अभी का जमाना स्मार्टफोन का है इसमें मोबाइल के दाहिनी तरफ पिन की मदद से सिम कार्ड को लगाया और निकाला जाता है. सिम कार्ड का मुख्य इस्तेमाल मोबाइल, राउटर, जीपीएस ट्रैकर इत्यादि में किया जाता है।

SIM Card के प्रकार –

सिम कार्ड अपने आविष्कार के कुछ वर्षों तक बड़े आकार में पाया जाता था लेकिन समय बदलने के साथ साथ सिम कार्ड का आकार भी छोटा होता गया साथी अभी के समय में E Sim Card का भी प्रचलन शुरू हो चुका है. जिसमें मोबाइल में किसी भी प्रकार का सिम कार्ड लगाना नहीं पड़ता इसे नेटवर्क प्रोवाइडर द्वारा इंस्टॉल अथवा डाउनलोड किया जाता है।



मेमोरी कार्ड क्या है (What is Memory Card)

मेमोरी कार्ड ऐसा प्रकार का भण्डारण मीडिया होता है जिसे की डाटा जैसे की ऑडियो, विडियो, फोटो आदि भण्डारण करने के लिए प्रयोग किया जाता है।

इसे फ्लेस मेमोरी कार्ड का विकल्प भी कहा जाता है. इसका इस्तमाल इलेक्ट्रॉनिक उपकरणों में डेटा संग्रह के लिए किया जाता है. इस प्रकार के उपकरणों में मेमोरी कार्ड का उपयोगिता कार्ड, डिजिटल कैमकोर्डर, हैंडहेल्ड कंप्यूटर, एमपी3 प्लेयर, पीडीए, सेल फोन, गेम कंसोल और प्रिंटर।

मेमोरी कार्ड के प्रकार

आज बाजार में कई प्रकार के मेमोरी कार्ड उपलब्ध है। उपयोगकर्ता के मन में यह संशय हमेशा बना रहता है कि किस प्रकार का मेमोरी कार्ड कहाँ प्रयोग किया जाना चाहिए। इसलिए चलिए मेमोरी कार्ड के प्रकार (type) के बारे में जानना जरूरी हो जाता है जिससे यह पता रहे कि कौन सा मेमोरी कार्ड कहाँ प्रयोग करना चाहिए व इन सभी में क्या अंतर हैं।

SD Memory Card

SD की फुल फॉर्म है Secure Digital Card. ये सबसे आधारभूत फोरर्मेट होता है SD card में इस मानक एसडी कार्ड के आयाम 32 मिमी गुणा 24 मिमी गुणा 2-1 मिमी, साथ में भंडारण क्षमता 4 जीबी तक है। इसके कार्य का स्तर उतना नही होता जितना दुसरे मेमोरी के प्रकार की होती है. रोग की गुणवत्ता के स्तर एसडी मेमोरी कार्ड के प्रकार हैं।

SDHC मेमोरी कार्ड

SDHC का निसस वितउ होता है Secure Digital High Capacity. इसे तब लाया गया जब एचडी विडियो और उच्च रिजोल्यूशन इमेज रिकोर्डिंग की मॉग बढ गई। इसे अभी भी बहुत से लोग एचडी युक्त उपकरणों में इस्तेमाल करते है।

SDHC cards की भी वही समान आकार और आकृति होती है जैसे कि एक स्तरीय एसडी कार्ड की होती है लेकिन ये नई एसडी वर्जन 2–0 की विशिष्टता का अनुसरण करते है। अगर एसडी कार्ड की मेमोरी क्षमता 4 जीबी या उससे अधिक होती है। तो उसे एसडीएचसी कार्ड की श्रेणी में रखा जाता है।

एसडीएचसी विशिष्टताओं के हिसाब से मेमोरी कार्डों की क्षमता 4 जीबी से 32 जीबी के भीतर होनी चाहिए। इसलिए अगर आप एक एसडीएच कार्ड खरीद रहे है तब ये जॉच करें कि वो उपकरण जिसमें इस इस्तेमाल किया जाने वाला है वह इस कार्ड के अनुकूल होना चाहिए।

SDXC Memory Card

SDXC का फुल फॉर्म होता है Secure Digital Extended Capacity- SDXC cards एक उच्च क्षमता वाला वर्जन होता है एसडी एक्ससी कार्ड की क्षमता 64 जीबी से शुरू होती है। ये अधिकतम 2 टीबी तक पहुॅच सकती है।

MicroSD Memory Card

जैसे की नाम से ये पता चलता है की microSD memory cards बहुत ही छोटे होते हैं बेसिक एसडी कार्ड की तुलना में. साथ में इनका ज्यादातर इस्तेमाल ले जाने योग्य उपकरणों में जैसे की मोबाइल फोन में किया जाता है।

microSDHC माइक्रो एसडी कार्ड का नया वर्जन है, जिसे की सन 2007 में पहली बार लाया गया किया गाया. इसमें करीब 32 GB की डाटा होता है ओर इसकी डाटा स्थानांतरण की गति 10 एमबी तक पहुॅच सकती है। माइक्रो एसडी एचसी कार्ड पुराने माइक्रो एसडी उपकरणों के लिए नहीं बना है।

माइक्रो एसडीएक्ससी

एसडीएक्ससी कार्ड की तरह ही माइक्रो एसडीएक्ससी कार्ड की भी भण्डारण क्षमता 32 जीबी से 2 टीबी के मध्य होती है। इस कार्ड की डाटा स्थानांतरण की गति बहुत ही तेज होती है। माइक्रो एसडी और माइक्रो एसडीएचसी की तुलना में ये केवल उन्ही उपकरणों के साथ योग्य होता है जिनमें एक माइक्रो एसडीएक्ससी स्लॉट नही होता है।

Compact Flash Card

इस प्रकार की मेमोरी कार्ड भौतिक रूप से बडी होती है। एक एसडी कार्ड की तुलना में और इसमें बहुत सारे कनेक्शंस होते है। इनका इस्तेमाल उतना ज्यादा नहीं होता है। जितना कि एसडी कार्ड की होती है लेकिन कुछ की बहुत ही ज्यादा क्षमता होती है और बहुत ही तेजी से ये कार्य कर सकते है। ये अक्सर व्यावसायिक फोटोग्राफर के द्वारा इस्तेमाल किये जाते है। किसी दूसरे इलेक्ट्रोनिक उपकरण की तरह ही इसकी भी उचित देखभाल करनी होती है। जिससे इनकी आयु को बढाया जा सके।

मोबाइल में डाटा स्टोरेज

एक मोबाइल फोन में निम्न लोकेशन पर डाटा स्टोर हो सकता हैः—

- मोबाइल फोन कि internal मेमोरी में
- सिम कार्ड में

❖क्लाउड स्टोरेज में
❖मेमोरी कार्ड में

मोबाइल फोन की विभिन्न स्थानों (लोकेशन) से नीचे वर्णित डाटा प्राप्त किया जा सकता है :–

एड्रैस बुक, कॉल हिस्ट्री, एसएमएस, एमएमएस, ईमेल, वेब हिस्ट्री, फोटो, विडियो, म्यूजिक, डॉकयुमेंट, कलेंडर नोट्स, गूगल मॅप की लोकेशन, सोशल नेटवर्किंग एप्लिकेशन से संबन्धित डाटा, मोबाइल एप्लिकेशन से संबन्धित डाटा। कभी कभी कुछ विशिष्ट मोबाइल से सपोर्ट होने पर मोबाइल से डिलीट कर दिया गाया डाटा भी प्राप्त किया जा सकता है।

वे अपराध जिनमें मोबाइल फोन प्रयोग में लाया जा सकता है –

मोबाइल फोन आज रोज के कार्यों में प्रयोग होता है अतः इसका प्रयोग कई प्रकार के अपराधिक मामलों में प्रत्यक्ष या अप्रत्यक्ष रूप से किया जा सकता है। इनमें से कुछ निम्न है–

•Blue jacking and Blue snarfing: ब्लू जैकिंग का अर्थ है ब्लूटूथ डिवाइस से किसी अन्य ब्लूटूथ सक्षम डिवाइस पर संदेश भेजना।

- ब्लू बगिंग
- विशिंग
- स्मिशिंग (एसएमएस फिशिंग)
- मैलवेयर
- बम ट्रिगर के रूप में मोबाइल फोन
- बैंकर
- जासूसी

मोबाइल फोरेंसिक

डिजिटल फोरेंसिक की वह शाखा जो एक मोबाइल डिवाइस से साक्ष्य या डिजिटल डेटा को बहुत ही गहन अध्ययन करके संग्रहीत करने से संबंधित है मोबाइल फोरेंसिक कहलाती है।

मोबाइल फोरेंसिक प्रक्रिया के महत्वपूर्ण चरण

i.) **Seizure:** इस चरण में जिम्मेदार अधिकारी को मोबाइल डिवाइस को उचित तरीके से seizure करना होता है जिससे मोबाइल पूर्ण रूप नेटवर्किंग से अगल हो जाये या प्रथक हो जाये।

मोबाइल प्राप्त हो जाने के तुरंत बाद ही उसे airplane मोड़े पर कर देना चाहिए जिससे की मोबाइल फोन को सिम द्वारा नेटवर्क न मिल सके। Seizure करते समय Faraday Bag का प्रयोग करना चाहिए जिससे मोबाइल नेटवर्क से दूर हो जाये या मोबाइल द्वारा सिगनल प्राप्त न हो सकें।

ii.)**Extraction:** इस चरण में फोरेंसिक परीक्षक द्वारा किसी फोरेंसिक्स टूल जैसे कि Cellibrite UFED, XRY, Oxygen forensics, Hancom GMD etc या किसी अन्य मोबाइल फोरेंसिक टूल से मोबाइल से डाटा निकाला जाता है।

iii.) **Analysis** – इस चरण में मोबाइल से निकाले गए डाटा का विश्लेषण करना होता है जिसमे आवश्यक साक्ष्य को ढूंढ कर उसका सत्यापन किया जाता है।

iv.)Reporting- अंतिम चरण में विश्लेषण के बाद जो डाटा प्राप्त होता है उसे किसी आसानी से समझे जा सकने वाले स्वरूप में तैयार किया जाता है। यह चरण डाटा का निर्यात (एक्सपोर्ट) कहलाता है। यह फारमैट अत्यंत ही सुगम व गैर तकनीकी (नॉन टेक्निकल) व्यक्ति

को आसानी से समझ में आ सकने वाला होता है। यह PDF, DOCX, EXCEL या HTML फारमैट में उपलब्ध हो सकता है।

Extraction Report
Celebrite UFED Reports

Summary

UFED Physical Analyzer version	6.1.0.202
Report creation time	4/4/2017 3:25:26 PM +05:30
Time zone settings (UTC)	Original UTC value
Case number	1
Case name	1
Evidence number	1
Examiner name	1
Department	1
Location	1
Notes	1

Source Extraction

Logical	
Extraction start date/time	4/4/2017 3:08:32 PM
Extraction end date/time	4/4/2017 3:11:13 PM
UFED Version	6.[redacted].10
Internal Version	4.3.[redacted]1010
Selected Manufacturer	OnePlus
Selected Device Name	3 [redacted]
Connection Type	Cable No. 170
Extraction Type	Logical
Extraction ID	[redacted]
Report type	Phone
Unit Identifier	75[redacted]

मोबाइल डिवाइस से साक्ष्य प्राप्त करने के लिए शर्त

किसी भी मोबाइल से या डिजिटल डिवाइस से प्राप्त डाटा को निम्न शर्तों पर खरा साबित होना होता है तभी वह साक्ष्य (evidence) कहलाएगा। ये साक्ष्य के नियम भी कहलाते है। जो निम्न प्रकार से है–

a)स्वीकार्यता (Admissible)-साक्ष्य को लेते समय यह ध्यान रखना चाहिए कि उसकी कोर्ट में स्वीकार्यता होनी चाहिए। यदि द्वितीयक साक्ष्य ली जा रही है तो उसके साथ धारा 65बी भारतीय साक्ष्य अधिनियम का प्रमाण पत्र अवश्य लगा होना चाहिए।

b)प्रमाणिकता (Authentic) – साक्ष्य लेते समय यह अनन्य रूप से सिद्व होना चाहिए कि वह विवाधक तथ्य को अकाट्य रूप से सिद्व करता हो या असिद्व करता हो। उदाहरण के लिए यदि किसी विडियो के बारे में यह विवाद पैदा होता है कि उसमें कोई व्यक्ति 'क' का है तो इसमें यह सिद्व करना ही होगा कि विडियो में जो व्यक्ति है वह केवल और केवल 'क' ही है।

c)पूर्णता (Complete)- साक्ष्य आधा अधूरा नहीं होना चाहिए वह जिस तथ्य को सिद्व करने के लिए लाया गाया है उसके द्वारा जहॉ तक उस तथ्य को सिद्व या असिद्व करना है वहॉ तक अपने आप में पूर्ण होना चाहिए।

d)भरोसेमंद (Reliable)- जो साक्ष्य को प्रस्तुत किया जाना है उसके लिए अनुसंधान अधिकारी को यह सिद्व करना होगा कि वह भरोसेमंद है।

e)विश्वसनीय (Believable)- लोक अभियोजक उसकी विश्वसनीयता को इस प्रकार से प्रस्तुत करने की उसके बारे में न्यायालय को कोई संदेह न हो।

2 फोरेंसिक का उचित अभ्यास (proper forensic practice)
साक्ष्य (Evidence) की सुरक्षा
साक्ष्य (Evidence) को preserve(रक्षित) करना

3 उचित दस्तावेज (Proper Documentation)
यदि किसी भी प्रकार को कोई बदलाव हुआ है तो उसे दस्तावेज करना।

मोबाइल फोरेसिक्स में प्रयोग होने वाले टूल्स व तकनीकी

मोबाइल फोरेंसिक मेन निम्न टूल प्रयोग किए जाते है हो सर्वाधिक प्रचलित है–
1.Cellibrite UFED (Universal Forensic Extraction Device)
2-Hancom
3-Oxygen forensics
4-Mobiledit
5-Belkasoft evidence center
6-MSAB XRY
7-Final Mobile
8-Elcomsoft

Hancom

ForensIQ One


Oxygen Forensic Detective


FINALMobile Forensics

Sanderson Forensic Toolkit for SQLite

Elcomsoft iOS Forensic Toolkit


Elcomsoft Mobile Forensic Bundle

Belkasoft Evidence Center

Eclipse 3 Pro Kit

Cellebrite UFED

मोबाइल से डाटा निकालने के तरीके :

यद्यपि अलग अलग मोबाइल फोरेंसिक टूल के काम करने का तरीका अलग अलग है परंतु कुछ सामान्य वर्गों (catagory) जो लगभग सभी मोबाइल फोरेंसिक टूल्स में होती है वे निम्न तीन है –

1 फिजिकल डाटा extraction – इस विधि द्वारा मोबाइल डिवाइस पर उपलब्ध (present) डाटा , डिलीट (Deleted) किया गया डाटा व अन्य छुपा दिये गए डाटा को प्राप्त किया जा सकता है।

2 लॉजिकल डाटा extraction– इस विधि द्वारा मोबाइल डिवाइस पर उपलब्ध(present) डाटा ही प्राप्त किया जा सकता है।

3 फाइल सिस्टम डाटा निष्कासन – इस विधि द्वारा मोबाइल डिवाइस पर उपलब्ध (Present) डाटा व अन्य छुपा (Hidden) दिये गए डाटा को प्राप्त किया जा सकता है।

इकाई– 7
सोशल नेटवर्किंग/मीडिया साइट्स

सोशल नेटवर्किंग/मीडिया साइट्स

सोशल नेटवर्किंग, घूमने वाले व्यक्तियों को वेबसाइटों और वेब–आधारित(Web based) Application का उपयोग करते हुए एक–दूसरे के संपर्क(Contact) में रहने की अनुमति देता है। फेसबुक, माइस्पेस, ट्विटर और लिंक्डइन सोशल नेटवर्किंग साइट्स उदाहरण हैं। "सोशल नेटवर्क'शब्द की परिभाषा अभी भी बहुत ढीली है, क्योंकि यह अभी भी एक अपेक्षाकृत नई तकनीक है जो तेजी से बदलाव के अधीन है।सोशल नेटवर्किंग दोस्तों, परिवार, सहकर्मियों, ग्राहकों या ग्राहकों के साथ जुड़े रहने के लिए इंटरनेट–आधारित सोशल मीडिया साइटों(Internet&Based Social Media Sites) का उपयोग है। सोशल नेटवर्किंग का एक सोशल उद्देश्य, एक व्यावसायिक उद्देश्य या दोनों हो सकता है, जैसे कि फेसबुक, ट्विटर, लिंक्डइन और इंस्टाग्राम जैसी अन्य साइटों के माध्यम से। सोशल नेटवर्किंग ग्राहकों को संलग्न(attach) करने की मांग करने वाले Marketers के लिए एक महत्वपूर्ण आधार (Base) बन गया है।

- ☑ सोशल नेटवर्किंग दोस्तों, परिवार या साथियों के साथ जुड़े रहने के लिए इंटरनेट–आधारित सोशल मीडिया प्लेटफार्मों का उपयोग है।
- ☑ हमेशा बदलते समय, अमेरिका में सबसे लोकप्रिय सोशल नेटवर्किंग साइट्स में फेसबुक, इंस्टाग्राम और ट्विटर शामिल हैं।
- ☑ मार्केटर्स ब्रांड की पहचान बढ़ाने और ब्रांड निष्ठा को प्रोत्साहित करने के लिए सोशल नेटवर्किंग का उपयोग करते हैं।

एक सोशल नेटवर्क को व्यक्तियों और उनके व्यक्तिगत संबंधों (Personal relationship) की एक श्रृंखला के रूप में परिभाषित किया गया है। अन्य लोगों के साथ एक कनेक्शन का विस्तार करना एक ऐसी तकनीक है जिसका उपयोग व्यक्तिगत (Personal) या व्यावसायिक (Business) दोनों कारणों से किया जा सकता है। सोशल नेटवर्किंग एप्लिकेशन अन्य लोगों के साथ नए कनेक्शन के निर्माण को सुविधाजनक बनाने के लिए व्यक्तियों के बीच

संघों (Network) का उपयोग करते हैं। इसका उपयोग नए दोस्तों से मिलने और पुराने लोगों से जुड़ने के लिए किया जा सकता है, जैसे कि कई लोग फेसबुक पर करते हैं, या किसी के पेशेवर कनेक्शन (Profession) का विस्तार करने के लिए किया जाता है।

सोशल नेटवर्किंग कैसे काम करता है (How does social networking work)?

मार्केटर्स ब्रांड की पहचान बढ़ाने और ब्रांड निष्ठा को प्रोत्साहित करने के लिए सोशल नेटवर्किंग का उपयोग करते हैं। चूंकि यह एक कंपनी को नए ग्राहकों के लिए अधिक सुलभ बनाता है और मौजूदा ग्राहकों के लिए अधिक पहचान योग्य है, सोशल नेटवर्किंग ब्रांड की आवाज और सामग्री (Content) को बढ़ावा देने में मदद करता है।

विपणक रूपांतरण दरों (Marketers conversion rates) में सुधार के लिए सोशल नेटवर्किंग का उपयोग करते हैं। निम्नलिखित के निर्माण से नए, हाल ही में और पुराने ग्राहकों तक पहुंच और संपर्क स्थापित होता है। सोशल मीडिया पर ब्लॉग पोस्ट, चित्र, वीडियो या टिप्पणियां साझा (Comment Share) करने से अनुयायियों (Follower) को कंपनी की वेबसाइट पर प्रतिक्रिया (reaction) करने और ग्राहक (Customer) बनने की अनुमति मिलती है।

सोशल नेटवर्किंग साइट्स का उदाहरण (EÛample of social networking sites)

- Facebook–इंटरनेट पर सबसे लोकप्रिय सोशल नेटवर्किंग वेबसाइट। फेसबुक उपयोगकर्ताओं के लिए पर्सनल लोकेशन शेयर करने और दोस्तों के साथ जुड़ने, इमेज साझा करने, फिल्में साझा करने, जो आप कर रहे हैं, उसके बारे में बात करने आदि के लिए एक लोकप्रिय गंतव्य(Destination) है।
- Instagram–एक मोबाइल फोटो शेयरिंग सेवा और आईफोन, एंड्रॉइड और विंडोज फोन प्लेटफार्मों के लिए उपलब्ध एप्लिकेशन।
- LinkedIn–वर्तमान और पिछले सहकर्मियों(Co&Worker) और संभावित भविष्य के नियोक्ताओं(Future Employer) के साथ जुड़ने के लिए सबसे अच्छे स्थानों(Location) में से सबसे अच्छा।

- Twitter–एक और शानदार सेवा जो उपयोगकर्ताओं को अपने फोन और इंटरनेट से 140 Character लंबी पोस्ट करने की अनुमति देती है। दुनिया भर में क्या हो रहा है की नब्ज पाने के लिए एक शानदार तरीका।
- Pinterest–एक लोकप्रिय तस्वीर और साझाकरण सेवा जो किसी को भी तस्वीरें साझा करने, संग्रह बनाने और बहुत कुछ करने की अनुमति देती है।
- Youtube–वीडियो ब्लॉग या असवहे और अन्य मजेदार और रोमांचक वीडियो पोस्ट करने वाले उपयोगकर्ताओं का एक उत्कृष्ट नेटवर्क।

सोशल मीडिया प्लैटफार्म के प्रकार

सोशल मीडिया को उनके काम करने के आधार पर निम्न वर्गों मे विभाजित किया गया है –

1 सोशल नेटवर्किंग – फेसबुकए लिंक्डइनए इंस्टाग्रामए टेलीग्राम

2 बुकमार्किंग साइट्स – Pinterest, Flipboard, Digg Social News, StumbleUpon, Reddit, Slashdot, Scope-it

3 मीडिया शेयरिंग – Pinterest, YouTube, Vimeo, MX TakaTak, Tiktok

4 माइक्रोफीड – ट्विटरए फेसबुक, प्लर्क, Identi-ca, फ्राइड, पोस्टीरियस, मिमी, टाउट, इमा हिमा, डेलीबूथ, असोकू आदि।

सोशल मीडिया से संबन्धित अपराध

सोशल मीडिया पर या उसके संबन्धित सामान्य अपराध निम्न है :–

1- **ऑनलाइन धमकियों, पीछा, साइबर बदमाशी** (Online Threats, Stalking, Cyber bullying)

सोशल मीडिया पर होने वाले सबसे अधिक रिपोर्ट किए गए और देखे जाने वाले अपराधों में लोग धमकी, बदमाशी, उत्पीड़न और दूसरों को ऑनलाइन पीछा करना शामिल हैं। जबकि इस प्रकार की अधिकांश गतिविधि बिना किसी सजा के चली जाती है, या इसे गंभीरता से नहीं लिया जाता है, इस प्रकार के अपराधों के पीड़ितों को अक्सर यह नहीं पता होता है कि पुलिस को कब कॉल करना है।

2- **हैकिंग और धोखाधड़ी(Hacking & Fruad)**

हालांकि एक शर्मनाक स्थिति संदेश पोस्ट करने के लिए किसी मित्र के सोशल मीडिया अकाउंट में लॉग इन करना दोस्तों के बीच स्वीकार्य हो सकता है, लेकिन तकनीकी रूप से, एक गंभीर अपराध हो सकता है। इसके अतिरिक्त, लोगों को बरगलाने के लिए नकली खाते या प्रतिरूपण खाते बनाना (सिर्फ गुमनाम रहने के विपरीत), नकलीध्प्रतिरूपण खाताधारक द्वारा की जाने वाली कार्रवाइयों के आधार पर धोखाधड़ी के रूप में दंडित किया जा सकता है।

3- **अवैध चीजें खरीदना (Illegal buying)**

व्यावसायिक संबंध बनाने, या कानूनी सामान या सेवाएं खरीदने के लिए सोशल मीडिया से जुड़ना पूरी तरह से वैध हो सकता है। हालाँकि, ड्रग्स, या अन्य विनियमित, नियंत्रित या प्रतिबंधित उत्पादों को खरीदने के लिए सोशल मीडिया से जुड़ना संभवतः अवैध है।

4- छुट्टी डकैती (Vacation Robberies)

दुर्भाग्य से, चोरों के बीच एक आम बात यह है कि सोशल मीडिया का उपयोग यह पता लगाने के लिए किया जाता है कि कोई संभावित शिकार कब छुट्टी पर है। यदि आपके अवकाश स्थिति अपडेट सार्वजनिक रूप से पोस्ट किए गए है यह न कि मित्र समूहों तक सीमित होने के, अपितु चोरों तक भी पाहुचने वाला है जिसका वह पूर्ण रूप से लाभ लेंगे।

5- फर्जी प्रोफाइल बनाना (Creation of fake profile)

किसी व्यक्ति की नकली प्रोफाइल बनाना और नकली प्रोफाइल पर मॉर्फ की गई तस्वीरों सहित आपत्तिजनक सामग्री पोस्ट करना आज एक कॉमन क्राइम हो चुका है।

6- ऑनलाइन नकली दोस्ती (Fake online friendship)

सोशल मीडिया पर ऑनलाइन दोस्ती विकसित करना (बिना वास्तविक जीवन की परिचितता के और भावनात्मक जुड़ाव का उपयोग करके) आपको किसी बहाने से फंड ट्रांसफर करने के लिए मजबूर कर देना जैसे कि मेडिकल इमरजेंसी, कानूनी परेशानी, विदेश में समस्याएं आदि सभी नकली अकाउंट से माध्यम से किया जा रहा है।

निवारक उपाय/सावधानियां

1- सार्वजनिक खोजों से प्रोफाइल ब्लॉक करें (Block profiles from public searches).
2- ऑनलाइन खोज के माध्यम से आपको कौन ढूंढ सकता है, इसे प्रतिबंधित करें (Restrict who can find you via online search-)
3- आपके बारे में लोग नेट पर खोज कर क्या क्या जान सकते हैं इस जानकारी को सीमित करें (Limit what people can learn about you through searching on net.)
4- प्रत्येक सत्र के बाद लॉग आउट करें(Log out after each session).
5- सोशल मीडिया क्रेडेंशियल साझा न करें (Don't share social media credentials).
6- अनजान लोगों की फ्रेंड रिक्वेस्ट स्वीकार न करें(Don't accept friend requests from unknowns).
7- संदिग्ध लिंक पर क्लिक न करें (Don't click suspicious links).
8- अपने सोशल मीडिया प्रोफाइल की गोपनीयता सेटिंग्स को सबसे प्रतिबंधित स्तरों पर रखें, विशेष रूप से सार्वजनिक/अन्य लोगों के लिए (Keep the privacy settings of your social media profile at the most restricted levels, especially for public/others)
9- याद रखें कि कई पोस्ट, फोटो, स्टेटस, कमेंट आदि में बिखरी हुई जानकारी एक साथ आपके बारे में पर्याप्त खुलासा कर सकती है जिससे एक धोखेबाज आपकी पहचान चुरा

सकता है और आपको धोखा दे सकता है। इसलिए, कुछ भी ऑनलाइन साझा करते समय अधिकतम सावधानी बरतें।

सोशल मीडिया अपराध करने के लिए सबसे आम लक्षित वेबसाइटें/ऐप्स

वर्तमान में 4 मुख्य सोशल मीडिया साइट है जिनका प्रयोग सोशल मीडिया अपराध में हो रहा है–

1 Facebook
2 Instagram
3 Twitter
4 LinkedIn
5 Telegram

सोशल मीडिया के अपराध की कार्य प्रणाली (Modus operandi in social media crime)

सामान्य तौर पर, मोडस ऑपरेंडी किसी भी अपराधी द्वारा सफल होने के लिए उपयोग की गई विधि है जिससे वह अपराध को आसानी से कर पाता है। प्रत्येक ऑपरेंडी कम में तीन बुनियादी तत्व शामिल होते है जो निम्न है –

- अपराध की सफलता सुनिश्चित करना (Ensure success of the crime)
- पहचान की रक्षा करना (Protect identity)
- प्रभावी पलायन की सुविधा(Facilitate effective escape)

साइबर अपराधियों द्वारा आमतौर पर सफल होने के लिए विभिन्न तौर–तरीके अपनाए जाते हैं उनके अपराध करने के सामान्य रूपों का वर्णन आगे इस किताब में किया गया है।

साइबर आर्थिक अपराधों में अपराधियों के काम करने का ढंग तकनीक संचालित होता है। ये अपराधी प्रौद्योगिकी में भेद्यता (Vulnerability) खोजकर उसका फायदा उठाने की कोशिश करते हैं । अपराधी प्रौद्योगिकी में कमजोरियों (vulnerability in technology)या प्रक्रिया में कमियों(lacunas in procedure) का उपयोग करते हैं या अपराध करने के लिए मानव मन के नियमों और धोखे या मनोवैज्ञानिक हैक करके अपराध करते है । प्रत्येक अपराधी के काम करने के तरीके अलग अलग होते है।

सोशल मीडिया अपराधों के लिए जांच प्रक्रिया(Investigation procedure for social media crimes)

सोशल मीडिया से संबन्धित अपराध की जांच करने के लिए उस सोशल मीडिया प्लैटफार्म या एप्लिकेशन की कार्य प्रदाली की जानकारी होना बहुत आवश्यक है। सभी सोशल मीडिया प्रकरणों में , जांच अधिकारी को अपने विवेक से अपनी जाच को आगे बढ़ाना चाहिए। कुछ मूलभूत कदम जिनके द्वारा सोशल मीडिया संबंधी प्रकरणो में सफलता प्राप्त की जा सकती है वे निम्न है –

❖ **रुचि के व्यक्तियों की पहचान (Identifying Persons of Interest)** –

कानून प्रवर्तन संस्था (Law enforcement agencies) सक्रिय रूप से संदिग्ध सोशल मीडिया खातों पर निगरानी कर सकतीं है परंतु यहाँ जरूरी है कि उनके खातों से जानकारी सार्वजनिक की जा रही हो है और इस तरह की सोशल मीडिया उपस्थिति को देखने या निगरानी करने में कोई कानूनी बाधाएं न हों। पोस्ट, ट्वीट, फोटो या अन्य संभावित सबूतों को उजागर करने के अलावा, कानून प्रवर्तन जांचकर्ता चाहे गए व्यक्तियों से संबन्धित सहयोगियों की भी पहचान कर सकते हैं। एक खुफिया दृष्टिकोण से यह मादक पदार्थों की तस्करी और वेश्यावृत्ति जैसे संगठित अपराध नेटवर्क की निगरानी और तोड़ने में अत्यधिक प्रभावी साबित हो सकता है जो आमतौर पर अपनी आपराधिक गतिविधि को बढ़ावा देने के लिए सोशल मीडिया का उपयोग करते हैं।

❖ **आपराधिक गतिविधि के स्थान की पहचान करना** (Identifying Location of Criminal Activity)

ग्लोबल पोजिशनिंग सिस्टम (जीपीएस) तकनीक की लोकप्रियता में वृद्धि और Android o iPhones जैसे मोबाइल उपकरणों पर ऐसी तकनीक की उपलब्धता होने से , सोशल मीडिया द्वारा किसी व्यक्ति के स्थान–को पता कर पाना काफी आसान हो जाता है। सोशल मीडिया साइट पर यह सुविधा पहले से ही उपलब्ध है जिसके द्वारा किसी व्यक्ति कि भौगोलिक स्थिति का पता लगाया जा सकता है।

यह प्रक्रिया जियोलोकेशन कहलाती है। उपयोगकर्ता विभिन्न प्रकार के सोशल मीडिया सॉफ्टवेर का प्रयोग करके उनमें जियोलोकेशन टैग कर सकते है। जांचकर्ता किसी व्यक्ति की जानकारी के बिना उसकी आपराधिक गतिविधि के स्थान की पहचान करने के अलावा उसकी निगरानी करने के लिए उससे संबन्धित भौगोलिक स्थान डेटा का उपयोग कर सकते हैं।

❖**साक्ष्य की पुष्टि करने के लिए फोटोग्राफ या वक्तव्य एकत्र करना** (Gathering Photographs or Statements to Corroborate Evidence)

सोशल मीडिया के मामले में किसी व्यकी द्वारा उसके स्टेटस अपडेट और फोटोग्राफ और कभी–कभी दोनों किसी व्यक्ति विशेष की आपराधिक मानसिकता को साबित करते हैं। इन दोनों की सहायता से उस अपराधी के बारे में पता लगाने में काफी आसानी होती है। यह कार्य कई तरीकों से किया जा सकता है। उदाहरण के लिए किसी फोटो द्वारा किसी अपराधी की उस समय की एसतिथि के बारे के जाना जा सकता है। सोशल मीडिया साइटों पर पोस्ट की गई तस्वीरें, संदिग्धों को पीड़ितों से जोड़ सकती हैं या कसी एक तथ्य के अस्तित्व को साबित कर सकती है। इसके अलावा, सोशल मीडिया साइटों पर पोस्टिंग एक विशेष आपराधिक कृत्य की पुष्टि साबित कर सकती है।

❖**आपराधिक गतिविधि की पहचान (Identifying Criminal Activity)**

कानून प्रवर्तन संथाएं नियमित रूप से अपराधी की पहचान करने और उसे दोषी ठहराने के लिए सोशल मीडिया का उपयोग करती रहती है। इस प्रकार की गतिविधियां फेसबुक, ट्विटर और यूट्यूब जैसी साइटों पर देखी जा सकती है।

अ.)साइबर आवरण (Cybercasing) – साइबरकेसिंग से तात्पर्य है कि जियोटैग किए गए टेक्स्ट, फोटो और वीडियो को अपराधियों या किसी अन्य नकारात्मक रूप से प्रेरित तृतीय

पक्षों(जीपतक चंतजल) द्वारा कैसे उपयोग किया जा सकता जाता है। कई वेश्याएं सोशल मीडिया टूल्स का उपयोग अपने व्यापार को बढ़ाने के लिए बहुत सारे धानवान व्यक्तियों से संपर्क साधने में करती है। कानून प्रवर्तन के लिए यह बहुत जरूरी है कि इस प्रकार कि आपराधिक गतिविधियों कि जानकारी रखे और समयान्तराल पर इस प्रकार कि आपराधिक गतिविधि पर साइबरकेसिंग करे।

सोशल मीडिया से संबन्धित साक्ष्य का संग्रह और विश्लेषण के स्थान

सोशल मीडिया साक्ष्य आमतौर पर दो स्थानों में पाया जाता हैः–

☑मशीन या डिवाइस पर अवशिष्ट रूप में या

☑नेटवर्क/इंटरनेट पर (सोशल मीडिया साइट पर ही संग्रहीत).

सोशल मीडिया साक्ष्य की जांच के लिए भौतिक मशीन (कंप्यूटर या उपकरण) और संबंधित घटकों को भौतिक रूप से जब्त किया जा सकता है।

मेटाडाटा और सोशल मीडिया

वे छिपे हुए साक्ष्य जो कम्प्युटर की किसी लोकेशन पर उपलब्ध है , एक जब्त पीसी पर इंटरनेट ब्राउजर द्वारा कैश किए गए डेटा के अलावा, सोशल मीडिया पोस्टिंग में प्रयोग होते है ये सभी मेटाडेटा कहलाते है।

फेसबुक किसी विशेष उपयोगकर्ता से संबंधित विशेष मेटाडेटा को कैश में स्टोर करके रख सकता है या किसी मित्र की प्रोफाइल से संबन्धित जानकारी भी रख सकता है। प्रत्येक Facebook उपयोगकर्ता, Facebook खाता बनाने के समय से ही पर एक विशिष्ट प्रोफाइल ID नंबर दिया जाता है, जो कि आमतौर पर उपयोगकर्ता को पता नही होता यह एड्रैस बार में प्रदर्शित होता है।

इसके अलावा, फेसबुक चौट से संबन्धित मेटाडेटा (जैसी कलाकृतियां, भेजे गए संदेश का समय, संदेश आईडी (जो प्रत्येक फेसबुक संदेश के किए अद्वितीय होता है) और इसे किससे भेजा गया था यह सभी जानकारी होती है।

"क्लाउड स्टोरेज'में सोशल मीडिया संबंधी आरटिफक्ट्स

सोशल मीडिया पर सभी प्रकार का डाटा अधिकतर क्लाउड स्टोरेज पर ही स्टोर होता है जिसमें मुख्य रूप से फेसबुक, इस्टाग्राम व अन्य सोशल मीडिया है। सोशल मीडिया अकाउंट से संबन्धित फोटो, विडियो, चौट मैसेज व अन्य इवैंट संबंधी डाटा क्लाउड पर स्टोर होता है। सभी सोशल मीडिया एप्लिकेशन अलग योजनाबद्ध तरीके से डाटा को लोकल स्टोरेज (फोन मेमोरी या डिस्क मेमोरी) पर स्टोर करते है। यह सभी डाटा सोशल मीडिया सॉफ्टवेर अपने सर्वर पर डेटाबेस के रूप मेन रखते है। एक कानून प्रवर्तक जांच कर्ता को इस प्रकार के सभी एप्लिकेशन के कार्यप्रदाली की जानकारी होनी आवश्यक है।

एक कानून प्रवर्तक जांचकर्ता के लिए समझना जरूरी है की क्लाउड पर डाटा किस प्रकार स्टोर होता है व उचित कानूनी माध्यम द्वारा डाटा को मंगवाना चाहिए। अधिकतर सोशल मीडिया साइट्स की अपनी एक समर्पित टीम होती है जो की किसी काननों प्रवर्तक शाखाओं द्वारा व्यक्ति विशेष की जानकारी उपलब्ध कराने में सहायक होते है।

इकाई–8
राजस्थान पुलिस में अपराध अनुसंधान और अपराध रोक के लिए उपलब्ध टूल्स/साफ्टवेयर

जब हम कॉल करते है तो हमें तीन प्रकार मध्यवर्तियों की आवश्यकता होती हैः

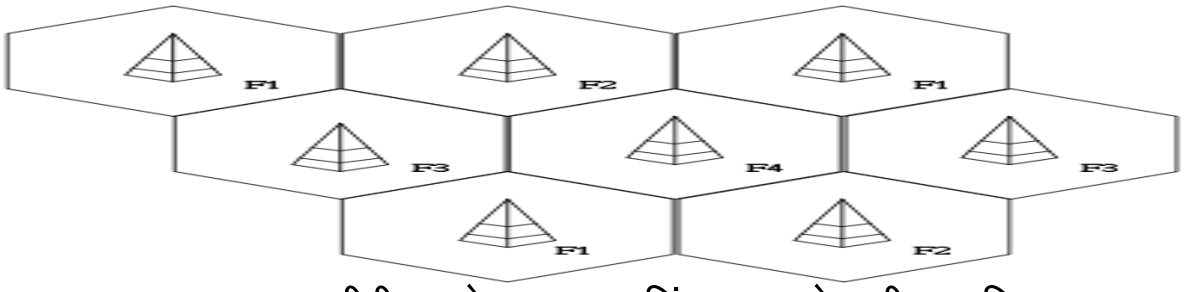
- मोबाइल डिवाइस
- मोबाइल सिम
- मोबाइल कंपनी

जब कोई व्यक्ति मोबाइल से कॉल करता है तो उसके पास किसी मोबाइल कंपनी के द्वारा उपलब्ध कराई एक सिम होती है जो मोबाइल फोन और मोबाइल सेवा प्रदाता कंपनी के मध्य एक सेतु का कार्य करती है। उस सिम के अर्न्तगत कंपनी का नाम, कंपनी का डेटा प्लान और अन्य महत्तवपूर्ण जानकारी होती है जिसके आधार पर मोबाइल कॉल की की पहचान कंपनी द्वारा की जाती है। मोबाइल में एक एंटेना होता है जो किसी मोबाइल कंपनी के मोबाइल टॉवर से जुडा होता है। मोबाइल टॉवर से सही प्रकार से जुडने पर ही मोबाइल कॉल धारक अपनी कॉल के सिग्नल को called number से जोड कर बात कर पाता है। कॉलर को किसी दूसरे मोबाइल से बात करने के लिए हमेशा किसी न किसी मोबाइल टॉवर से जुडा रहना पडता है। मोबाइल टॉवर की अपनी अद्वितीय कॉल आईडी होती है जिसके आधार पर विश्व में उसकी पहचान की जाती है। आइये आगे बढने से पहले हम किसी मोबाइल टॉवर की तकनीक के बारे में जानेः–

मोबाइल फोन एक रेडियो उपकरण है जो किसी क्षेत्र या सेलुलर या मोबाइल नेटवर्क पर ध्वनि संकेतों को प्रसारित और प्राप्त करके संचार करते है। इस प्रकार एक लेलुलर मोबल नेटवर्क को हम एक रेडियो नेटवर्क भी कह सकते है। यह नेटवर्क देश में फेले मोबाइल टॉवर के माध्यम से कार्य करता है। इन टॉवरों की सिग्नल को प्राप्त करने का एक क्षेत्र होता है। इस क्षेत्र का आकार एक सेल की तरह माना गाया है। जिसके केन्द्र में मोबाइल टॉवर को माना जाता है। इसी कारण मोबाइल टॉवर को बेस रिसीवर या सेल टॉवर भी कहा जाता है। सेलुलर मोबाइल नेंटवक्र में निम्नलिखित शामिल हैः–

बीटीएस–

जब हम कॉल करते है तब हमारा मोबाइल कॉल सबसे पहले बीटीएस अर्थात् बेस ट्रांसरिसीवर स्टेशन से सम्पक्र करता है। मोबाइल बीटीएस के द्वारा जो सिग्नल भेजे और प्राप्त किए जाते है उनका एक विशिष्ट क्षेत्र होता है। बीटीएस पर सिग्नल समान दिशा में प्रसारित या प्राप्त नहीं होते है। बल्कि एक विशिष्ट आकृति में प्राप्त होते है। वह आकृति एक सेल की तरह होती है। इस कारण बीटीएस को सेल साइट भी कहा जाता है।



बीटीएस के द्वारा प्राप्त सिंग्नल का क्षेत्र की आकृति

बीएससी

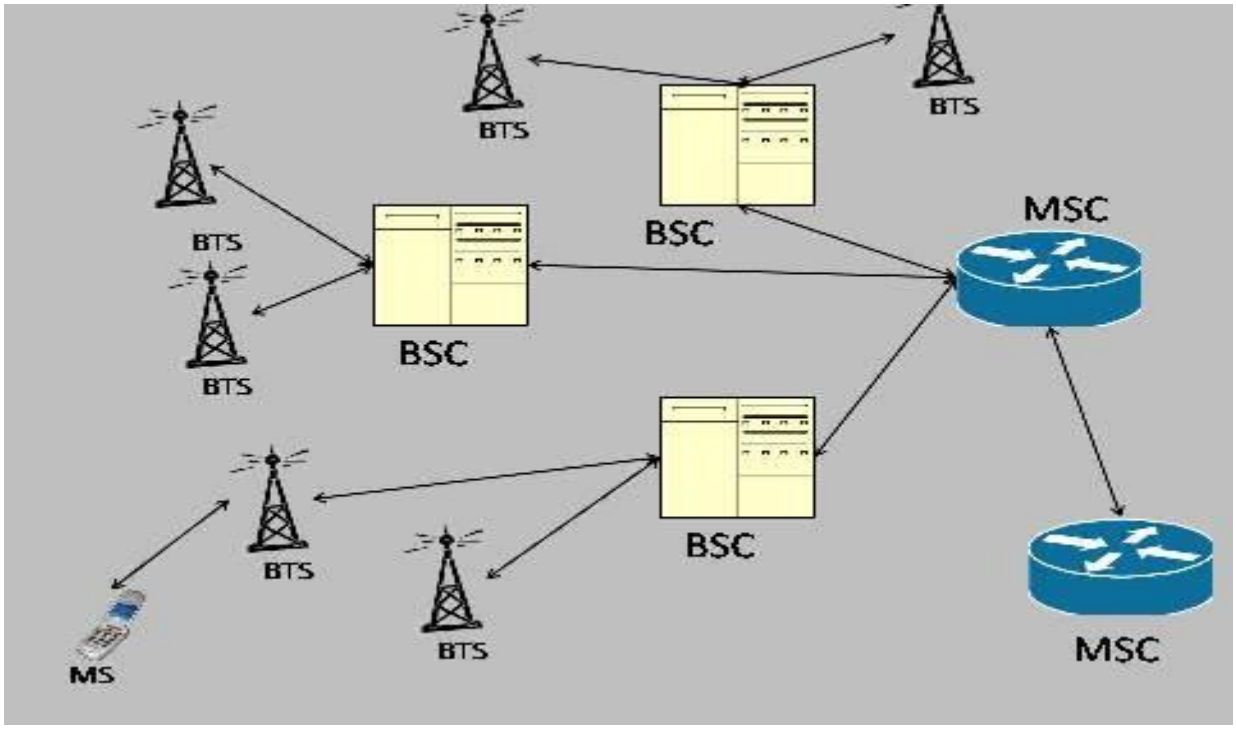
कई बेस ट्रांसरिसीवर स्टेशन बीएससी अर्थात बेस स्टेशन कंट्रोलर से जुडा होता है। इसके बाद कॉल के सिग्नल को बीटीएस द्वारा बीएससी अर्थात् बेस स्टेशन कंट्रोलर के पास भेजा जाता है। बेस ट्रांसमिशन स्टेशन एमएससी अर्थात् मोबाइल स्वीचिंग सेण्टर से जुडा होता है।

एमएससी–

एमएससी से कई बीएससी जुडे होते है। यही पर एचएलआर अर्थात होम लोकेशन रजिस्टर जिसमें कंपनी के उस स्थान के सब्स्क्राईबर की जानकारी होती है। उससे कॉल करने वाले की पहचान की जाती हैं। यदि कॉल धारक किसी दूसरे एमएससी का है तो उस एमएससी के वीएलआर अर्थात विजिटर लोकेशन रिकोर्ड की पहचान प्राप्त करता है। एमएससी अन्य एमएससी से जुडा होता है।

एमएससी के कार्य–

सिम सब्सक्राईबर का सम्पूर्ण डेटा होता है जो प्रमाणित करता है कि जिसके द्वारा कॉल किया गाया है। उसका डेटा प्लान क्या है? उसकी सिम नंबर क्या है? हम किसी भी मोबाइल धारक के बारे में जो भी रिपोर्ट प्राप्त करते है, वह सब यही रिकोर्ड होती है और कंपनी के नोडल अधिकारी द्वारा यही से दी जाती है। सब्सक्राईबरों के मध्य मेसेज यही पर ही आता है। सब्सक्राईबर की बीटीएस लोकेशन को ट्रेक करता है।



इस प्रकार किसी मोबाइल सेवा प्रदाता के द्वारा एमएससी द्वारा महत्तवपूर्ण कार्य सम्पादित किए जाते है।

सेल साइट्स एनालाइजर

सेल साइट विश्लेषण, जिसे ''सेल मैपिंग'' के रूप में भी जाना जाता है। जब एक निश्चित समय पर सेल टावरों का उपयोग करके वॉयस कॉल, एसएमएस संदेश या डेटा भेजा या प्राप्त किया जाता है तो इनके आधार पर मोबाइल फोन के भौगोलिक क्षेत्र को निर्धारित किया जाता है। यह कैसे किया जाता है?

हर बार जब कोई मोबाइल डिवाइस मोबाइल नेटवर्क पर संचार करता है तो सेवा प्रदाता कॉल विभिन्न प्रकार के डेटा को रिकोर्ड करता है। जो निम्न प्रकार हैः–

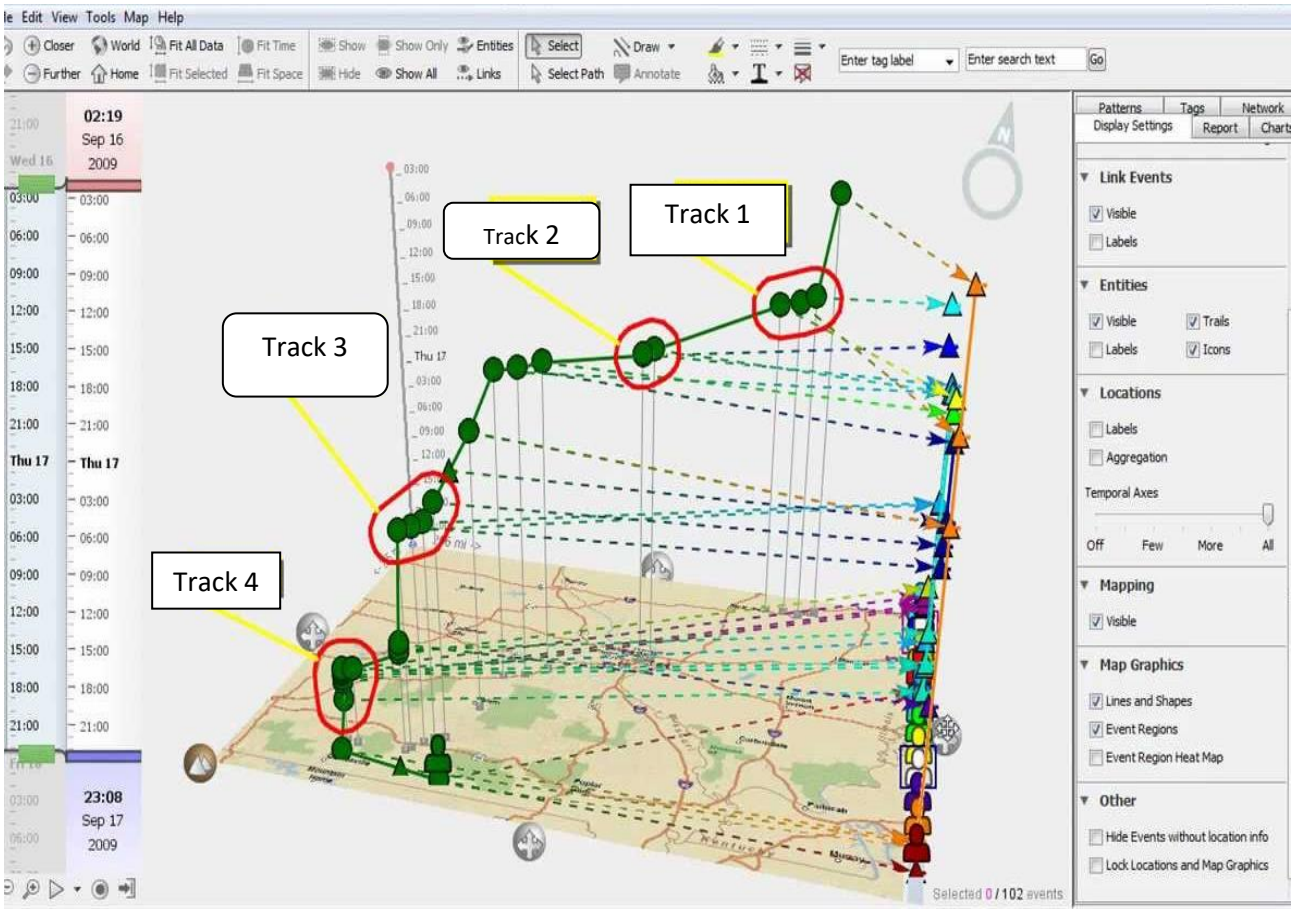
- कॉल का प्रकार – वॉयस, एसएमएस, डेटा
- कॉल करने वाले के मोबाइल नंबर
- कॉल दिशा – इनकमिंग बनाम आउटगोइंग
- अवधि
- पहला सेल टॉवर और अज़ीमुथ
- अंतिम सेल टॉवर और अजीमुथ

सेल साइट एनालाइजर एक ऐसा टूल/साफ्टवेयर है जो इस डेटा का विश्लेषण करने और कॉल डेटा रिकॉर्ड्स (सीडीआर) और नेटवर्क इवेंट लोकेशन सिस्टम (एनईएलओएस) रिपोर्ट की मैपिंग करने के लिए उपयोग में लाया जाता हैं। सेल साइट एनालाइजर एक या एक से अधिक सेल्युलर नंबरों का एक साथ विश्लेषण कर सकता हैं। सेल साइट विश्लेषक अनुसंधान अधिकारी को न केवल सेलुलर टावर के स्थान की कल्पना करने की क्षमता प्रदान करने के साथ यह समझने में सहायता कर सकता है कि कोई व्यक्ति किसी दिए गए क्षेत्र में

था या नहीं। संदिग्ध फ़ोन नंबरों की पहचान करने व सभी संभावित संदिग्धों को समझने के लिए महत्वपूर्ण होता है।

दुनिया भर में मोबाइल फोन के उपयोग के कारण, सिविल और आपराधिक जांच दोनों के भीतर सेल साइट विश्लेषण अधिक से अधिक महत्वपूर्ण होता जा रहा है। कई व्यक्तियों के पास एक से अधिक मोबाइल फोन होने के कारण, मोबाइल डिवाइस की गाति और स्थान का निर्धारण करने करना अनुसंधान अधिकारी के लिए महत्त्वपूर्ण है और अक्सर आज अदालत में उपयोग किए जाने वाले महत्वपूर्ण साक्ष्य होते हैं।

मोबाइल सेवा प्रदाता द्वारा जो हमें सीडीआर अर्थात् कॉल डिटेल रिपोर्ट या इंटरनेट सेवा प्रदाता द्वारा आईपीडीआर दी जाती है वह कच्चे अर्थात रॉ मेटेरियल में होती है। जिसके आधार पर अनुसंधान अधिकारी को अनुसंधान करने में कठिनाई होती है साथ ही समय भी अधिक लगता है। उक्त का विश्लेषण करने के लिए कई प्रकार के टूल्स/साफ्टवेयर की आवश्यता होती है। जब अनुसंधान अधिकारी को अपने द्वारा अनुसंधान किए जा रहे अपराध की आवश्यकता के आधार पर अपराधी या पीडित या अन्य के लिए यह जानकारी लेनी हो कि किसी विशिष्ट समय या स्थान पर उसकी उपस्थित कहा पर थी उसके द्वारा किस मार्ग पर यात्रा की गई जिसे रूट चार्ट भी कहते है की जानकारी के लिए समय बचत हेतु इस प्रकार के टूल्स/साफ्टवेयर का उपयोग करता है जो किसी विशिष्ट मोबाइल धारक के द्वारा अपने मोबाइल के साथ तय किए गए पथ का एक चार्ट अनुसंधान अधिकारी की आवश्यक के अनुसार दो–दिशीय व तीन–दिशीय आधार पर बनाये जाते है।



प्रश्नः सीडीआर विश्लेषण टूल्स क्या है? इसकी उपयोगिता के बारे में वर्णन कीजिए।

जैसा कि हमने कॉल डिटेल वाले अध्याय में यह जाना कि मोबाइल प्रदाता कंपनी डाटा जो रिकोर्ड उपलब्ध कराया जाता है वह एक एक्सेल सीट में होता है जिसका फोर्मेट निश्चित होता हैं। जिसमें विभिन्न कॉलम होते है। उन कॉलम्स में हमें सीडीआर को हमारे द्वारा मॉगी गई सूचना भर कर भेजी जाती है। यह उपलब्ध कराई गई मात्रा बहुत बडी में होती है। जिसका अनुसंधान अधिकारी को अपराध की जरूरत के हिसाब से विश्लेषण करना होता है। जो बहुत मेहनत का काम है। जिसमें गलती होने की संभावना बनी रहती है। इसलिए इन कार्यों के लिए टूल का उपयोग किया जाता है, जो आवश्यकतानुसार सूचना का विश्लेषण करके तुरंत प्रदर्शित कर देते है। कुछ सीडीआर विश्लेषण टूल्स हैः सीबीएफएस, सीडीएमएएस इत्यादि।

इस प्रकार के टूल्स से हमे जानकारी मिलती हैः–

- अधिकतम कॉल, अधिकतम अवधि तक कॉल किस नंबर पर किए गए है
- विशिष्ट दिनांक को मोबाइल धारक द्वारा किए गए अधिकतम कॉल
- मोबाइल कॉल धारक का रूट चार्ट
- दिन और रात में उपस्थिति स्थल
- सीडीआर में संदिग्ध नंबरों की उपस्थिति
- सिम कितनी बार बदली गई
- कितने मोबाइल हैंड सेट का उपयोग किया गाया

दो या अधिक सीडीआर का विश्लेषण–

- दो या अधिका सीडीआर की तुलना
- समान व असमान नंबरों की उपस्थिति
- मोबाइल काल धारको का रूट चार्ट
- मोबाइल कॉल धारको की आपस में दूरी
- कितनी बार आपस में कॉल किये गए।
- कॉल का समय रिकोर्ड व क्रम बनाना।

इत्यादि कार्य सीडीआर विश्लेषक टूल्स से किए जा सकते है।

मोबाइल फोरेंसिक टूल्स के कार्य

मोबाइल डिवाइस फोरेंसिक डिजिटल फोरेंसिक की एक शाखा है जो फोरेंसिक रूप से आदर्श स्थितियों के तहत मोबाइल डिवाइस से डिजिटल साक्ष्य या डेटा की प्राप्ति से संबंधित है। मोबाइल डिवाइस वाक्यांश आमतौर पर मोबाइल फोन को कहा जाता है; हालांकि, यह किसी भी डिजिटल डिवाइस से भी संबंधित हो सकता है जिसमें आंतरिक मेमोरी और संचार क्षमता दोनों हो। जिसमें शामिल हैः पीडीए डिवाइस, जीपीएस डिवाइस और टैबलेट कंप्यूटर।

मोबाइल उपकरणों का उपयोग कई प्रकार की व्यक्तिगत जानकारी जैसे सम्पर्क, फोटो, कैलेंडर और नोट्स, एसएमएस और एमएमएस संदेशों को सुरक्षित भण्डारण के लिए

किया जा सकता है। स्मार्टफ़ोन में इनके अलावा वीडियो, ईमेल, वेब ब्राउज़िंग जानकारी, स्थान की जानकारी और सामाजिक नेटवक्रिंग संदेश और सम्पर्क आदि भी शामिल होते हैं।

कई कारणों से मोबाइल फोरेंसिक की आवश्यकता बढ़ रही है और कुछ प्रमुख कारण हैं:

●व्यक्तिगत और व्यापारिक जानकारी को संग्रहीत और प्रसारित करने के लिए मोबाइल फोन का उपयोग

●ऑनलाइन लेनदेन में मोबाइल फोन का अधिक उपयोग

●अपराधियों द्वारा मोबाइल फोन का उपयोग करने से कानून प्रवर्तन एजेंसियों के लिए जरूरी है कि मोबाइल फोन का उपयोग किया जावे।

मोबाइल फोन में के बारे में हम मोबाइल डिवाइस वाले अध्याय में पढ चुके है।

मोबाइल फोरेसिक्स में प्रयोग होने वाले टूल्स व तकनीकी: मोबाइल फोरेंसिक मेन निम्न टूल प्रयोग किए जाते है हो सर्वाधिक प्रचलित है–

1. Cellibrite UFED (Universal Forensic Extraction Device)
2. Hancom
3. Oxygen forensics
4. Mobiledit
5. Belkasoft evidence center
6. MSAB XRY
7. Final Mobile
8. Elcomsoft

विडियो और फोटो वुद्धिकरण टूल्स

- Kinesense
- Ampedfive
- Impress
- OceanSystem
- Ikena
- Verifeyed
- Adobe Photoshop

राजस्थान पुलिस अकादमी स्थित सीसीपीडब्लूसी लैब में स्थित विभिन्न साफ्टवेयर व टूल्स का विवरण

क्र सं	साफ्टवेयर व टूल्स का नाम	कार्य	विवरण
1.	UFED 4PC	मोबाइल और क्लाउड	मोबाइल फोरेंसिक जिसमें कॉल लॉग, फोन बुक, वीडियो, ऑडियो, चित्र,

		फोरेंसिक	पीडीएफ,डॉक्यूमेंट, व्हाट्सएप, टेलीग्राम, फेसबुक, फेसबुक, मैसेंजर, से डेटा की प्राप्ति लोकेशन, हटाए गए डेटा, स्मृति कार्ड, सिम, आईएमईआई से डेटा की प्राप्ति।
2.	Encase	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।
3.	CDMAS	सीडीआर विश्लेषण	सीडीआर, आईपीडीआर, गेटवे सीडीआर, टीडीआर का विश्लेषण।
4.	Amped 5	विडियो और फोटो की गुणवत्ता बढाने वाला	विडियो और फोटो की गुणवत्ता बढाने वाला
5.	X1 social discovery	सोशल मीडिया प्लेटफार्म विश्लेषण	सोशल मीडिया अकाउण्ट के डाटा का विश्लेषण कर रिपोर्ट बनाता है।
6.	Pathfinder 87K	निष्कासन	यह विभिन्न इलेक्ट्रोनिक डिवाइसों से प्राप्त डाटा का नुलनात्मक विश्लेषण कर उनमें मौजूद कॉमन डाटा की रिपोर्ट बनाता है।
7.	Write blocker	Write सुरक्षा	हाड्रवेयर लोजिकल एवं फिजिकल डिलीटेड डाटा को संग्रहीत करते हुए अन्वेषणाधीन डिवाईस की हैसवेल्यू यथावत् रखता है।
8.	Logicube Falkon	समान ईमेज की प्राप्ति	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।
9.	Passware password recovery	पासवर्ड क्रेक्रिग	कम्प्यूटरों फाईलों एवं फोल्डर के मॉर्मल पावड्र को क्रेक करता है।
10.	DEK Kit		फोरेंसिक उपकरणों का संग्रह है जिसमें अपराध में आवश्यक किट के साथ हाड्रवेयर होते है।

राजस्थान एटीएस के पास उपलब्ध फोरेंसिक टूल्स का विवरण

क्र सं	टूल का नाम	टूल का उद्देश्य	टूल के कार्य
1.	HTCI EDAJ FOX LLC	हाई डेफिनेशन वक्र स्टेशन	फोरेंसिक कार्य करने की क्षमता में वृद्धि अर्थात् समय की बचत एवं डाटा संग्रह क्षमता भी अधिक।

2.	X1 Social Discovery	सोशल मीडिया प्लेटफार्म विश्लेषण	सोशल मीडिया अकाउण्ट के डाटा का विश्लेषण कर रिपोर्ट बनाता है।
3.	Oxygen Forensic	मोबाइल और क्लाउड फोरेंसिक	मेबाइल फोन का लौजिकल एवं फिजिकल (डिलीटेड) डाटा को सॉफ्टकॉपी में संग्रहीत कर विश्लेषण कर रिपोर्ट बनाता है।
4.	Encase	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।
5.	FTK	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
6.	OS Forensic	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
7.	Falcon	समान ईमेज की प्राप्ति	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।
8.	Write Blocker	Write सुरक्षा	हाड्रवेयर लोजिकल एवं फिजिकल डिलीटेड डाटा को संग्रहीत करते हुए अन्वेषणाधीन डिवाईस की हैसवेल्यू यथावत् रखता है।
9.	Solo-4 Image Master	समान ईमेज की प्राप्ति	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।

नेशनल साइबर फोरेंसिक लैब, एनसीएफएल (14C), नई दिल्ली में स्थित फोरेंसिक टूल्स व कार्य

क्र सं	टूल का नाम	टूल का उद्देश्य	टूल के कार्य
1.	Forensic Work Station	हाई डेफिनेशन	फोरेंसिक कार्य करने की क्षमता में वृद्धि अर्थात् समय की बचत एवं डाटा

		वक्र स्टेशन	संग्रह क्षमता भी अधिक।
2.	FRED-C	हाई डेफिनेशन वक्र स्टेशन	फोरेंसिक कार्य करने की क्षमता में वृद्धि अर्थात् समय की बचत एवं डाटा संग्रह क्षमता भी अधिक।
3.	Amped Five	विडियो और फोटो की गुणवत्ता बढाने वाला	विडियो और फोटो की गुणवत्ता बढाने वाला
4.	Ocean System Clear Id	विडियो और फोटो की गुणवत्ता बढाने वाला	विडियो और फोटो की गुणवत्ता बढाने वाला
5.	Network Miner	नेटवर्क विश्लेषण	नेटवर्क डाटा के पैकेट को केपचर करता है। उसके पी–केप डाटा का विश्लेषण करता है।
6.	Damaged Mobie Forensic	मेबाइल फोरेंसिक	डेमेज मोबाइल फोन को रिकवरी स्थिति में तैयार करने का काम करता है। जिससे डाटा प्राप्त किया जा सकता है।
7.	MOBLedit	मोबाइल फोरेंसिक	मोबाइल फोन का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
8.	Oxygen Forensic	मोबाइल और क्लाउड फोरेंसिक	मोबाइल फोन का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
9.	UFED 4PC	मोबाइल और क्लाउड फोरेंसिक	मोबाइल फोरेंसिक जिसमें कॉल लॉग, फोन बुक, वीडियो, ऑडियो, चित्र, पीडीएफ,डॉक्यूमेंट, व्हाट्सएप, टेलीग्राम, फेसबुक, फेसबुक, मैसेंजर, से डेटा की प्राप्ति लोकेशन, हटाए गए डेटा, स्मृति कार्ड, सिम, आईएमईआई से डेटा की प्राप्ति।
10.	XRY	मोबाइल और क्लाउड फोरेंसिक	मोबाइल फोरेंसिक जिसमें कॉल लॉग, फोन बुक, वीडियो, ऑडियो, चित्र, पीडीएफ,डॉक्यूमेंट, व्हाट्सएप, टेलीग्राम, फेसबुक, फेसबुक, मैसेंजर, से डेटा की प्राप्ति लोकेशन, हटाए गए डेटा, स्मृति कार्ड, सिम, आईएमईआई से डेटा की प्राप्ति।
11.	Belkalite	डेटा	मैक बुक व हाड्र डिस्क, एसएसडी,

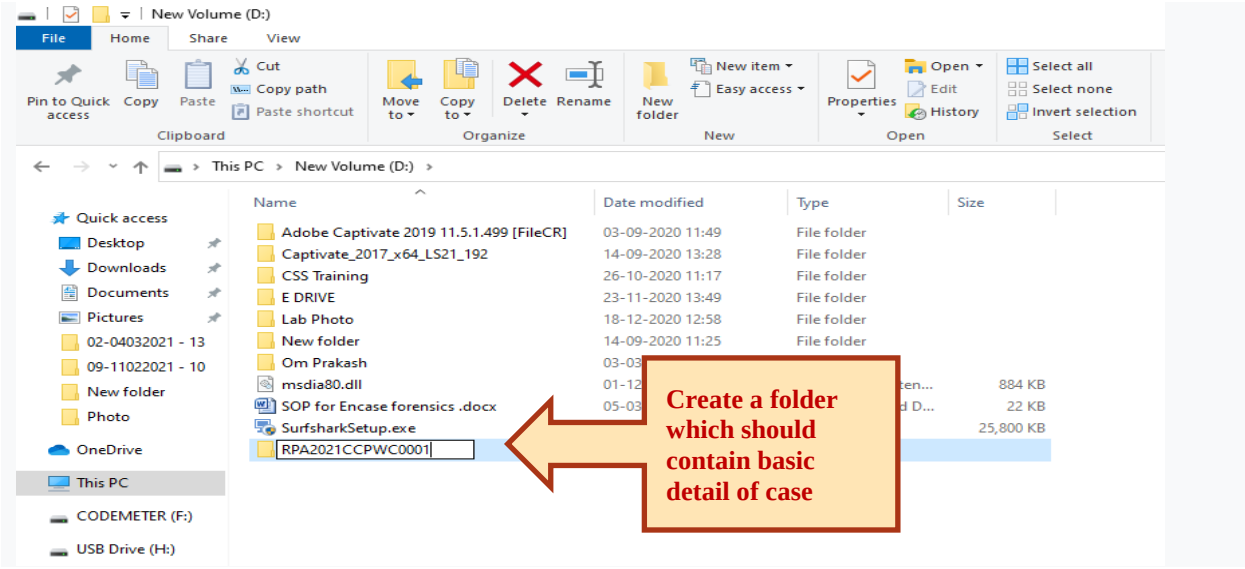
	Inspector Evidence	निष्कासन एवं विश्लेषण	रिमूवेबल हाड्र डिसक/पैन ड्राईव/मैमारी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
12.	Damaged Hard Drive Forensic	डेटा निष्कासन एवं विश्लेषण	डेमेज हाड्र ड्राईव को रिकवरी स्थिति में तैयार करने का काम करता है, जिससे डाटा प्राप्त किया जा सकता है।
13.	Solo-4 (Acquisition Tool)	समान ईमेज की प्राप्ति	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।
14.	Encase	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत करता है।
15.	FTK	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
16.	Nuix	डेटा निष्कासन एवं विश्लेषण	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को संग्रहीत विश्लेषण कर रिपोर्ट बनाता है।
17.	Digital Collector & Inspector (Macquisition)	डेटा निष्कासना	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को साफ्टकॉपी में संग्रहीत करता है।
18.	Ditto Dx (Acquisition Tool)	डेटा निष्कासना	हाड्र डिस्क, एसएसडी, रिमूवलेबल हाड्र डिस्क/पैन ड्राईव/मैमोरी कार्ड का लोजिकल एवं फिजिकल (डिलीटेड) डाटा को साफ्टकॉपी में संग्रहीत करता है।
19.	Ciphertrace	क्रिप्टोकरेंसी का विश्लेषण	क्रिप्टोकरेंसी और ब्लोकचैन का विश्लेषण

20.	Sis Pro	ऑडियो और इमेज की गुणवत्ता उपकरण	ऑडियो और इमेज की गुणवत्ता बढाना।
21.	Write Blocker	Write सुरक्षा	हाड्रवेयर लोजिकल एवं फिजिकल डिलीटेड डाटा को संग्रहीत करते हुए अन्वेषणाधीन डिवाईस की हैसवेल्यू यथावत् रखता है।

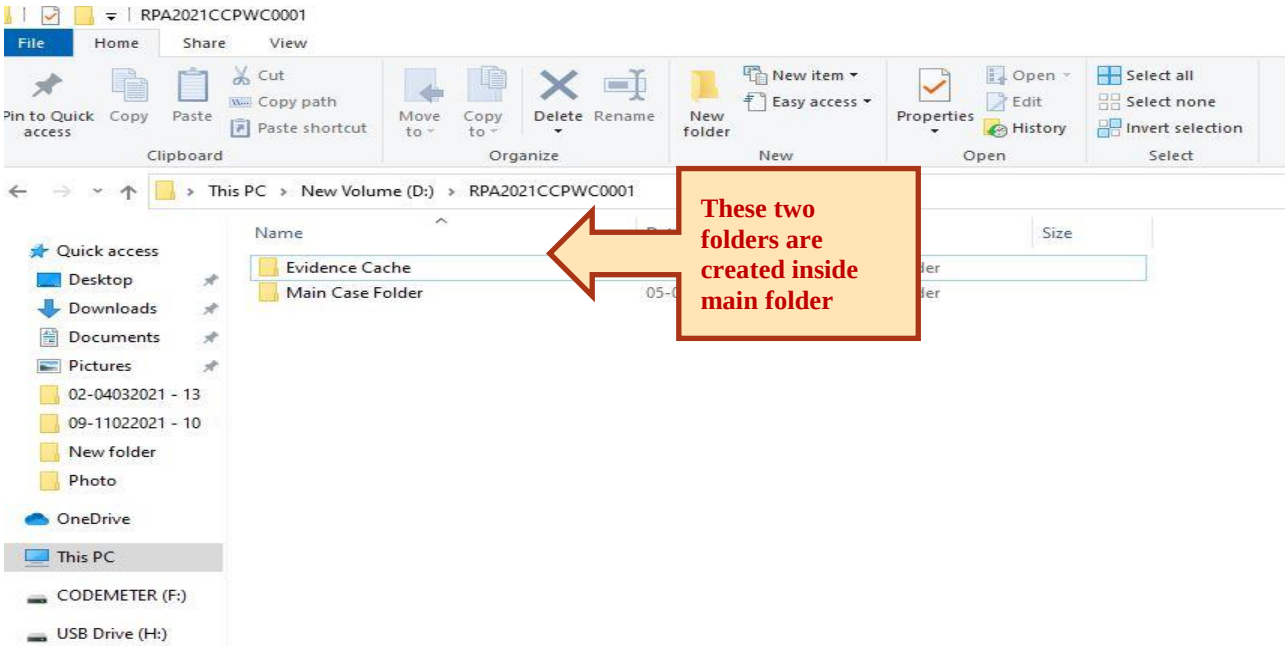
कंप्यूटर फॉरेसिक्स या मेमोरी फॉरेंसिक एक परिचयः

कंप्यूटर फॉरेंसिक फॉरेंसिक साइंस ब्रांच है जिसमें फॉरेंसिक साइंस अनुप्रयोग करते हुए कंप्यूटर से संबंधित साक्ष्यों को जुटाया जाता है। जो कि कानूनी रूप से स्वीकार्य हैं। कंप्यूटर फॉरेंसिक से संबंधित सॉफ्टवेयर काबिल होते हैं कि वह कंप्यूटर मैं उपलब्ध चाहे गए सबूतों को निकालकर उपलब्ध करा सके।

कंप्यूटर फॉरेसिक्स किसी कंप्यूटर डिवाइस पर एक स्ट्रक्चर्ड तरीके सेइन्वेस्टिगेशन करने का तरीका है जिससे कि किसी एविडेंस के माध्यम से यह पता लगाया जा सकता है कि क्या हुआ था, कौन इसका जिम्मेदार रहा और यह कब हुआ। जैसा कि यह एक फॉर्मल डॉक्यूमेंट भी तैयार करता है जो कि चेन ऑफ एविडेंसेस मेंटेन करता है।



□□□□□ **1 :** □□□ □□□ □□□□□□ □□□□□

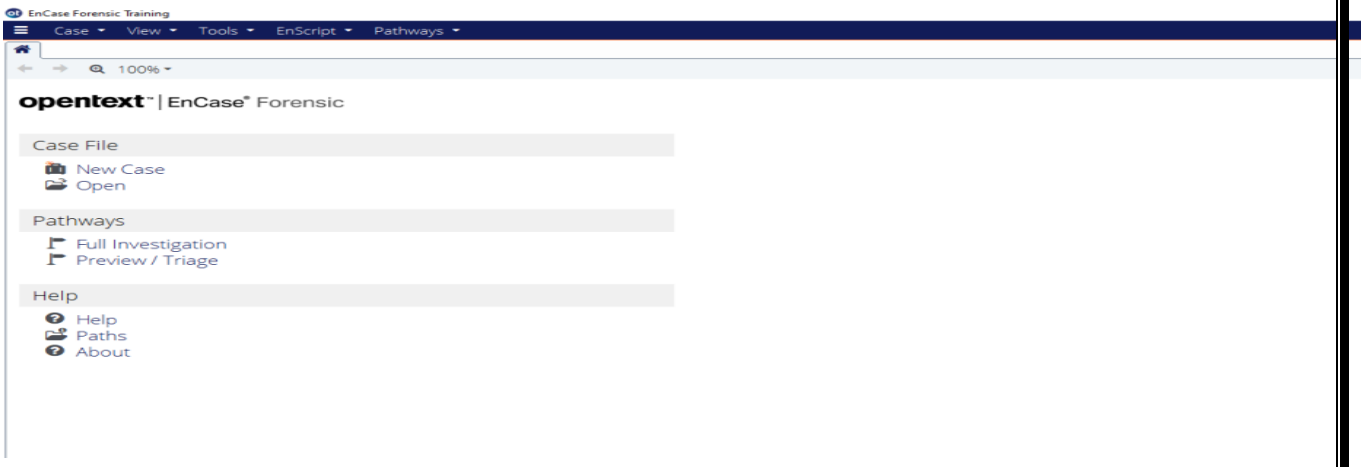


□□□□□ **2 :** □□ □□ (□□) □□□□□□

□□□□□ **2 :** Encase 20.2 □□□□□□□□□ □□ □□□□ □□□□□□□ □□ □□□□□ □□□□□□□ □□ □□□ □□□□□

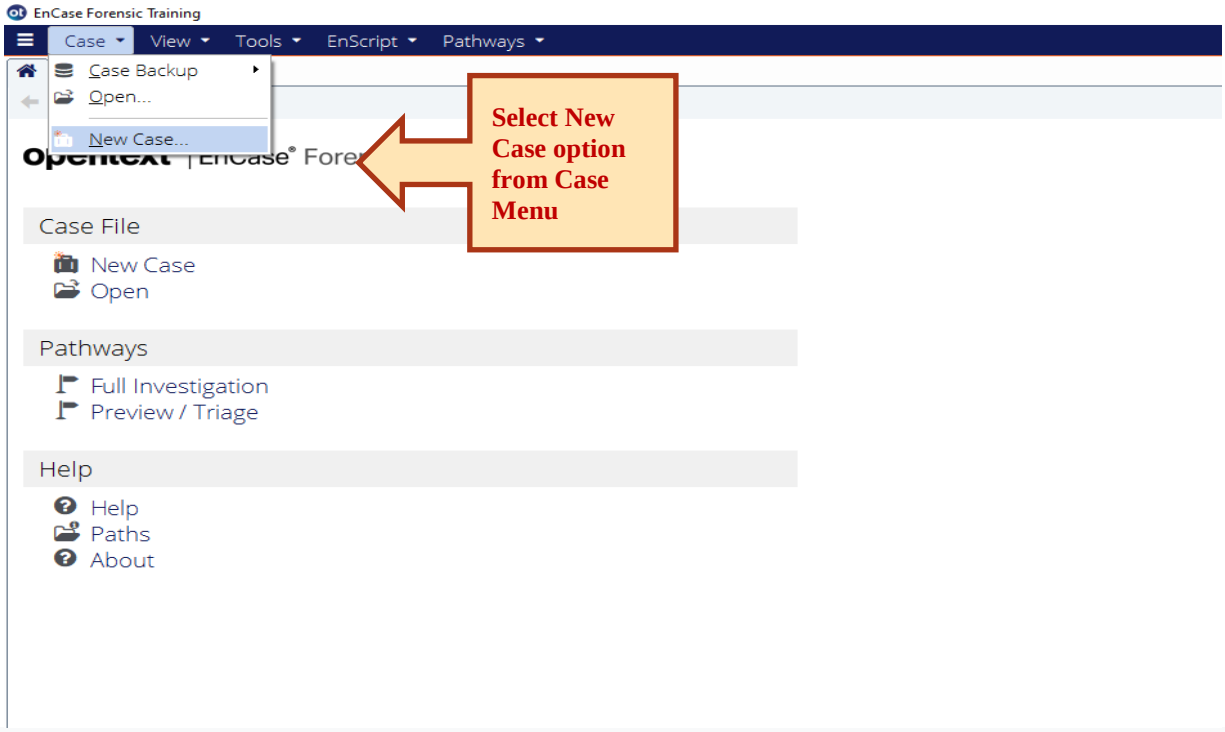

Double click this icon to open Encase

□□□□□ 3 : □□□□□ □□□□□□□□□ □□ □□□□


EnCase Forensic Training
Case
View
Tools
EnScript
Pathways
100%
opentext | EnCase Forensic
Case File
New Case
Open
Pathways
Full Investigation
Preview / Triage
Help
Help
Paths
About

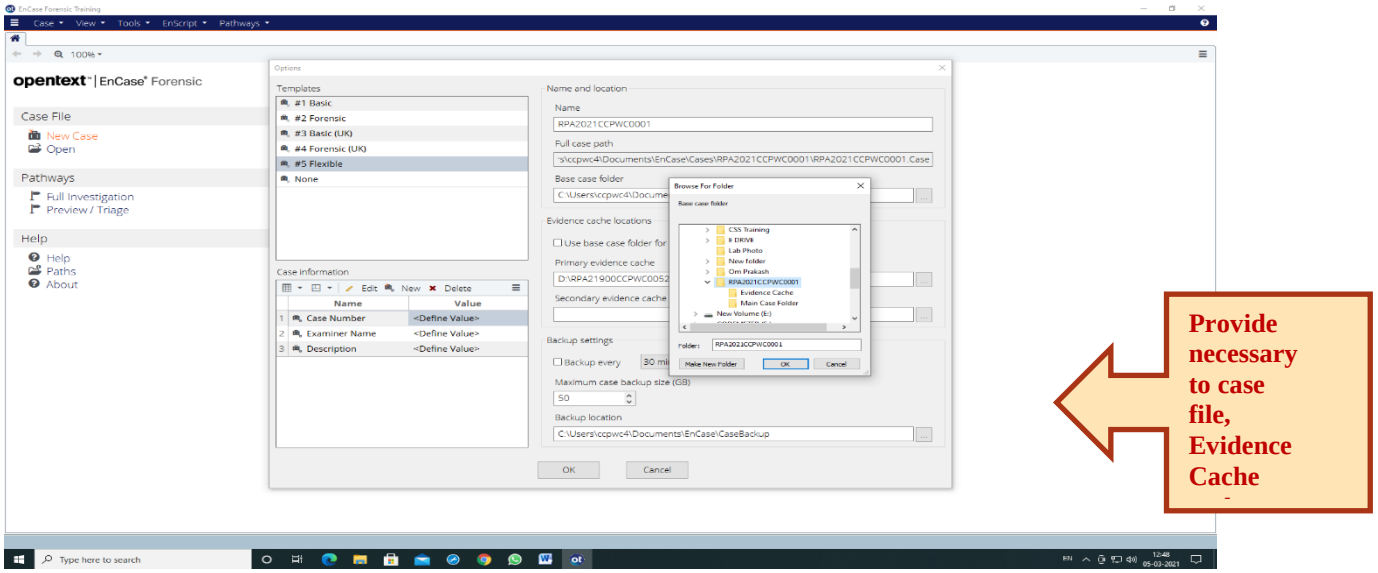
□□□□□ 4 : □□□□□ □□□□□ □□□

□□□□□ 3 : □□□ □□□□ □□ □□□□□ □□ □□□□ □□□□□ □□ □□□□□□□ □□ □□.


EnCase Forensic Training
Case
View
Tools
EnScript
Pathways
Case Backup
Open...
New Case...
Select New Case option from Case Menu
Case File
New Case
Open
Pathways
Full Investigation
Preview / Triage
Help
Help
Paths
About

□□□□□ 5 : □□□ □□□□ □□ □□□□□ □□□□ □□□ □□□ □□□□□

□□□□□ **4 :** केस नाम दें जैसे कि RPA2021CCPWC0001- इसके साथ साथ ही केस का पूरा पाथ एवं एविडेंस कैट फोल्डर जो कि हमने पहले ही बनाया था। इसके साथ ही हम सेकेंडरी एविडेंस कैश फोल्डर का पाथ भी दे सकते हैं, यह आवश्यक नहीं है। यह जो नाम दिया गया है यह एनके सॉफ्टवेयर के केस फाइल का नाम है ना कि स्टोरेज मीडिया की फॉरेंसिक इमेज का।



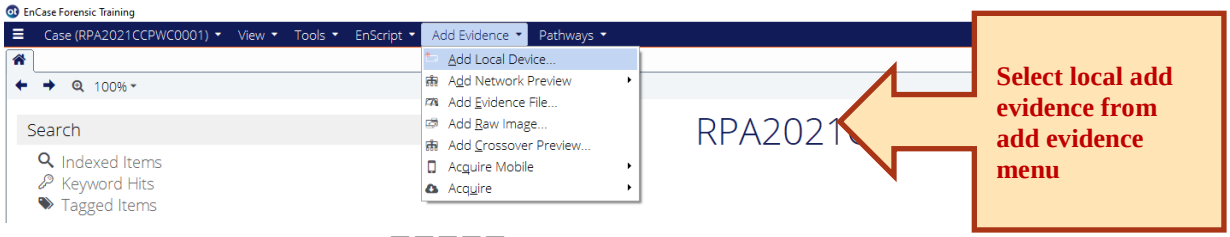
चित्र 4 : केस से संबंधित विभिन्न फोल्डर की लोकेशन निर्धारित करना

नोट: एनकैश द्वारा इमेजिंग बिना लाइसेंस सॉफ्टवेयर के किया जा सकता है लेकिन केस पथ भिन्न हो सकता है।

स्टेप 5 : अब हार्ड डिस्क या यूएसबी या किसी दूसरे स्टोरेज डिवाइस को राइट ब्लॉक कर से जोड़ दें और राइट ब्लॉक कर की पावर को ऑन कर दें. एनकैश में उपलब्ध इन बिल्ड राइट ब्लॉकर को भी इस्तेमाल में लिया जा सकता है जो कि एक सॉफ्टवेयर राइट ब्लॉकर है

स्टेप 6: एड एविडेंस मेनू में जाएं और अपनी आवश्यकता के अनुसार निम्नलिखित ऑप्शंस में से आवश्यक ऑप्शन का चुनाव कर लें : –

- यदि एग्जिट भौतिक रूप से फॉरेंसिक वर्क स्टेशन से जुड़ा हुआ है तो एड लोकल डिवाइस ऑप्शन सेलेक्ट करें
- यदि एविडेंस फाइल पहले से ही बनी है तो ऐड एविडेंस फाइल ऑप्शन सेलेक्ट करें
- यदि इमेज फाइल रो फॉर्मेट में है तो रॉय इमेज ऑप्शन सिलेक्ट करें जोकि DD फॉर्मेट में होगा.



□□□□□ 5 : □□ □□□□□□□□ □□□□

□□□□□ 7: एक डायलॉग बॉक्स दिखाई देगा इस डायलॉग बॉक्स में से डिटेक्ट टैब्ल्यू हार्डवेयर, ओनली शो राइट ब्लॉग और डिटेक्ट लगे सीफास्ट ब्लॉक ऑप्शन के चेक बॉक्स पर टिक कर दें और नेक्स्ट बटन को दबा दें।

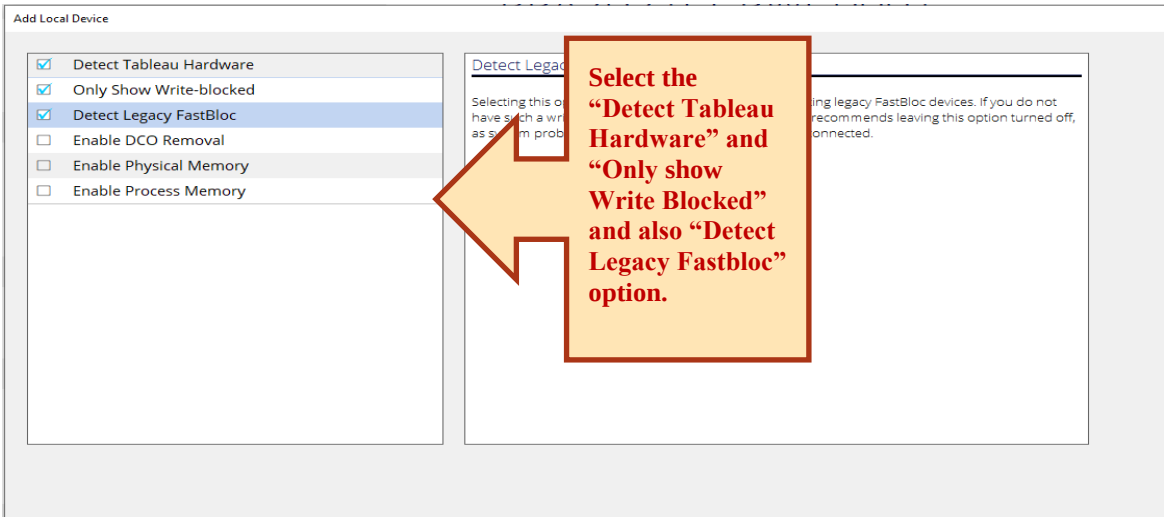


Fig.8 Add Evidence dialog box

□□□□□ 8: एक डायलॉग बॉक्स दिखाई देगा इस डायलॉग बॉक्स में से डिटेक्ट टैब्ल्यू हार्डवेयर, ओनली शो राइट ब्लॉग और डिटेक्ट लगे सीफास्ट ब्लॉक ऑप्शन के चेक बॉक्स पर टिक कर दें और नेक्स्ट बटन को दबा दें ।

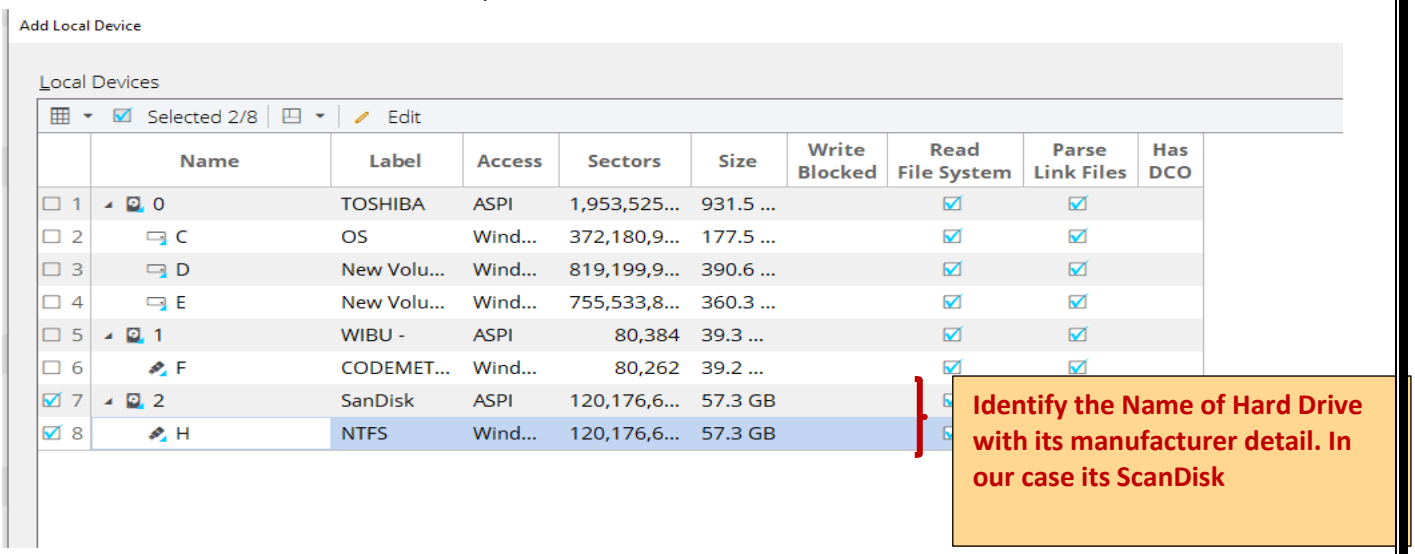
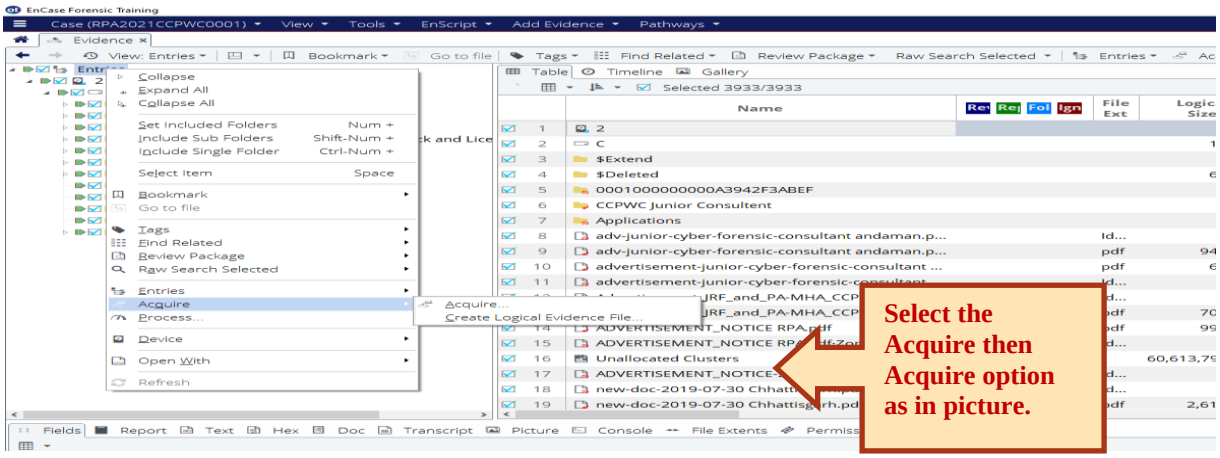


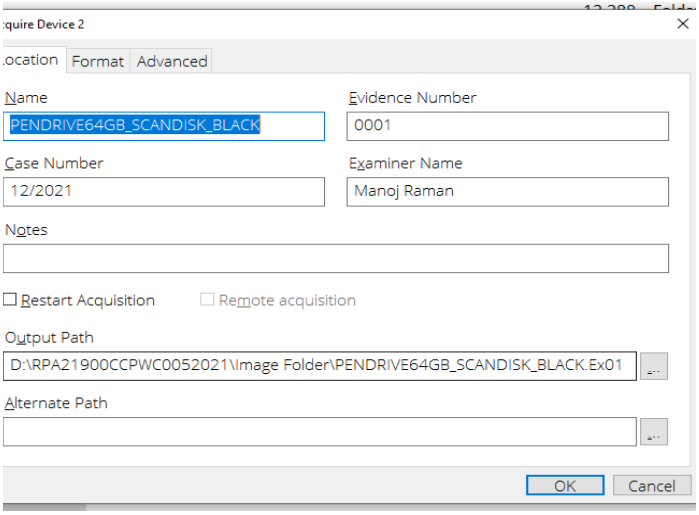
Fig.9 Identification of actual evidence disk or drive

□□□□□ 9: नया डायलॉग बॉक्स ओपन होगा जिसमें ड्राइव का लेटर नंबर जैसे कि 1,2,3 मैं से इलॉजिकल ड्राइव एवं इसके कंटेंट को देख ले। ड्राइव के लेटर पर डबल क्लिक करें , डबल क्लिक हो जाने के बाद एक छोटे से चेकबॉक्स को सिलेक्ट करें एवं एरो पूरी सिलेक्ट कर ले. अब ड्राइव लेटर पर राइट क्लिक करने के बाद एक्वायर ऑप्शन मैं से स्क्वायर सिलेक्ट करें.एक डायलॉग बॉक्स दिखाई देगा इस डायलॉग बॉक्स में से डिटेक्ट टैब्ल्यू हार्डवेयर, ओनली शो राइट ब्लॉग, और डिटेक्ट लगे सीफास्ट ब्लॉक ऑप्शन के चेक बॉक्स पर टिक कर दें और नेक्स्ट बटन को दबा दें।

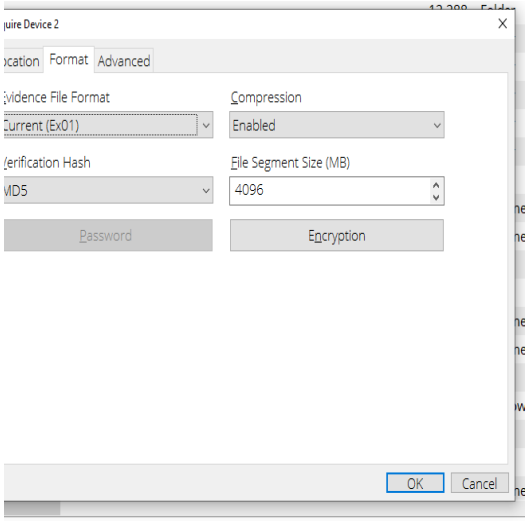


□□□□□ 4 : □□□□□□ □□□□□ □□ □□□□□ □□ □□□□□□□ □□□□

□□□□□ 10: एक छोटा सा डायलॉग बॉक्स खुलेगा इस डायलॉग बॉक्स में आवश्यक जानकारी जैसे कि केस का नाम, एविडेंस नंबर, एग्जामिनर का नाम भरने के बाद ओके पर क्लिक करें और प्रतीक्षा करें जब तक की एक्वायरिंग और वेरिफिकेशन दोनों समाप्त ना हो जाए. वेरिफिकेशन आवश्यक नहीं है इसे स्केप भी जा सकता है. इमेजिंग हो जाने के बाद एविडेंस हटाया जा सकता है।

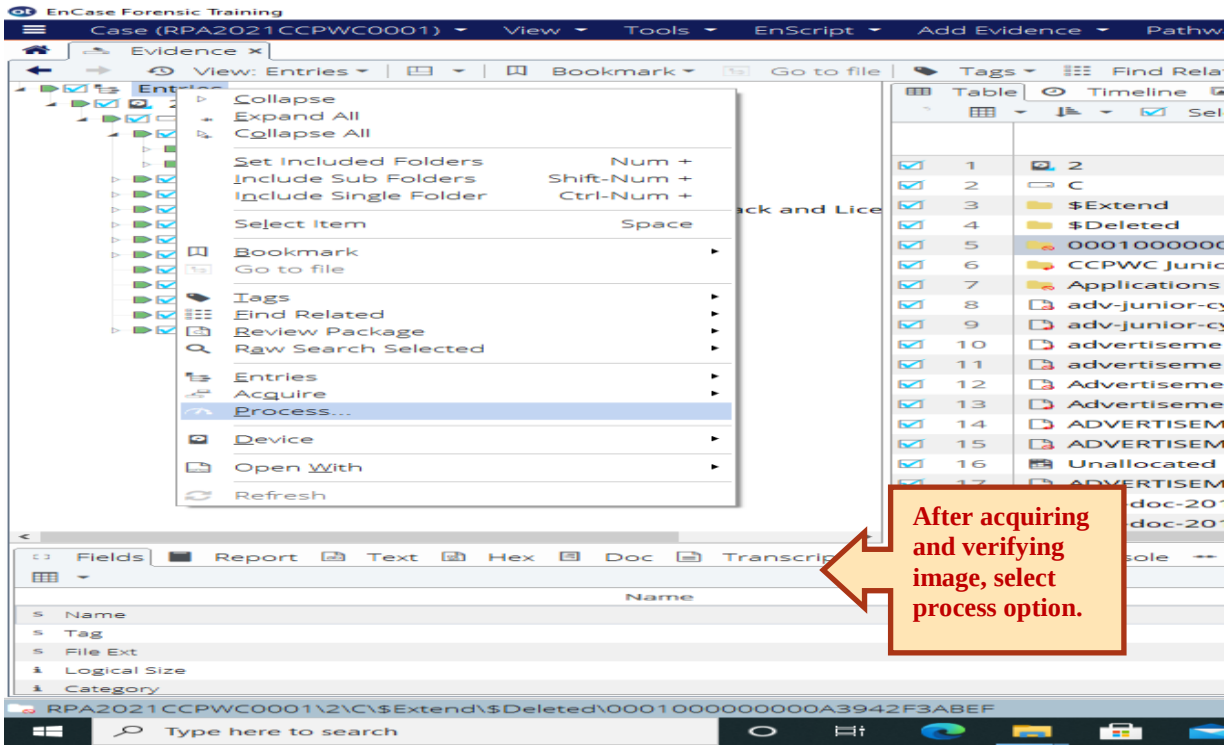


चित्र 11 (अ) सबूत से संबंधित नाम व अन्य जानकारियां



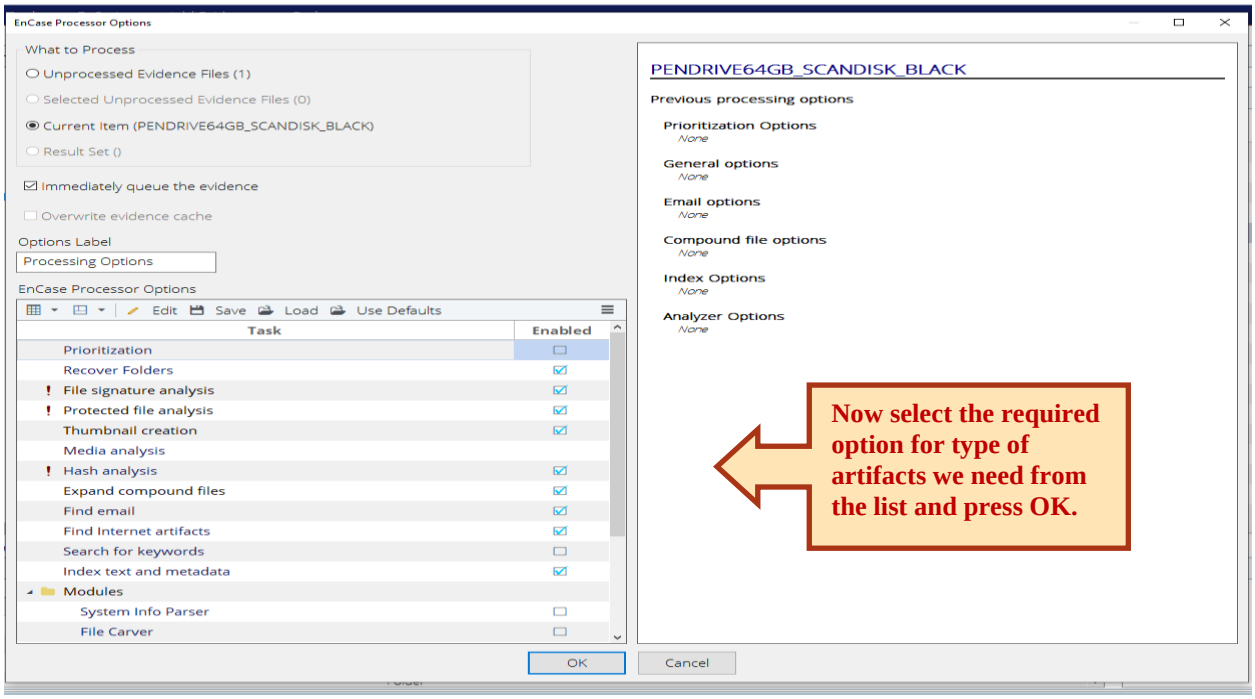
चित्र 11 (ब) सेगमेंट के साइज का निर्धारण

□□□□□ 11: जैसे ही एक्वायरिंग और वेरिफिकेशन प्रोसेस कंप्लीट हो अब हमें एविडेंस फाइल की प्रोसेसिंग करनी है. प्रोसेसिंग एक इंडेक्सिंग का तरीका है जिससे कि विभिन्न प्रकार की फाइलों को अलग–अलग प्रकार पृथक किया जा सके. फिर से एंट्रीज ऑप्शन पर राइट क्लिक करें एवं प्रोसेस ऑप्शन को चुन लें..



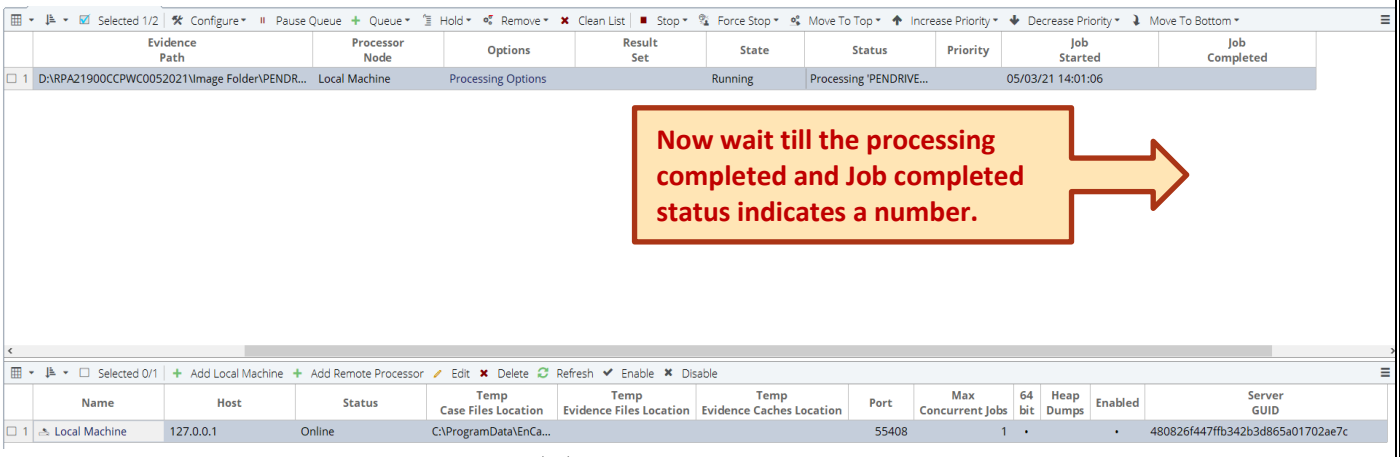
□□□□□ 12 : एक्वायर्ड इमेज की प्रोसेसिंग

प्रोसेस मैन्यू में से अपनी आवश्यकता अनुसार ऑप्शंस का चुनाव कर ले एवं ओके पर क्लिक करें।



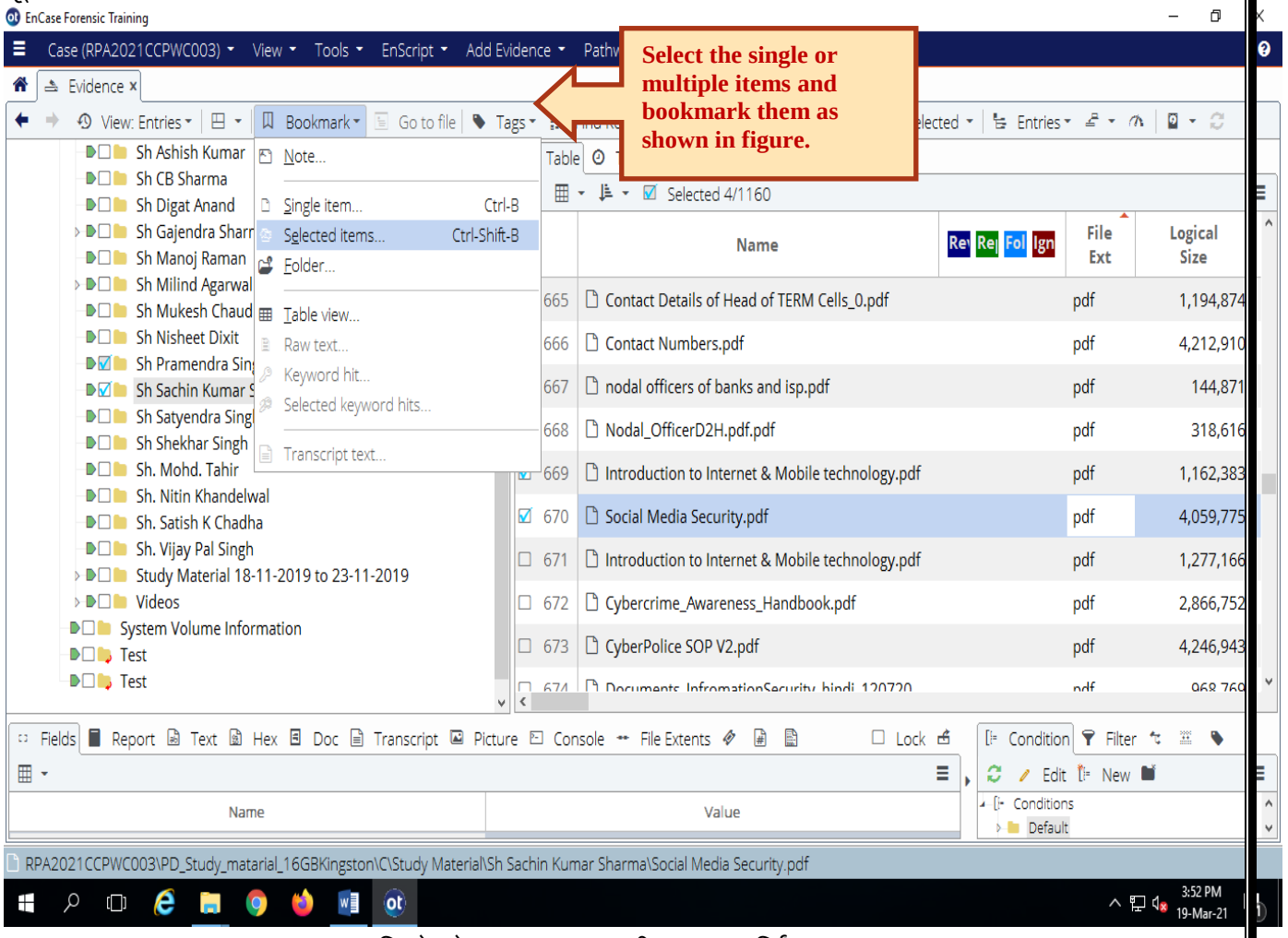
□□□□□ 13 : आवश्यक आर्टीफैक्ट्स के अनुसार प्रोसेसिंग ऑप्शंस का चुनाव

अब व्यू मैंने में जाकर प्रोसेस मैनेजर ऑप्शन सेलेक्ट कर ले जो की प्रोसेसिंग का स्थिति दिखाता है।



चित्र 14 : प्रोसेसिंग की स्थिति जांचना

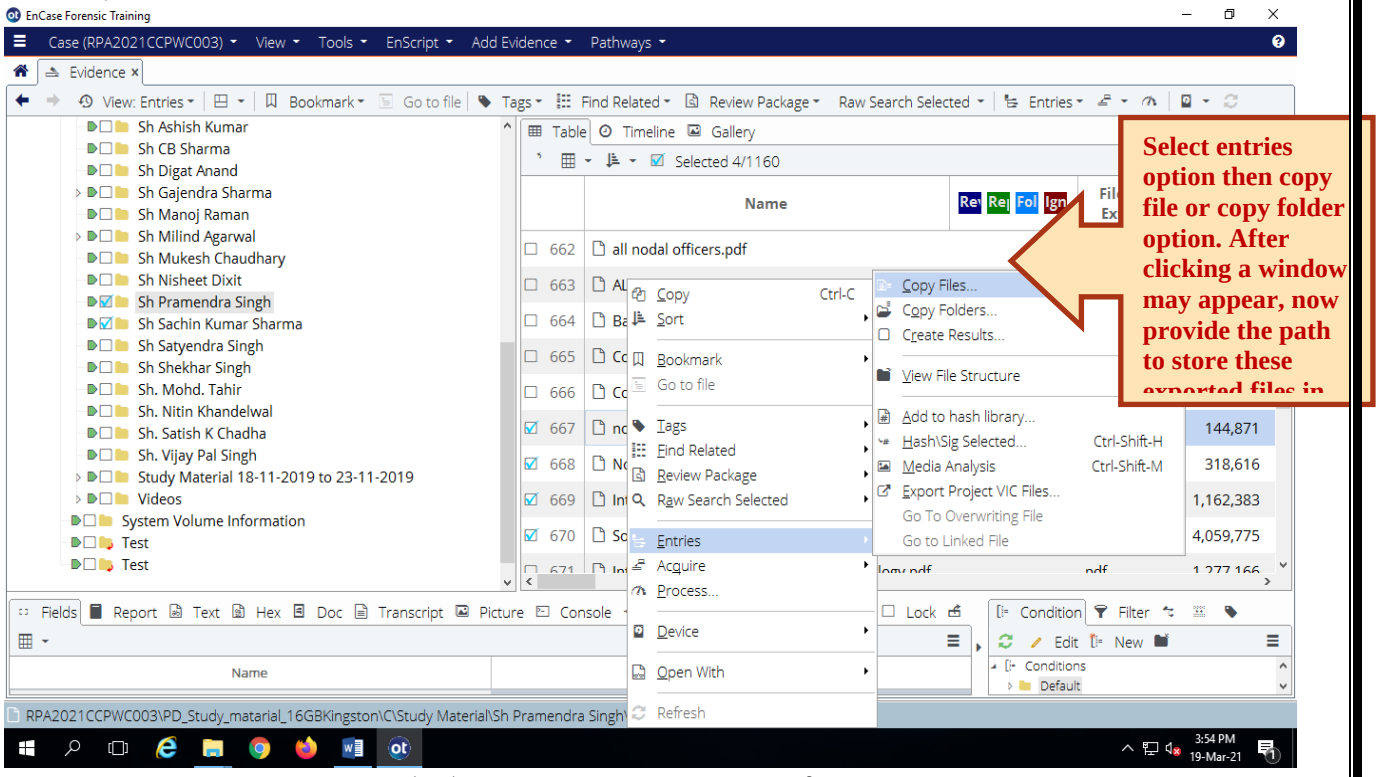
स्टेप 12 : प्रोसेसिंग ठीक रूप से समाप्त हो जाने के पश्चात एविडेंस विंडो से अपनी आवश्यकता अनुसार एविडेंस को सिलेक्ट कर बुकमार्क करें. सिलेक्ट की हुई फाइलों एवं फोल्डर को एक दूसरे फोल्डर में रिपोर्ट के नाम से सेव कर ले



चित्र 15 : सिलेक्टेड आइटम्स की बुक मार्किंग करना

सिलेक्टेड फाइल्स या आर्टइफैक्ट्स को रिपोर्ट के रूप में एक्सपोर्ट करने के लिए सिलेक्टेड आइटम्स के ऊपर राइट क्लिक करें सिलेक्टेड आइटम ऑप्शन सेलेक्ट करें

और एंट्रीज ऑप्शन में जाकर अपने चाहे गए किसी फोल्डर में एक्सपोर्ट कर ले।



□□□□□ 16 : सिलेक्टेड आइटम्स की बुक मार्किंग करना

सिलेक्टेड फाइल्स या आर्टइफैक्ट्स को रिपोर्ट के रूप में एक्सपोर्ट करने के लिए सिलेक्टेड आइटम्स के ऊपर राइट क्लिक करें सिलेक्टेड आइटम ऑप्शन सेलेक्ट करें और एंट्रीज ऑप्शन में जाकर अपने चाहे गए किसी फोल्डर में एक्सपोर्ट कर ले।

इकाई–9
डार्कनेट, डार्कवेब और क्रिप्टोकरेंसी की धारणा

डार्क नेट

एक डार्क नेट इंटरनेट के भीतर एक ओवरले नेटवर्क है जिसे केवल विशिष्ट सॉफ़्टवेयर, कॉन्फ़िगरेशन या ऑथोराइजेशन के साथ एक्सेस किया जा सकता है और अक्सर एक विशिष्ट प्रकार के नेटवर्क संचार का उपयोग करता है।

एक ओवरले नेटवर्क एक कंप्यूटर नेटवर्क है जो दूसरे नेटवर्क के ऊपर स्तरित होता है।

डार्कनेट के दो विशिष्ट प्रकार है जो निम्न प्रकार है

1 सोशल नेटवर्क (आमतौर पर पीयर–टू–पीयर कनेक्शन के साथ फाइल होस्टिंग के लिए उपयोग किया जाता है), और

2 गुमनामी प्रॉक्सी नेटवर्क जैसे टॉर कनेक्शन की एक गुमनाम श्रृंखला के माध्यम से।

- ✓ "डार्कनेट" शब्द को टोर ओनियन सेवाओं के साथ संबद्ध करने के लिए प्रमुख समाचार आउटलेट्स द्वारा लोकप्रिय बनाया गाया था
- ✓ Tor, I2P और Freenet का उद्देश्य सुरक्षा, गुमनामी या सेंसरशिप प्रतिरोध प्रदान करके डिजिटल अधिकारों की रक्षा करना था और इसका उपयोग अवैध और वैध दोनों कारणों से किया जाता है।
- ✓ डार्कवेब को खोजने के लिए जिस नेट का इस्तेमाल किया जाता है वह वह डार्कनेट है जो अपनी गुमनामता के कारण जाना जाता है।
- ✓ "डार्कनेट" को 1970 के दशक में सुरक्षा उद्देश्यों के लिए ARPANET (सरकार द्वारा स्थापित सैन्य/शैक्षणिक नेटवर्क जो इंटरनेट में विकसित हुआ) से बताने के लि, इस शब्द का प्रयोग किया गाया।

डार्कनेट का उपयोग

- नागरिको की गोपनीयता बनाये रखने के लिए ताकि वे अपनी प्राइवेसी के अधिकारों को बनाए रखे हुए एक दूसरे के साथ संचार कर सकते है।
- इसके माध्यम से कई प्रकार के साइबर अपराधों जैसे कि नकली दवाइयों की तस्करी, आतंकवाद, हैंकिंग, क्रैकिंग, आदि को आसानी से गुमनामी के सांथ अंजाम दिया जाता है।
- जब किसी समूह को अपनी राजनीतिक व्यवस्था के प्रति प्रतिरोधों को अपने सदस्यों के मध्य प्रचारित करने के लिए ताकि वे राजनीतिक व्यस्था द्वारा उन पर जो नजर रखेते हुए पांबंदियॉ लगाई जाती है उन से सुरक्षित रह सके।
- ○ गोपनीय फाइलों को भेजने के लिए जिनमें व्यक्तिगत फाइलें, पोर्नोग्राफी, गोपनीय फाइलें, अवैध या नकली सॉफ्टवेयर, आदि सम्मिलित है।
- ○ डार्कनेट बाजारों पर प्रतिबंधित सामानों की बिक्री करने के लिए, व्हिसलब्लोइंग और समाचार लीक जैसे कार्य संपादित करने के लिए इसका इस्तेमाल होता रहा।
- ○ अवैध या अवैध सामान या सेवाओं की खरीद या बिक्री

- नेटवर्क सेंसरशिप और सामग्री–फ़िल्टरिंग सिस्टम को दरकिनार करना, या प्रतिबंधात्मक फ़ायरवॉल नीतियों को दरकिनार कर शामिल है।

डार्कनेट से संबंधित सॉफ्टवेयर

- anoNet नेटवर्क है जिसे वीपीएन और सॉफ्टवेयर का उपयोग करके बनाया गाया है।
- क्रिप्टोकरेंसी एक्सचेंज के लिए Bisq एकमात्र सच्चा पीयर–टू–पीयर फिएट है।
- Decentralized Network 42 (गुमनामी के लिए नहीं बल्कि अनुसंधान उद्देश्यों के लिए)।
- Freenet, GNUnet, RetroShare, Riffle लोकप्रिय डार्कनेट प्लेटफ़ॉर्म है।
- I2P (अदृश्य इंटरनेट प्रोजेक्ट) एक ओवरले प्रॉक्सी नेटवर्क है
- IPFS में एक ब्राउज़र एक्सटेंशन है जो लोकप्रिय वेबपेजों का बैकअप ले सकता है।
- OpenBazaar एक ओपन सोर्स प्रोजेक्ट है जो ई–कॉमर्स लेनदेन के लिए एक प्रोटोकॉल है
- Tor (The Onion Router) एक गुमनाम नेटवर्क है जो ओनियन सेवाओं के माध्यम से एक डार्कनेट भी है ।

SecureDrop-

सिक्योरड्रॉप जैसे फ्री **Software** के उपयोग के माध्यम से व्हिसल–ब्लोअर, कार्यकर्ताओं, पत्रकारों और समाचार संगठनों के बीच अनाम संचार की सुविधा भी डार्कनेट द्वारा की जाती है।

वेबसाइट

इंटरनेट के युग में वेबसाइट्स की अवधारणा बहुत महत्त्वपूर्ण है। जब हम इंटरनेट की बात करते तो किसी न किसी रूप में हम वेबसाइट की भी बात कर रहे होते है। इसलिए पूरे विश्व के इंटरनेट को वर्ल्ड वाइल्ड वेब के संदर्भ में लिया जाता है। जब कोई उपयोगकर्ता इंटरनेट का उपयोग कर रहा होता तो वह किसी न किसी वेबसाइट पर पहुच रहा होता है। इसलिए वेबसाइट को जानना हमारे लिए एक पुलिस अधिकारी होने के नाते बहुत महत्त्व का होता है। इंटरनेट पर खोज किए जाने की आसानी के आधार पर वेबसाइट्स तीन प्रकार की होती है:–

1. सतही वेबसाइट
2. डीप वेब
3. डार्क वेब

1. सतही वेबसाइट–

सरफेस वेब (जिसे विजिबल वेब, इंडेक्सेड वेब, इंडेक्सेबल वेब या लाइटनेट भी कहा जाता है) वर्ल्ड वाइड वेब का वह हिस्सा है जो आम जनता के लिए आसानी से उपलब्ध है और मानक वेब सर्च इंजन के साथ खोजा जा सकता है।

सरफेस वेब वो है हर राज उपयोग करते है। इनको लोकप्रिय खोज इंजनों के माध्यम से खोजा जा सकता है। लोकप्रिय सर्च इंजन जैसे गुगल, याहु आदि में इन वेब साइटों की अनुक्रमण अर्थात इंडेक्सिंग होती है जिसके कारण इन्हे खोज पाते है।

सरफेस वेब के अन्तर्गत सम्पूर्ण वेबसाइटों का केवल 4 प्रतिशत ही आता है शेष 96 प्रतिशत भाग डीप वेब और डार्क वेब के अन्तर्गत आता है।

डीप वेब–

अस्पृश्य वेब या हिडन वेब वर्ल्ड वाइड वेब के वेब लाईट सामान्य इंटरनेट वेब खोज–इंजन लेखित की तरह हैं। यह सतह वेब के विपरीत है, जो इंटरनेट का उपयोग करने वाले किसी भी व्यक्ति के लिए सुलभ है।

डीप वेब के अंदर ऐसी लिंक्स हैं जो कभी भी गुगल, याहु किसी भी व्यक्ति द्वारा सर्च इंजन में खोजा नहीं जा सकता है। जैसे कि आप गुगल ड्राइव पर कोई फाइल अपलोड करके जो यूआरएल आता है वह यदि गुगल में खोज करें तो उसकी जानकारी नहीं मिल पायेगी। ये लिंक डीप वेब के अन्तर्गत आयेंगे।

डार्क वेब–

डार्क वेब वर्ल्ड वाइड वेब सामग्री है जो डार्कनेट पर मौजूद है यह ओवरले नेटवर्क का उपयोग करते हैं जिससे इन्हे एक्सेस करने के लिए विशिष्ट सॉफ्टवेयर, कॉन्फिगरेशन या प्राधिकरण की आवश्यकता होती है। डार्क वेब के माध्यम से, निजी कंप्यूटर नेटवर्क उपयोगकर्ता के स्थान जैसी पहचान संबंधी जानकारी को प्रकट किए बिना गुमनाम रूप से संचार और गातिविधि कर सकते हैं डार्क वेब, डीप वेब का एक छोटा–सा हिस्सा है। वेब का वह हिस्सा जिसे वेब सर्च इंजन द्वारा अनुक्रमित नहीं किया जाता है, हालांकि कभी–कभी डीप वेब शब्द का प्रयोग गलती से डार्क वेब के लिए किया जाता है।

डार्क वेब के अंदर कुछ ऐसी onion साइटस है, जो आपको कभी भी गुगल, याहु जैसे सर्च इंजन में नहीं मिलेंगी, और ना ही आप उनको अपने सामान्य ब्राउजर (क्रोम, मोजिला, फायरफोक्स) से उन तक पहुच सकते हो भले ही उनका यूआरएल क्यू न पता हो और आप अपने नार्मल आईपी पते से भी उन तक नहीं पहुचा जा सकता है I इसके लिए टोर ब्राउके माध्यम से या किसी सोफटवेयर के माध्य से ही उन तक जाया जा सकता है।

डार्क वेब साइटस के बारे में

- टोर ब्राउजर के सर्च इंजन का नाम ''डग डग गो'' है।
- डार्क वेबसाइटस के डोमेन नेम में अंत में onion जुडा होता है।
- डार्क वेब साइटस का डोमेन नेम अस्थाई होता है जिसका सर्वर डार्क वेबसाइटस के धारक का अपना लेपटॉप हो सकता है।

- जिस तरह से सामान्य com डोमेन पंजीकृत होते हैं, उस तरह से onion डोमेन पंजीकृत नहीं होते हैं। प्रत्येक onion डोमेन एक कुंजी का हैश है जो टोर में onion साइट बनाने पर कम या ज्यादा बेतरतीब ढंग से उत्पन्न होता है।

डार्क वेबसाइट को विजिट करने से पहले अपनाई जानी वाली सावधानियॉ वरना हैकिंग जैसे किसी अपराध का शिकार हो सकते है।

- वचफ्रअल मशीन का उपयोग करे।
- वीपीएन का उपयोग करे।
- टोर ब्राउजर के माध्यम से ही सर्च करे।

उक्त तीनों हमारी पहचान इंटरनेट पर गुप्त रखते है जिसके कारण हैकर द्वारा आसानी से हैक नहीं किया जा सकता है।

क्रिप्टोकरेंसी

क्रिप्टोकरेंसी एक डिजिटल या आभासी मुद्रा है जिसे क्रिप्टोग्राफी द्वारा सुरक्षित किया जाता है, जिससे नकली या दोहरा खर्च करना लगभग असंभव हो जाता है। कई क्रिप्टोकरेंसी ब्लॉकचैन तकनीक पर आधारित विकेन्द्रीकृत नेटवर्क हैं जो कंप्यूटर के एक अलग नेटवर्क द्वारा लागू एक वितरित खाता बही। क्रिप्टोकरेंसी की एक परिभाषित विशेषता यह है कि वे आम तौर पर किसी भी केंद्रीय प्राधिकरण द्वारा जारी नहीं की जाती हैं, जो उन्हें सैद्धांतिक रूप से सरकारी हस्तक्षेप या हेरफेर से प्रतिरक्षा प्रदान करती हैं।

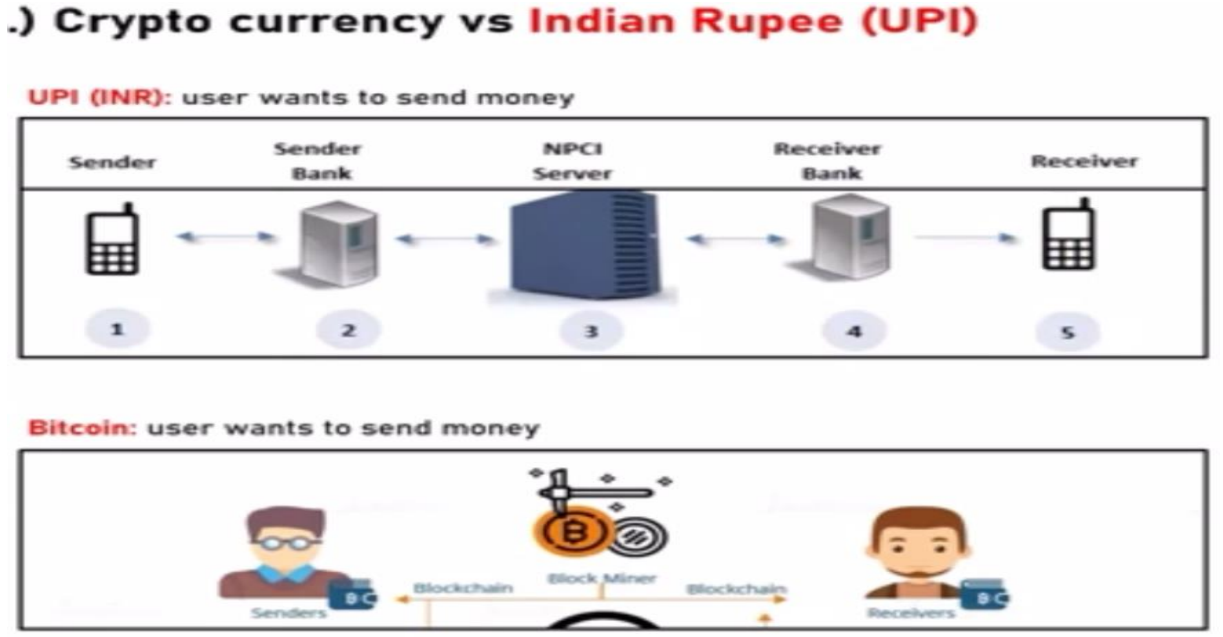
क्रिप्टोकरेंसी की विशेषताएॅः–

- क्रिप्टो करेंसी एक डिजिटल मनी या वचफ्रअल मनी है।
- वह पैसा है लेकिन यह भौतिक रूप से उपलब्ध नहीं है
- यह बहुत सुरक्षित है। जो ब्लोकचेन तकनीक का प्रयोग करती है।
- सरल शब्दों में हम कह सकते हैं कि क्रिप्टोकरेंसी एक मुद्रा विनिमय प्रक्रिया है।
- क्रिप्टोकरेंसी का सबसे लोकप्रिय उदाहरण बिटकॉइन है। क्रिप्टोकरेंसी के कुछ अन्य उदाहरण एथेरियम, एक्सआरपी हैं
- इसे नकली बनाना संभव नहीं है क्योंकि यह क्रिप्टोग्राफी द्वारा सुरक्षित है ।
- यह एक विकेन्द्रीकृत प्रक्रिया है इसलिए किसी के द्वारा नियंत्रित नहीं हैं।

- क्रिप्टोकरेंसी टैक्स फ्री होती हैं और इनका बीमा भी नहीं होता है।
- क्रिप्टोकरेंसी के लिए सरकार या बैंक जिम्मेदार नहीं हैं।
- कई देशों ने क्रिप्टोकरेंसी पर प्रतिबंध लगा दिया है।

क्रिप्टोकरेंसी कैसे काम करती है?

- यह ब्लॉक चेन तकनीक का उपयोग करता है।
- खरीदार और विक्रेता दोनों विवरण एक दूसरे बिना देखे और बिना किसी दलाल के ट्रांजेक्शन कर सकता है। उदाहरण के लिए यदि हमें शेयर बाजार से कोई शेयर खरीदना है तो हम ब्रोकर की मदद से इसे आसानी से कर सकते हैं। लेकिन क्रिप्टोकरेंसी में ऐसा नहीं होता है।
- क्रिप्टोकरेंसी में तीसरे व्यक्ति की भागीदारी की आवश्यकता नहीं है क्योंकि सभी लेनदेन एक सामान्य स्थान पर संग्रहीत होते हैं और इसे देखा जा सकता है। लेन–देन करने वाले व्यक्ति की पहचान एन्क्रिप्ट की गई है।

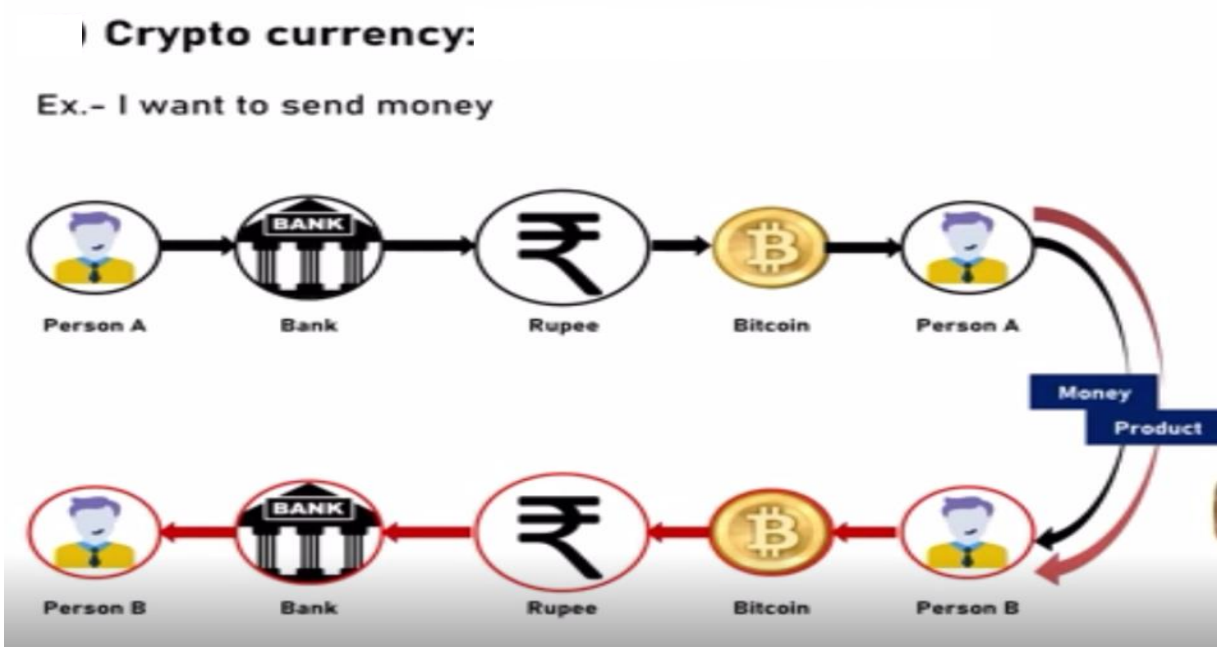


क्रिप्टोकरेंसी कैसे बनाई जाती है?

- अधिकांश क्रिप्टोकरेंसी माइनिंग नामक प्रक्रिया का उपयोग करके बनाई जाती हैं।
- खनन एक एल्गोरिथम के अलावा और कुछ नहीं है। यह ब्लॉकचेन लेजर में लेन–देन जोड़ने की प्रक्रिया है।
- नेटवर्क पर नोड्स के माध्यम से आम सहमति होने पर ही ट्रांजेक्शन को मान्यता प्राप्त होती है।
- सभी क्रिप्टोकरेंसी माइनिंग द्वारा नहीं बनाई जाती हैं। कुछ मुद्राएं विभिन्न अन्य टोकन जैसी तकनीक का उपयोग करके बनाई गई हैं।

क्या क्रिप्टोकरेंसी को नकद में परिवर्तित किया जा सकता है

उपरोक्त प्रश्न का उत्तर हां है। उदाहरण के लिए क्रिप्टोकरेंसी बिटकॉइन में से एक को क्रिप्टो एक्सचेंज पर नकद में एक्सचेंज किया जा सकता है। कॉइनबेस और क्रैकेन जैसे प्लेटफॉर्म हैं जो उपयोगकर्ताओं को डिजिटल पैसे को भौतिक नकदी में बदलने में मदद करते हैं।



क्रिप्टोकरेंसी कितनी सुरक्षित है?

- क्रिप्टोकरेंसी का उपयोग करके किए गए लेनदेन अत्यधिक सुरक्षित हैं।
- म्यूचुअल फंड या शेयर बाजार की तुलना में बड़ी रकम कमाने का मौका है लेकिन यह एक उच्च जोखिम के साथ आता है। क्योंकि क्रिप्टोकरेंसी की अस्थिरता बहुत अधिक है। या तो हम उच्च प्रतिफल अर्जित करते हैं या जो हमारे पास है उसे खो देते हैं।

क्या क्रिप्टो अवैध है?

यह एक देश से दूसरे देश में भिन्न होता है। कुछ देशों में यह कानूनी है और कुछ देशों ने इसे प्रतिबंधित कर दिया है। यू.एस. जापान और यू.के. जैसे कुछ सबसे विकसित देशों में क्रिप्टो कानूनी है। यह भारत जैसे विकासशील देश में भी कानूनी है लेकिन इसका कोई नियामक ढांचा नहीं है। अल्जीरिया, मोरक्को, नेपाल, पाकिस्तान जैसे देशऔर वियतनाम ने इस पर प्रतिबंध लगा दिया है।

क्रिप्टोकरेंसी का नुकसान क्या है?

- ✓ क्रिप्टोकरेंसी की सबसे बड़ी कमी में से एक इसकी सुरक्षा है।
- ✓ कई उदाहरण है जब एक्सचेंजों को हैक कर लिया गाया है और उन एक्सचेंजों में मुद्रा रखने वाले लोगों ने सब कुछ खो दिया है। बहुत से ऐसे लोग हैं जिनके पास कम अनुभव और ज्ञान है जिससे भारी नुकसान होता है।
- ✓ चूंकि यह पूरी तरह से डिजिटल है, इसलिए इसमें तकनीकी दिक्कतें हैं जैसे कि नेटवर्क की समस्या आदि।
- ✓ ग्लोबल वार्मिंग भी इसकी एक समस्या है।

इकाई–10

आईआईटीए, आईपीसी और एसएलएल के साथ अपराधों की मैंपिंग

भारतीय सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008 (आईआईटीए), भारतीय दण्ड संहिता, 1860 (आईपीसी), स्पेशल एवं लोकल लॉ (एसएसएल) के आधार पर अपराधिक मामलों में निम्न प्रकार से कानून की धारा व सजा व वर्णन किया गया हैः–

क्र0	शिकायत की प्रकृति	लागू धारा और दंड आईटीएए 2008 - के तहत	अन्य के तहत लागू धारा कानून और सजा
1.	खोया/चोरी मोबाइल फोन		धारा 379 आईपीसी 3 साल तक कारावास या जुर्माना या दोनों
2.	चोरी के कंप्यूटर/मोबाइल फोन /डेटा (डेटा या कंप्यूटर या मोबाइल प्राप्त करना अन्यथा आपके स्वामित्व वाला फोन किसी के हाथ में पाया जाता है	धारा 66 बी आईटीएए 2008] 3 साल तक कारावास या रुपये एक लाख जुर्माना या दोनों	धारा 411 आईपीसी 3 साल तक कारावास या जुर्माना या दोनों
3.	डेटा जिस पर किसी का अधिकारी है या कंपनी से डेटा को किसी भी रूप में चोरी करना।	आईटीएए 2008– की धारा 66 जिसमें 3 साल तक कारावास या जुर्माना पांच लाख रुपये तक या दोनों	धारा 379 आईपीसी 3 साल तक कारावास या जुर्माना या दोनों
4.	कपटपूर्ण उद्देश्य के लिए पासवर्ड चोरी और इस्तेमाल करना।	आईटीएए 2008–की धारा 66सी 3 साल तक कारावास या एक लाख रुपए जुर्माना धारा 66 डी आईटीएए 2008–3 साल तक कारावास या एक लाख रुपए जुर्माना	धारा 419 आईपीसी 3 साल तक कारावास या जुर्माना धारा 420 आईपीसी – 7 साल तक कारावास या जुर्माना
5.	पासवर्ड का उपयोग करके किसी के ईमेल को धोखे से पढना।	आईटीएए 2008 की धारा 66– 3 साल तक कारावास या जुर्माना पांच लाख रुपये तक जुर्माना या दोनों	

		आईटीएए की धारा 66सी 2008– 3 साल तक कारावास या एक लाख रुपए जुर्माना	
6.	बायोमेट्रिक थंब छाप का दुरुपयोग करना	आईटीएए की धारा 66सी 2008–3 साल तक कारावास या एक लाख रुपए जुर्माना	
7.	इलेक्ट्रॉनिक हस्ताक्षर/ डिजिटल हस्ताक्षर का दुरुपयोग करना	आईटीएए 2008–की धारा 66सी 3 साल तक कारावास या एक लाख रुपए जुर्माना	
8.	एक फिशिंग ई–मेल भेजना।	धारा 66 डी ITAA 2008– 3 साल तक की कैद या एक लाख रुपये जुर्माना या जुर्माना	धारा 419 आईपीसी – 3 साल तक कारावास या जुर्माना
9.	किसी व्यक्ति की इच्छा या ज्ञान के बिना उसके निजी क्षेत्र की छवि को खींचना या प्रकाशित करना या संचारित करना	आईटीएए 2008 की धारा 66 ई– 3 साल तक की कैद या दो लाख रुपये से अधिक का जुर्माना या दोनों	धारा 292 आईपीसी– 2 साल तक कारावास और 2000 रुपये जुर्माना और दूसरी बार अपराध पर 5 साल तक कारावास और 5000 रुपये जुर्माना
10.	कंप्यूटर स्रोत दस्तावेज के साथ छेड़छाड़	आईटीएए 2008 की धारा 65– 3 साल तक की कैद या दो लाख रुपये तक का जुर्माना या दोनों आईटीएए 2008 की धारा 66– 3 साल तक कारावास या पांच लाख रुपये तक जुर्माना या दोनों	
11.	डेटा संशोधन	ITAA 2008 की धारा 66– 3 साल तक की कैद या पांच लाख रुपये तक का जुर्माना या दोनों	
12.	संचार सेवा आदि के माध्यम से आपत्तिजनक संदेश भेजना		IPC की धारा 500 – 2 वर्ष तक कारावास या जुर्माना या दोनों धारा 504 आईपीसी – 2 साल

			तक कारावास या जुर्माना या दोनों धारा 506 आईपीसी – 2 साल तक कारावास या जुर्माना या दोनों अगर धमकी मौत या गंभीर चोट, आदि का कारण बनती है – 7 साल तक कारावास या जुर्माना या दोनों धारा 507 आईपीसी 506 आईपीसी के साथ – 2 साल तक कारावास या जुर्माना -धारा 508 आईपीसी – 1 – 1 साल तक कारावास या जुर्माना या दोनों धारा 509 आईपीसी 1 साल तक कारावास या जुर्माना या दोनों
13.	इलेक्ट्रॉनिक रूप में अश्लील सामग्री का प्रकाशन या संस्टेप	आईटीएए 2008 की धारा 67 – प्रथम बार 3 साल की सजा और 5 लाख तक जुर्माना दूसरी बार – 5 वर्ष तक सजा और 10 लाख तक जुर्माना	धारा 292 आईपीसी– 2 साल तक की कैद और 2000 रुपये जुर्माना और और दूसरी बार दोषसिी में 5 साल तक की सजा और 5000 रुपये जुर्माना
14.	बच्चों को चित्रित करने वाली इलेक्ट्रोनिक यौन सामग्री को प्रकाशित करना या उसका संस्टेप करना।	आईटीएए 2008 धारा 67 बी – पहली बार अपराध पर 5 वर्ष . तक की सजा और 10 लाख .तक जुर्माना दूसरी बार अपराध पर 7 साल की सजा और 10 लाख तक	धारा 292 आईपीसी– 2 साल तक की कैद और 2000 रुपये जुर्माना और और दूसरी बार दोषसिी में 5 साल तक की सजा और 5000 रुपये जुर्माना
15.	एक वाई–फाई कनेक्शन का दुरूपयोग करना यदि वह देश के विरूद्ध किया जावे।	आईटीएए 2008 की धारा 66 जिसमें – 3 साल तक की सजा और पाँच रुपये लाख तक जुर्माना या दोनों आईटीएए की धारा 66 एफ 2008 – आजीवन कारावास	

16.	राज्य के विरूद्ध ऐसा कार्य जिसमें कम्प्यूटर वायरस का रोपण किया गाया हो।	आईटीएए 2008 की धारा 66 जिसमें – 3 साल तक की सजा और पाँच रुपये लाख तक जुर्माना या दोनों आईटीएए की धारा 66 एफ 2008 – आजीवन कारावास	
17.	सरकारी कम्प्यूटर से विरूद्ध डिनायल ऑफ सर्विस आक्रमण करना।	आईटीएए 2008 की धारा 66 जिसमें – 3 साल तक की सजा और पाँच रुपये लाख तक जुर्माना या दोनों	
18.	राष्ट्रीय सुरक्षा के महत्त्व के किसी सरकारी कम्प्यूटर से डेटा की चोरी	आईटीएए की धारा 66 एफ 2008 – आजीवन कारावास	
19.	किसी प्राधिकारी को संचार को बाधित न करने देना जो उसके कम्प्यूटर या नेटवर्क से हो कर जाता है।	आईटीएए की धारा 69 2008 – कारावास 7 साल तक और जुर्माना	
20.	मध्यवर्ती द्वारा जिसके कम्प्यूटर में सूचना संग्रहित है उस तक वैध प्राधिकारी को पहुॅचे से रोकना।	आईटीएए की धारा 69 2008 – कारावास 7 साल तक और जुर्माना	
21.	जब किसी वेबसाइट को ब्लॉक करने का आदेश दिया गाया है और वह उसकी	आईटीएए की धारा 69 । 2008 – कारावास 7 साल तक जुर्माना	
22.	ईमेल के माध्यम से धमकी भरे संदेश भेजना।		धारा 504 आईपीसी – 2 साल तक कारावास या जुर्माना अथवा दोनों
23.	किसी महिला की मर्यादा को ठेस पहुचाने वाले ईशारे या कार्य करना।		धारा 509 आईपीसी – 1 साल तक कारावास या जुर्माना अथवा दोनों
24.	ईमेल के माध्यम से बदनाम करने वाले मेसेज भेजना।		धारा 500 आईपीसी – 2 साल तक कारावास या जुर्माना अथवा दोनों

25.	फर्जी वेबसाइट, साइबर धोखाधड़ी	धारा 66 डी आईटीएए 2008–3 वर्षों तक की सजा या एक लाख रुपये तक जुर्माना	धारा 419 आईपीसी – 3 साल तक कारावास या जुर्माना धारा 420 आईपीसी – 7 साल तक कारावास या जुर्माना
26.	ईमेल स्पूफिंग	धारा 66C आईटीएए 2008– 3 वर्षों तक की सजा कैद होना या एक लाख रुपये तक जुर्माना	धारा 465 आईपीसी – 2 साल तक कारावास या जुर्माना धारा 468 आईपीसी – 7 साल तक कारावास और जुर्माना
27.	झूठा डाक्यूमेंट बनाना	धारा 66 डी आईटीएए 2008– 3 वर्षों तक की सजा कैद होना या एक लाख रुपये तक जुर्माना	धारा 465 आईपीसी – 2 साल तक कारावास या जुर्माना
28.	धोखा देने का उद्देश्य से जालसाजी करना।	धारा 66 डी आईटीएए 2008– 3 वर्षों तक की सजा या एक लाख रुपये तक जुर्माना	धारा 468 आईपीसी – 7 साल तक कारावास और जुर्माना
29.	प्रतिष्ठा को नुकसान के लिए जालसाजी करना।	धारा 66 डी आईटीएए 2008– 3 वर्षों तक की सजा या एक लाख रुपये तक जुर्माना	धारा 469 . 3 साल तक कारावास और जुर्माना
30.	ईमेल पर गाली देना।		धारा 500 आईपीसी – 2 साल तक कारावास या जुर्माना
31.	आपराधिक धमकी		धारा 506 आईपीसी – 2 साल तक कारावास या जुर्माना या दोनों – यदि धमकी मौत का कारण हो या क्षतिकर आहत, आदि – 7 साल तक कारावास या जुर्माना अथवा दोनों
32.	कॉपीराइट उल्लंघन	धारा 66 आईटीएए 2008– 3 वर्षों तक की सजा कैद होना या 5 लाख	धारा 63, 63बी कॉपीराइट अधिनियम, 1957

33.	कंप्यूटर हार्डवेयर की चोरी		धारा 379 आईपीसी साल तक कारावास या जुर्माना अथवा दोनों
34.	नशीली दवाओं की ऑनलाइन बिक्री		एनडीपीएस अधिनियम
35.	हथियारों की ऑनलाइन बिक्री		आर्मस एक्ट

इकाई–11
फोरेंसिक अनुसंधान लैब सीसीपीडब्लूसी लैब का परिदृश्य एवं उसमें उपलब्ध टूल्स/साफ्टवेयर

सीसीपीडब्लूसी स्कीम–

महिलाओं व बच्चों के विरूद्ध साइबर अपराध (सीसीपीडब्लूसी) स्कीम के उद्देश्य–

देश में महिलाएं और बच्चे विरूद्ध होने वाले साइबर अपराधों से निपटने के लिए एक प्रभावी तंत्र का होना।

योजना के मुख्य घटक निम्नलिखित हैं–

1.ऑनलाइन साइबर अपराध रिपोर्टिंग इकाई

ऑनलाइन साइबर क्राइम रिपोर्टिंग पोर्टल सीसीटीएनएस परियोजना का एक केंद्रीय नागरिक पोर्टल है। साइबर क्राइम के शिकार लोगों द्वारा इस पोर्टल का उपयोग करके ऑनलाइन साइबर–अपराध शिकायत कर सकते हैं। जिसकी निम्नलिखित विशेषताएँ है–

- यह ऐसे सभी के लिए एक केंद्रीय भंडार प्रदान करेगा।
- साइबर अपराधों के संबंध में विश्लेषणात्मक रिपोर्ट उनके रुझान और उपचारात्मक उपाय आदि के बारे में तैयार की जावेगी। जिनका उपयोग वार्षिक प्रकाशित करने के लिए किया जाएगा। साइबर अपराधों के
- साथ ही साइबर अपराध सम्बंधित जानकारी के लिए राष्ट्रीय, राज्य और स्थानीय स्तर पर कानून प्रवर्तन और नियामक एजेंसियों के संदर्भ में यह इकाई के लिए एक केंद्रीय भंडार प्रदान करेगी।
- नागरिकों द्वारा इस पोर्टल पर ऑनलाइन शिकायत दर्ज की जा सकती है जिसमें दो आधार व शिकायत होती है। एक– महिलाओं व बच्चों के विरूद्ध होने वाले साइबर अपराधों के बारे में तथा दूसरी एक ऑनलाइन साइबर फ्राड के बारे में इस पर शिकायत होती है।
- शिकायत में गोपनीयता के लिए शिकायतकर्ता के लिए जरूरी नहीं की वह अपनी पहचाने बताए। इस लिए उससे मोबाइल नंबर जैसी आधारभूत जानकारी नहीं मॉगी जाती। जिसका उद्देश्य है कि महिलाओ और बच्चों के प्रति होने वाले साइबर क्राइम तक कानून प्रवर्तन एजेंसियों की ज्यादा से ज्यादा पहुॅच बढे।
- इस पोर्टल की वेबसाइट https://cybercrime.gov.in/ है जिस पर कोई भी नागरिक अपनी साइबर शिकायत ऑनलाइन दर्ज करा सकता है।
- इस पोर्टल से कई साइबर स्वयंसेवक भी जुडे हुए है।

2. फोरेंसिक यूनिट

आईटी अधिनियम और साक्ष्य अधिनियम के प्रावधान के तहत् राज्यों व केंद्र स्तर पर साइबर अपराध और इसके विश्लेषण के लिए संबंधित साक्ष्य का उचित संग्रह और संरक्षण हेतु 24 धण्टे सातों दिन यह लैब स्थापित की गई है। एक राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला संचालित होगी। इसमें सभी टूल सेटअप नवीनतम फोरेंसिक होंगे। इस यूनिट में विशद प्रकार के इलेक्ट्रॉनिक फोरेंसिक विश्लेषण करने के लिए पेशेवर साइबर सुरक्षा की टीम होगी। प्रयोगशाला सभी गहरे और उन्नत स्तरों की फोरेंसिक विश्लेषण के लिए कानून प्रवर्तन एजेंसियों की सहायता करेगी।

3. क्षमता निर्माण इकाई

यह इकाई सेंट्रल, राज्य पुलिस बल, अभियोजक, न्यायिक अधिकारी और अन्य सभी संबंधित हितधारक सभी के लिए आवश्यक साइबर अनुसंधान के लिए क्षमता निर्माण करेगी। इसका उद्देश्य दीर्घकालीन साइबर संबंधित विभिन्न प्रकार के कोर्सेज के माध्यम से क्षमता निर्माण हेतु प्रशिक्षण प्रदान करना है। इस योजना के तहत् तीन प्रकार के प्रशिक्षण कोर्स आयोजित किए जा रहे है। जिसमें 3 दिवसीय साइबर अपराधों के प्रति जागरूकता कोर्स और 5 दिवसीय अनुसंधान कोर्स शामिल है।

4.अनुसंधान एवं विकास इकाई

अश्लील सामग्री का पता लगाने और साइबर स्पेस में आपत्तिजनक सामग्री के लिए प्रभावी उपकरण विकसित करने के लिए निरंतर शोधन की आवश्यकता है। इसलिए, अनुसंधान और शैक्षणिक संस्थानों के साथ साझेदारी करने की आवश्यकता है। इन पहलों से प्रौद्योगिकी में सुधार करने में मदद मिलेगी और किसी भी तरह की स्थिति का सामना करने के लिए तैयार रहेंगे। साइबर अपराध गातिविधियों के अनुसंधान और विकास के लिए देश के कई हिस्सों में उत्कृष्टता केंद्र (सीओई) विकसित किये जावेंगे।

5. जागरूकता निर्माण इकाई

साइबर अपराधों के प्रति नागरिक जागरूकता की आवश्यकता है। इस हेतु भारत सरकार द्वारा कार्यक्रम आयोजित किये जाने का उद्देश्य रखा गाया है जिसमें साइबर अपराध के बारे में क्या करें और क्या न करें? की जानकारी नागरिकों के मध्य प्रसारित की जा रहीं है। इस पहल से नागरिक साइबर क्राइम और साइबर हाइजीन के प्रति जागरूक होंगें। इसके तहत् देश के स्कूलों में पढने वाले बच्चों व प्रौढ को लक्षित करके प्रचार किया जा रहा है। साइबर के मामलों में जागरूकता के इसी उद्देश्य से स्कूल पाठ्यक्रम के एक घटक के रूप में इसे सम्मिलित किया जा रहा है। इसी के तहत् @cyberdost नाम से ट्यूटर एकाउण्ट बनाया गाया है। साइबर अपराध और सुरक्षित रूप से उपयोग करने के तरीके के बारे में जानकारी वेब पोर्टल और मोबाइल ऐप के माध्यम से व्यक्ति को विभिन्न प्रकार के बारे में सूचित किया जा रहा है। जिसमें साइबर प्रौद्योगिकी के गलत उपयोग से खुद को बचाने के लिए जागरूकता अभियान जैसे एक दिवसीय कार्यशाला, निबंध, देश भर में कॉलेज स्तर और स्कूलों में भाषण प्रतियोगिता आदि का आयोजन किया जा रहा है। साइबर शिष्टाचार से संबंधित कार्यक्रम ब्रोशर, क्या करें और क्या न करें और पुरस्कार वितरित किए जा रहे है।

राजस्थान में सीसीपीडब्लू स्कीम के तहत् साइबर अपराध के मामलों में क्षमता निर्माण के लिए न्यायिक अधिकारियों, लोक अभियोजकों और पुलिस अधिकारियों हेतु प्रशिक्षण कार्यक्रम राजस्थान पुलिस अकादमी, जयपुर में किया जा रहा है। जिसके द्वारा प्रशिक्षण कार्यक्रम दिनांक 16.12.2020 से शुरू किये गये। इस योजना में कुल तीन प्रकार के प्रशिक्षण कोर्स का आयोजन किया जा रहा है। जिनका विवरण निम्न प्रकार से हैः–

- पुलिस अधिकारियों के लिए साइबर अपराधों के संबंध में जागरूकता 3 दिवसीय कोर्स।
- न्यायिक अधिकारियों व लोक अभियोजकों के लिए साइबर अपराधों के संबंध में जागरूकता 3 दिवसीय कोर्स।
- पुलिस अधिकारियों के लिए साइबर अपराधों के संबंध में अनुसंधान हेतु 5 दिवसीय कोर्स।

महिलाओं व बच्चों के विरूद्ध साइबर अपराध (सीसीपीडब्लूसी) लैब की स्थापना राजस्थान पुलिस अकादम, जयपुर में की गई है। जिसमें उक्त तीनों प्रकार के कोर्सेज का आयोजना किया जा रहा है।

इकाई–12
केस स्टडी–1

प्राथमिकी का GIST: –

अरूणाचल पुलिस एक महिला से लिखित शिकायत प्राप्त हुई कि उसकी चचेरी बहन के इंस्ट्राग्राम अकाउण्ट से किसी ने उसकी फोटो ले कर उनमें कॉटछॉट करके उसकी अन्य लोगों के साथ नकली नग्न तस्वीरें बनाई गई। जिसे ''देशीमशाला बोर्ड'' नामक अश्लील वेबसाइट पर अपलोड किया गाया है। इससे पीड़िता को असहनीय मानसिक आघात पहुंचा था और इस प्रकार वह अपनी शिकायतों के निवारण के लिए आई थी।

तदनुसार, अपराध शाखा पुलिस स्टेशन की प्राथमिकी संख्या 09/2021 U/S 292(2)()/509 IPC R/W धारा 6 के तहत महिलाओं का अश्लील प्रतिनिधित्व (निषेध) अधिनियम, R/W Sec- आईटी अधिनियम के 67 (ए) पंजीकरण किया गाया।

गॉडफादर नाम की प्रोफाइल वेबसाइट https://desimasalaboard.org की मॉडरेटर/एडमिन है। उक्त प्रोफाइल में तीन ईमेल आईडी अर्थात dmbgodfather@gmail.com, तथा tmfsupport@gmail.com व admin@desimasalaboard.com शामिल हैं।

साइबर विशेषज्ञों और उन्नत डिजिटल साक्ष्य संग्रह तकनीकों का उपयोग किया गाया और पाया गाया कि dmbgodfather@gmail-com और tmfsupport@gmail-com खाते श्री अविनाश वर्मा, आयु 37 वर्ष, पुत्र श्री राजेंद्र प्रसाद वर्मा, R/OH/No के हैं। 3ई–108 दयानंद नगर, नेहरू नगर III, ब्लॉक ई, गाजियाबाद, उत्तर प्रदेश। उन्होंने मोबाइल नंबर 99''''''22 का इस्तेमाल गूगल, फ्लिपकाट्र, ओला कैब, स्विगी और एमेजॉन अकाउंट बनाने के साथ–साथ देसीमसाला के ट्विटर अकाउंट के लिए किया है।

अनुसंधान–

आरोपी श्री अविनाश वर्मा के वर्तमान स्थान के साथ–साथ घर के पते का पता लगाने के बाद, सीजेएम युपिया की अदालत से एक गैर–जमानती वारंट और तलाशी वारंट प्राप्त किया गाया था और इंस्पेक्टर चपांग लोवांग, एसआई वोकिम मुंगरे, सीटी के नेतृत्व में एक चार सदस्यीय एसआईटी टीम थी। जीएल रे और सीटी। संजीव कुमार ने एनसीआर क्षेत्र में जाकर आरोपी श्री अविनाश वर्मा को एक्सोटिका ड्रीमविले, गौर सिटी 2, नोएडा, उत्तर प्रदेश से गिरफ्तार किया और ट्रांजिट रिमांड पर अपराध शाखा पुलिस स्टेशन, (एसआईटी) पीएचक्यू ईटानगर लाया।

- तलाशी के दौरान एक एपल मैकबुक और एक आईफोन मोबाइल हैंडसेट जब्त किया गाया।

पूछताछ–

आरोपी अविनाश वर्मा ने स्वीकार किया कि वह अश्लील वेबसाइट 'देसीमासालबोर्ड' का मालिक है और सामग्री अपलोड करने वाले 'गॉडफादर' नाम का सुपर मॉडरेटर भी है।

वह 2018 से इस वेबसाइट को इसके एकमात्र मालिक के रूप में चला रहा है। पीड़ित की मॉफ़्ड तस्वीरें जनवरी 2019 में अपलोड की गई थीं।

वेबसाइट के पास विभिन्न श्रेणियों जैसे नग्न लड़कियों की छवियों, अश्लील वीडियो आदि की सामग्री तक पहुंच है।

बिजनेस मॉडल– वह तीन स्रोतों से पैसा कमाता है –

- अतिथि ग्राहकों को प्रीमियम या प्लैटिनम सदस्य बनाकर उनसे डिजिटल वॉलेट प्लेटफॉर्म Razorpay पर AVIFITNESS के खाते में सदस्यता शुल्क के नाम से राशि जमा कराता था।
- वह अपने वेबपेज पर Juicyads-com व अन्य वेबसाइट से विज्ञापनों को होस्ट करता था जिसके बदले में Crypto.com और Coinbase प्लेटफॉर्म पर एक वॉलेट में बिटकॉइन क्रिप्टोकरेंसी के रूप में पैसा मिलता है।
- वह ऑनलाइन लेखों की बिक्री और खरीद के विज्ञापन के माध्यम से भी कमाता है जो वेबसाइट में विज्ञापन साइटों से संबंधित हैं, जिसे वह कॉइनबेस के में प्राप्त करता था।

केस स्टडी–2
अर्न्तराज्यीय नकली सिम अपराध

एफआईआर का संक्षिप्त परिचयः–

- पीडित की फेसबुक आईडी से को अपने कब्जे में लिया गाया।
- पीडित की फेसबुक आईडी के माध्यम से रूपयों की मॉग की गई तो पीडित के दोस्तों ने उसे सूचित किया कि कोई पेटीएम खाते में 10000 रुपये की मांग कर रहा है।
- पूछताछ में पता चला कि पेटीएम खाते के लिए इस्तेमाल किया गाया नंबर बल्क सिम खरीद का हिस्सा था

अपराध की मोडस ओपेरेंडीः–

- फर्म पंजीकरण दस्तावेजों का उपयोग करके टीएसपी कर्मचारी द्वारा थोक में कई सिम जारी करने करवाकर उन्हे सक्रिय किया गाया था।
- **आयुष्मान योजना** के तहत लिए गए निर्दोष ग्रामीणों के बायोमेट्रिक और फोटो का लेकर उनका इस्तेमाल पेटीएम खाता खोलने और उन सभी सिम को सक्रिय करने के लिए किया गाया।
- उन सक्रिय सक्रिय UPI वाले सिम को सोशल मीडिया समूहों के माध्यम से थोक में बेचा गाया।

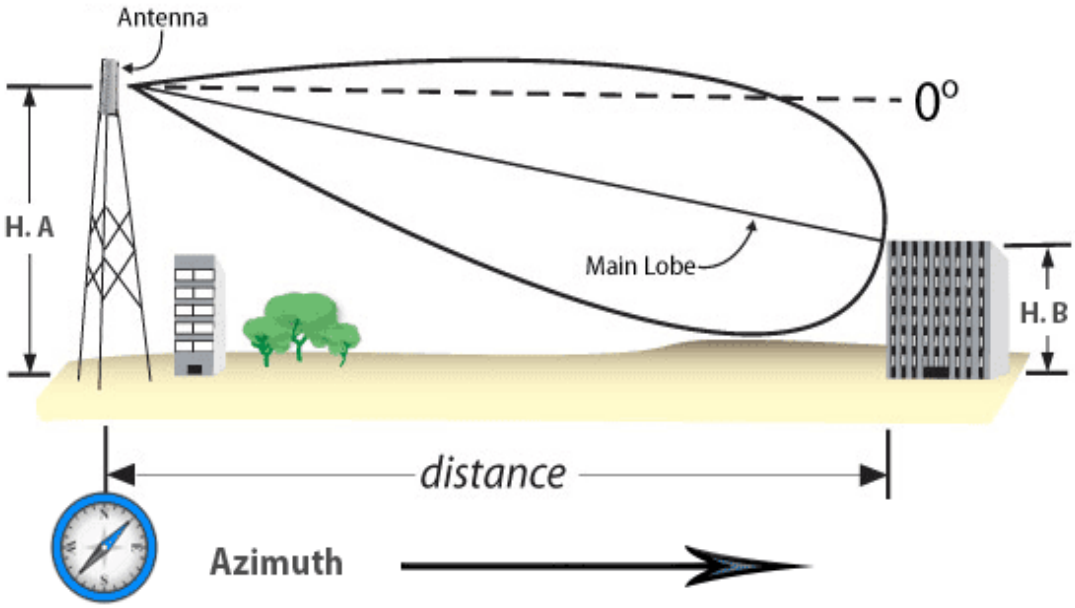
अनुसंधान की चुनौतियॉः–

- जिन ग्रामीणों के नाम से सिम बना कर यूपीआई को रजिस्टड्र किया गाया था उन सब को इसके बारे में कोई जानकारी नहीं थी।
- जिस रिटेलर ने सिम को इश्यू किया था उस पते पर अब कोई नहीं था।
- जबलपुर क्षेत्र से इश्यू हुई इन सभी सिम का उपयोग देश के विभिन्न हिस्सों मे किया जा रहा था।
- जो मोबाइल थे उनकी आईएमईआई के आधार पर जॉच की तो पता चला कि उन पर कोई कॉल नहीं आई थी न ही की गई थी केवल मेसेजों का आदान प्रदान हुआ था।
- जो यूपीआई बने थे वे सब निर्दोष ग्रामीणों के नाम पर बने थे।
- संदिग्धों के बारे में टॉवर लोकेशन के अलावा अन्य कोई क्लू नहीं था।

अनुसंधान की दिशाः–

कैफ	पेटीएम नंबरों की मोबाइल कंपनी से कैफ, सीडीआर और आईएम आई प्राप्त की गई। 89 नंबरों की कैफ प्राप्त की गई। संदिग्ध सिम 4 आईएमआई नंबरों पर चली थी।
सीडीआर	इन सिम की सीडीआर प्राप्त की गई। जिसमें देखा की ये

	सिम 21 आईएमईआई नंबरों को डिटेक्ट किया गाया। जिसकी आगे सूचना प्राप्त की गई तो इन 21 आईएमईआई नंबरों से कुल 10000 सिम चलाई गई थी। सभी नंबर जबलपुर में सक्रिय किए गए थे जो देश के विभिन्न हिस्सों में उपयोग किए जा रहे थे।
संदिग्ध आईएमईआई	उन आईएमईआई की टावर लोकेशन एक घनी आबादी में आ रही थी। कोण का ढलान, टॉवर लोकेशन ऐप और अजीमुथ के आधार पर लोकेशन तय की गई थी।



कोण का झुकाव व अजीमुथ

टावर लोकेटर ऐप

अनुसंधान की अन्य दिशाः–

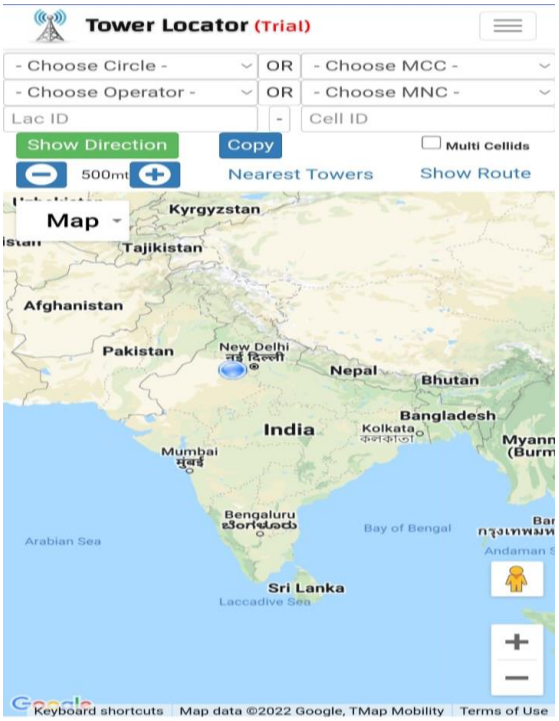
- संदिग्ध IMEI के पास UPI सक्रिय हुए फ़ोन नंबर थे
- सभी खाताधारकों को अपने पेटीएम सक्रियण के बारे में जानकारी नहीं थी, लेकिन सभी ने आयुष्मान योजना के लिए एक ही व्यक्ति द्वारा पंजीकरण कराया था।
- आयुष्मान एजेंट और टीएसपी एजेंट मुख्य संदिग्ध से जुड़े थे जो सिम रैकेट का हिस्सा था।
- संदिग्ध फेसबुक ग्रुप का हिस्सा था जो विभिन्न राज्यों के अन्य ऑपरेटरों से सिम बेचता और प्राप्त करता था।
- कई अतिरिक्त सीएएफ का उपयोग बल्क सिम जारी करने के लिए किया गाया पाया गाया
- 8500 से अधिक सिम सक्रिय पाए गए और अन्य राज्यों में भेजे गए।

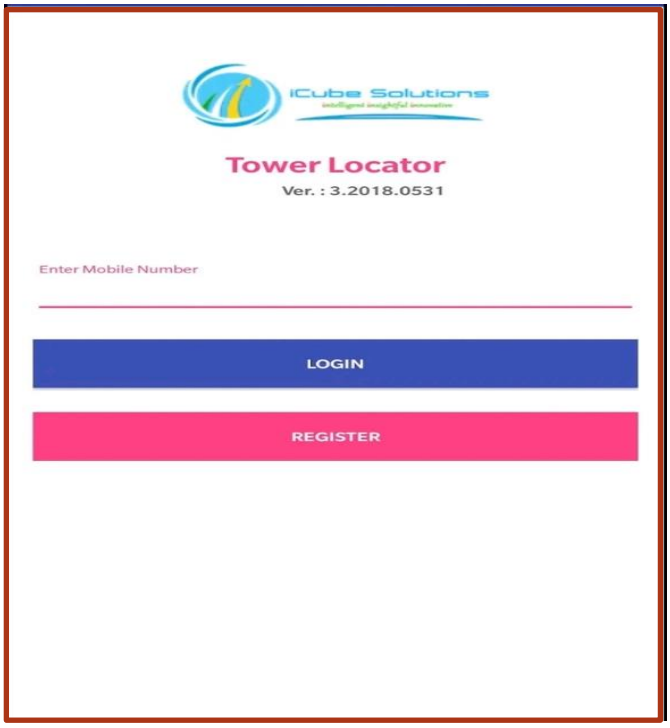
वे साफ्टवेयर व टूल्स जिनका उपयोग किया गायाः–

सीडीआर विश्लेषण	आई क्यूब सोल्यूशन का I9 साफ्टवेयर komlab
सीसीटीएलएस	डेटा शेयरिंग आईसीजेएस पोर्टल
संदिग्ध लोकेशन	आई क्यूब सोल्यूशन का टॉवर लोकेटर

अनुसंधान का प्रभावः–

- अनुसंधान के बाद टीएसपी द्वारा 8500 संदिग्ध सिम और 2470 पेटीएम खाते निष्क्रिय कर दिए गए।
- टीएसपी के कर्मचारी फर्मों के झूठे पते का सत्यापन करके व्यवस्थित रूप से बल्क सिम जारी कर रहे थे, इस घोटाले में टीएसपी के 2 कर्मचारियों के अलावा 3 अन्य को गिरफ्तार किया गाया था।
- फेसबुक ने सिम ट्रांसकेशन के लिए 1 लाख लोगों वाले ग्रुप को निष्क्रिय कर दिया जिससे इंटर स्टेट नेटवर्क की रीढ़ टूट गई।
- अन्य राज्यों के एलईए ने पाया कि कई साझा नंबरों का इस्तेमाल अपराध करने के लिए किया जा रहा है, वे जांच के लिए जबलपुर पहुंचे और जानकारी साझा की।
- अपराध की रोकथाम – हजारों संभावित अपराध टल गए, निर्दोष नागरिकों को बचाया गाया।


Tower Locator (Trial)
- Choose Circle -
OR
- Choose MCC -
- Choose Operator -
OR
- Choose MNC -
Lac ID
-
Cell ID
Show Direction
Copy
Multi Cellids
500mt
Nearest Towers
Show Route
Map
Kyrgyzstan
Tajikistan
Afghanistan
Pakistan
New Delhi
नई दिल्ली
Nepal
Bhutan
Bangladesh
India
Kolkata
কলকাতা
Mumbai
मुंबई
Bengaluru
Arabian Sea
Bay of Bengal
Sri Lanka
Laccadive Sea
Keyboard shortcuts
Map data ©2022 Google, TMap Mobility
Terms of Use


iCube Solutions
Tower Locator
Ver. : 3.2018.0531
Enter Mobile Number
LOGIN
REGISTER

केस स्टडी–3
अन्तर्राष्ट्रीय क्रिप्टोकरेंसी रेकेट

- एक युवा व्यवसायी ऑनलाइन डेटिंग ऐप **बम्बल** के जरिए कथित तौर पर विदेशी मूल की एक महिला के सम्पर्क में आया, जिसका नाम "डोरिस^था।
- महिला ने खुद को एक व्यवसाय और अर्थशास्त्र विश्लेषक होने का दावा किया और युवा व्यवसायी को फ़िशिंग वेबपेज के माध्यम से मसालों के व्यापार में निवेश करने के लिए फंसाया, जिसका डैशबोर्ड बिना किसी वास्तविक लेनदेन के लाइव था।
- व्यवसायी ने विभिन्न खातों में ऑनलाइन पैसे ट्रांसफर किए।
- जब व्यवसायी ने लाभ बुक करने की कोशिश की, तो उसे पता चला कि वेबसाइट दुर्भावनापूर्ण है और लाइव UI के साथ डैशबोर्ड नकली है
- लगभग 01 करोड़ रूपयों की दिल्ली, गुरुग्राम और राजकोट स्थित 05 नकली कंपनियों के चालू खाते में संदिग्धों द्वारा ठगी की गई।

अनुसंधानः–

- चीनी नागरिकों के अनुरोध पर सीए और सीएस के सिंडिकेट द्वारा बनाए गए बैंक खातों का उपयोग करके शेल कंपनियों का पता लगाया गाया था।
- इन शेल कंपनियों के खातों से, भारत के विभिन्न हिस्सों से संचालित क्रिप्टो डीलरों को धोखाधड़ी के पैसे ट्रांसफर किए जा रहे थे, जिन्होंने इस पैसे को क्रिप्टोकरेंसी में बदल दिया और ट्रांसफर कर दिया।
- क्रिप्टो एक्सचेंजों से प्राप्त जानकारी से, उपरोक्त क्रिप्टोकरेंसी के लाभार्थी की पहचान एक पाकिस्तानी नागरिक के रूप में की गई थी।
- मास्टरमाइंड, कथित तौर पर चीनी था जो, एक राष्ट्रीय और एक अंतर्राष्ट्रीय क्रिप्टो करेंसी एक्सचेंज में स्थित 04 क्रिप्टो वॉलेट की मदद से भारतीय सीमाओं के बाहर से सभी मॉड्यूल को नियंत्रित कर रहा था।
- दिल्ली, गुरुग्राम और राजकोट से 07 आरोपित गिरफ्तार, अभी और गिरफ्तारियां, जांच अभी जारी

अपराध के माड्यूलः–

इस अपराधों को पॉच माड्यूल के द्वारा अंजाम दिया गाया। जो है–

- दिल्ली व एनसीआर मोड्यूल–सीए और सीएस के सिंडीकेट के द्वारा जो शेल कंपनिया बनाई वे सब 6 से 8 घण्टे पहले अपने रिश्तेदारों और अप्रवासी मजदूरो के नाम से बनाई। शेल कंपनियॉ बना कर उसकी सूचना मास्टरमाईण्ड चीनी नागरिक को दी गई।
- पाकिस्तानी माड्यूल– पाकिस्तानी क्रिप्टो व्यवसायी द्वारा प्राप्त की गई अपराध की राशि को क्रिप्टो में परिवर्तित किया गाया।
- गुजरात माड्यूल– कुछ शेल कंपनियों को फर्जी नाम, पते व ईमेल आईडी, बैंक खाते के साथ गुजरात में खोला गाया। इनके द्वारा अपराध की राशि को क्रिप्टो में परिवर्तित करने के लिए आगे भेजा गाया।

- क्रिप्टोक्यूरेंसी मॉड्यूल–भारत के विभिन्न हिस्सों (गुजरात मजस्थान, चंडीगढ़, तमिलनाडु आदि) से संचालित होने वाले डीलरों का उपयोग किंगपिन द्वारा क्रिप्टोकुरेंसी एक्सचेंजों (भारतीय क्रिप्टोकुरेंसी एक्सचेंज वज़ीरक्स और टैक्स हेवन केमैन आइलैंड्स में क्रिप्टोकुरेंसी एक्सचेंज बिनेंस सहित) के माध्यम से धन को लूटने के लिए किया जा रहा था वे भारत स्थित एक्सचेंज वज़ीरक्स और टैक्स हेवन केमैन आइलैंड्स में क्रिप्टोकरेंसी एक्सचेंज बिनेंस थे।

सीडीआर/आईपीडीआर द्वारा अनुसंधान–

- 60 से अधिक सीडीआर का विश्लेषण किया गाया।

- संदिग्ध/अभियुक्तों के बीच संबंध स्थापित करना और संदिग्धों के बारे में जानकारी प्राप्त करना जो अपराधियों के खिलाफ पुख्ता सबूत हो सकते हैं यह एक चुनौति थी।
- भारतीय मोबाइल नंबरों का इस्तेमाल विदेशी व्हाट्सएप संचार के लिए भारतीय नागरिकों के रूप में छिपाने के लिए किया जाता था।
- आरोपियों ने कई हैंडसेट का इस्तेमाल किया। उनके बीच संबंध स्थापित करना भी चुनौतीपूर्ण था।
- विभिन्न सेवाओं के आईएसपी से कई आईपीडीआर ली गई जैसे भुगतान वॉलेट, ईमेल क्लाइंट, व्हाट्सएप, इंटरनेट बैंकिंग और क्रिप्टो वॉलेट।
- अपराधी अपनी असली पहचान छिपाने के लिए वीपीएन/प्रॉक्सी सर्वर का इस्तेमाल कर रहे थे और उनकी पहचान उजागर करना एक मुश्किल काम था

बैंक खाता और क्रिप्टो वालेट–

- बहुत कम समय में हजारों लेनदेन में शामिल कई शेल कंपनियों के बैंक खाते। जिसमें एकाधिक प्रेषक और लाभार्थी शामिल थे।
- 30–35 करोड़ के लेन–देन संदिग्ध थे
- इंटरनेट बैंकिंग सुविधा का उपयोग करके ट्रांसफर किया गाया था और ट्रांसफर मोड आईएमपीएस/एनईएफटी और यूपीआई था।
- आईपीडीआर विश्लेषण ने वास्तविक अपराधी का पता लगाने में महत्वपूर्ण भूमिका निभाई।
- कपटपूर्ण धन का उपयोग क्रिप्टो मुद्रा (बिनेंस और वज़ीरएक्स जैसे एक्सचेंजों पर) खरीदने के लिए किया गाया था जिसे अंततः चीन और पाकिस्तान में स्थानांतरित कर दिया गाया था।
- भारतीय बैंक खातों का प्रबंधन चीनी नागरिकों द्वारा उनके वर्तमान बैंक खातों की इंटरनेट बैंकिंग पहुंच प्राप्त करके किया गाया था।

ईमेल अनुसंधान–

- विभिन्न बैंक खातों, मनी वॉलेट और संचार के लिए एकाधिक ईमेल आईडी का उपयोग किया गाया था।
- उनसे लिंक किए गए मोबाइल, कनेक्टेड मोबाइल/फोन उपयोगकर्ताओं के नाम और आईपी विवरण का पता लगाना चुनौती थी।
- गिरफ्तार आरोपियों का ईमेल बैकअप बनाया गाया और पूछताछ के दौरान जब्त कर लिया गाया, यह भी चीनियों की संलिप्तता की ओर इशारा करता है

सफलता–

- क्रिप्टो एक्सचेंजों और सोशल मीडिया क्रॉलिंग टूल की जानकारी का उपयोग पाकिस्तानी नागरिक की पहचान सुनिश्चित करने के लिए किया गाया था।
- उपरोक्त जानकारी का उपयोग पहचाने गए पाकिस्तानी नागरिक के खिलाफ अकाट्य दस्तावेजी साक्ष्य प्राप्त करने के लिए किया गाया था।
- पहली बार साक्ष्य एक सप्ताह से भी कम समय में, एक टैक्स हेवन (केमैन द्वीप) से एमएलएटी/एलआर का सहारा लिए बिना प्राप्त किया गाया था।

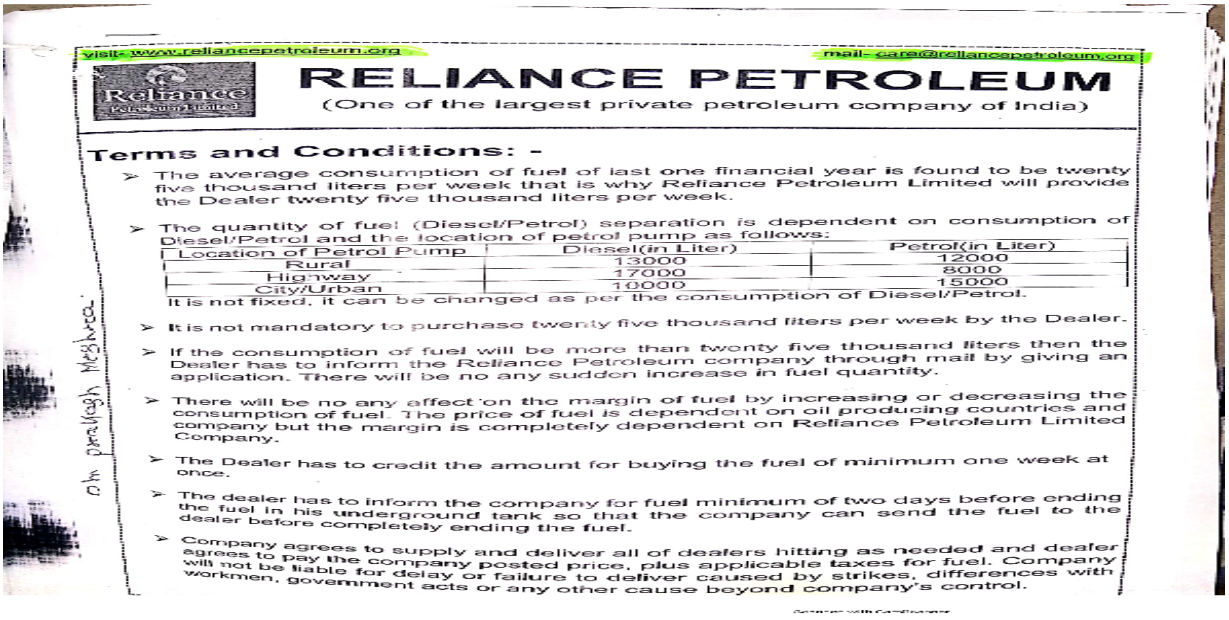
केस स्टडी–4
रिलायंस पेट्रोल पंप के लिए फर्जी डीलरशिप

शिकायतकर्ता – श्री ओमप्रकाश मिश्रा आयु 37 वर्ष, पुत्र प्रमोद कुमार मिश्रा निवासी ग्राम/पी.ओ. / पी.एस. भुबन, जिला. ढेंकनाल

शिकायत की तिथि – 03.01.2019

संक्षिप्त विवरण –

उन्होंने एक पेट्रोल पंप की डीलरशिप के लिए दिनांक 01.11.2018 को रिलांयस कंपनी की वेबसाइट releasepetroleum.org के माध्यम से आवेदन किया। दिनांक 02.11. 2018 को पुष्टि के संबंध में care@releasepetroleum.org से मेल हुआ। उन्हें विभिन्न मामलों में पेट्रोल पंप, एनओसी आवेदन शुल्क, लाइसेंस शुल्क, बीमा शुल्क, सुरक्षा जमा शुल्क और क्रेडिट जमा शुल्क के लिए पंजीकरण शुल्क का भुगतान करने के लिए कहा गाया था। विभिन्न नंबरों से कॉल पर आरटीजीएस के माध्यम से विभिन्न बैंकों के खातों के माध्यम से दिनांक 12.11.2018 से 28.12.2018 के मध्य 40,45,000/– (पैंतालीस लाख पैंतालीस हजार) रूपये की ठगी की गई।



visit- www.reliancepetroleum.org mail- care@reliancepetroleum.org

Reliance Petroleum Limited

RELIANCE PETROLEUM

(One of the largest private petroleum company of India)

Terms and Conditions: -

- The average consumption of fuel of last one financial year is found to be twenty five thousand liters per week that is why Reliance Petroleum Limited will provide the Dealer twenty five thousand liters per week.
- The quantity of fuel (Diesel/Petrol) separation is dependent on consumption of Diesel/Petrol and the location of petrol pump as follows:

Location of Petrol Pump	Diesel(in Liter)	Petrol(in Liter)
Rural	13000	12000
Highway	17000	8000
City/Urban	10000	15000

It is not fixed, it can be changed as per the consumption of Diesel/Petrol.

- It is not mandatory to purchase twenty five thousand liters per week by the Dealer.
- If the consumption of fuel will be more than twenty five thousand liters then the Dealer has to inform the Reliance Petroleum company through mail by giving an application. There will be no any sudden increase in fuel quantity.
- There will be no any affect on the margin of fuel by increasing or decreasing the consumption of fuel. The price of fuel is dependent on oil producing countries and company but the margin is completely dependent on Reliance Petroleum Limited Company.
- The Dealer has to credit the amount for buying the fuel of minimum one week at once.
- The dealer has to inform the company for fuel minimum of two days before ending the fuel in his underground tank so that the company can send the fuel to the dealer before completely ending the fuel.
- Company agrees to supply and deliver all of dealers hitting as needed and dealer agrees to pay the company posted price, plus applicable taxes for fuel. Company will not be liable for delay or failure to deliver caused by strikes, differences with workmen, government acts or any other cause beyond company's control.

Om Prakash Mishra

अनुसंधान–

- शिकायतकर्ता की परीक्षा
- गवाहों की परीक्षा
- शिकायतकर्ता से दस्तावेजों की जब्ती
- गवाहों से दस्तावेजों की जब्ती
- कथित वेबसाइट www.releasepetroleum.org की होस्टिंग सर्वर विवरण के लिए who.is पर जॉच की।
- कथित वेबसाइट www.releasepetroleum.org की वर्तमान स्थिति तथा कब बनाई गई की जाँच की गई "Archive-org" पर की गई।

बैंक और मोबाइल सेवा प्रदाताओं से प्राप्त की गई सूचना–

- धोखाधड़ी करने वालों के खाते के संबंध में खाता खोलने के फॉर्म, लेनदेन विवरण और अन्य प्रासंगिक जानकारी प्रस्तुत करने के लिए केनरा बैंक और सेंट्रल बैंक ऑफ इंडिया को धारा 91 सीआरपीसी के तहत नोटिस दे कर प्राप्त की गई।
- मोबाइल सेवा प्रदाता से उस सेल नंबर का सीएएफ जिसके द्वारा आरोपी व्यक्ति ने पीड़ित के साथ संवाद किया।

अन्य पत्राचार

- शिकायतकर्ता के मोबाइल नंबर के संबंध में सीडीआर, एसडीआर और सीएएफ के लिए मोबाइल सेवा प्रदाता (AIRTEL, IDEA) और साथ ही उस सेल नंबर से जहां आरोपी व्यक्ति ने शिकायतकर्ता के साथ संचार किया था।
- धारा 91 सीआरपीसी से डोमेन रजिस्ट्री Godaddy.com से फर्जी वेबसाइट **www.reliancepetroleum.org** जो फर्जी वेबसाइट का होस्टिंग सर्वर है, जानकारी प्राप्त की गई।
- कानूनी जांच सहायता, Google Inc 1600, एम्फीथिएटर पाक्रवे, माउंटेन व्यू, CA 94043, USA को सीआरपीसी के तहत रिलायंस पेट्रोल पंप के नाम से बनाई गई फर्जी मेल आईडी यानी **petroleumreliance@gmail.com** के संबंध में नोटिस।
- सूचना और विश्लेषण – GODADDY की रिपोर्ट
- लेनदेन इस प्रकार हुआ– भारतीय रुपया (INR) भुगतान 1,452.50
- भुगतान किया गाया डेबिट कार्ड (ट्रांस आईडी CCAFJ7BGB111) प्रोसेसर CCAvenue_GD_INR
- प्रकार डेबिट कार्ड प्रोसेसर CCAvenue&GD_INR_CCAvenue Ref#: 1377800190_I_1452-50_INR_0_19749384 6
- अतिरिक्त जानकारी वीज़ा की प्राप्त की गई।
- गोडैडी की रिपोर्ट के विश्लेषण के दौरान, यह पता चला कि आरोपी व्यक्तियों ने 9/18/2018 समय 6:25:20 बजे मोबाइल नंबर+91 8768758042 (पश्चिम बगल वोडाफोन) और रिकवरी ई– मेल आईडी jiotower007@gmail.com का उपयोग करके फर्जी वेबसाइट बनाई थी। साथ ही आरोपी ने दिनांक 18.09.2018 को CCAVENUE पेमेंट गेटवे साइट का उपयोग करके गो डैडी में वेबसाइट बनाने के लिए 1452.50/– रुपये भी दिए थे। ।

सूचना और विश्लेषण –

Google की रिपोर्ट

google.Inc की ओर से ईमेल आईडी– petroleumrelease@gmail-com के संबंध में GOOGLE सब्सक्राइबर जानकारी

- नामः reliance petroleum dealership

- ई–मेलः petroleumreliance@gmail.com
- स्थितिः Enabled
- Recovery e-Mail: jiotower007@gmail.com
- बनाने की दिनांक व समयः 2018/10/24-16:34:36-UTC
- Terms of Service IP: 157.35.244.244, on 2018/10/24-16:34:36-UTC Language Code: en_GB SMS: +916205957653 [IN]

विश्लेषण के दौरान, यह पता चला कि आरोपी व्यक्तियों ने मोबाइल नंबर–6205957653 (बिहार रिलायंस जियो) और रिकवरी ई–मेल आईडी: jiotower007@gmail-com का उपयोग करके 24.10.2018 को फर्जी ईमेल आईडी यानी **petroleumreliance@gmail.com** बनाया है।

Correspondence with CC Avenues India Pvt. Ltd. Address : Plaza Asiad, Level II, S.V.Road, Santa Cruz, Mumbai

- गोडैडी में नकली वेबसाइट www-releasepetroleum.org की खरीद के संबंध में जानकारी प्रस्तुत करने के लिए यू/एस 91 सीआरपीसी से सीसी एवेन्यू को उनकी मेल आईडी– risk@ccavenue.com, service@ccavenue.com पर भेजें।
- नीलेश पालकर, सीनियर एग्जीक्यूटिव – रिस्क, –इन्फीबीम सीसी एवेन्यूज लिमिटेड प्लाजा की रिपोर्ट। जवाब दिया कि लेनदेन आईसीआईसीआई बैंक डेबिट कार्ड का उपयोग करके संसाधित किया गाया है। किसी भी अतिरिक्त विवरण के लिए, कृपया आईसीआईसीआई बैंक से सम्पर्क करें।

Google से प्राप्त मोबाइल नंबर 6205957653 के संबंध में CDR, SDR और CAF के लिए मोबाइल सेवा प्रदाता (Jio) को पत्र।

जीओ से प्राप्त सूचना का विश्लेषण–

- SDR (Subscriber Detailed Report) का संबंध Hidanand Singh, S/O-Brijnandan Singh, At.kanai, Po-Dhrubdihan, Dist.kanal Bhojpur, State-Bihar से था।
- मोबाइल नंबर 6205957653 की सीडीआर का विश्लेषण किया गाया तो उक्त मोबाइल नंबर दिनांक 04.01.2019 से बंद था।
- मोबाइल की आईएमईआई नंबर 868645044104100 और 868645044104118 थे तथा मोबाइल हैंडसेट एमआई कंपनी का था।
- अंतिम लोकेशन बिहार की थी।

अन्य मोबाइल नंबरों की अंतिम लोकेशन का विश्लेषण किया गाया तो मोहाली, पंजाब आई।

मोहाली पंजाब में अनुसंधान–

- टीम टगेरी इलाके के लिए रवाना हुई।
- शहीद उधम सिंह कॉलेज, टगेरी, मोटेमरजा, मोहाली, पंजाब के अंदर मोबाइल फोन का पता लगाया।
- साथ ही लड़का श्रेयंस श्री, पुत्र अजीत कुमार झा, अत–खजुर्बना, महेंद्रू, पटना, बिहार, बीटेक कंप्यूटर साइंस प्रथम वर्ष का अध्ययन कर रहा था, जो उक्त मोबाइल फोन का उपयोग कर रहा था।
- श्रेयंस का यू/एस–161 सीआरपीसी दर्ज किया गाया था – उसे आकाश की गातिविधि पर संदेह है कि आकाश ने बहुत पैसा खर्च करता है और एक अच्छे अपाट्रमेंट में रहता है लेकिन वह कुछ भी नहीं करता है। श्रेयंस कहता है कि उसे आकाश के स्थायी पते के बारे में पता नहीं है, केवल यह जानता है कि वह नालंदा जिले से ताल्लुक रखता है। श्रेयंस ने आकाश कुमार का मोबाइल नंबर 7488141389 दिया
- निम्नलिखित विनिर्देश वाले बैटरी इनबिल्ट के साथ सुनहरे रंग के मोबाइल फोन की जब्ती–मेक–एमआई, आईएमईआई– 868645044104100, 86864504410418.

बिहार में अनुसंधान–

- आईओ पटना, बिहार के लिए रवाना हुआ।
- मोबाइल नंबर –7488141389 23.11.2019 से बंद था।
- आईएमईआई खोज – शून्य परिणाम।
- मोबाइल नंबर–7488141389 के सीडीआर का विश्लेषण ZOMATO से खाना मंगवाया
- डिलीवरी पता और आईपी विवरण प्रदान करने के लिए ZOMATO नोडल अधिकारी के साथ पत्राचार।
- डिलीवरी का पता – सिद्धार्थ प्राची अपाट्रमेंट, जगदेवपथ, हवाई अड्डा पीएस, पटना, बिहार।
- छापेमारी 28–29.11.2019 की देर रात की गई थी।
- आकाश और उसके दोस्त शुभम प्रियदर्शी दोनों गिरफ्तार।

दोनों आरोपियों से बरामदगी–

- मोबाइल फोन
- सिम कार्ड
- एटीएम/डेबिट कार्ड
- लैपटॉप
- पेन ड्राइव
- नकद 5,44,000/–रुपये
- डोंगल,

- एक जाली आधार कार्ड रोहित कुमार सिंह के नाम पर है जिसमें शुभम प्रियदर्शी की तस्वीर है,
- रिलायंस पेट्रोल पंपों की डीलरशिप देने के लिए जनता को धोखा देने के लिए संचार कौशल वाले 02 पृष्ठ (दोनों तरफ) वाले हाथ से लिखे गए एक नोट

आरोपियों का कबूलनामा–

- स्वीकार किया कि लालू/कौशलेंद्र कुमार नाम के एक व्यक्ति ने उन्हे खाते उपलब्ध कराये है। जिनमें पीड़ितों ने पैसे डाले।
- लालू आए दिन एटीएम काउंटर से पैसे निकालने के लिए कंकड़बाग इलाके में घूमता रहता था।
- लालू कंधे पर बैग के साथ मिला।
- उसके पास से कई एटीएम/डेबिट कार्ड ,03 मोबाइल फोन और 3,15,000/–रुपये नकद भी बरामद किए गए हैं।
- 29.11.2019 को आरोपी व्यक्तियों की गिरफ्तारी
- प्रथम दृष्टया सुस्थापित साक्ष्य के आधार पर निम्नलिखित अभियुक्तों को गिरफ्तार किया गाया–
- आकाश कुमार (21 वर्ष),
- शुभम प्रियदर्शी (19 वर्ष)
- कौशलेंद्र कुमार/लल्लू (23 वर्ष)

• U/s -419/420/467/468/471/120-B/34 IPC r/w Sec. 66-C/66-D of Information Technology Act, 2000.

केस स्टडी–5
लोन मामला

- शिकायतकर्ता ने वर्ष 2019 में तत्काल ऋण ऐप से ऋण प्राप्त किया और ऋण का भुगतान किया।
- बाद में उसकी जानकारी के बिना अगस्त, 2020 के महीने में उसके खाते में 10,500/– रुपये जमा किए गए और उसे सूचित किया गाया कि यह गलती से उसके खाते में जमा हो गाया था और उसे वापस करने के लिए कहा गाया था।
- उसने अपने फोन पे खाते के माध्यम से राशि का भुगतान किया। बाद में विभिन्न आवेदनों से उसकी सहमति के बिना उसके खाते में राशि जमा कर दी गई और उसे ऋण राशि चुकाने के लिए कहा गाया।
- चूंकि उसने अपनी इच्छा से ऋण प्राप्त नहीं किया, इसलिए उसने कुछ भुगतान किया लेकिन पूरी ऋण राशि का भुगतान नहीं कर सकी और बाद में विभिन्न ऐप्स के टेली कॉलर्स ने उसे और उसके भाई को अपमानजनक भाषा का उपयोग करके कई कॉलों के साथ परेशान करना शुरू कर दिया।

केस स्टडी–6
फिशिंग

पीडित मिस्टर ए को एक्स नाम के एक अनजान व्यक्ति का इंटरनेशनल कॉल और ई–मेल मैसेज आया, उस व्यक्ति ने बताया कि वह उसका एशियन इंटरनेशनल कार्ड बना देगा और जिसके लिए उसने पैसे की मांग की। उसने पीड़ित को 12 मिलियन पाउंड की विरासत संपत्ति जो किसी अज्ञात व्यक्ति द्वारा छोड़ा गाया था, के बारे में ईमेल भी मिला। । मेल भेजने वाले ने उसे लुभाया कि वह एशियन इंटरनेशनल कार्ड के माध्यम से उस सम्पत्ति को प्राप्त कर सकता है। उससे कहा कि उसके लिए उसे विभिन्न प्रकार के करों का भुगतान करना होगा। पीड़ित उसके जाल में फंस गाया और उसने 29 अलग–अलग भारतीय खातों में 38 लाख रुपये का भुगतान किया। अंत में उसने खुद को प्रतिरूपण द्वारा ठगा हुआ पाया और साइबर धोखाधड़ी का शिकार हो गाया।

अनुसंधान के चरणः–

- पीड़िता ने अज्ञात जालसाजों के खिलाफ प्राथमिकी दर्ज कराई
- पीड़ित का बयान लिया।
- खाता विवरण और अन्य विवरण के लिए संबंधित बैंकों को 91crpc के तहत नोटिस भेजा गाया।
- कॉल करने वालों के विवरण और आईएमईआई विवरण के लिए मोबाइल नोडल को नोटिस 91crpc भेजा गाया।
- जीमेल अकाउंट की जानकारी के लिए गूगल को 91crpc नोटिस भेजा।

डेटा का विश्लेषण की बाधाएँः–

- पूरे भारत से 29 अलग–अलग धोखाधड़ी वाले बैंक खाते सामने आए। उक्त खातों के सत्यापन पर अधिकांश खाता पता धारक नहीं मिले।
- सत्यापन करने पर कॉलर नंबर और अन्य संबंधित नंबर सीएएफ आईडी भी नहीं मिले।
- जीमेल ने प्रदान किया कि उपयोगकर्ता आईपी विदेशी आधारित था, इसलिए डेटा नहीं मिला।

डेटा विश्लेषण के सकारात्मक पक्षः–

- बैंक खाताधारक के पते को सत्यापित करने के लिए टीम भेजी गई, उन्होंने अरुणाचल प्रदेश, मेघालय, असम आदि में कुछ खातों का सत्यापन किया।
- दिल्ली और एनसीआर क्षेत्र में पाए गए खातों से पैसे की निकासी।
- उन इलाकों में मोबाइल नंबर लोकेशन मिली।
- एटीएम से निकासी की फुटेज मिली।

केस पर आगे विश्लेषणः–

- अरुणाचल प्रदेश के 03 लाभार्थियों का सत्यापन किया गाया और उन्हें गिरफ्तार किया गाया।
- आरोपी ने साथी सह आरोपी के बारे में बताया।
- एटीएम फुटेज के आधार पर दो नाइजीरियाई आरोपियों की पहचान की गई और उन्हें गिरफ्तार किया गाया।
- संबंधित डेटा वाले मोबाइल फोन जब्त किए गए। आरोपियों के पास से संबंधित एटीएम कार्ड बरामद किए गए हैं।
- लोगों को लुभाने के लिए धोखाधड़ी वाले खाते खोलने में शामिल एक पुरुष और दो महिलाओं को कानून की संबंधित धाराओं में नोटिस दिया गाया था।
- कुल 08 आरोपियों के खिलाफ चार्जशीट दाखिल की गई थी।
- नाइजीरियाई आरोपी भी साइबर क्राइम पुलिस स्टेशन उत्तराखंड में दर्ज एक और मामले में शामिल पाए गए, जिसमें उन्होंने एक विदेशी महिला का रूप धारण करके पीड़ित को धोखा दिया और नकली औषधीय बीज और लगभग 98 लाख रुपये हड़प लिए।

केस की मोड्स ओपरेंडीः–

- आरोपित नाइजीरियाई लोगों ने अमीर व्यक्ति, सुंदर महिला आदि का रूप धारण करके और वीओआइपी कॉल, फोन कॉल, ई–मेल, फेसबुक आदि के माध्यम से पीड़ितों से सम्पर्क किया। उन्होंने उन्हें विदेशी मुद्रा आदि के रूप में आसान पैसे का लालच दिया और उनसे करों का भुगतान करने के लिए कहा। विभिन्न प्रकार के उक्त धोखाधड़ी खातों में उनकी गाढ़ी कमाई को हड़प लिया जाता है।
- जालसाज अन्य व्यक्तियों को लाभ का प्रतिशत देकर उनके बैंक खाते का उपयोग करते हैं।
- जालसाज फर्जी आईडी के सिम कार्ड का इस्तेमाल करते हैं।
- जालसाज फर्जी ईमेल आईडी फर्जी सोशल मीडिया अकाउंट बनाते हैं।

केस स्टडी–7
साइबर स्पेस में यौन उत्पीडन

- **SECTION 354C/354D IPC & 66E/67/67A IT Act**
- शिकायतकर्ता महिला (पीड़ित) का मामला दर्ज होने की तारीख से पिछले तीन वर्षों से आरोपी नामित प्राथमिकी के साथ संबंध था।
- आरोपी बज बज इंस्टीट्यूट ऑफ टेक्नोलॉजी के चौथे वर्ष बीटेक का छात्र था।
- आरोपी ने पीड़िता से शादी का वादा किया था।
- समय के साथ शिकायतकर्ता आरोपी पर भरोसा करने लगी।
- भावनात्मक आधार पर आरोपी ने पीड़िता की कुछ निजी नग्न तस्वीरें उससे एकत्र कीं।
- बाद में आरोपी पीड़िता को ब्लैकमेल करता रहा
- आरोपी ने पीड़िता के इनकार करने पर निजी तस्वीरें सोशल मीडिया में अपलोड करने की धमकी भी दी और अश्लील साइट www.pornhub.com पर अपलोड कर दी।
- पीड़िता को मोबाइल नंबर 9733185096 और 8240136385 से धमकाता था।

अनुसंधान–

- जांच के दौरान सीआईडी ने आरोपी अनिमेष बॉक्सी की ई–मेल आईडी और उन ईमेल आईडी के बारे में विवरण एकत्र किया।
- इसे 65B इंडियन एविडेंस एक्ट स्टेटमेंट के साथ जब्त किया गाया था
- आरोपियों का फोन और सिम कार्ड भी बरामद किया गाया है।
- सीआईडी के आईओ ने अपलोड की गई तस्वीर के विवरण के लिए www.pornhub.com को लिखा।
- www.pornhub.com से उत्तर प्राप्त हुआ।
- उस आरोपी एनी बॉक्सी ने 08/08/2015 को www.pornhub.com पर अपनी ईमेल आईडी 'animeshbokshi18@gmail.com' द्वारा प्रोफाइल नाम **Anibokshi** के साथ एक खाता बनाया और फोटो अपलोड की।
- जब्त मोबाइल फोन आईएमईआई और सिम का मिलान आईपी विवरण से किया गाया, जिसका इस्तेमाल पोर्न हब में फोटो अपलोड करने के लिए किया गाया था।

केस स्टडी–8
फर्जी वेबसाइट

- मेघालय बोर्ड ऑफ स्कूल एजुकेशन, धर्मशाला बोर्ड ऑफ सेकेंडरी एजुकेशन एचपी, भारती विद्यापीठ पुणे, महाराष्ट्र स्टेट ओपन स्कूल पुणे, बनस्थली विद्यापीठ, राजस्थान स्टेट ओपन स्कूल जयपुर, सिक्किम नर्सिंग काउंसिल आदि जैसे विभिन्न प्रमुख संस्थानों की 32 फर्जी वेबसाइटें बनाई गईं।
- आरोपी उन विश्वविद्यालयों को निशाना बनाते थे जो बंद होने के कगार पर थे या जिनकी अच्छी प्रतिष्ठा नहीं थी।
- आरोपी छात्रों को बेतरतीब ढंग से बुलाते थे और फर्जी डिग्री के लिए मोटी रकम लेते थे।
- वे उन छात्रों को ब्लॉक करते हैं जो डिग्री सत्यापन के लिए उन्हे कॉल करते थे।

अनुसंधान का प्रथम चरणः–

- डोमेन ieuniversity.org को who.is लुकअप पर चेक किया गाया
- डोमेन नाम GoDaddy पर पंजीकृत था।
- GoDaddy ने KYC प्रदान कियाः जीमेल आईडी, कार्ड भुगतान विवरण, एक्सेस आईपी और फोन नंबर
- सीसी एवेन्यू ने भुगतान के दौरान उपयोग किए गए आईपी विवरण प्रदान किए
- Iptracker.com पर IP की जाँच की गई।
- IP को दिल्ली स्थित ISP के साथ पंजीकृत किया गाया था
- आईएसपी ने मॉडेम मैक आईडी के साथ आईपी विवरण प्रदान किया।
- पहला आरोपी भारती जिसके नाम से मॉडम जारी किया गाया था, उसकी पहचान हो गई।
- भारती को एक अन्य आरोपी डेवलपर मो. सलीम के साथ गिरफ्तार किया गाया।

गुगल/गो डैडी के माध्यम से अनुसंधान–

- Google ने Gmail लॉगिन/लॉगआउट IP पते प्रदान किए हैं।
- आईपी एयरटेल आईएसपी से जुड़े थे।
- आईपीडीआर विश्लेषण से आरोपी भारती के बारे में खुलासा हुआ।
- Godaddy ने वेबसाइट को एक्सेस करने के लिए उपयोग किए जाने वाले IP प्रदान किए हैं
- आईपी एयरटेल आईएसपी से जुड़े थे
- आईपीडीआर विश्लेषण से भारती और मो. सलीम को आरोपी सिद्व करते है।
- कोटक महिंद्रा बैंक के साथ आगे पत्राचार जिसमें भारती व मो. सलीम अपने खातों का रखरखाव कर रहा था जिससे साथ जुडा हुआ फोन नंबर और उनका सही पता मिल गाया।

आरोपियों की गिरफ्तारी–

- तीन आरोपी ऐनान अहमद, मो. सलीम और भारती को एसडीपीओ बद्दी के नेतृत्व वाली टीम ने 05/02/21 को दिल्ली से गिरफ्तार किया था।
- भारती मो. सलीम (webmoretechnologies.com नाम की एक कंपनी चला रहे हैं) और जिनके नाम पर लक्षित मैक पते के साथ मॉडेम का उपयोग किया गाया था।
- मो. सलीम ने फर्जी वेबसाइट बनाई थी।
- ऐनान अहमद ने उपरोक्त आरोपितों को नाममात्र की फीस में इस वेबसाइट को विकसित करने के लिए कहा था।
- ऐनन अहमद केवल बैकएंड से वेबसाइट को संचालित करने के लिए उपयोग करते हैं।
- वह दिल्ली के शाहीन बाग में एक स्थानीय प्रिंटिंग प्रेस से डिग्रियों की छपाई करवाता था।
- प्रिंटिंग प्रेस मालिक की गिरफ्तारी के लिए जिला पुलिस द्वारा प्रयास जारी है।

पुलिस रिमांड के दौरान जब्ती–

- 32 नकली वेबसाइटों के स्रोत कोड की जब्ती Hostinger.com और Wisesolution.com पर होस्ट किए गए उनके एडमिन पैनल के माध्यम से की गई थी और हैश मान उत्पन्न किए गए थे और आईटी अधिनियम के अनुसार जब्ती ज्ञापन में दर्ज किए गए थे।
- मोहम्मद के जीमेल खाते की जब्ती सलीम और भारती के साथ पूरा डेटा (गूगल टेकआउट का इस्तेमाल करके) किया गाया।
- चौथा आरोपी मनीष कुमार को पंजाब के फाजिल्का से गिरफ्तार किया गाया, जो आईईसी यूनिवर्सिटी से फर्जी डिग्री हासिल करता था।
- पुलिस रिमांड के दौरान आरोपी द्वारा किए गए खुलासे के दौरान उसके संबंध स्थापित हो गए थे।

अनुसंधान के दौरान जब्ती–

- मॉडेम जिसके माध्यम से नकली वेबसाइट iecuniversity.org बनाई गई।
- दिल्ली से 4 लैपटॉप, 3 मोबाइल, 78 विश्वविद्यालयों के 656 माक्रशीटधडिग्रीध्सट्रिफिकेट, पूरे भारत में फैले 165 नकली टिकट, 270 होलोग्राम जब्त किए गए।
- 32 नकली वेबसाइटों (देश भर में फैली हुई) की जब्ती उनके एडमिन पैनल के माध्यम से की गई थी और आईटी अधिनियम के अनुसार हैश मान बनाए गए और जब्ती ज्ञापन में दर्ज किए गए थे।

वित्तीय अनुसंधान–

- ऐनान अहमद के घर से दिल्ली से साढ़े चार लाख रुपये नकद बरामद

- ऐनान अहमद की सहयोगी पांचवीं आरोपी अर्चना सिंह को हरिद्वार से गिरफ्तार किया गाया था जिसके खाते में फर्जी डिग्री घोटाले की सारी कमाई जाती थी।
- उसके खाते में लगभग 11 करोड़ रुपये का लेनदेन था।
- उनकी ओर से समानांतर जांच के लिए ईडी और आयकर विभाग के साथ भी जानकारी साझा की गई थी।
- वेबसाइट को विकसित करने और होस्ट करने के लिए वेबसाइट डेवलपर ऐनन अहमद द्वारा किए गए क्रेडिट कार्ड भुगतान विवरण का पता लगाया गाया।
- डेवलपर द्वारा अपने कर्मचारी भारती को किए गए ऑनलाइन भुगतान की भी पुष्टि की गई
- अर्चना सिंह के खाते से पैसे निकालकर ऐनान अहमद के खातों में जमा किए जाने से भी आरोपियों को अवैध लाभ होने की पुष्टि हुई।

केस स्टडी–9
एटीएम स्कीमिंग केस

- त्रिपुरा के विभिन्न थानों में उनके बैंक खातों से अनधिकृत रूप से पैसे निकालने के संबंध में 47 प्राथमिकी दर्ज की गईं। घटना 14.11.2019 से शुरू हुई थी। जांच के दौरान 2 तुर्की, 2 बांग्लादेशी और 1 भारतीय को एटीएम स्किमिंग धोखाधड़ी के अंतरराष्ट्रीय रैकेट में शामिल होने पर गिरफ्तार किया गाया।
- बैंक अधिकारियों से समन्वय कर और शिकायतों की प्रकृति को देखते हुए, छेड़छाड़ किए गए एटीएम को चिन्हित किया गाया। दो विदेशियों को पैसे जमा करने या निकालने के अलावा एटीएम के अंदर संदिग्ध गातिविधियां करते हुए देखा गाया।

- आरोपी व्यक्तियों की पहचान–
- एटीएम के सीसीटीवी फुटेज में आरोपियों की मौजूदगी की पुष्टि हुई है।
- वेब पर सर्च करने पर पाया गाया कि इसी तरह की धोखाधड़ी गुवाहाटी में भी हुई थी।
- गुवाहाटी पुलिस द्वारा पहले ही दो आरोपी व्यक्तियों के नाम और तस्वीर के साथ एलओसी जारी किया गाया था जो तुर्की के नागरिक हैं। एसबी से एलओसी की प्रति एकत्र की गई जिससे जांच में मदद मिली।
- आगे की लीड के लिए यात्रा की तारीखों और फुटेज के लिए एयरपोर्ट अथॉरिटी से सम्पर्क किया गाया था।

छापे, गिरफ्तारी और वसूली–

- मुंबई से हवाई टिकट बुक किए गए और एयरपोर्ट अथॉरिटी ने मोबाइल नंबर जो आरोपी ने बोर्डिंग के समय दिया था मुहैया कराया।
- 18–11–2019 को कोलकाता में उनके स्थान का पता लगाया गाया और बाद में गिरफ्तार किया गाया– उनके कब्जे से 32000 USD, 30 लाख INR, एक लैपटॉप और 7 मोबाइल फोन आदि जब्त किए गए।
- बाद में, यह पता चलन पर एक आरोपी को श्रीलंका में भी गिरफ्तार किया गाया था।

कार्य प्रणाली–

समझौता किए गए एटीएम में स्किमिंग डिवाइस फिट करके एटीएम क्लोनिंग और डेटा चोरी करना

चुनौतियां और आगे का रास्ता–

- फोटोग्राफ के बावजूद आरोपियों की पहचान
- अन्य राज्य पुलिस के साथ समन्वय
- तस्वीरों के साथ डेटा साझा करना

अनुसंधान–

1. व्यक्ति और प्रौद्योगिकी में समन्वय (सीसीटीएनएस/क्रि–मैक में वैश्विक खोज)
   - बैंकों/वॉलेट/पेमेंट गेटवे के साथ समन्वय
   - टीएसपी के साथ समन्वय
   - एटीएम सेवा प्रदाता (अनुपालन न करने पर आरबीआई बैंकों को दंडित करता है)
   - एकीकरण
   - प्रौद्योगिकी में दक्षता और सहायता
   - डिजिटल पदचिह्न और गुमनामी
   - हमें भौगोलिक स्थानों के साथ समन्वय बैठाते हुए सीडीआर, आईपीडीआर, खाता विवरण के बीच एकीकरण स्थापित किया गाया।
   - ब्लॉकचेन प्रौद्योगिकी और इसके निहितार्थ को भी ध्यान में रखा गाया। जैसे बिटकॉइन एक देश (चीन) में कानूनी है और भारत में मान्यता प्राप्त है लेकिन आरबीआई द्वारा कोई नियम नहीं है।
   - उभरती प्रौद्योगिकी और इसके उपयोगों के प्रति जांच अधिकारियों को एक्सपोजर और प्रशिक्षण दिया गाया।

केस स्टडी–10
ऑनलाइन धोखाधडी

- मामले के तथ्य ये है कि आरोपी व्यक्तियों ने माननीय मुख्य न्यायाधीश, उच्च न्यायालय, कलकत्ता के मोबाइल नंबर पर मोबाइल नंबर 708514 ''''' का उपयोग करके एक नकली और झूठे संदेश भेजकर सूचित किया कि उनके व्हाट्सएप नंबर ने 2 करोड़ 75 लाख रु व्हाट्सएप ग्लोबल 2020 में जीते है।

- संदिग्ध ने माननीय मुख्य न्यायाधीश से उनका अपना विवरण ईमेल rbidelhi@rbigovt.in पर भेजने के लिए कहा। लेकिन माननीय मुख्य न्यायाधीश, उच्च न्यायालय, कलकत्ता सतक्र हो गए और इस तरह के प्रलोभन के शिकार नहीं हुए। उन्होंने तुरंत मामले की जानकारी कोलकाता पुलिस के वरिष्ठ अधिकारियों को दी और बाद में साइबर थाना, कोलकाता में अनुसंधान शुरू किया गाया।

अनुसंधान–

- जांच के दौरान सार्वजनिक डोमेन रजिस्ट्री से सम्पर्क किया गाया ताकि पूछताछ किए गए डोमेन rbigovt.in का विवरण प्राप्त किया जा सके।
- संबंधित डोमेन सेवा प्रदाता के जवाब से पता चला कि कथित ईमेल पता मोबाइल नंबर 91 98719 '''' से जुड़ा है और संबंधित टीएसपी से पता चला है कि उक्त नंबर एक एम. कुमार, नई दिल्लीके नाम पर है।
- साथ ही एक फिनो बैंक खाते के साथ खाता संख्या 10002437'''' के माध्यम से एक इंडसइंड बैंक खाते का पता लगाया गाया।
- जांच के दौरान, यह भी पता चला है कि इंडसइंड बैंक खाते और फिनो बैंक दोनों से कुछ लेनदेन एक आईसीआईसीआई बैंक खाते में किए गए हैं, जिसके नंबर 001105 ''''' थे। जो एक फोन नंबर 989992 से जुड़ा है। '''' जो दिल्ली सक्रिल में भी चल रहा है।
- जांच के दौरान नई दिल्ली इलाके में छापेमारी की गई।
- छापेमारी के दौरान उक्त एम कुमार से पूछताछ की जिसने बताया कि वह राजू पाक्र क्षेत्र, नई दिल्ली में एक मोबाइल रिचार्ज की दुकान चला रहा है और कथित नंबर 989992''' की पहचान एक नाइजीरियाई नागरिक जॉन एफे उफ्र साइमन के रूप में हुई।
- टावर लोकेशन और अन्य स्रोत के अनुसार उक्त जॉन एफे उफ्र साइमन के आवास का पता लगाया और उसके घर में छापेमारी की।
- कथित मोबाइल फोन की तलाशी के दौरान जॉन एफे उफ्र साइमन के पास से एक सिम कार्ड मिला।
- उचित पूछताछ के बाद यह पता चला कि उक्त व्यक्ति की मामले में सीधी मिलीभगत है और उसे गिरफ्तार कर लिया गाया।
- उक्त आरोपी पासपोर्ट और वीजा की कोई मूल या फोटोकॉपी पेश नहीं कर सका।
- उसके पास से एक लैपटाप बरामद हुआ है।

- जांच के दौरान यह भी पता लगाया गाया कि उसने धोखे से अपने नाम से वीजा हासिल किया है और बाद में बिना किसी वैध वीजा के भारत में रहा।
- यह सत्यापित करने के लिए कदम उठाए गये कि उसके नाम के खिलाफ कोई वास्तविक पासपोर्ट और वीजा जारी किया गाया है या नहीं।
- जांच के दौरान निदेशक, पश्चिमी अफ्रीका डिवीजन, विदेश मंत्रालय और पुलिस उपायुक्त, विदेशी क्षेत्रीय पंजीकरण अधिकारियों से सम्पर्क किया गाया। यह पता लगाया गाया कि उनके खिलाफ कोई वास्तविक पासपोर्ट और वीजा जारी किया गाया था या नहीं।
- निदेशक, पश्चिमी अफ्रीका प्रभाग, विदेश मंत्रालय से उत्तर प्राप्त हुआ है जिसमें वे बिना किसी वीजा या पासपोर्ट संख्या के पुष्टि नहीं कर सकते थे।
- जांच के दौरान, जब आरोपी व्यक्ति पुलिस हिरासत में था, तत्काल मामले के आलोक में उससे बारीकी से पूछताछ की गई।
- पूछताछ में बताया कि आरोपी व्यक्तियों ने खुद ही BigRock को डोमेन पंजीकृत करने के लिए एक्सेस किया, अर्थात् बिग रॉक आईडी olilviaparker87@gmail.com का उपयोग करके अपराध करने के लिए संदिग्ध डोमेन rbigovt.in बनाया।
- साइबर पीएस की टीम फिर से तलाशी/जब्ती करने के लिए दिल्ली पहुंची, लेकिन न तो डिवाइस और न ही पासपोर्ट या वीजा की कोई प्रति बरामद की जा सकी। परिणामस्वरूप विदेशी अधिनियम 1946 की धारा 14 को कानून की मौजूदा धाराओं के साथ जोड़ा गाया है।
- आरोपी व्यक्तियों द्वारा अपराध करने के लिए इस्तेमाल किए गए इलेक्ट्रॉनिक उपकरणों यानी लैपटॉप और मोबाइल फोन का इंटरनेट एविडेंस फाइंडर (आईईएफ) सहित विभिन्न साइबर फोरेंसिक उपकरणों द्वारा विश्लेषण किया गाया था।
- HDD की छवि FTK इमेजर लाइट का उपयोग करके बनाई गई है
- Encase का उपयोग करके उसकी जांच की।
- सीडीआर/आईपीडीआर विश्लेषण उपकरण यानी सी–5 सीडीआर विश्लेषक की मदद ली गई।
- सेलेब्राइट का उपयोग करके उनके मोबाइल फोन का डेटा निकाला गाया और यह पाया गाया कि उन्होंने न केवल शिकायतकर्ता बल्कि कई अन्य पुरुषों से भी चौट की और उन्हें विभिन्न बहाने से धोखा दिया। उनके झूठे प्रतिनिधित्व से आकर्षित और ठगे जाने पर, भारतीय व्यक्ति मूल्यवान उपहार प्राप्त करने के लिए विभिन्न बैंकों के वांछित खातों में बड़ी मात्रा में धन हस्तांतरित कराता था।

चार्जसीट व सजा–

जांच पूरी होने के बाद एलडी, कोर्ट के समक्ष दिनांक 19/09/2020 को चार्जशीट पेश की। ट्रायल बहुत ही कम समय में पूरा कर लिया है और 28/09/2020 को ट्रायल के बाद एल.डी. कोर्ट ने आरोपी व्यक्ति को दोषी ठहराते हुए प्रसन्नता व्यक्त की और उसे निम्नानुसार सजा सुनाईः

- यू/एस–66सी आईटी एक्ट–2000 के तहत अपराध करने पर 6 माह का साधारण कारावास एवं 10 हजार रुपये जुर्माना लगाया।
- U/S 66D IT Act–2000 के तहत अपराध करने पर 6 माह का साधारण कारावास और 10 हजार रुपये जुर्माना लगाया।
- धारा 419 आईपीसी के तहत अपराध करने पर 15 दिन का साधारण कारावास और 5000/– रुपये का जुर्माना लगाया।
- धारा 420/511 आईपीसी के तहत अपराध करने पर 15 दिन का साधारण कारावास और 5000/– रुपये का जुर्माना लगाया।
- यू/एस–14 फॉरेनर्स एक्ट के तहत अपराध करने पर छह माह का साधारण कारावास और दस हजार रुपये जुर्माना लगाया।
- कारावास की सभी मूल सजाएं साथ–साथ चलेंगी। जुर्माने की चूक में कारावास, अधिरोपित कारावास की मूल सजा के अतिरिक्त होगा।
- एल.डी. कोर्ट ने यह भी आदेश पारित किया कि सजा पूरी होने पर आरोपी व्यक्ति को धारा–14 फॉरेनर्स एक्ट के तहत दोषी ठहराए जाने के मद्देनजर उसे उसके मूल देश में वापस भेज दिया जाएगा।

अनुसंधान में आई कठिनाईयॉ–

- आरोपी व्यक्ति ने अपनी पहचान छुपाने के लिए कई मोबाइल फोन और नंबरों का इस्तेमाल किया। उन्होंने जाली और मनगढ़ंत दस्तावेजों का उपयोग करके अन्य व्यक्तियों के नाम पर लाभार्थी के बैंक खाते खोले। शुरुआत में पुलिस टीम के हाथ में कोई सुराग नहीं लगा।

- जांच अधिकारी और उनकी टीम की कड़ी मेहनत से मामले का पर्दाफाश हो सका और एक आरोपी को गिरफ्तार किया जा सका। यह बहुत आश्चर्यजनक बात है कि उक्त गिरोह ने जाली और मनगढ़ंत दस्तावेजों की मदद से कई बैंक खाते खोले और जिससे अपराधी को पकड़ना मुश्किल हो गया।

केस स्टडी–11
बच्चों से संबंधित आपत्तिजनक सामग्री की ऑनलाइन बिक्रि

संक्षिप्त एफआईआर–

गृह मंत्रालय की साइबर टिपलाइन पर नोडल अधिकारी, साइबर क्राइम डिवीजन, सीआईडी कर्नाटक चाइल्ड सेक्सुअल एव्यूज मेटेरियल अर्थात् सीएसएएम सामग्री का ऑनलाइन वितरण, कब्जे, बिक्री और के बारे में जानकारी प्राप्त हुई।

- जिसमें सोशल मीडिया और डिजिटल भुगतान चैनल जैसे इंस्टाग्राम, टेलीग्राम, फेसबुक, पेटीएम, गूगल पे, फोनपे आदि का इस्तेमाल किया
- सामग्री साझा करने के लिए न्यूजीलैंड स्थित क्लाउड स्टोरेज सेवा Mega.nz उपयोग की जा रही थी।
- धारा लागू
- 66बी आई.टी. अधिनियम, 2000
- धारा 15 पॉक्सो, 2012

शिकायत प्रति के साथ अनुलग्नक

➢साइबर टिपलाइन रिपोर्ट (पासवर्ड से सुरक्षित)

साइबर टीपलाइन के बारे में–

- बच्चे के संबंध में अश्लीलता और बाल यौन शोषण सामग्री NCMEC स्टैंडअलोन कंप्यूटर पर टिपलाइन रिपोर्ट से प्राप्त होने वाली शिकायतों के लिए एनसीआरबी को नामित किया हुआ है।
- एनसीआरबी को टिपलाइन रिपोर्ट प्राप्त होने पर वह उसे कानूनी कार्रवाई के लिए भारत में प्रवर्तन एजेंसियों से साझा करती है।
- टिपलाइन रिपोर्ट में यदि एनसीएमईसी सामग्री को वीपीएन के माध्यम से प्राप्त किया जा रहा है तो उसकी सूचना NCMEC द्वारा भारत के एमएचए/एनसीआरबी के साथ साझा की जावेगी।
- NCMEC इस संबंध में एनसीआरबी को तकनीकी प्रशिक्षण समय समय पर देता रहेगा।
- एनसीआरबी इस संबंध में एनसीएमईसी को अपना फीडबैक देगा।
- एनसीआरबी सरकारी कानून प्रवर्तन एजेंसियां के अलावा गैर–अधिकृत उपयोगकर्ताओं अर्थात अन्य संगठनों के साथ साइबर टिपलाइन रिपोर्ट साझा नहीं कर करेगा।

सर्वोत्तम प्रथाएं

चूंकि यह मामला मासूम बच्चों के शोषण से संबंधित है, इसलिए संबंधितों को प्राथमिकी को कर्नाटक राज्य पुलिस की वेबसाइट परअपलोड करने से छूट देने के लिए निवेदन किया गाया।

ध्यान दें

माननीय सुप्रीम अदालत द्वारा ने ललिता कुमारी बनाम उत्तर प्रदेश राज्य में एफआईआर को वेबसाइट पर अपलोड करना अनिवार्य कर दिया गाया है।

जांच– गिरफ्तारी से पहले

- आईओ ने एनसीएमईसी द्वारा साझा की गई रिपोर्ट का विस्तृत अध्ययन किया।
- आरोपी व्यक्ति की संभावित स्थान की पहचान करने के लिए सीडीआर विश्लेषण किया गाया।
- सीडीआर में सेवा संदेशों पर विशेष ध्यान दिया गाया और बैंक खाते का विवरण की पहचान की गई।

जांच– बैंक के साथ समन्वय

- बैंक को अपराध की गंभीरता और संवेदनशीलता के बारे में बताया।
- एकत्रित संदिग्ध खाते का विवरण और खाते को फ्रीज करने का नोटिस जारी किया गाया था।
- सेवाओं को निष्क्रिय करने के बारे में आरोपी बैंक से सम्पर्क किया।
- चूंकि बैंक को पुलिस जांच के बारे में पहले से ही जानकारी थी, इसलिए उन्होंने आरोपी की तलाश में पुलिस का सहयोग किया।
- इसलिए बैंक उसे आगे स्पष्टीकरण के लिए शाखा में जाने के लिए कहता है।

जांच– गिरफ्तारी के दौरान–

- टावर की लोकेशन व संदिग्धों की उपस्थिति निश्चित की गई।
- इलेक्ट्रॉनिक गैजेट्स विनाश से बचाने के लिए को संदिग्ध को उनसे अलग किया गाया।
- पंच गवाहो की उपस्थिति में इलेक्ट्रॉनिक साक्ष्य की गिरफ्तारी और जब्ती

आरोपियों से जब्त की गई जानकारी

- आरोपी का क्लाउड स्टोरेज डेटा डाउनलोड किया गाया और
- नए और खाली पर सहेजा गायाः सैंडिस्क अल्ट्रा, डुअल ड्राइव M3
- आरोपी व्यक्ति की सात ईमेल आईडी डंप लिया गाया।

जांच– डेटा विश्लेषण–

- सीडीआर विश्लेषण
- टावर लोकेशन
- ईमेल फोरेंसिक और विश्लेषण
- जब्त वस्तुओं की फोरेंसिक जांच की गई
- मोबाइल फोरेंसिक के लिए सेलब्राइट UFED

जांच–पड़ताल– सेवा प्रदाताओं से सूचना

- बैंक
- मोबाइल सेवा प्रदाता
- तार
- Mega.nz
- फेसबुक
- इंस्टाग्राम
- गूगल

आरोपी को उसके मोबाइल नंबर और ईमेल आईडी से लिंक करना

- आवास बुक करने के लिए जोलो ऐप का इस्तेमाल

जोलो ने निम्नलिखित जानकारी प्रदान की

- मोबाइल फोन नंबर
- ईमेल आईडी
- आईडी प्रूफ
- फोटोग्राफ

- सीएसएएम की सामग्री ऑनलाइन की बिक्री के लिए ग्राहकों को आकर्षित करने के लिए आरोपियों द्वारा एक अलग Instagram विज्ञापन पेज बनाया गाया था।
- ग्राहकों को आकर्षित करने के लिए 466 पृष्ठ का प्रचार एल्बम तैयार किया गाया था।

मोबाइल फोन फोरेंसिक निष्कर्षण–

- सीएसएएम सामग्री मिली।
- साइबर टिपलाइन द्वारा साझा किए गए ईमेल पते और अन्य विवरण मोबाइल के साथ जुड़े थे।
- लगभग 702 सीएसएएम फाइलें क्लाउड पर संग्रहीत थी।

ऑनलाइन बिक्री और वितरण

➢ **इंस्टाग्राम**

स्क्रीन नाम

- Picseller_7860
- Picseller_7867

➢ **टेलीग्राम ऐप**

वह वितरण में शामिल कई समूहों का हिस्सा था

1, PicsBox: विशेष – चित्रों और वीडियो के लिए

2, Albumsonly – एल्बम के लिए

भुगतान–

- इलेक्ट्रॉनिक वॉलेट जैसे PhonePe, PayTM और Google Pay बरामद किये गये।
- सिंडिकेट बैंक के बचत बैंक खाते की पहचान की गई।

इलेक्ट्रॉनिक साक्ष्य से निपटना

- मौजूदा कानून के अनुसार, हमने इलेक्ट्रॉनिक साक्ष्य के बारे में परीक्षक से राय ली है
- I-O ने प्रश्नावली का मसौदा तैयार किया जो मामले के लिए प्रासंगिक था और उसे भेजा गाया।
- CFSL ने विस्तृत विश्लेषण किया और निष्कर्ष प्रदान किए।

जाँच – परिणाम

- जब्त की गई वस्तुओं में कई सीएसएएम सामग्री शामिल थी।
- भुगतान विवरण भी बरामद किया गाया।
- विज्ञापन भी स्थापित किया गाया।

इलेक्ट्रॉनिक साक्ष्य से निपटना

- न्यायालय में कानून के अनुसार इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता के लिए सभी प्रक्रियात्मक पहलुओं की फोटोग्राफी की गई तथा डेटा को एक नए और स्टेराइल एसडी मेमोरी कार्ड पर संग्रहीत किया गाया।
- एसडी मेमोरी कार्ड को भारतीय साक्ष्य अधिनियम, 1872 की धारा 62 के तहत मूल रूप में प्रस्तुत किया गाया था।

सर्वोत्तम प्रथाएं–

- चूंकि मामला आईटी अधिनियम 2000 के तहत दर्ज किया गाया था, इसलिए कोई मामला पुलिस निरीक्षक से निम्न पद के पुलिस अधिकारी डेटा संकलन की जिम्मेदारी नहीं दी गई।
- डेटा की निकासी अदालत से अनुमति प्राप्त करने के बाद ही की गई थी
- निर्देशानुसार डीएसपी साइबर क्राइम डिवीजन चालान तक आईओ बना रहा।

केस स्टडी–12
साइबर हनी ट्रेप

कार्य प्रणाली

• संदिग्ध ने पीड़िता से दोस्ती करने के लिए फेसबुक ऐप का इस्तेमाल किया और एक–दूसरे के साथ मोबाइल नंबरों का आदान–प्रदान किया।

• व्हाट्सएप/फेसबुक पर बातचीत शुरू करने के बाद आरोपी ने शिकायतकर्ता को फुसलाया।

• उपहार भेजने, सीमा शुल्क का भुगतान करने और अन्य वित्तीय मदद मांगने के बहाने, आरोपी ने शिकायतकर्ता से लगभग 65 लाख रुपये प्राप्त करके धोखाधड़ी की।

पीड़ित से राज्य साइबर अपराध प्रकोष्ठ, सीआईडी द्वारा एकत्र की गई जानकारी–

• संदिग्ध का फेसबुक प्रोफाइल।

• आरोपी द्वारा इस्तेमाल किए गए मोबाइल नंबर।

• संदिग्ध व्यक्ति के बैंक खाते का विवरण।

एफआईआर आईपीसी की धारा 406, 420, 114 और आईटी संशोधन अधिनियम–2008 की धारा 66 (डी), 66 (सी) के तहत दर्ज की गई थी।

जाँच – पड़ताल

- संदिग्ध के फेसबुक प्रोफाइल की जांच की गई लेकिन पता चला कि आरोपी ने पहले ही अकाउंट को डिलीट कर दिया था।
- आगे की जांच में बैंक खाता विवरण, बैंक स्थान और खाताधारक के केवाईसी क्रमशः दिल्ली, कोलकाता और बैंगलोर से हैं।
- पीड़ितों द्वारा प्रदान किए गए विभिन्न मोबाइल नंबरों के लिए हमने एमएसपी से सीडीआर/एसडीआर/सीएएफ विवरण एकत्र किया और विभिन्न पुलिस दल द्वारा उसका विश्लेषण किया।
- पता चला कि एक मोबाइल नंबर भारत से बाहर का है और अन्य 5 मोबाइल नंबर क्रमशः दिल्ली और हरियाणा के थे। 5 मोबाइल नंबरों के विस्तृत विश्लेषण पर दिल्ली में अधिकतम लोकेशन और अधिकतम कॉल की गई।
- हमारी पड़ताल में संदिग्ध के मोबाइल के मैक्सिमम लोकेशन एरिया की मदद से थर्ड पार्टी के मोबाइल नंबरों का पता लगाने की कोशिश की गई तो हमने पाया कि आरोपी ने एक स्थानीय व्यक्ति से 75 बार बात की।
- हमारी एक टीम जांच के लिए दिल्ली गई और आरोपियों के मोबाइल नंबर की लोकेशन ढूंढी और उस लोकेशन को देखने के लिए एक स्थानीय व्यक्ति को भी खड़ा किया।
- शामिल स्थानीय व्यक्ति को पकड़ लिया और उससे पूछताछ की, जिससे आरोपी का वास्तविक नाम और सही पता पता चला।
- दिल्ली के स्थानीय पुलिस स्टेशन से सम्पर्क किया और उनसे अच्छी मदद ली और उनकी मदद से आरोपी की जगह पर छापेमारी की गई.

- इस प्रकार टीम द्वारा एक नाइजीरियाई व्यक्ति (अभियुक्त) को गिरफ्तार किया गया।

मिले डिजिटल उपकरणः
4 मोबाइल फोन
1 लैपटॉप।
4 सिम कार्ड।

उपरोक्त उपकरणों से अपराध में प्रयुक्त मोबाइल नंबर, आरोपी की फेसबुक प्रोफाइल और पीड़ितों के साथ साझा की गई अन्य तस्वीरें मिलीं।
पूछताछ के दौरान, संबंधित जानकारी एकत्र की गई।

इससे जुटाए गए डेटा को ऑल स्टेट के साथ शेयर किया गाया है। मुख्य आरोपी अभी भी सलाखों के पीछे है।

इस कार्यप्रणाली के आधार पर, सार्वजनिक जागरूकता के लिए सोशल मीडिया प्लेटफॉर्म पर पोस्ट बनाए और साझा किए गए।

साइबर अपराधों से संबंधित माननीय उच्च न्यायालयों और उच्चतम न्यायालय के महत्त्वपूर्ण निर्णय

CRL.MC NO. 3654 OF 2021 Manual v. State of Kerala	
केस का संक्षिप्त विवरण	मामले में याचिकाकर्ता ने 'फ्रेंड्स' नाम से एक व्हाट्सएप ग्रुप बनाया था। ग्रुप में उसके अलावा दो और एडमिन थे, जिनमें से एक इस मामले का पहला आरोपी है। मार्च 2020 में पहले आरोपी ने ग्रुप पर चाइल्ड पोर्न पोस्ट किया।
न्यायालय के द्वारा विचारणीय बिन्दु	ग्रुप एडमिन के खिलाफ सूचना और प्रौद्योगिकी अधिनियम की धारा 67 बी (ए, बी और डी) और पॉक्सो अधिनियम की धारा 13, 14 और 15 के आधार पर मामला दर्ज किया गया था। समूह बनाने के बाद से याचिकाकर्ता को दूसरा आरोपी बनाया गया था। इसके चलते उन्होंने कोर्ट का दरवाजा खटखटाया।
न्यायालय का निर्णय	**सदस्यों द्वारा आपत्तिजनक पोस्ट के लिए व्हाट्सएप एडमिन उत्तरदायी नहीं है।** अदालत ने कहा, "व्हाट्सएप ग्रुप के एडमिन और उसके सदस्यों के बीच कोई मास्टर–नौकर या प्रिंसिपल–एजेंट संबंध नहीं है। यह आपराधिक कानून के बुनियादी सिद्धांतों के खिलाफ है कि ग्रुप के सदस्य द्वारा प्रकाशित पोस्ट के लिए एडमिन को जिम्मेदार ठहराया जाए।" .
निर्णय के विस्तृत अध्ययन के लिए लिंक	**https://hckinfo.kerala.gov.in/digicourt/Casedetailssearch/fileview?token=MjAzNzAwMDM2NTQyMDIxXzEucGRm&lookups=b3JkZXJzLzIwMjE=**

CRIMINAL APPEAL NO.2003 OF 2012,Ritesh Sinha vs State Of Uttar Pradesh	
केस का संक्षिप्त विवरण	अपीलकर्ता, रितेश सिन्हा और उनके सहयोगी के खिलाफ एक प्राथमिकी दर्ज की गई थी, जिसमें आरोप लगाया गया था कि वह पुलिस में नौकरी के वादे पर अलग–अलग लोगों से पैसे इकट्ठा करने में शामिल था। सहयोगी को गिरफ्तार कर उसके पास से एक मोबाइल फोन बरामद किया गया है। यह सत्यापित करने के लिए कि क्या फोन पर रिकॉर्ड की गई बातचीत सहयोगी और अपीलकर्ता के बीच थी, जांच प्राधिकरण ने मुख्य न्यायिक मजिस्ट्रेट, सहारनपुर (सीजेएम) के समक्ष एक आवेदन दायर कर अपीलकर्ता को अपनी आवाज का नमूना देने के लिए अदालत से समन करने का अनुरोध किया। सीजेएम के इस आदेश को अपीलकर्ता ने इलाहाबाद उच्च न्यायालय के समक्ष सीआरपीसी की धारा 482 के तहत चुनौती दी, जिसने अपील को खारिज कर दिया। मामला सुप्रीम कोर्ट की दो जजों की बेंच के सामने आया, जिसने अलग–अलग राय दी और मामले को तीन जजों की बेंच के पास भेज दिया।

न्यायालय के द्वारा विचारणीय बिन्दु	क्या संविधान के अनुच्छेद 20(3) का विस्तार किसी आरोपी को किसी अपराध की जांच के दौरान अपनी आवाज का नमूना देने के लिए मजबूर होने से बचाने के लिए किया गया हैय और क्या सीआरपीसी में किसी प्रावधान के अभाव में, एक मजिस्ट्रेट जांच एजेंसी को किसी अपराध के आरोपी व्यक्ति की आवाज के नमूने को रिकॉर्ड करने के लिए अधिकृत कर सकता है।
न्यायालय का निर्णय	कोर्ट ने कहा कि अनुच्छेद 20(3) आरोपी को अपनी आवाज का नमूना रिकॉर्ड करने के लिए मजबूर करने पर रोक नहीं लगाता है। कहा कि जब तक स्पष्ट प्रावधान लागू नहीं हो जाते हैं संसद द्वारा सीआरपीसी में, एक न्यायिक मजिस्ट्रेट को अनुच्छेद 142 के तहत अपनी शक्ति का प्रयोग करते हुए, किसी व्यक्ति को अपराध के अनुसंधान के उद्देश्य से अपनी आवाज का नमूना देने का आदेश देने की शक्ति को स्वीकार किया जाना चाहिए। इसके अलावा, अदालत ने विचार किया कि क्या किसी आरोपी को आवाज का नमूना देने के लिए मजबूर करना उसके निजता के अधिकार का उल्लंघन होगा के बारे में कहा कि निजता के मौलिक अधिकार को निरपेक्ष नहीं माना जा सकता है और सार्वजनिक हित के लिए ऐसा किया जा सकता है।
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/18061439/

CRIMINAL APPEAL NO. 108/2013 Kishan Tripathi @ Kishan Painter vs The State, Delhi High Court	
केस का संक्षिप्त विवरण	किशन त्रिपाठी, जो चित्रकार था। उसे 22 और 23 फरवरी, 2009 के बीच की रात में सच्चिदानंद झा की हत्या करने के लिए आजीवन कारावास के दण्ड से दोषी ठहराया गया था। दण्ड की धारा 302 के तहत किशन त्रिपाठी को आजीवन व 75,000 रूपये के अर्थदण्ड से दण्डित किया गया।
न्यायालय का निर्णय	सीसीटीवी फुटेज को डायरेक्ट साक्ष्य माना गया।
न्यायालय के द्वारा विचारणीय बिन्दु	किशन त्रिपाठी का दोषसिद्धि मुख्य रूप से सीसीटीवी फुटेज के रूप में इलेक्ट्रॉनिक साक्ष्य पर आधारित थी।
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/24959116/

Shreya Singhal v. UOI	
केस का संक्षिप्त विवरण	एक राजनीतिक नेता के निधन के बाद मुंबई को पूरी तरह से बंद करने के संबंध में फेसबुक पर कथित रूप से आपत्तिजनक पोस्ट और आपत्तिजनक टिप्पणी करने के बाद दो महिलाओं को आईटी अधिनियम की धारा 66 ए के तहत गिरफ्तार किया गया था। आईटी अधिनियम की धारा 66 ए में यदि कोई व्यक्ति कंप्यूटर संसाधन या संचार का उपयोग करता है, ऐसी जानकारी जो आपत्तिजनक, झूठी है, या झुंझलाहट, असुविधा, खतरा, अपमान, घृणा, चोट, या दुर्भावना का कारण बनती है, तो दंड का प्रावधान है। महिलाओं ने गिरफ्तारी के जवाब में आईटी अधिनियम की धारा 66ए की संवैधानिकता को इस आधार पर चुनौती देते हुए याचिका दायर की कि यह भाषण और अभिव्यक्ति की स्वतंत्रता का उल्लंघन है।
न्यायालय के द्वारा विचारणीय बिन्दु	मौजूदा मामले में आईटी एक्ट की धारा 66ए की वैधता को सुप्रीम कोर्ट में चुनौती दी गई थी।
न्यायालय का निर्णय	सुप्रीम कोर्ट ने तीन अवधारणाओं पर अपना निर्णय आधारित कियाः चर्चा, वकालत और उत्तेजना। यह देखा गया कि केवल चर्चा या किसी कारण की वकालत, चाहे वह कितनी भी अलोकप्रिय क्यों न हो, भाषण और अभिव्यक्ति की स्वतंत्रता के केंद्र में है। यह पाया गया कि धारा 66A संचार के सभी रूपों को प्रतिबंधित करने में सक्षम थी । इसमें किसी विशेष विषय पर केवल वकालत या चर्चा के बीच और आक्रामक व उकसाना शब्दों जो सार्वजनिक अव्यवस्था, सुरक्षा, स्वास्थ्य से संबंधित है के मध्य कोई अंतर नहीं था। अदालत ने माना कि धारा 66ए अस्पष्ट है, और यह अभिव्यक्ति की स्वतंत्रता के अधिकार का उल्लंघन है और यह अपनी सीमा के भीतर उस भाषण को भी लेती है जो निर्दोष भी है। इसने आईटी अधिनियम, 2000 से एक मनमाना प्रावधान हटा दिया और भारत में नागरिकों के अभिव्यक्ति की स्वतंत्रता के मौलिक अधिकार को बरकरार रखा। यह विचार था कि भले ही धारा 66 ए को समाप्त कर दिया गया हो, भारतीय दंड संहिता, 1860 में प्रावधान कोई भी भाषण जो नस्लवादी भाषण, किसी महिला की शीलता को ठेस पहुंचाता है या शत्रुता को बढ़ावा देने के उद्देश्य से भाषण, अपमानजनक भाषा, आपराधिक धमकी, जातिवाद, आदि पर रोक लगाने के लिए लागू रहेंगे, ।
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/110813550/

Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr	
केस का संक्षिप्त विवरण	ग्राहक ने धीरूभाई अंबानी पायनियर योजना के तहत एक रिलायंस हैंडसेट और रिलायंस मोबाइल सेवाओं को एक साथ खरीदा। ग्राहक अन्य सेवा प्रदाताओं की बेहतर टैरिफ योजनाओं से आकर्षित थे और इसलिए, अन्य सेवा प्रदाताओं में स्थानांतरित करना चाहते थे। याचिकाकर्ताओं (टाटा इंडिकॉम के स्टाफ सदस्य) ने इलेक्ट्रॉनिक सीरियल नंबर (इसके बाद 'ईएसएन'के रूप में संदर्भित) को हैक कर लिया। रिलायंस हैंडसेट के मोबाइल आइडेंटिफिकेशन नंबर (मिन) को ईएसएन के साथ अपरिवर्तनीय रूप से एकीकृत किया गया था, ईएसएन के रीप्रोग्रामिंग ने डिवाइस को याचिकाकर्ता के सेवा प्रदाता द्वारा मान्य किया जाएगा न कि रिलायंस इन्फोकॉम द्वारा।
न्यायालय के द्वारा विचारणीय बिन्दु	क्या आईटी अधिनियम की धारा 2(1)(प) के तहत टेलीफोन हैंडसेट एक 'कंप्यूटर' है? क्या मोबाइल हैंडसेट में प्रोग्राम किए गए ईएसएन में हेराफेरी आईटी अधिनियम की धारा 65 के तहत स्रोत कोड में परिवर्तन के समान है?
न्यायालय का निर्णय	आईटी अधिनियम की धारा 2(1)(प) में प्रावधान है कि 'कंप्यूटर' का अर्थ किसी भी इलेक्ट्रॉनिक, चुंबकीय, ऑप्टिकल, या अन्य उच्च गति डेटा प्रोसेसिंग डिवाइस या सिस्टम से है जो तार्किक, अंकगणित और स्मृति कार्य करता है। इलेक्ट्रॉनिक, चुंबकीय, या ऑप्टिकल आवेगों के जोड़तोड़ द्वारा, और इसमें सभी इनपुट, आउटपुट, प्रोसेसिंग, स्टोरेज, कंप्यूटर सॉफ्टवेयर या संचार सुविधाएं शामिल हैं जो कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क में कंप्यूटर से जुड़े या संबंधित हैं। इसलिए, एक टेलीफोन हैंडसेट आईटी अधिनियम की धारा 2(1)(i) के तहत परिभाषित 'कंप्यूटर' के दायरे में आता है। ईएसएन का परिवर्तन टाटा इंडिकॉम जैसे अन्य सेवा प्रदाताओं द्वारा विशेष रूप से उपयोग किए जाने वाले हैंडसेट को प्रयोग करने योग्य बनाता है। इसलिए, ईएसएन का परिवर्तन आईटी अधिनियम की धारा 65 के तहत एक अपराध है क्योंकि प्रत्येक सेवा प्रदाता को अपना स्वयं का एसआईडी कोड बनाए रखना होता है और अपने ग्राहकों को प्रदान की गई सेवाओं का लाभ उठाने के लिए उपयोग किए जाने वाले प्रत्येक उपकरण के लिए एक विशिष्ट नंबर देना होता है।
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/1459676/

Christian Louboutin SAS v. Nakul Bajaj & Ors	
केस का संक्षिप्त विवरण	लग्जरी जूतों के निर्माता, शिकायतकर्ता ने नकली सामान बेचने वाले के साथ ट्रेडमार्क उल्लंघन करने के लिए एक ई–कॉमर्स पोर्टल www.darveys.com के खिलाफ निषेधाज्ञा की मांग करते हुए एक मुकदमा दायर किया।
न्यायालय के द्वारा विचारणीय बिन्दु	अदालत के समक्ष सवाल यह था कि क्या प्रतिवादी द्वारा वादी के चिह्न, लोगो और छवि का उपयोग आईटी अधिनियम की धारा 79 के तहत संरक्षित है।
न्यायालय का निर्णय	न्यायालय ने पाया कि प्रतिवादी एक मध्यस्थ से अधिक इस आधार पर है कि वेबसाइट का अपने प्लेटफॉर्म के माध्यम से बेचे जाने वाले उत्पादों पर पूर्ण नियंत्रण है। यह पहले अपने उत्पादों को बेचने के लिए तीसरे पक्ष की पहचान करता है और फिर उसे बढ़ावा देता है। कोर्ट ने आगे कहा कि ई–कॉमर्स प्लेटफॉर्म की सक्रिय भागीदारी उसे आईटी एक्ट की धारा 79 के तहत बिचौलियों को दिए गए अधिकारों से छूट के अन्तर्गत नहीं दी जा सकती हैं।
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/99622088/

Anvar P.V vs P.K.Basheer & Ors' Supreme court of India, CIVIL APPEAL NO. 4226 OF 2012	
केस का संक्षिप्त विवरण	शिकायत एक स्वतंत्र सदस्य की थी जिसे वामपंथी कम्युनिस्ट पार्टी का समर्थन प्राप्त था। उन्होंने एरानाड विधान सभा निर्वाचन क्षेत्र के चुनाव में दूसरा स्थान हासिल किया और चुनाव जीतने वाले प्रतिवादी को भारतीय राष्ट्रीय कांग्रेस और यूनाइटेड डेमोक्रेटिक फ्रंट के कुछ अन्य दलों का समर्थन प्राप्त था। 12 अप्रैल, 2011 को, यूनाइटेड डेमोक्रेटिक फ्रंट के एक सदस्य, जिन्होंने प्रतिवादी का समर्थन किया,याचिकाकर्ता को बदनाम करने और प्रतिवादी के चुनाव जीतने की संभावना बढ़ाने के स्पष्ट इरादे से एक लेख अपने समाचार पत्र में प्रकाशित किया। जिसके साक्ष्य के रूप में वादी ने एक सीडी माननीय न्यायालय में प्रस्तुत की। प्रतिवादी के विद्वान अधिवक्ता ने कहा कि अपीलकर्ता द्वारा प्रस्तुत इलेक्ट्रॉनिक रिकॉर्ड भारतीय साक्ष्य अधिनियम की धारा 65बी की आवश्यकताओं को पूरा नहीं करता है। इसलिए, इसे प्रासंगिक सबूत नहीं माना जा सकता है। अदालत के सामने पेश की गई सीडी प्राथमिक साक्ष्य नहीं है और यह भारतीय साक्ष्य अधिनियम की धारा 65ए और 65बी के तहत दी गई शर्तों को पूरा नहीं करती है। इस प्रकार इसे अस्वीकार्य माना जाता है। चूंकि प्रतिवादी का मुख्य आरोप

	प्रस्तुत सीडी पर आधारित था,
न्यायालय के द्वारा विचारणीय बिन्दु	भारतीय साक्ष्य अधि0 की धारा 65बी के तहत् प्रस्तुत किए जाने वाले प्रमाण पत्र के बारे में।
न्यायालय का निर्णय	प्रत्येक इलेक्ट्रोनिक साक्ष्य के लिए आवश्यक है कि उनके साथ अनिवार्य रूप से भारतीय साक्ष्य अधि0 की धारा 65बी के तहत् प्रमाण पत्र का होना अनिवार्य है।
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/187283766/

Shafhi Mohammad vs The State Of Himachal Pradesh, 2018	
केस का संक्षिप्त विवरण	अपराध के दृश्य की वीडियोग्राफी का उपयोग माननीय न्यायालय के समक्ष विचार का विषय था। जिसमें वीडियोग्राफी वास्तव में जांच प्रक्रिया में मदद करेगी। ऑडियो और वीडियो टेप प्रौद्योगिकी को अपनाये जाने के लिए मामला लाया गया। यह भी बताया गया कि दंड प्रक्रिया संहिता, 1973 की धारा 54ए और 164 के प्रावधान क्रमशः पहचान प्रक्रिया और इकबालिया बयान की वीडियोग्राफी के लिए प्रदान करते हैं और उपायों को अपनाने के लिए सुझाव दिए गए थे ताकि मरने वाले बयानों और पोस्टमार्टम को वीडियो में भी दर्ज किया जा सके।
न्यायालय के द्वारा विचारणीय बिन्दु	मुख्य मुद्दा इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता के संबंध में भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) की व्याख्या थी।
न्यायालय का निर्णय	इलेक्ट्रॉनिक साक्ष्य की ग्राह्यता के लिए उस पार्टी द्वारा, जिसके पास वह उपकरण नहीं है जिससे दस्तावेज तैयार किया गया है। ऐसे पक्ष को भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी के तहत प्रमाण पत्र प्रस्तुत करने की आवश्यकता नहीं है। यदि न्याया हित में हो तो न्यायालय द्वारा प्रमाण पत्र की आवश्यकता के लिए शिथिलता प्रदान की जा सकती है। चुकि धारा 65बी इलेक्ट्रॉनिक साक्ष्य की की प्रक्रियात्मक बताती है।
निर्णय के विस्तृत अध्ययन के लिए लिंक https://indiankanoon.org/doc/71699420/	

Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal	
केस का संक्षिप्त विवरण	अर्जुन बनाम कैलाश में, अदालत को एक चुनावी याचिका पर फैसला सुनाना पड़ा, जिसमें जालना–101 विधान सभा निर्वाचन क्षेत्र से श्री अर्जुन पंडितराव खोटकर के चुनाव को इस आधार पर चुनौती दी गई थी कि नामांकन पत्र निर्धारित समय सीमा के बाद दाखिल किए गए थे। प्रतिवादी यह साबित करने के लिए वीडियो कैमरा रिकॉर्डिंग पेश की कि उम्मीदवार ने निर्धारित समय सीमा के बाद अपना नामांकन दाखिल किया था। उच्च न्यायालय द्वारा दिए गए निर्देश के अनुसार चुनाव आयोग ने सीडी बना कर पेश की। जिसमें वीडियो कैमरा रिकॉर्डिंग की एक प्रति थी। हालांकि, याचिकाकर्ता द्वारा बार बार अनुरोधों के बावजूद, चुनाव आयोग द्वारा धारा 65 बी (4) के अनुसार आवश्यक प्रमाण पत्र प्रस्तुत नहीं किए गए थे। जिरह के दौरान, चुनाव आयोग के एक अधिकारी ने गवाही दी कि वीडियो कैमरा रिकॉर्डिंग प्रामाणिक थी। इस गवाही के आधार पर, उच्च न्यायालय ने वीडियो रिकॉर्डिंग के साक्ष्य को स्वीकार किया, भले ही धारा 65 बी (4) के अनुसार प्रमाण पत्र प्रस्तुत नहीं किया गया था। उच्च न्यायालय ने माना कि धारा 65 बी का पर्याप्त अनुपालन किया गया क्योंकि एक सक्षम अधिकारी ने गवाही दी थी कि वीडियो रिकॉर्डिंग प्रामाणिक थी।
न्यायालय के द्वारा विचारणीय बिन्दु	क्या धारा 65बी(4) के तहत प्रमाण पत्र तब भी प्रस्तुत किया जाना चाहिए जब इलेक्ट्रॉनिक साक्ष्य का एक मूल रिकॉर्ड उपलब्ध हो, या क्या यह केवल तभी दिया जाना चाहिए जब इलेक्ट्रॉनिक साक्ष्य का द्वितीयक रिकॉर्ड प्रस्तुत किया जाए? क्या धारा 65बी(4) का अनुपालन उस स्थिति में भी अनिवार्य है जब सक्षम संस्था से प्रमाण पत्र प्राप्त करना संभव नहीं है? मुख्य राय न्यायमूर्ति नरीमन द्वारा दी गई थी और एक सहमति राय न्यायमूर्ति वी रामसुब्रमण्यम द्वारा दी गई थी।
न्यायालय का निर्णय	न्यायमूर्ति नरीमन ने कहा कि धारा 65बी (1) मूल इलेक्ट्रॉनिक रिकॉर्ड के बीच अंतर करती है, जो उस कंप्यूटर में निहित है जिसमें जानकारी पहले संग्रहीत की जाती है और द्वितीयक प्रतियां जो प्राथमिक इलेक्ट्रॉनिक रिकॉर्ड से बनाई जाती हैं। उदाहरण के लिए, वर्तमान मामले में, मूल इलेक्ट्रॉनिक रिकॉर्ड चुनाव आयोग का कंप्यूटर होगा जिसमें वीडियो फुटेज को पहले संग्रहीत किया जाता है। सीडी जहां वीडियो रिकॉर्डिंग की सामग्री की प्रतिलिपि बनाई गई है, इलेक्ट्रॉनिक रिकॉर्ड की द्वितीयक प्रतियां होंगी। यह माना गया कि धारा 65बी(4) के तहत प्रमाण पत्र तभी प्राप्त करना होगा जब इलेक्ट्रॉनिक रिकॉर्ड की द्वितीयक प्रतियां न्यायालय के समक्ष पेश की जाती हैं। जब मूल इलेक्ट्रॉनिक रिकॉर्ड प्रस्तुत किया जाता है तो प्रमाण पत्र का उत्पादन आवश्यक नहीं होगा। मूल इलेक्ट्रॉनिक रिकॉर्ड को सीधे साक्ष्य के रूप में जोड़ा जा सकता है यदि कंप्यूटर/टेबलेट/मोबाइल फोन का मालिक गवाह बॉक्स में कदम रखता है और यह स्थापित करता है कि जिस डिवाइस में जानकारी पहले संग्रहीत की जाती है वह उसके स्वामित्व/संचालित होती है। यदि कंप्यूटर जहां इलेक्ट्रॉनिक रिकॉर्ड पहले संग्रहीत किया गया था, कंप्यूटर नेटवर्क या कंप्यूटर सिस्टम का हिस्सा होता है (जैसा कि सूचना प्रौद्योगिकी

	अधिनियम, 2000 के तहत परिभाषित किया गया है), और ऐसा नेटवर्क लाना संभव नहीं है अदालत में भौतिक रूप से प्रणाली, फिर द्वितीयक प्रतियां धारा 65 बी (4) द्वारा निर्धारित प्रमाण पत्र के साथ प्रस्तुत की जा सकती हैं। न्यायमूर्ति नरीमन ने अनवर बनाम बशीर में लिए गए विचार से भी सहमति व्यक्त की – जिसमें कहा गया था कि धारा 65 बी इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता के लिए अपने आप में एक पूर्ण कोड है और साक्ष्य अधिनियम के अन्य प्रावधानों से प्रभावित नहीं होगा। अनवर बनाम बशीर ने यह भी माना कि – यदि साक्ष्य अधिनियम की धारा 62 के तहत प्राथमिक साक्ष्य के रूप में एक इलेक्ट्रॉनिक रिकॉर्ड का उपयोग किया जाता है, तो यह साक्ष्य अधिनियम की धारा 65–बी में शर्तों के अनुपालन के बिना साक्ष्य में स्वीकार्य है। । न्यायमूर्ति नरीमन ने स्पष्ट किया कि साक्ष्य अधिनियम की धारा 62 के तहत शब्दों को हटाकर इस उक्ति को पढ़ा जाना चाहिए। ऐसा इसलिए है क्योंकि धारा 65बी इलेक्ट्रॉनिक साक्ष्य के लिए एक पूर्ण कोड है और धारा 62 जैसे अन्य प्रावधानों का स्थान लेगा। न्यायमूर्ति नरीमन का तात्पर्य यहां यह है कि धारा 62 का उल्लेख करना आवश्यक नहीं है, क्योंकि धारा 65बी(1) स्वयं मूल इलेक्ट्रॉनिक रिकॉर्ड और इलेक्ट्रॉनिक रिकॉर्ड की द्वितीयक प्रतियों के बीच अंतर करती है।
निर्णय के विस्तृत अध्ययन के लिए लिंक https://indiankanoon.org/doc/172105947/	

P.Gopalkrishnan @Dileep v. State of Kerela & Anr.	
केस का संक्षिप्त विवरण	क्या पेन–ड्राइव में इलेक्ट्रॉनिक रिकॉर्डिंग को साक्ष्य के रूप में स्वीकार किया जा सकता है और साक्ष्य अधिनियम, 1872 और भारतीय दंड संहिता की धारा 29 के अनुसार दस्तावेज के रूप में माना जा सकता है। इसके अलावा, चूंकि यह एक बलात्कार का मामला था, अभियोजन पक्ष का पूरा मामला पेन–ड्राइव की सामग्री पर निर्भर था, जिसमें कथित घटना की वीडियो रिकॉर्डिंग शामिल थी। जब आरोपी ने इसकी कॉपी मांगी तो पीड़िता को अपनी निजता की चिंता थी और वह आरोपी को पेन ड्राइव सौंपने से डरती थी क्योंकि उसे वीडियो के गलत इस्तेमाल की आशंका थी। आरोपी के इस अनुरोध ने गंभीर सवाल खड़े किए और पीड़ित के निजता के अधिकार और आरोपी के निः शुल्क परीक्षण के अधिकार को संतुलित करने की आवश्यकता को उठाया ताकि वह जान सके कि अभियोजन का मामला क्या है और उसके अनुसार तैयारी कर सकता है। ये दोनों अधिकार भारत के संविधान के अनुच्छेद 21 के दायरे में आते हैं जो जीवन का अधिकार है, जिसे कानून द्वारा स्थापित प्रक्रिया द्वारा ही कम किया जा सकता है। साथ ही ये दोनों अधिकार प्रकृति में निरपेक्ष नहीं हैं। जब इस तरह का विवाद उत्पन्न होता है तो एक मौलिक अधिकार को दूसरे पर वरीयता नहीं दी जा सकती। न्यायाधीशों ने दोनों अधिकारों को आंशिक रूप से संरक्षित करके

	संतुलन बनाया, जो अंततः सर्वोत्तम के लिए काम करता था।
न्यायालय के द्वारा विचारणीय बिन्दु	क्या सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 2(1)(टी) के तहत एक मेमोरी कार्ड/पेन–ड्राइव की सामग्री इलेक्ट्रॉनिक रिकॉर्ड होने के कारण भारतीय साक्ष्य अधिनियम, 1872 की धारा 3 और भारतीय दंड संहिता, 1860 की धारा 29 के तहत दस्तावेज के रूप में मानी जाएगी। । यदि हाँ, तो क्या मजिस्ट्रेट को बलात्कार के एक कथित अपराध के लिए अभियोजन का सामना कर रहे अभियुक्त को मेमोरी कार्ड/पेन ड्राइव की एक क्लोन प्रति देनी चाहिए थी क्योंकि उसे पुलिस रिपोर्ट में जोड़ा गया था और अभियोजन पक्ष ने आरोपी के खिलाफ इसका इस्तेमाल करने पर भरोसा किया था। . क्या अदालत बलात्कार की कथित घटना के संबंध में पेन ड्राइव की सामग्री की क्लोन प्रति प्राप्त करने के आरोपी के अनुरोध को इस आधार पर अस्वीकार कर सकती है कि इससे पीड़िता की गोपनीयता और गरिमा का उल्लंघन होगा और इसके दुरुपयोग की संभावना पर आरोपी द्वारा कॉपी किया गया संस्करण।
न्यायालय का निर्णय	जिसमें माननीय सर्वोच्च न्यायालय ने कहा था कि मेमोरी कार्ड/पेन ड्राइव की सामग्री इलेक्ट्रॉनिक रिकॉर्ड होने के कारण एक दस्तावेज के रूप में माना जाना चाहिए। यदि अभियोजन उसी पर भरोसा कर रहा है, तो आमतौर पर आरोपी को उसकी एक क्लोन कॉपी दी जानी चाहिए ताकि वह मुकदमे के दौरान प्रभावी बचाव पेश कर सके। हालांकि, **शिकायतकर्ता/गवाह की गोपनीयता या उसकी पहचान जैसे मुद्दों से जुड़े मामलों में, अदालत को मुकदमे के दौरान प्रभावी बचाव पेश करने के लिए आरोपी और उसके वकील या विशेषज्ञ को केवल निरीक्षण प्रदान करने के लिए उचित ठहराया जा सकता है। पहली बार माननीय सर्वोच्च न्यायालय ने पीड़ित की निजता का उल्लंघन करने वाले किसी भी दस्तावेज की आपूर्ति से इनकार किया।**
निर्णय के विस्तृत अध्ययन के लिए लिंक https://indiankanoon.org/doc/160693717/	

Sanjaysinh Ramrao Chavan vs Dattatray Gulabrao Phalke & Anr CRIMINAL APPEAL NO. 97 OF 2015, Supreme court	
केस का संक्षिप्त विवरण	मामला अपनी जमीन के गैर–कृषि उपयोग के लिए प्रमाण पत्र प्राप्त करने के लिए रिश्वत के रूप में 75,000/– रुपये की राशि का भुगतान की राशि लेने का था। जिसमें जो रिश्वत की राशि की बातचीत रिकोर्ड की गई थी। वह एक टेप रिकोर्ड में रिकोर्ड की गई थी। जो किसी कारणवश बाद में खराब हो गया। गवाहों के बयान और फर्द ट्रांसक्रिप्ट से

	जुडा हुआ था।
न्यायालय के द्वारा विचारणीय बिन्दु	मामलें में सोर्स की सत्यता पर माननीय न्यायालय को अपना निर्णय देना था।
न्यायालय का निर्णय	आरोप का समर्थन करने का एकमात्र आधार बातचीत है जिसे वॉयस रिकॉर्डर द्वारा रिकॉर्ड किया गया। फॉरेंसिक साइंस लैबोरेट्रीज, महाराष्ट्र राज्य के निदेशालय ने रिपोर्ट के माध्यम से कहा है कि बातचीत श्रव्य स्थिति में नहीं है और इसलिए, इसे स्पेक्ट्रोग्राफिक विश्लेषण के लिए नहीं माना जा सकता था। चूंकि वॉयस रिकॉर्डर स्वयं विश्लेषण के अधीन नहीं है, इसलिए अनुवादित संस्करण पर भरोसा करने का कोई मतलब नहीं है। स्रोत के बिना अनुवाद की कोई प्रामाणिकता नहीं है। स्रोत और प्रामाणिकता इलेक्ट्रॉनिक साक्ष्य के लिए दो प्रमुख कारक हैं।
निर्णय के विस्तृत अध्ययन के लिए लिंक https://indiankanoon.org/doc/86828078/	

Mr. Virendra Khanna vs State Of Karnataka 2020	
केस का संक्षिप्त विवरण	वादी द्वारा अनुसंधान अधिकारी को अपने मोबाइल के पासवर्ड नहीं दिया गया।

1. क्या किसी आरोपी को अपना मोबाइल फोन एक्सेस करने के लिए पासवर्ड या बायोमेट्रिक्स प्रस्तुत करने का निर्देश दिया जा सकता है?

जांच अधिकारी निश्चित रूप से आरोपी को पासवर्ड या किसी भी पहचान योग्य बायोमेट्रिक को आवश्यकतानुसार प्रदान करने का निर्देश दे सकता है या अनुरोध कर सकता है।

2. क्या अभियुक्त को अपना पासवर्ड या बायोमेट्रिक्स प्रस्तुत करने के लिए न्यायालय द्वारा स्वयं स्वप्रेरणा से आदेश जारी किया जा सकता है?

अदालत स्वयं आरोपी को पासवर्ड या बायोमेट्रिक्स प्रस्तुत करने के लिए स्वतः संज्ञान आदेश जारी नहीं कर सकती क्योंकि अदालत हमारे देश में जांच प्रक्रिया का हिस्सा नहीं है। इस प्रकार, अदालत द्वारा स्वतः संज्ञान आदेश जारी नहीं किया जा सकता है।

3. ऐसी स्थिति में जहां आरोपी पासवर्ड या बायोमेट्रिक्स उपलब्ध नहीं करा रहा है, जांच अधिकारी क्या कानूनी उपाय कर सकता है?

ऐसे में जांच अधिकारी मोबाइल फोन या किसी अन्य डिवाइस के लिए सर्च वारंट जारी करने के लिए अदालत का दरवाजा खटखटा सकता है।

4. स्मार्ट फोन या कंप्यूटर सिस्टम की तलाशी वारंट जारी कराने की क्या शर्त होंगी?
दो परिस्थितियॉ हो सकती है 1. साधारण और 2. आकस्मिक। साधारण में धारा 91 सीआरपीसी का नोटिस जारी करके सहमति ली जाए। यदि सहमति नहीं दे तो संबंधित न्यायालय से तलाशी वारंट जारी करवा सकता है।
आकस्मिकता होने पर अनुसंधान अधिकारी धारा 102 सीआरपीसी के तहत् उसे जब्त कर सकता है।

5. यदि उसके मोबाइल फोन/डिवाइस से आवश्यक डेटा एकत्र किया जाता है तो क्या आरोपी को दोषी पाया जाएगा?

नहीं, यदि मोबाइल फोन या आरोपी के किसी अन्य उपकरण से डेटा एकत्र किया जाता है, तो इसका मतलब यह नहीं है कि वह अपराध का पूरी तरह से दोषी है।

6. क्या पासवर्ड और अन्य विवरण प्रस्तुत करना सहमति की बाध्यता या आत्म–अपराध के समान होगा?

नहीं, आरोपी के मोबाइल फोन में केवल एक संबंधित दस्तावेज या फाइल की उपस्थिति उसके अपराध को साबित नहीं करती है और आरोपी को खुद को साबित करने का मौका दिया जाएगा।

7. क्या पासवर्ड देना या ईमेल खातों तक पहुंच देना आरोपी के निजता के अधिकार का उल्लंघन होगा?

अदालत ने स्पष्ट रूप से कहा है कि जांच के दौरान जांच अधिकारी द्वारा व्यक्तिगत और गोपनीय डेटा का उपयोग, निजता के अधिकार का उल्लंघन नहीं है । हालांकि, ऐसी जानकारी को गोपनीयता में सुरक्षित रखने की जिम्मेदारी केवल जांच अधिकारी द्वारा वहन की जाएगी।

8. यदि तलाशी वारंट जारी करने के बाद भी आरोपी या कोई व्यक्ति अपने मोबाइल या कम्प्यूटर का पासवर्ड, बायोमेट्रिक उपलब्ध नहीं कराता है और मना कर देता है तो उसके लिए क्या किया जाना चाहिए?

ऐसे मै दो स्थितियॉ हो सकती है जिसमें से एक जब वह पासवर्ड, पासकोड या बायोमेट्रिक दे ही नहीं तो यह उसके विरूद्ध पढा जावेगा।
दूसरी स्थिति में यदि वह देता भी है तो गलत देता है ऐसे स्थिति के कारण हो सकता है कि उस उपकरण में मौजूद डाटा डिलिट हो जावे। अतः उस व्यक्ति को अपना पासवर्ड बताने का केवल एक ही अवसर दिया जाना होगा।

इसके बाद अनुसंधान अधिकारी के न्यायालय में आवेदन से अनुमति ले कर किसी ऐसी ऐजेंसी की सहायता ले सकता जो उस पासवर्ड, पासकोड या बायोमेट्रिक को क्रेक करने में सक्षम है। जिसमें पासवर्ड, पासकोड या बायोमेट्रिक सेवा प्रदाता कंपनी या ईमेल कंपनी हो सकती है। यदि उस के द्वारा उस सबूत के मामले में डिजिटल साक्ष्य के किसी नियम का उल्लंघन होता है तो भी वह मान्य होगा। यदि ऐसे में किसी प्रकार की कोई हानि होती है तो उसके लिए वह आरोपी या व्यक्ति उसके लिए जिम्मेदार होगा और यह उसके विरूद्ध साक्ष्य में माना जावेगा।

9. अनुसंधान अधिकारी को स्मार्टफोन और/या इलेक्ट्रॉनिक उपकरणों के संबंध में क्या सुरक्षा और सुरक्षा लेनी होगी?

जांच अधिकारी या खोज दल को उचित और वैज्ञानिक तरीके से खोज करने की आवश्यकता है, खासकर इलेक्ट्रॉनिक उपकरण, स्मार्टफोन या ईमेल खाते में क्या खोजना है?

. पर्सनल कंप्यूटर या लैपटॉप के मामले में

1. किसी भी इलेक्ट्रॉनिक उपकरण, स्मार्टफोन या ई–मेल खाते के संबंध में परिसर की तलाशी लेते समय, एक योग्य फोरेंसिक परीक्षक के साथ खोज दल होना चाहिए।

2. परिसर की तलाशी लेते समय, जांच अधिकारी को साक्ष्य के लिए कंप्यूटर का उपयोग नहीं करना चाहिए या कंप्यूटर की खोज करने का प्रयास नहीं करना चाहिए। कंप्यूटर का उपयोग या खोज एक उचित रूप से अधिकृत और योग्य फोरेंसिक परीक्षक द्वारा किया जाना चाहिए।

3.तलाशी के समय जिस स्थान पर कंप्यूटर रखा या रखा जाता है उसकी फोटो इस प्रकार ली जानी चाहिए कि बिजली, नेटवर्क आदि सहित तारों के सभी कनेक्शन ऐसे फोटोग्राफ में कैद हो जाएं।

4. कंप्यूटर या लैपटॉप के आगे और पीछे, सभी बाह्य उपकरणों से जुड़ा है उनकी फोटो ली जानी चाहिए।

5. कंप्यूटर या लैपटॉप किस तरह से जुड़ा है, यह दिखाते हुए एक आरेख तैयार किया जाना चाहिए।

6. यदि कंप्यूटर या लैपटॉप पावर–ऑफ मोड में है, तो उसे चालू नहीं किया जाना चाहिए।

7. यदि कंप्यूटर चालू है और स्क्रीन खाली है, तो माउस को स्थानांतरित किया जा सकता है और जैसे ही छवि स्क्रीन पर दिखाई देती है, स्क्रीन की तस्वीर ली जानी चाहिए।

8. यदि कंप्यूटर चालू है, तो जांच अधिकारी को कंप्यूटर को बंद नहीं करना चाहिए। जहां तक संभव हो, जांच अधिकारी को अस्थिर मेमोरी यानी रैम में उपलब्ध डेटा को डाउनलोड करने के लिए कंप्यूटर फोरेंसिक परीक्षक की सेवा मिलने तक सुरक्षित रखना चाहिए क्योंकि उक्त डेटा कंप्यूटर या लैपटॉप के पावर डाउन होने पर खो जाएगा।

9. यदि कंप्यूटर चालू है और एक नेटवर्क से जुड़ा है, तो जांच अधिकारी एक फॉरेंसिक परीक्षक की सेवा प्राप्त करने तक आईपी एड्रेस, वास्तविक नेट वर्क कनेक्शन, नेट वर्क लॉग, आदि जैसे अस्थिर नेट वर्क डेटा को कैप्चर करने के लिए पहचाना के लिए सुरक्षित जाना चाहिए।

10. मैक पता का पता लगा कर उसे सुरक्षित किया जाना चाहिए।

11. फोरेंसिक परीक्षक के उपलब्ध न होने की संभावना न होने की स्थिति में, कंप्यूटर को अनप्लग करें, कंप्यूटर और तारों को लेबल करने के बाद अलग–अलग फैराडे कवर में पैक करें।

12. लैपटॉप के मामले में यदि पावर कॉर्ड को हटाने से लैपटॉप बंद नहीं होता है तो बैटरी को हटा देना चाहिए।

13. यदि लैपटॉप की बैटरी को हटाया नहीं जा सकता है, तो लैपटॉप को बंद कर दें और इसे फैराडे बैग में पैक कर दें ताकि लैपटॉप पर किसी भी संचार को ब्लॉक किया जा सके क्योंकि आजकल अधिकांश लैपटॉप में वायरलेस संचार सक्षम है, भले ही लैपटॉप स्टैंड बाई मोड में है।

नेटवर्क वाले उपकरणों की जब्ती:

कंप्यूटर, लैपटॉप आदि की जब्ती के संबंध में उठाए गए उपरोक्त कदमों के अलावा, यदि उक्त उपकरण किसी नेटवर्क से जुड़ा है।

.1. यह पता लगाने के लिए कि क्या उक्त उपकरण किसी रिमोट स्टोरेज डिवाइस या साझा नेटवर्क ड्राइव से जुड़ा है, तो रिमोट स्टोरेज डिवाइस और साझा नेटवर्क डिवाइस को जब्त किया जाना चाहिए।

2. वायरलेस एक्सेस पॉइंट्स, राउटर्स, मोडेम्स और ऐसे एक्सेस पॉइंट्स से जुड़े किसी भी उपकरण को जब्त करना होगा। यह भी हो सकता है राउटर्स, मोडेम्स गुप्त रूप से मौजूद हो।

3. यह पता लगाने के लिए कि क्या किसी असुरक्षित वायरलेस नेटवर्क को स्थान से एक्सेस किया जा रहा है। यदि ऐसा है तो उसकी पहचान करें और असुरक्षित वायरलेस उपकरणों को सुरक्षित करें क्योंकि हो सकता है कि आरोपी ने उक्त असुरक्षित वायरलेस उपकरणों का उपयोग किया हो।

.4. यह पता लगाने के लिए कि नेटवर्क का रखरखाव कौन कर रहा है और नेटवर्क को कौन चला रहा है – नेटवर्क के संचालन से संबंधित सभी विवरण प्राप्त करें और ऐसे नेटवर्क मैनेजर से जब्त किए जाने वाले उपकरणों की भूमिका प्राप्त करें।

5. नेटवर्क मैनेजर से जब्त की जाने वाली मशीन के नेटवर्क लॉग्स प्राप्त करे ताकि नेट वर्क की उक्त मशीन द्वारा की गई पहुंच का पता लगाया जा सके।

मोबाइल डिवाइस

मोबाइल डिवाइस का मतलब कंप्यूटर या लैपटॉप स्मार्टफोन, मोबाइल फोन, टैबलेट जीपीएस यूनिट आदि शामिल हैं। मोबाइल डिवाइस की जब्ती के संबंध में कंप्यूटर या लैपटॉप के लिए उठाए गए कदमों के अलावा, अतिरिक्त कदम निम्न हैः

1. डिवाइस को किसी फैराडे बैग में पैक करके नेटवर्क से संचार करने या वाईफाई या मोबाइल डेटा के माध्यम से किसी भी वायरलेस संचार को प्राप्त करने से रोकें।

2. डिवाइस को पूरे समय चार्ज रखें, क्योंकि अगर बैटरी खत्म हो जाती है, तो वोलेटाइल मेमोरी में उपलब्ध डेटा खो सकता है।

3. स्लिम–स्लॉट की तलाश करें सिम कार्ड को हटा दें ताकि मोबाइल नेटवर्क तक किसी भी पहुंच को रोकने के लिए, सिम कार्ड को फैराडे बैग में अलग से पैक करें।

4. यदि डिवाइस पावर–ऑफ मोड में है, तो बैटरी को हटाया भी जा सकता है और अलग रखा जा सकता है।

5. यदि डिवाइस चालू है, तो इसे एंड्रॉइड डिवाइस में एयरप्लेन मोड में या आईओएस डिवाइस में एयरप्लेन मोड में रखें।

उपरोक्त **सभी मामलों में, जब्त किए गए उपकरणों को**

- यथासंभव धूल रहित वातावरण और तापमान नियंत्रित में रखा जाना चाहिए।
- तलाशी के दौरान जांच अधिकारी को किसी भी इलेक्ट्रॉनिक स्टोरेज डिवाइस जैसे सीडी, डीवीडी, ब्लू–रे, पेन ड्राइव, एक्सटर्नल हार्ड ड्राइव, यूएसबी थंब ड्राइव, सॉलिड–स्टेट ड्राइव आदि को जब्त करना होगा। परिसर, लेबल और उन्हें एक फैराडे बैग में अलग से पैक करें।
- कंप्यूटर, स्टोरेज मीडिया, लैपटॉप आदि को मैग्नेट, रेडियो ट्रांसमीटर, पुलिस रेडियो आदि से दूर रखा जाना चाहिए, क्योंकि वे उक्त उपकरणों में डेटा पर प्रतिकूल प्रभाव डाल सकते हैं।
- निर्देश मैनुअल, दस्तावेज आदि प्राप्त करने के लिए परिसर की तलाशी लेना, साथ ही यह पता लगाना कि कहीं पासवर्ड तो नहीं लिखा गया है क्योंकि कई बार उक्त स्थान परउपकरण रखने वाले व्यक्ति ने बॉक, राइटिंग पैड या इसी तरह का पासवर्ड लिखा होगा।
- जांच/खोज दल के परिसर में प्रवेश करने से लेकर उनके बाहर निकलने तक पूरी

प्रक्रिया को लिखित रूप में प्रलेखित किया जाना है।	
निर्णय के विस्तृत अध्ययन के लिए लिंक	https://indiankanoon.org/doc/87379349/

Sharat Babu Digumarti Vs Govt Of NCT Of Delhi

वर्ष 2004 में, रवि राज द्वारा www.bazee.com (अब www.eBay.in) पर एक नाबालिग लड़की का एक Mms बिक्री के लिए अपलोड किया। उस अश्लील सामग्री की सूचना मिलने के बाद 38 घंटे के भीतर उसे हटाया गया लेकिन तुरंत नहीं हटाया गया। जिसमें साइट की सुरक्षा सुविधा बुरी तरह विफल रही।

जांच के बाद क्राइम ब्रांच ने आरोपित रवि राज के साथ सीईओ अवनीश बजाज, सीरियस मैनेजर शरत बाबू दिगुमर्ति को दबाया। आरोप पत्र आईटी अधिनियम, 2000 की धारा 292, 294 और धारा 67 के अनुसार तैयार किया गया था। (इसे baazie.com मामले के रूप में भी जाना जाता है)। हर आरोपी के लिए सजा का अनुपात अलग–अलग था।

अवनीश बजाज ने सीआरपीसी (1973) की धारा 482 के तहत दिल्ली उच्च न्यायालय में याचिका प्रस्तुत करते हुए दावा किया कि अश्लील सामग्री के प्रकाशन और बिक्री में उनकी कोई संलिप्तता नहीं है, इसलिए आईपीसी की धारा 292, 1860 और आईटी अधिनियम , 2000 की धारा 67 के तहत आरोप नहीं लगाया जाना चाहिए। अदालत ने आईपीसी के प्रावधानों को रद्द कर दिया, लेकिन आईटी अधिनियम, 2000 की धारा 67 और 85 के साथ प्रक्रिया की अनुमति दी। हालांकि, वर्ष 2012 में, शीर्ष अदालत ने दिल्ली उच्च न्यायालय के इस फैसले को उलट दिया और अवनीश बजाज को जिम्मेदार नहीं ठहराया जा सकता है। प्रतिपक्षी दायित्व के लिए, और आईटी अधिनियम के तहत दोषी नहीं ठहराया जा सकता क्योंकि फर्म पर एक आरोपी के रूप में आरोप नहीं लगाया गया था।

इसके बाद तीसरे पक्ष से प्राप्त सामग्री के संबंध में बिचौलियों को सुरक्षा प्रदान करने के लिए आईटी अधिनियम की धारा 79 में संशोधन किया गया।

निर्णय के बिन्दु	यदि एक अपराधी को आईटी अधिनियम, 2000 की धारा 67 के तहत छूट मिल जाती है, तो क्या वह आईपीसी, 1860 की धारा 292 के तहत उत्तरदायी होगा या नहीं?
निर्णय	याचिकाकर्ता का तर्क (शरत बाबू दिगुमर्ति)– आईटी अधिनियम की धारा 67 एक विशेष प्रावधान है इसलिए यह आईपीसी, 1860 की धारा 292 को ओवरराइड करता है। भले ही आरोप खड़े हों, शरत को आईटी अधिनियम की धारा 79 के तहत किए गए हालिया संशोधन की रक्षा की जाएगी। इस तर्क के लिए, विद्वान वकील ने 2000 के आईटी अधिनियम की धारा 81 पर भरोसा किया। श्रेया सिंघल बनाम यूओआई के निर्णय का हवाला देते हुए, जहां सुप्रीम कोर्ट ने धारा 79 की व्याख्या करते हुए पाया कि इंटरनेट से आपत्तिजनक सामग्री हटाने से पहले मध्यस्थ को` सरकार से या अदालत के आदेश या नोटिस

	के माध्यम से वास्तविक जानकारी प्राप्त करनी चाहिए। प्रतिवादी का तर्क (दिल्ली का राष्ट्रीय राजधानी क्षेत्र)– याचिकाकर्ता पर विशेष रूप से वेबसाइट के ट्रस्ट और सुरक्षा प्रबंधक के रूप में उनकी भूमिका के लिए मुकदमा चलाया जा रहा है। आईपीसी, 1860 की धारा 292 के तहत याचिकाकर्ता के आरोप पर रोक लगाने का कोई प्रावधान या नियम नहीं था। निर्णय– शीर्ष अदालत ने पाया कि लीक हुए एमएमएस एक इलेक्ट्रॉनिक मीडिया था। चूंकि धारा 67 विशेष रूप से इलेक्ट्रॉनिक मीडिया के बारे में बात करती है, यह आईपीसी की धारा 292 पर लागू होगी क्योंकि यह कागज, ड्राइंग, पेंटिंग, लेखन में बनाई गई अश्लील सामग्री से संबंधित है, लेकिन इलेक्ट्रॉनिक मीडिया से नहीं। साथ ही, आईटी अधिनियम की धारा 79 द्वारा दी जाने वाली मध्यस्थ को सुरक्षा की भी अनदेखी नहीं की जा सकती है। इसके अलावा, जैसा कि अपराध विशेष कानून के तहत आता है जो कि आईटी अधिनियम है, अपीलकर्ता पर किसी अन्य कानून के साथ आरोप लगाने से दोहरा खतरा हो सकता है (भारत के संविधान के अनुच्छेद 20 (2) के अनुसार गारंटीकृत मौलिक अधिकार के तहत उल्लंघन)। इसलिए, अपील की अनुमति दी जाती है, उच्च न्यायालय और निचली अदालत द्वारा पारित आदेशों को अपास्त किया जाता है और अपीलकर्ता के खिलाफ दर्ज आपराधिक मुकदमा रद्द किया जाता है।
लिंक	https://indiankanoon.org/doc/153597150/

मॉडल प्रश्न व उत्तर

प्रश्नः1 डिजिटल साक्ष्य के बारे में उसके विधिक प्रावधानों के साथ विस्तार से बताईये। द्वितीयक साक्ष्य के लिए क्या अनिवार्यताएँ है? डिजिटल साक्ष्य के स्रोत व उनमें स्थित डिजिटल साक्ष्य के बारे में उदाहरण देते हुए वर्णन करों।

उत्तरःडिजिटल साक्ष्य को आईटी संशोधन अधिनियम 2008 की धारा 79ए में परिभाषित किया गया हैा वह संभावित मूल्य जिसे इलेक्ट्रॉनिक रूप में संग्रहीत या प्रसारित किया जा सकता हैा उसे डिजिटल साक्ष्य कहते हैा कंप्यूटर, डिजिटल ऑडियो, डिजिटल वीडियो, सेल फोन, फैक्स मशीन, स्टोरेज डिवाइस आदि डिजिटल साक्ष्य है। अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 5 का अवलोकन करे।

प्रश्नः2 अपराध स्थल पर हमें जाते समय हमें यह पता होना चाहिए कि वहॉ पर किस प्रकार के डिजिटल साक्ष्य प्राप्त हो सकते है। उन तरीकों का विश्लेषण कीजिए जिनके आधार पर एक अनुसंधान अधिकारी को साक्ष्यों को जब्त करते समय विभाजित करना होगा।

उत्तरः अपराध स्थल पर डिजिटल साक्ष्यः–

डिजिटल साक्ष्य को उनकी उत्पत्ति के आधार पर निम्न प्रकार से विभाजित किया गया–

1.उपयोगकर्ता द्वारा सृजितः इन साक्ष्यों में उपयोग कर्ता द्वारा बनाई गई फाइलें होती हैं जैसे कि पाठ्य दस्तावेज, ईमेल, चौट, चित्र, वीडियो और सिस्टम पर उपयोक्ता द्वारा बनाए गए वेब पृष्ठ।

2. उपयोगकर्ता द्वारा सुरक्षितः इन साक्ष्यों में वे फाइल या डिवाइस है जो उपयोगकर्ता द्वारा पासवर्ड का उपयोग करके सुरक्षित किए जाते हैं। साक्ष्य प्राप्त करने या उसका विश्लेषण करने के लिए इन डिजिटल साक्ष्यों तक पहुच प्राप्त करने से पहले उपयोगकर्ता से प्रमाण पत्र प्राप्त करने की आवश्यकता होती है। उदाहरणों में उपयोगकर्ता द्वारा या सिस्टम द्वारा बनाई गई फाइलें या पासवर्ड का उपयोग करके उपयोगकर्ता द्वारा संरक्षित फाइलें शामिल हैं।
3. सिस्टम द्वारा उत्पन्नः ऑपरेटिंग सिस्टम द्वारा स्वत उपयोगकर्ता के बिना बनाए जाते हैं।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 8 का अवलोकन करे।

प्रश्नः 3 कम्प्यूटर की जब्ती करते समय उसके केटेगरी के आधार पर विभाजन करते हुए उसका चार्ट बनाईये।
उत्तरः जानकारी के लिए इस पुस्तक के पेज नंबर 12 का अवलोकन करे।

प्रश्नः लैपटॉप की जब्ती का उसकी केटेगरी के अनुसार चार्ट बनाईये।
उत्तरः जानकारी के लिए इस पुस्तक के पेज नंबर 24 का अवलोकन करे।

प्रश्नः4 बिना किसी पासवर्ड या लॉक के मोबाइल फोन ऑन कंडीशन में है तो उसकी जब्ती परिवहन व सावधानियों के बारे में बताईये।
उत्तरः
1. घटनास्थल को पीले टेप की सहायता से सुरक्षित करते हैं

2- अपराध स्थल की फोटोग्राफी और वीडियोग्राफी करें।

3- अगर डिवाइस "ON'मोड में है तो सबसे पहले उसे तुरंत फ्लाइट मोड (Flite mode – मोबाइल डिवाइस को इंटरनेट कनेक्टिविटी से बाहर करने के लिए) पर डाल दें।

4- कनेक्टिंग केबल, चार्जर, पैकेजिंग मैनुअल, फोन बिल आदि को जब्त कर लें

5- मोबाइल हैंडसेट से संबंधित बिल या अन्य कोई कागज यदि उपलब्ध हो तो संलग्न करें

6- ध्यान रखें कि कुछ मोबाइल फोन हैंडसेट में स्वचालित हाउसकीपिंग फंक्शन हो सकते

7- दो गवाहों के साथ फर्द जब्ती पर हस्ताक्षर करें

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 37 का अवलोकन करे।

प्रश्नः5 साइबर अपराध जांच के लिए चुनौतियां क्या क्या है?

उत्तरः साइबर अपराधी गुमनाम हो कर अपराध करता है क्योकि ऐसा करने में साइबर तकनीक उन्हे सक्षम बनाती है। यह गुमनामी अनुसंधान के लिए एक बडी चुनौती है।

- अत्यंत नाजुक है।
- पर्याप्त ज्ञान और प्रशिक्षण
- सामंजस्यपूर्ण राष्ट्रीय साइबर–अपराध कानूनों और अंतर्राष्ट्रीय की कमी
- साक्ष्य आवश्यकताओं का मानकीकरण नहीं होना।
- तकनीक में तेजी से बदलाव होना।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 48 का अवलोकन करे।

प्रश्नः6 मोबाइल सेवा प्रदाता के बारे में विस्तार से बताइये ? मोबाइल सेवा प्रदाता के नोडल अधिकारी की जिम्मेदारियों के बारे में बताईये। उनसे अनुसंधान अधिकारी द्वारा कौन कौनसी सूचनाएँ अपने अनुसंधान में प्राप्त की जा सकती है? विभिन्न सूचना प्राप्त करने की समय रेखा बताइये।

उत्तरः एक टीएसपी या एमएसपी एक प्रकार का संचार सेवा प्रदाता है जो परंपरागत रूप से टेलीफोन और अन्य समान सेवाएं प्रदान करता है। इन दिनों दूरसंचार और मोबाइल सेवा प्रदाता न केवल दूरसंचार सेवाएं प्रदान कर रहे हैं बल्कि इंटरनेट सेवाएं भी प्रदान कर रहे हैं।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 52 का अवलोकन करे।

प्रश्नः7 वेबसाइट क्या है ? ये कितने प्रकार की होती है? अनुसंधान अधिकारी किसी वेबसाइट से क्या जानकारी प्राप्त कर सकता है?

उत्तरः एक वेबसाइट वेब पेजों और संबंधित सामग्री का एक संग्रह है जिसे एक सामान्य डोमेन नाम से पहचाना जाता है और कम से कम एक वेब सर्वर पर होता है जिस पर उसे चलाया जाता है। उल्लेखनीय उदाहरण हैं wikipedia-org, google.com और amazon.com

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 59 का अवलोकन करे।

प्रश्नः8 वीओआइपी (वॉयस ओवर इंटरनेट प्रोटोकॉल) के बारे में बताइये। आजकल वीओआइपी कॉलिंग से अपराध क्यों बढ रहे है? वीओआइपी सेवा प्रदाता से अनुसंधान अधिकारी कौन कौन सी सूचना प्राप्त कर सकता है?

उत्तरः इसे आईपी टेलिफोनी, इंटरनेट टेलिफोनी भी करते है। वीओआइपी विडियों व ऑडियो कॉलिंग की आधुनिक इंटरनेट सेवा है जिसमें कॉल करने के लिए इंटरनेट का उपयोग किया जाता है। पहले जो हम वॉयस कॉलिंग करते थे वह केवल ओडियों कॉल ही होती थी जिसमें एनालॉग सिंग्नलों का उपयोग किया जाता था।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 61 का अवलोकन करे।

प्रश्नः9 निम्न पर टिप्पणी लिखिऍं–

(1)इंटरपोल

(2)इंटरपोल–इंडिया

(3)राष्ट्रीय केन्द्रीय ब्यूरो (एनसीबी)

उत्तरः अंतर्राष्ट्रीय आपराधिक पुलिस संगठन (आईसीपीओ) इसका पूरा नाम है। इसमें कुल 194 सदस्य देश है। जिसका मुख्यालय –लिओंस, फ्रांस में स्थित है। इसके छह महत्वपूर्ण अंग हैं।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 64 का अवलोकन करे।

प्रश्नः10 अनुरोध पत्र तैयार किये जाने के समय जाँच एजेन्सी द्वारा क्या क्या सावधानियाँ बरती जानी चाहिए ?

उत्तरः जानकारी के लिए इस पुस्तक के पेज नंबर 71 का अवलोकन करे।

प्रश्नः11 खोजी उपकरण के रूप में ई–मेल हेडर की सीमाएं क्या है?

उत्तरः किसी ईमेल के मूल अर्थात ओरिजनल आईपी पते के बारे में सही जानकारी ईमेल हेडर से मिल सके ऐसा हर मामले में संभव नहीं है।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 83 का अवलोकन करे।

प्रश्नः12 कॉल डिटेल रिकोर्ड के बारे में आप क्या जानते है? इसके कानूनी प्रावधान क्या क्या है? सीडीआर के प्रकार के बारे में बताईये।

उत्तरः मोबाइल पर कॉल करने के लिए निम्न तीन की महत्त्वपूर्ण भूमिका हैः–

- मोबाइल फोन
- मोबाइल सिम
- मोबाइल सेवा प्रदाता कंपनी

जब हम किसी व्यक्ति से उसके मोबाइल पर बात करना चाहते है तो आवश्यक है कि हमारे पास एक मोबाइल फोन हो। उस मोबाइल फोन में एक सिम लगी हुई हो जो या तो उसमें बाहर से ले कर लगाई जावेगी या उस मोबाइल के अंदर ही मोजूद हो जैसे–ई सिम। साथ ही सिम मोबाइल सेवा प्रदाता से जुडी हुई हो।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 83 का अवलोकन करे।

प्रश्नः13 आईपीडीआर का परिचय दीजिए। ये कितने प्रकार की होती है? इसकी विभिन्न शब्दावलियों के बारे में बताइये।

उत्तरः एक आईपीडीआर जिसे इंटरनेट प्रोटोकॉल डेटा रिकॉर्ड के रूप में भी जाना जाता है, एक आईओ को उपयोगकर्ता की इंटरनेट गातिविधियों का पूरा विवरण प्राप्त करने में मदद करता है, जैसे कि विजिट की गई वेबसाइटें, एक्सेस किए गए ऐप्स और उपयोग किए गए सोशल मीडिया एप्लिकेशन। जिस प्रकार मोबाइल से साधारण कॉल करने के लिए हमें मोबाइल नंबरों

की आवश्यकता होती है। उसी प्रकार जब हम इंटरनेट के माध्यम से कोई डेटा को खोज रहे है या इंटरनेट सेवा का उपभोग कर रहे है तो इंटरनेट सेवा प्रदाता हमें एक गातिशील आईपी पता आबंटित करता है। जो इंटरनेट पर हमारी पहचान होता है। डेटा सत्र की जानकारी को कैप्चर करता है, जो आईपीडीआर में उपलब्ध कराया जाता है।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 93 का अवलोकन करे।

प्रश्नः14 मोबाइल में डाटा स्टोरेज के बारे में आप क्या जानते है?

उत्तरः एक मोबाइल फोन में निम्न लोकेशन पर डाटा स्टोर हो सकता हैंः–

- ❖मोबाइल फोन कि internal मेमोरी में
- ❖सिम कार्ड में
- ❖क्लाउड स्टोरेज में
- ❖मेमोरी कार्ड में

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 107 का अवलोकन करें।

प्रश्नः15 सोशल नेटवर्किंग/मीडिया साइट्स से आप क्या समझते है? सोशल नेटवर्कि• कैसे काम करता है? सोशल नेटवर्किंग साइट्स का उदाहर.ा बताइये।

उत्तरः सोशल नेटवर्किंग, घूमने वाले व्यक्तियों को वेबसाइटों और वेब–आधारित(Web based) Application का उपयोग करते हुए एक–दूसरे के संपर्क(Contact) में रहने की अनुमति देता है। फेसबुक, माइस्पेस, ट्विटर और लिंक्डइन सोशल नेटवर्किंग साइट्स उदाहरण हैं। "सोशल नेटवर्क'शब्द की परिभाषा अभी भी बहुत ढीली है, क्योंकि यह अभी भी एक अपेक्षाकृत नई तकनीक है जो तेजी से बदलाव के अधीन है।सोशल नेटवर्किंग दोस्तों, परिवार, सहकर्मियों, ग्राहकों या ग्राहकों के साथ जुड़े रहने के लिए इंटरनेट–आधारित सोशल मीडिया साइटों(Internet&Based Social Media Sites) का उपयोग है। सोशल नेटवर्किंग का एक सोशल उद्देश्य, एक व्यावसायिक उद्देश्य या दोनों हो सकता है, जैसे कि फेसबुक, ट्विटर, लिंक्डइन और इंस्टाग्राम जैसी अन्य साइटों के माध्यम से। सोशल नेटवर्किंग ग्राहकों को संलग्न(attach) करने की मांग करने वाले Marketers के लिए एक महत्वपूर्ण आधार (Base) बन गया है।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 114 का अवलोकन करें।

प्रश्नः16 राजस्थान पुलिस अकादमी स्थित सीसीपीडब्लूसी लैब में स्थित विभिन्न साफ्टवेयर व टूल्स का विवरण के बारे में बताइये।

उत्तरः जानकारी के लिए इस पुस्तक के पेज नंबर 126 का अवलोकन करें।

प्रश्नः17 डार्क नेट क्या है?

उत्तरः एक डार्क नेट इंटरनेट के भीतर एक ओवरले नेटवर्क है जिसे केवल विशिष्ट सॉफ़्टवेयर, कॉन्फ़िगरेशन या ऑथोराइजेशन के साथ एक्सेस किया जा सकता है और अक्सर एक विशिष्ट प्रकार के नेटवर्क संचार का उपयोग करता है।

एक ओवरले नेटवर्क एक कंप्यूटर नेटवर्क है जो दूसरे नेटवर्क के ऊपर स्तरित होता है।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 140 का अवलोकन करें।

प्रश्नः18 डार्क वेब से आप क्या समझते है? वेब कितने प्रकार की होती है?

उत्तरः डार्क वेब वर्ल्ड वाइड वेब सामग्री है जो डार्कनेट पर मौजूद है यह ओवरले नेटवर्क का उपयोग करते हैं जिससे इन्हे एक्सेस करने के लिए विशिष्ट सॉफ्टवेयर, कॉन्फिगरेशन या प्राधिकरण की आवश्यकता होती है। डार्क वेब के माध्यम से, निजी कंप्यूटर नेटवर्क उपयोगकर्ता के स्थान जैसी पहचान संबंधी जानकारी को प्रकट किए बिना गुमनाम रूप से संचार और गातिविधि कर सकते हैं डार्क वेब, डीप वेब का एक छोटा–सा हिस्सा है। वेब का वह हिस्सा जिसे वेब सर्च इंजन द्वारा अनुक्रमित नहीं किया जाता है, हालांकि कभी–कभी डीप वेब शब्द का प्रयोग गलती से डार्क वेब के लिए किया जाता है।

डार्क वेब के अंदर कुछ ऐसी onion साइटस है, जो आपको कभी भी गुगल, याहु जैसे सर्च इंजन में नहीं मिलेंगी, और ना ही आप उनको अपने सामान्य ब्राउजर (क्रोम, मोजिला, फायरफोक्स) से उन तक पहुच सकते हो भले ही उनका यूआरएल क्यू न पता हो और आप अपने नार्मल आईपी पते से भी उन तक नहीं पहुचा जा सकता है ा इसके लिए टोर ब्राउके माध्यम से या किसी सोफटवेयर के माध्य से ही उन तक जाया जा सकता है।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 142 का अवलोकन करें।

प्रश्नः19 क्रिप्टोकरेंसी क्या है? क्रिप्टोकरेंसी की विशेषताए बताइये। क्रिप्टोकरेंसी कैसे काम करती है?

उत्तरः क्रिप्टोकरेंसी एक डिजिटल या आभासी मुद्रा है जिसे क्रिप्टोग्राफी द्वारा सुरक्षित किया जाता है, जिससे नकली या दोहरा खर्च करना लगभग असंभव हो जाता है। कई क्रिप्टोकरेंसी ब्लॉकचैन तकनीक पर आधारित विकेन्द्रीकृत नेटवर्क हैं जो कंप्यूटर के एक अलग नेटवर्क द्वारा लागू एक वितरित खाता बही। क्रिप्टोकरेंसी की एक परिभाषित विशेषता यह है कि वे आम तौर पर किसी भी केंद्रीय प्राधिकरण द्वारा जारी नहीं की जाती हैं, जो उन्हें सैद्धांतिक रूप से सरकारी हस्तक्षेप या हेरफेर से प्रतिरक्षा प्रदान करती हैं।

अधिक जानकारी के लिए इस पुस्तक के पेज नंबर 143 का अवलोकन करें।

प्रश्नः20 सोशल मीडियॉ पर होने वाले साइबर अपराधों में लगने वाली सूचना प्रौधोगिकी अधिनियम और भारतीय दण्ड संहिता की धाराओं की तुलनात्मक सारणी प्रस्तुत कीजिए।

उत्तरः जानकारी के लिए इस पुस्तक के पेज नंबर 146 का अवलोकन करें।

भारतीय साक्ष्य अधिनियम की धारा 65 (बी) का प्रमाण पत्र

मैं अद्योहस्तारकर्ता नाम_____ व्यवसाय_____.
थाना _____राजस्थान, अपनी सर्वोत्तम जानकारी और विश्वास के अनुसार अंकित करता हुँ कि

1. मुझे साइबर क्राइम/पुलिस स्टेशन में दिनांक_____ को पीड़ित/शिकायतकर्ता नाम:_____ व्यवसाय:_____.
निवासी:_____. को ईमेल पते _____@_____से स्पष्ट/अपमानजनक ईमेल प्राप्त करने के संबंध में शिकायत प्राप्त हुई है। प्राप्त शिकायत की प्रकृति के आधार पर अपराध बनना पाया जाने पर सूचना प्रौद्योगिकी अधिनियम (आज तक संशोधित) की धारा _____ के तहत अपराध दर्ज किया गया है। शिकायतकर्ता के अनुसार संदिग्ध का ईमेल पता_____@_____और उनका नाम है।
पीड़ित को संदिग्ध से अश्लील/अपमानजनक संदेश/फोटो/वीडियो प्राप्त हुए थे, और मैंने ऐसे ईमेल के स्क्रीनशॉट लिए हैं, और मैंने ईमेल हेडर के साथ ईमेल डाउनलोड किया है और उसका प्रिंट आउट जमा कर दिया है, मैंने ये सब दस्तावेज मेरे द्वारा जमा कर दिए गए है।

2. मैं फिर से पुष्टि करता हूं कि मैंने स्क्रीनशॉट ले लिए हैं, ईमेल को इसके हेडर के साथ डाउनलोड कर लिया है और इन दस्तावेजों की प्रति जमा कर दी है। मुझे ईमेल का उपयोग करने, ईमेल से संबंधित अनुलग्नकों को संभालने, स्क्रीनशॉट लेने, ईमेल हेडर डाउनलोड करने और कंप्यूटर और प्रिंटर का उपयोग करके प्रिंट आउट लेने की जानकारी है। मैं जिस कंप्यूटर और प्रिंटर का उपयोग उपरोक्त गतिविधियों को किया है वे मेरी जानकारी के अनुसार सामान्य रूप से काम कर रहे है। मैंने इन दस्तावेजों को पीड़ित/शिकायतकर्ता की उपस्थिति में उनकी सहमति से दो गवाहों की उपस्थिति में लिया है जो आवश्यकता पड़ने पर गवाही दे सकते हैं।

3. मैं उपरोक्त सूचीबद्ध दस्तावेजों के साथ यह प्रमाण पत्र जमा करता हूं, मैं पुष्टि करता हूं कि मैंने इन दस्तावेजों (स्क्रीनशॉट, हेडर या प्रिंटआउट) में कोई बदलाव नहीं किया है।

क्रम संख्या	फाइल नाम व पथ	टूल और उसका संस्करण	MD5 hash value	SHA 1 hash value

गवाह 1 का नाम और हस्ताक्षर_____.

गवाह 2 का नाम और हस्ताक्षर_____.

पीड़ित/शिकायतकर्ता का नाम और हस्ताक्षर: _____.

जांच अधिकारी का नाम

जांच अधिकारी की मुहर और हस्ताक्षर

दिनांक:

पुलिस विभाग की अभिरक्षा (ट्रेकिंग फॉर्म की श्रृंखला)

मुकदमा नंबर	**25/2022**	मुकदमा दिनांक	**1 अप्रैल, 2022**
अंतर्गत धारा	66सी, 66डी आईटीएए 2008 एवं 419, 420 आईपीसी	**पुलिस थाना व जिला**	साइबर क्राईम पुलिस स्टेशन जिला जयपुर
जॉच अधिकारी का नाम व पद	यतींद्र कुमार खटाना, पुलिस निरीक्षक	**अभियोगी का नाम व पता**	सोनू कुमार जिला जयपुर
आइटम की जब्ती की दिनांक व समय	2 अप्रैल, 2022 समय 12:30 पीएम	**जब्ती का स्थान**	आमेर, जयपुर
संदिग्ध का नाम	रवि, अमित, शरद व सुरेश		

साक्ष्य का विवरण		
आइटम का नाम	**मात्रा**	**आइटम का विवरण (मॉडल, सीरियल नंबर, मार्क्स स्क्रैचेज इत्यादि)**
मोबाइल फोन	2	आइटम से संबंधित यूनिक नंबर जैसे आईएमईआई नंबर, मैक पता, सीरियल नंबर, मॉडल इत्यादि का विवरण
कम्प्यूटर	1	
लैपटॉप	1	
डीवीआर	2	

हिरासत में लेने की कडी				
आइटम का नाम	**दिनांक व समय**	**जारीकर्ता के हस्तारक्षर व आईडी**	**प्राप्तकर्ता के हस्ताक्षर व आईडी**	**विशेष टिप्पणी/स्थान**

कम्प्यूटर / परिधीय साक्ष्य जब्ती फॉर्म (Computer / Peripheral Evidence Seizure Form)

कार्यालय का नाम:
दिनांक:

पुलिस थाना _____.
जिला _____.
राजस्थान _____.

मुकदमा नंबर	26 / 2022	मुकदमा दिनांक	1 अप्रैल, 2022
अंतर्गत धारा	66सी, 66डी आईटीएए 2008 एवं 419, 420 आईपीसी	पुलिस थाना व जिला	साइबर क्राईम पुलिस स्टेशन जिला जयपुर
जॉच अधिकारी का नाम व पद	यतींद्र कुमार खटाना, पुलिस निरीक्षक	अभियोगी का नाम व पता	सोनू कुमार जिला जयपुर
आइटम की जब्ती की दिनांक व समय	2 अप्रैल, 2022 समय 12:30 पीएम	जब्ती का स्थान	आमेर, जयपुर
संदिग्ध का नाम	रवि, अमित, शरद व सुरेश		

साक्ष्य का विवरण:–

Item Number	Device	Manufacturer	Model	Serial No.	Description
Example: 1	Laptop	HP	P2-1033W	MYL12345678	Black colour HP Laptop in an off condition

Computer – ON Condition

Computer Live Information				
BIOS Date		BIOS Time		
Actual Date		Actual Time		
Time zone		Asset Tag		
Operating System		Operating System Version		
RAM Size		RAM DumpTaken?		
Hash Value (MD5)		Hash Value (SHA1 / SHA256)		
Software Used for RAM Dump		Hard Drive 1 Size		
Hard Drive 2 Size		Hard Drive Interface / Type	SATA ☐	IDE ☐ SSD ☐
Hash Value (MD5)		Hash Value (SHA1 / SHA256)		

Software used for Hashing	Write Blocker Used?	Yes ☐	No ☐

Computer – OFF Condition

Drive Information						
Hard Drive Type	SATA ☐	IDE ☐	SSD ☐	Manufacturer		
Model				Serial Number		
Hard Drive Size				Hash Value 1 (MD5)		
Hash Value 2 (SHA1 / SHA256)				Software / Hardware Used for hashing		
Image File Name				Notes		
Storage Type	USB ☐	SD Card ☐		Manufacturer		
Model				Serial Number		
Drive Size				Hash Value 1 (MD5)		
Hash Value 2 (SHA1 / SHA256)				Write Blocker Used?	Yes ☐	No ☐

Drive Information						
Hard Drive Type	SATA ☐	IDE ☐	SSD ☐	Manufacturer		
Model				Serial Number		
Hard Drive Size				Hash Value 1 (MD5)		
Hash Value 2 (SHA1 / SHA256)				Software / Hardware Used for hashing		
Image File Name				Notes		
Storage Type	USB ☐	SD Card ☐		Manufacturer		
Model				Serial Number		
Drive Size				Hash Value 1 (MD5)		
Hash Value 2 (SHA1 / SHA256)				Write Blocker Used?	Yes ☐	No ☐

गवाह 1 का नाम और हस्ताक्षर_____.

गवाह 2 का नाम और हस्ताक्षर_____.

पीड़ित/शिकायतकर्ता का नाम और हस्ताक्षरः _____.

जांच अधिकारी का नाम

जांच अधिकारी की मुहर और हस्ताक्षर

दिनांकः

एफएसएल केस अग्रेषण पत्र प्रारूप

कार्यालय का नाम_____

पत्रांकः **दिनांकः**

श्रीमान निदेशक,
विधि विज्ञान प्रयोगशाला,
नेहरू नगर, राजस्थान, जयपुर।

एफएसएल केस अग्रेषण पत्र

पुलिस थाना		जिला	
राज्य		**एफआईआर संख्या**	
मुकदमा कायमी दिनांक		**अंतगर्त धारा**	

केस का संक्षिप्त विवरण

_____

_____

_____

_____

_____

हिरासत में लिए गए व्यक्ति का विवरण

नाम	
आयु	
अन्य विवरण	
किसके द्वारा हिरासत में लिया गया	

परीक्षा के लिए भेजे गए प्रदर्शों/पार्सल की सूची

क्र सं	**प्रदर्शों**/मार्किंग का विवरण	प्रदर्श का स्रोत	पार्सल और सील का विवरण	प्रदर्श किसके द्वारा संकलित किया गया

अपेक्षित परीक्षा की प्रकृति/ प्रश्नावली

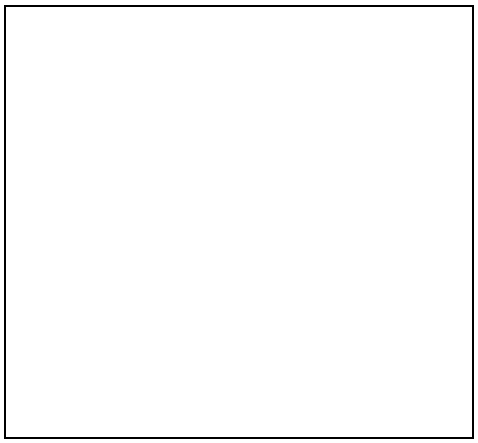
I_____

II._____

III._____

IV._____

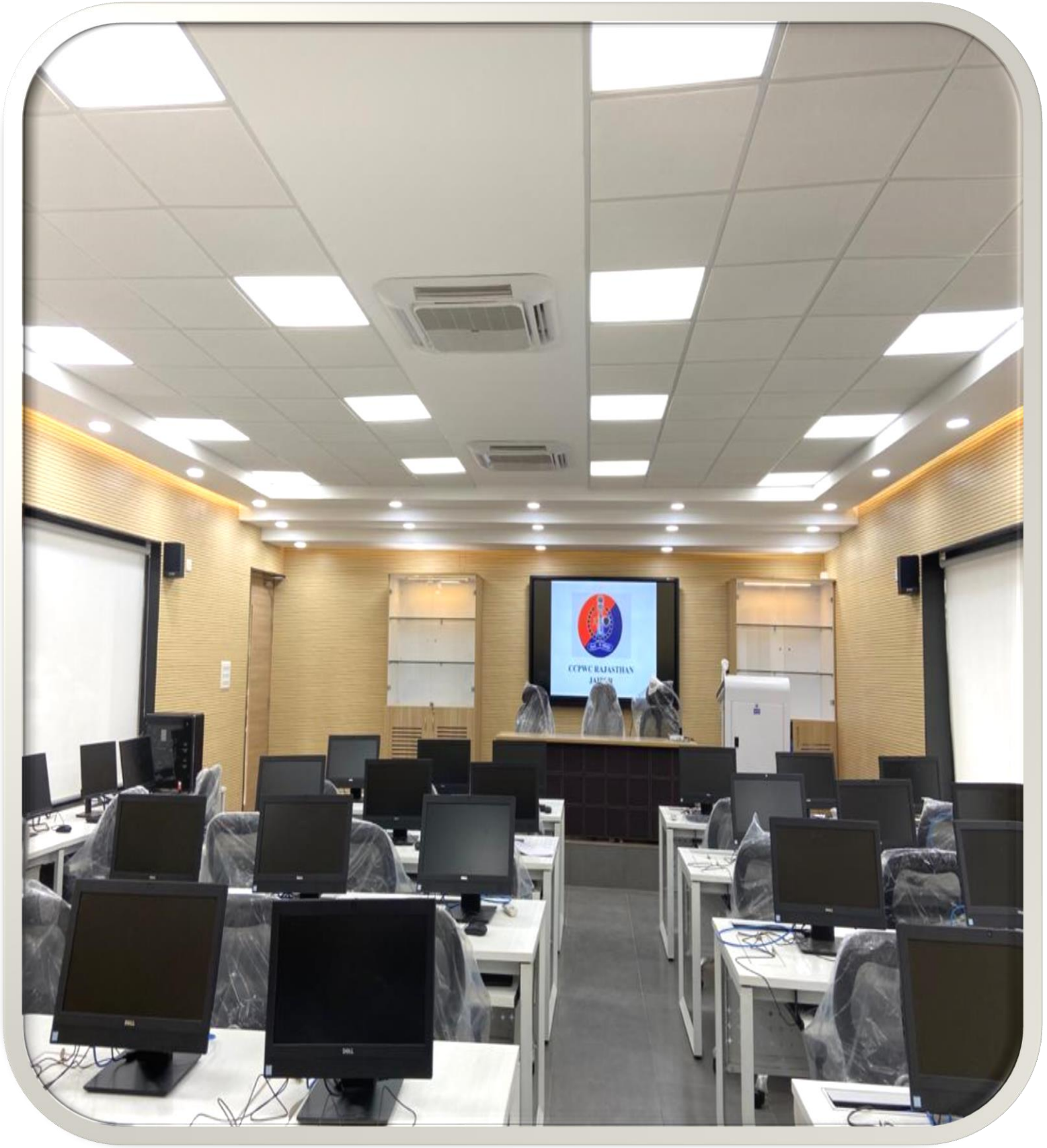
_____



पार्सल पर लगाई गई सील की नमूना सील

अनुसंधान अधिकारी का हस्ताक्षर,
नाम, पदनाम, पता, सील, मोबाइल नंबर व फेक्स नंबर

अग्रेषण अधिकारी का हस्ताक्षर,
नाम, पदनाम, पता, सील, मोबाइल नंबर व फेक्स नंबर



“Rather than fearing or ignoring cyber-attacks, do ensure your cyber resilience to them.”

— Stephane Nappo