INTRODUCTION TO CYBER CRIME AND INVESTIGATION

INDEX

SR. No.	TOPIC NAME	PAGE No.
1	INTRODUCTION TO CYBER CRIME	1
2	BANKING AND CARD RELATED FRAUDS	7
3	INFORMATION TECHNOLOGY ACT 2000	13
4	LIABILITY OF SERVICE PROVIDERS UNDER IT ACT	22
5	INVESTIGATION OF CYBER CRIMES	27
6	CRIME SCENE, FIR AND CHARGESHEET	43
7	SEARCH AND SEIZURE OF DIGITAL DEVICES	48
8	DIGITAL FORENSIC AND DIGITAL EVIDENCE	56
9	INTERNATIONAL CYBERCRIME	67
10	CYBER CRIME AGAINST WOMEN	70
11	CELL PHONE TECHNOLOGY	73
12	CALL DETAIL RECORD (CDR) AND ANALYSIS	83
13	ANNUXERS	93

INTRODUCTION TO CYBER CRIME

Computer और Internet के बढ़ते उपयोग ने तकनीकी क्षेत्र में हमे बहुत आगे पहुंचा दिया है। आज हमारी daily life काफी हद तक इस पर depend है। Technological growth और development में तेजी के कारण आज हमारे पास opportunities की कोई कमी नही है लेकिन ये तकनीके अपने साथ कई financial और security threats भी ले कर आयी है जिनके बारे में आपको पता होना चाहिए।

Cybercrime या "साइबर अपराध" एक ऐसा खतरा है जो बीते कुछ वर्षों में तेजी से बढ़ा है और इसने दुनियाभर में internet इस्तेमाल करने वाले लाखों लोगों को अपनी चपेट में लिया है। Hackers और spammers इन cyber attacks के द्वारा एक individual से लेकर business तक को बुरी तरह damage पहुंचा सकते है।

खुद को Cybercrimes के effect से बचाने का एक ही तरीका है कि आपको इनके बारे में knowledge होनी चाहिए। इस chapter में हम जानेंगे कि साइबर क्राइम क्या होता है? Cybercrime के प्रकार साथ ही cyber threats को कैसे avoid करे।

साइबर अपराध क्या है –

Cybercrime एक ऐसी illegal activity है, जिसमे अपराध को अंजाम देने के लिए digital technologies (Computer, Mobile, Internet) को use में लिया गया हो। इन Cybercrime से किसी person या nation की security और financial health को बड़ा threat हो सकता है। साइबर अपराधों में विभिन्न types की criminal activity शामिल होती है, जिसमे identity fraud, data theft, viruses attack, online fraud, child pornography इत्यादि include है।

इन crimes को करने वाले अपराधियों को Cybercriminals कहते है। ये computing device को use में लेकर किसी व्यक्ति की personal information, secret business information और government information को access करने कोशिश करते है। हालांकि एक आम व्यक्ति भी जाने-अनजाने internet पर Cybercrime कर सकता है।

यदि आप Cybercrime के प्रभाव से बचना चाहते है, तो आपके लिए उन illegal activities को identify करना बेहद important है। हालांकि आज के समय हर country के पास अपने cyber laws है और इनसे निपटने के लिए वे cyber security की भी मदद लेते है।

साइबर क्राइम के उदाहरण

नीचे different types के Cybercrime की list दी गयी है-

1. Thiefs किसी Social networks से person की identity को illegally प्राप्त करते है ताकि वह fake id बनाकर उसका misuse कर सके।
2. Online transaction fraud भी Cybercrime का एक बेहतरीन example है। ये कई तरीके से किया जा सकता है जिसमे criminals आपके plastic card की details को collect करके आपके bank account को खाली कर देते है।
3. Malicious software (adware, spyware, computer virus, etc.) को develop करना या उसे distribute करना भी Cybercrime के अंतर्गत आता है।
4. बिना permission के किसी person या organization के Copyright content को use करना भी crime है।
5. Social media पर अन्य person के against कोई inappropriate post या indecent comment करना भी साइबर अपराध है।
6. अवैध समान (illicit goods) जैसे drugs व guns को online purchase या sell करना भी Cybercrime का हिस्सा है।

7. Child pornography बनाना या उसका ऑनलाइन व्यापार करना ये भी गंभीर साइबर अपराध है।
8. किसी copyrighted किये गए Software को copy अथवा use करना वो भी बिना खरीदे।
9. बिना किसी prior approval के हजारों लोगों को spam emails distribute करना।
10. Computer और network का access gain करने की कोशिश करना या system को crash करना Cybercrime है।

साइबर अपराधों का वर्गीकरण – Classification of Cyber Crime

Cybercrimes को crime के subject के base पर classified किया जाता है। इस आधार पर साइबर अपराध की मुख्य तीन श्रेणियां है जिसमे:

- Individuals के खिलाफ अपराध
- Organizations के खिलाफ अपराध
- Society के खिलाफ अपराध शामिल है

1-Individuals के खिलाफ अपराध

इस तरह के crime किसी person या उनकी properties के against किये जाते है इसके अंतर्गत आने वाले main crimes के examples निम्न है-

Unauthorized Access: जब कोई person किसी computer system, network या किसी दूसरे व्यक्ति के online resources पर unauthorized तरीके से पहुंचने की कोशिश करता है तो उसे अनाधिकृत पहुंच कहा जाता है। Unauthorized access अक्सर व्यक्तिगत लाभ के लिए दूसरे व्यक्ति का डेटा प्राप्त करने या उसे नुकसान पहुचाने के इरादे से किया जाता है।

Online fraud: ये fraudsters के लिए सबसे उपयोगी तकनीक है जिसमे वे computer और internet को एक weapon के रूप में use करते है। Online fraud करने के हज़ारों तरीके है और इनमें लगातार बढ़ोतरी हो रही है। इसके पीछे का reason भी आपकी personal information को चुराना और उसे अपने फायदे के लिए इस्तेमाल करना ही है।

CyberStalking: internet services के use से किसी person के against बार-बार harassment करना Cyber Stalking कहलाता है। इसके अंतर्गत cybercriminals द्वारा victim को follow करना, harassing emails करना, उसे social media में threat करना इत्यादि शामिल है।

Hacking: इसका अर्थ है, किसी computer device में मौजूद information/data को erase या change कर देना। Hacking आज के समय Cybercrime की सबसे common form है। ये अलग-अलग रूप में हो सकती है जिसमे virus attack से लेकर password hacking तक सब शामिल है।

Plastic Card Fraud: एक दिन में आप कई बार Online transaction करते होंगे लेकिन जान-बूझकर या अनजाने में internet पर अपने Credit card या Debit card की information reveal कर देने से आप trouble में पड़ सकते है। यदि आप electronic transaction को secure नही करते है तो आपकी card details को hackers द्वारा चुराया जा सकता है.

Spoofing: ये ऐसा तरीका है, जिसमें hacker's एक genuine user के रूप में अपने को प्रस्तुत करते है। Spoofing का उपयोग computer तक access प्राप्त करने और infected links के द्वारा malware फैलाने के लिए किया जाता है.

Identity theft: जब scammers आपकी personal और financial information को चुरा कर use करे तो उसे identity theft कहते है। यदि आप social sites पर ऐसी जानकारी को public करते है तो आपके साथ ये होने का खतरा बढ़ जाता है।

2-Organizations के खिलाफ अपराध

आज के दौर में लगभग सभी बड़ी companies और organizations अपनी online growth को लेकर अधिक focus होती है। ऐसे में इन्हें भी cybercrime से निपटना पड़ता है। कुछ मुख्य साइबर अपराध जो संस्थाओं के विरुद्ध किये जाते उनके उदाहरण है-

Data breach: ये एक ऐसा cyber attack है जिसमे किसी business की private और sensitive information को unsecured environment में release कर दिया जाता है। Data breaches से व्यवसायों और उससे जुड़े उपभोक्ताओं को विभिन्न तरीकों से नुकसान उठाना पड़ सकता है।

Cyber terrorism: इस तरह के crime किसी देश की Government, military installation, power plants, banks, telecommunication network इत्यादि के against किये जाते है। ये एक traditional terrorism की तुलना में अधिक खतरनाक होती है। ये cyber attacks, domestic के अलावा international स्तर में भी किये जाते है।

Warez distribution: किसी organization की copyright properties का duplicate version बनाकर उसे release कर देना warez distribution के अंतर्गत आता है। ये warez material एक commercial software का pirated version हो सकता है।

Denial of service (DoS) attack: ये एक ऐसा cyber-attack है जिसमे किसी organization के computer resource या server में इतनी request या traffic send किया जाता है, जिसे वह handle नही कर पाता और crash हो जाता है। Resources के crash हो जाने से authorized user उस service को access नही कर पाते। इससे उस कंपनी को बड़ा नुकसान उठाना पड़ता है।

3-Society के खिलाफ अपराध शामिल है

ऐसे cybercrimes जो पूरी society को effect करते है उनके उदाहरण नीचे दिए गए है जिनमे-

Child pornography: इसके अंतर्गत child sexual acts को describe या show करना through films, pornographic websites. इसके अलावा child pornographic material को computer और internet के use से download और transmit करना भी इसके अंतर्गत आता है। आज दुनियाभर में बच्चों का योन शोषण करने और उनका दुरप्रयोग करने के लिए internet का उपयोग बढ़ता ही जा रहा है।

Online gambling: किसी भी तरह की सट्टेबाजी या betting जिसे internet के साथ computer या mobile के उपयोग से खेला जाए उसे online gambling कहते है। आज के समय online gambling का business इतना बढ़ चुका है कि इससे कई तरह की problem खड़ी हुई है।

Selling illegal article: आज internet पर कई ऐसी auction websites है, जो banned और illegal products को लोगो को बेच रही है। इस तरह के crime को emails के द्वारा भी किया जाता है जिसमे आपको ऐसे product दिखाये जाते है जिन्हें कोई मान्यता प्राप्त नही है।

Forgery: लोगों के साथ fraud करने के intent से fraudsters, documents, stamps, legal certificate, contract, currency notes इत्यादि की नकली कॉपी (counterfeit copy) बना लेते है। इसके अलावा किसी अन्य व्यक्ति की पहचान का उपयोग करना भी forgery है।

Spamming: आज के समय commercial advertisement के माध्यम से लोगों के साथ spam करना आसान है। आपके पास भी कभी ऐसे messages या mails आते होंगे जिनमें bumper offers और नई-नई तरह की schemes

दी जाती होंगी। उदाहरण के लिए महंगा माल सस्ते में और अपना पैसा डबल कीजिये। असल मे ये सच्चाई नही होती बल्कि scammers आपको फंसाने के लिए ऐसे जाल बिछाते है।

उपरोक्त बताये गए type के अलावा Cyberspace में कई दूसरे प्रकार के online crimes भी मौजूद होते है जिनके बारे शायद अधिकतर लोगों को कोई जानकारी नही होती। इसलिए उपयोगी ये होगा कि आप इसके बारे अधिक से अधिक जानने की कोशिश करे।

Cyber Criminals की Categories

Cybercriminals उन्हें कहा जाता है जो technology का use करके malicious activity को अंजाम देते है। ऐसा करने की इनकी intension किसी व्यक्ति या कंपनी की personal data/information चुराकर उससे profit generate करना होती है। Cybercriminals के types और उनकी technique को समझने से आप उनसे बच सकते है। साइबर अपराधियों के common types में include है:

Hackers और Crackers

Computer और network की security को break करने के लिए प्रतिबद्ध प्रत्येक कार्य hacking है। इस तरह के कार्य करने के लिए Hackers एक computer program को develop करके targeted system पर attack करते है। Crackers किसी computer system में मौजूद data को steal और modify करते है। वे system को damage करने के लिए viruses और worms को भी insert भी करते है।

Scammers

ये अधिकतर emails और messages के माध्यम से आपको track करते है। Profitable और attractive लगने वाली fraudulent scheme के झांसे में अक्सर लोग फंस जाते है। Scammers सबसे पहले thousand emails address को collect करते है और फिर उन्हें इस तरह के spam emails send किये जाते है।

Phishers

यदि कभी आपको ऐसी phone call या message आये जिसमे ये claim किया जाए कि आपका account expire या block हो चुका है और हम आपको एक message भेज रहे उसमे attached link पर click करके आप इसे फिर से चालू कर सकते है। ये इन phishers की technique होती है जिसमे वे आपको believe कराते है कि ये करना आपके लिए जरूरी है।

Internet Stalkers

ये ऐसे cybercriminals होते है, जो किसी person की online activity को लगातार monitor करते है। जरूरत पड़ने पर ये उनके साथ social networking sites पर relation build करते है और उनका विश्वास जीतते है। एक बार इन stalkers की पहुँच आपकी important information तक हो जाती है फिर शुरू होता है blackmailing का खेल। ये आपसे रिश्वत की मांग करते है ना देने पर आपकी बदनामी भी कर सकते है।

साइबर खतरों से कैसे बचाव करें

ऊपर बताये गए Cybercrime के इतने सारे types देखकर **हम** थोड़ा nervous हो सकते है, परन्तु ये सच है, कि **हम** online पूरी तरह से secure नही है। आपके साथ कभी भी scam हो सकता है ऐसे में Cybercrime से prevention यानी बचाव की सही knowledge ही आपको इसमे फसने से बचा सकती है।

नीचे बताई गयी prevention tips को follow करके आप Cybercrime victim बनने से बच सकते है.

1) Internet Cybercrime के types से खुद को educate करने पर आप उन सभी online crimes के प्रति aware रहते है।

2) जब भी आप emails check कर रहे हो या messenger पर chatting कर रहे हो तो किसी भी unknown person के द्वारा भेजें message में attached link पर click करते वक्त careful रहे।

3) Web पर navigate करते समय आपको phony websites को avoid करने की जरूरत है जो आपकी personal information के लिए पूछती है। किसी भी तरह की जानकारी के लिए Search engine का use करे ये आपको correct web address पर भेजते है।

4) Safe surfing करने के अलावा आपको online shopping करते वक्त भी careful रहने की जरूरत है। Shopping site पर payment information को enter करने से पहले साइट के बारे में थोड़ी investigation कर ले।

5) जब भी payment page पर हो, तो अपने browser में lock symbol की तलाश करे। ये indicate करता है कि site आपकी information को safe रखने के लिए encryption का use करती है। Site के address बार मे ये भी देखे की क्या URL "https://" के बजाय कहीं "http://" से तो start नही है।

6) Firewall software का use करे। ये एक network security system है, जो computer/network और internet के बीच traffic की monitoring करता है और intruders यानी घुसपैठियों को रोकता है।

7) Antivirus program का उपयोग करे साथ ही अपने system को updated रखे। क्योंकि hackers के पास आपके system और information तक access प्राप्त करने के कई तरीके होते है।

8) एक unsecured wireless network पर transit करने के दौरान भी hackers आपका data access कर सकते है। आप अपने router पर firewall को enable करे और router के administration password को change करना आवश्यक है।

9) Short password याद रखना easier होता है जो आपके birthday, middle name, mobile no. पर आधारित हो परंतु इस प्रकार के password को break करना hackers के लिए भी easy होता है। Strong password आपकी account को secure रखने में मदद करते है।

10) अपनी personal information को online post करने से बचे और sensitive information जैसे – security number और credit and debit card number को share न करे। किसी भी link पर click करने या किसी भी application को download करने के दौरान careful रहे।

11) हमेशा Cybercrime के प्रति alert रहे क्योंकि ये हमेशा नए-नए तरीकों से लोगो को अपना शिकार बनाते है।

12) किसी भी ऐसी online scheme जिसमें आपके पैसे जितने या कोई प्राइस जितने की बात की गई हो उसमे बिल्कुल भी विश्वास न करे।

भारत मे Online Frauds की Report कहां करें?

भारत मे cybercrimes और online frauds के cases दिन-प्रतिदिन बढ़ते ही जा रहे है लेकिन वे लोग जो Cybercrime victim है वो इस बारे में कुछ अधिक कर नही पाते। इसलिए आपको **पता होना चाहिये** कि cybercrime के against complaints या report कैसे file की जाती है।

Cyber crime complaint को आप Indian government के Cyber crime portal में जाकर online submit कर सकते है। इसके अलावा भारत के लगभग सभी बड़े cities में cyber cell मौजूद है। ये cybercrime department दोनों तरीके से online और offline दी जाने वाली complaints से deal करते है।

यदि कोई आपकी fake profile बनाकर उससे illegal और unlawful activity करता है तो आपको बस cyber crime investigation cell को report करना है। आप cyber police को call भी कर सकते है। Report file

करने से पहले आपको formal complaint बनानी है जिसमे crime के against पूरे facts और details के साथ evidence मौजूद होने चाहिए।

यदि आप चाहे तो National Cyber Crime Reporting Portal के Helpline Number – 155260 पर call भी कर सकते है। यदि आप अपने शहर में मौजूद Cyber Cell के बारे में जानना चाहते है तो भारत मे मौजूद Cyber cells की list देखे।

Cyber Cell

Cyber Cell एक विभागीय निकाय है जो Cybercrime से related cases को handle करता है। IT act 2000 आने के बाद India के लगभग सभी बड़े cities में इन cyber cell को open किया गया था। ये विभाग भी criminal investigation department के अंतर्गत ही आता है परन्तु ये सिर्फ internet से related criminal activity के मुद्दों को संभालते है.

Cyber Crime Law

Technology के उप्पर बढ़ती हमारी dependency के कारण आज के समय Cyber law की importance बहुत अधिक बढ़ चुकी है। Cybercrime के विरुद्ध बनाये ये laws हमे किसी भी तरह के digital crime से protect करते है। भारत मे Cybersecurity laws की शुरुवात IT act 2000 को लागू करके की गई थी। इस law अंतर्गत different types के crime को cover किया गया था।

IT Act का उद्देश्य:

E-transaction के लिए कानूनी मान्यता प्रदान करना ।

Digital signature को स्वीकार करने के लिए उसे valid signature की कानूनी मान्यता देना।

Bankers और दूसरी organizations को electronic accounting book रखने की legal recognition देना ।

Online privacy और Cybercrime से protection प्रदान करना ।

हालांकि IT act के लागू होने के बाद इसमें कई बदलाव किए गए और कुछ ही सालों में almost सभी online activity इसके under आ गयी। ये जरूरी भी है, यदि हम digitally grow करना चाहते है तो हमे cyber security risk को कम करना होगा। Cyberspace को secure करने के लिए ये कानून लाया गया।

भारत मे इन cyber law का मुख्य उद्देश्य कंप्यूटर अपराध, ऑनलाइन डेटा की चोरी, और इलेक्ट्रॉनिक लेन-देन में होने वाली धोखाधड़ी को रोकना है। इसके अलावा cyber criminals के लिए विभिन्न प्रकार के IT act sections बनाये गए है जिनके अंतर्गत उनको punishment दी जाती है।

BANKING AND CARD RELATED FRAUDS

ऑनलाइन बैंकिंग धोखाधड़ी

अवैध तरीकों का उपयोग करके किसी दूसरी वित्तीय संस्था के स्वामित्व वाले धन, पूँजी, या अन्य सम्पत्ति को प्राप्त कर लेना (हथिया लेना) बैंक कपट (Bank fraud) कहलाता है। इसके अलावा, झूठे ही अपने को किसी बैंक या अन्य वित्तीय संस्थान कहकर/बताकर जमाकर्ताओं से धन प्राप्त करना भी बैंक कपट है।

डिजिटल लेन-देन के बढ़ते दौर में बैंक अकाउंट से धोखाधड़ी की घटनाएं तेजी से बढ़ी है, जहां गैर कानूनी ढंग से बैंक अकाउंट (Bank account) से अनधिकृत लेनदेन (Unauthorized transactions) होते हैं। इसे ऑनलाइन फ्रॉड, डिजिटल फ्रॉड या साइबर फ्रॉड की परिभाषा दी गई है। हैकर्स आपके अकाउंट की डीटेल हासिल करके उससे पैसे निकाल लेते हैं।

फिशिंग

जिस प्रकार मछली पकडने के लिये कॉटे में चारा लगाकर डाला जाता है और चारा खाने के लालच या धोखे में आकर मछली कॉटें में फंस जाती है। उसी प्रकार फ़िशिंग (Phishing) भी हैकर्स (Hackers) द्वारा इन्टरनेट पर नकली वेबसाइट (Fake Website) या ईमेल (Email) के माध्यम से इन्टरनेट यूजर्स के साथ की गयी धोखेबाजी (scams) को कहते हैं। जिसमें वह आपकी निजी जानकारी (personal information) को धोखेबाजी (scams) के माध्यम से चुरा लेते हैं और उसका गलत उपयोग करते हैं -

यह वो criminal activity है जिसकी help से hackers किसी user की sensitive information जैसे की password, credit card numbers, bank account या कोई financial detail निकलने की कोशिश करते है | जो hackers फिशिंग trick use करते है वो web and programming experts होते है | फिशिंग activity के लिए hackers tricks का use करते है and fake email, chat message की help से आपकी details जैसे की password, account numbers या दूसरी financial detail लेने की कोशिश करते है | इसके आलावा phishing मे आपको एक bogus website URL की ट्रिक भी use की जा सकती है जिसमे आपकी information को enter करने के लिए कहा जाता है | आपको website देख कर लगता है की यह सही website है | आप website मे sensitive information एंटर कर देते है |एक बार आप उनको information दे देते है या send कर देते है तो वो आपके account से financial fraud कर सकते है |

स्पूफ़िंग

SPOOF का मतलब होता है **नकली पहचान** और **SPOOFING** का मतलब होता है **नकली पहचान का इस्तेमाल करना।** किसी भी कम्युनिकेशन मीडियम में कम से कम 2 यूजर होते हैं सेंडर और रिसीवर। इसमें सेंडर अपनी तरफ से इंफॉर्मेशन सेंड करता है और यह इंफॉर्मेशन रिसीवर को मिलती है। लेकिन क्या हो अगर आप सेंडर को अपने पहचान का मान कर उसकी दी हुई इनफॉरमेशन पर यकीन करके उसे इस्तेमाल कर लेते हैं लेकिन असली सेंडर ने कभी भी आपको वह इंफॉर्मेशन भेजी ही नहीं हो तो।

स्पूफ़िंग एक ऐसी प्रक्रिया है जिसमें सेंडर अपनी असली पहचान छुपाकर किसी नकली पहचान को एक मास्क की तरह इस्तेमाल करके आपको गलत इंफॉर्मेशन देता है और उसके बदले में आप से असली इंफॉर्मेशन हासिल कर लेता है जिसका वह मनमाने तरीके से इस्तेमाल कर सकता है।

स्पूफ़िंग का सबसे बड़ा नुकसान यह है की इसमें रिसीवर या विक्टिम (जिसके साथ धोखाधड़ी हुई है) को हमेशा यही भ्रम रहता है की वह ओरिजिनल सोर्स से इंफॉर्मेशन हासिल कर रहा है जबकि वह source नकली होता है। स्पूफिंग का इस्तेमाल जानकारी इकट्ठा करने, धोखाधड़ी करने या कभी-कभी सिर्फ मनोरंजन के लिए किया जाता है। लेकिन कोई भी कारण हो स्पूफ़िंग एक क्राइम है।

स्पूफिंग को मेनली पांच भागों में बांटा गया है जो कि अलग-अलग कम्युनिकशन टेक्निक का इस्तेमाल करते हैं।

1. IP spoofing
2. Caller ID spoofing
3. Email spoofing
4. ARP spoofing
5. Content spoofing

क्रेडिट, डेबिट कार्ड धोखाधड़ी और आप उनसे कैसे बच सकते हैं

आजकल कैश की बजाय ऑनलाइन और कार्ड पेमेंट का चलन है। लोग बैंकों से पैसे निकालने की झंझट और समय से बचने के लिए डायरेक्ट कार्ड के जरिए पेमेंट करते हैं। लोगों की जेब में अब कैश की बजाय क्रेडिट (Credit Card) और डेबिट कार्ड (Debit Card) मौजूद होते हैं। लेकिन कार्ड पेमेंट मैथड बढ़ने के साथ-साथ कार्ड से जुड़े फ्रॉड भी बढ़ रहे हैं। कार्ड धोखाधड़ी में मूल रूप से आपके कार्ड पर पहचान या जानकारी की चोरी शामिल है। इस जानकारी का उपयोग एटीएम निकासी या ऑनलाइन या ऑफलाइन लेनदेन करने के लिए किया जाता है।

आपके कार्ड की जानकारी चुराने के लिए जालसाज़ विभिन्न तकनीकों का उपयोग करते हैं:

* **स्किमिंग:** इस तरह के फ्रॉड अक्सर कार्ड स्वैपिंग के वक़्त ही होते हैं। दुकानदार स्वैप मशीन से अटैच सिस्टम में की-लॉगर इनस्टॉल करके रखते हैं। ऐसे में जब यूजर बिल पे करने के लिए कार्ड स्वैप करता है तो की-लॉगर में उसका पासवर्ड और कार्ड से जुड़ी जानकारी जैसे सीवीवी नंबर और एक्सपायरी डेट सेव हो जाती है। बाद में ऑनलाइन ट्रांजेक्शन के लिए यूजर की इन्हीं डिटेल्स का इस्तेमाल किया जाता है और उसके अकाउंट से पैसे उड़ा लिए जाते हैं।

* **स्पूफिंग**: ठग कार्ड यूजर का मोबाइल नंबर, कार्ड नंबर, सीवीवी और एक्सपायरी डेट जैसे डेटा कहीं से उड़ा लेते हैं। फिर उसे कॉल करते हैं और खुद को बैंक का अधिकारी बताते हुए मोबाइल पर आया ओटीपी हासिल कर लेते हैं। इसके बाद ये उनके अकाउंट से पैसे गायब कर देते हैं।

* **क्लोनिंग:** इसमें आपके कार्ड का ही ड्यूप्लिकेट कार्ड बना लिया जाता है। कार्ड क्लोन करने के लिए ठग पहले स्कीमिंग वाला तरीका अपनाकर कार्ड की जानकारी ले लेते हैं। इसके बाद इस जानकारी को एक दूसरे कार्ड में ट्रांसफर कर दिया जाता है। इस तरह ड्यूप्लिकेट कार्ड तैयार हो जाता है और इसके जरिए पैसे उड़ा लिए जाते हैं।

* **शोल्डर सर्फिंग:** इस प्रकार की ठगी में ठगों द्वारा किसी एटीएम में एक निशिचित दूरी पर आपके पीछे खडे होकर आप द्वारा डाले जाने वाले पिन नंबर पता करने के लिये आपकी उंगलियों के मूवमेंट को देखते है तथा

आपके पिन का पता लगाते है। इस प्रकार के ठग आपके कार्ड के अटकने पर आपकी मदद करने की कोशिश करते हैं तथा आपका कार्ड लेकर उसके डाटा तथा पिन, सीवीवी नंबर चुरा लेते है।

* **फार्मिंग:** फ़ार्मिंग एक स्कैमिंग है जिसमें व्यक्तिगत कंप्यूटर (पीसी) या सर्वर पर दुर्भावनापूर्ण कोड स्थापित किया जाता है, जो उपयोगकर्ताओं को उनकी जानकारी या सहमति के बिना धोखाधड़ी वाली वेबसाइटों पर गलत दिशा में ले जाता है जो मूल के समान लगती है । इसका उद्देश्य उपयोगकर्ताओं के लिए अपनी व्यक्तिगत जानकारी इनपुट करना है। एक बार धोखाधड़ी वाली वेबसाइट पर क्रेडिट कार्ड नंबर, बैंक खाता संख्या या पासवर्ड जैसी जानकारी दर्ज करने के बाद वह अपराधियों के पास पहुंच जाती है जिसका प्रयोग कर वह आपको वित्तिय नुकसान पहुंचा सकते है।

* **कीस्ट्रोक लॉगिंग:** इसके अंतर्गत जालसाज द्वारा आपको ऐसे सॉफ्टवेयर इंस्टॉल करने के लिये कहां जाता है जिनके द्वारा आपके द्वारा डिवाईस पर टाईप की जा रही सूचना दूर बैठे व्यक्ति के पास पहुंच जाती है। इस प्रकार जब हम कोई ऑनलाईन खरीददारी करते है तथा सीवीवी, कार्ड नंबर, पिन इत्यादि जो भी टाईप करते है वह एक लॉग फाईल में सेव हो जाता है तथा वह लॉग फाईल कीस्ट्रोक सॉफ्टवेयर द्वारा दूर बैठे जालसाज तक पहुंचा दिया जाता है। उस फाईल में उपलब्ध जानकारी को जालसाजो द्वारा उपयोग कर आपको वित्तिय नुकसान पहुंचाया जाता हैं।

* **फिशिंग और विशिंग:** फ़िशिंग में स्पैम मेल के माध्यम से पहचान की चोरी शामिल है, जो वास्तविक स्रोत से प्रतीत होती है, जबकि विशिंग में संदेशों या एसएमएस का उपयोग करते हुए मोबाइल फोन के माध्यम से पासवर्ड, पिन या अकाउंट नंबर जानने की कोशिश करते हैं।

* **सिम स्वाइप फ्रॉड:** इसके अंतर्गत जालसाज आपके मोबाइल ऑपरेटर से फर्जी पहचान प्रमाण के साथ संपर्क करता है और डुप्लीकेट सिम कार्ड जारी करने के लिये डॉक्यूमेंट प्रदान करता है। डुप्लीकेट सिम जारी कर देने के बाद ऑपरेटर आपके मूल सिम को निष्क्रिय कर देता है जिससे अब कोई भी ऑनलाइन लेनदेन करने के लिए ओटीपी नई सिम वाले फोन पर प्राप्त होता है।

एटीएम सुरक्षा उपाय

- ATM या POS मशीन पर एटीएम कार्ड का इस्तेमाल करते समय अपने हाथ से कीपैड को कवर कर लें
- अपना पिन/कार्ड डीटेल्स कभी किसी के साथ शेयर ना करें
- अपने कार्ड पर कभी PIN ना लिखें
- अपने PIN के तौर पर कभी अपने बर्थडे, फोन, अकाउंट या कार के नंबर्स का इस्तेमाल ना करें
- अपनी ट्रांजैक्शन रसीद को नष्ट कर दें या सुरक्षित अपने पास रखें
- एटीएम में अपना ट्रांजैक्शन शुरू करने से पहले देख लें कि आपके पास स्पाई कैमरे तो नहीं हैं

- एटीएम या POS मशीन इस्तेमाल करते समय कीपैड मैनिपुलेशन, हीट मैपिंग और शोल्डर सर्फिंग से सावधान रहे
- अगर एटीएम टेढ़ी, ढीली या क्षतिग्रस्त दिखती है **तो अच्छी तरह जांच ले** हो सकता है कि किसी ने **कार्ड डालने वाली जगह पर** स्कीमिंग डिवाइस संलग्न किया **हो। इसके लिये कार्ड डालने वाली जगह को थोडा खींचकर देखें।**
- केवल अपने स्वयं के बैंक एटीएम का उपयोग करना उचित है। इसके अलावा, एटीएम से बाहर निकलने वाले किसी भी व्यक्ति की मदद लेने से बचें ।

5 TRAPS SET BY FRAUDSTERS AT THE ATM

1. हिडन कैमरा

पिनहोल कैमरों को आपके पिन को पकड़ने के लिए मशीन या ऐसी जगहो पर छिपाया जा सकता है जहां से कीपैड पर आसानी से नजर रखी जा सके तथा जैसे ही आप पिन डालते है वह कैमरे में रिकॉर्ड हो जाता है।

2. कार्ड स्किमर

इन उपकरणों को कार्ड रीडर स्लॉट पर स्थापित किया जाता है ताकि आपके कार्ड की चुंबकीय पट्टी से जानकारी की प्रतिलिपि बनाई जा सके।

* भारी स्लॉट: यदि स्लॉट थोड़ा भारी या गलत लगता है, तो सभी संभावना में वास्तविक कार्ड के ऊपर एक अतिरिक्त कार्ड रीडर स्लॉट रखा गया है।

* ढीला स्लॉट: यदि स्लॉट डगमगाने वाला या ढीला है, इंगित करता है कि एक छोटा प्लास्टिक डिवाइस है जो आपके कार्ड को मशीन में वापस रखता है।

3. शोल्डर सर्फर

ये वे लोग हैं जो एटीएम रूम में या बाहर हैं। यदि आपका कार्ड अटका **या ट्रांजेक्शन में कोई समस्या आती है तो वे आपकी सहायता करने के लिये कहते है। परंतु उनमें ऐसे जालसाज भी हो सकते है जो**

आपकी सहायता के नाम पर आपके कार्ड की चोरी या आपके कार्ड की जानकारी सहायता के नाम पर पता करके उसका दुरूपयोग कर सकते है। इसलिये किसी अंजान व्यक्ति से सहायता नहीं लेनी चाहिये।

4. मशीन का सामने का परिवर्तित हिस्सा

यह पता लगाना थोड़ा मुश्किल हो सकता है क्योंकि नकली सामने पूरी तरह से मूल मशीन को कवर करता है क्योंकि यह इसके शीर्ष पर स्थापित है। इससे धोखेबाज आपके पिन के साथ-साथ पैसे भी ले सकते हैं।

5. नकली कीपैड

यह वास्तविक कीपैड के शीर्ष पर रखा गया है। यदि कीपैड स्पर्श करने पर स्पंजी लगता है, तो अपना पिन दर्ज न करें।

ऑनलाइन सावधानियां

* **सुरक्षित साइटों का उपयोग करें:** केवल ई-शॉपिंग के लिए प्रसिद्ध, स्थापित साइटों पर जाएं। "इसका उपयोग करने से पहले साइट की वैधता की पुष्टि करना याद रखें और केवल उन पर खरीदारी करें, जो सुरक्षित सॉकेट लेयर सर्टिफाइड (एसएसएल) हैं । ब्राउज़र के URL बॉक्स के बगल में लॉक सिंबल के माध्यम से इनकी पहचान की जा सकती है

यह भी सुनिश्चित करें कि वेबसाइट, http 'के बजाय' https 'प्रोटोकॉल का उपयोग करती है, जहां 's ' stands for Secure । इसके अतिरिक्त, सुनिश्चित करें कि उस विकल्प पर क्लिक न करें जो किसी भी साइट पर आपके कार्ड के विवरण को सहेजने के लिए कहता है। आपको किसी साइट के भुगतान सत्यापन सिक्योरकोड को भी देखना चाहिए, जो यह सत्यापित करता है कि आपने ऑनलाइन लेनदेन की गोपनीयता की रक्षा करते हुए भुगतान को अधिकृत किया है।"

* **एंटी-वायरस सॉफ़्टवेयर:** आप मैलवेयर से बचने के लिए अपने कंप्यूटर और स्मार्टफोन पर एंटी-वायरस सॉफ़्टवेयर स्थापित करके लेनदेन को सुरक्षित कर सकते हैं। आप आधिकारिक ऐप स्टोर से अपने फोन पर पहचान की चोरी का पता लगाने वाले ऐप भी इंस्टॉल कर सकते हैं। इसके अलावा, अपने स्मार्टफ़ोन पर सॉफ़्टवेयर रखें जो मोबाइल चोरी होने की स्थिति में आपको दूरस्थ रूप से डेटा को मिटा देने में सक्षम बनाता है।

* **सीवीवी छुपाएं:** वेबसाइटों पर खरीदारी करते समय CVV विशेष रूप से महत्वपूर्ण है तथा सत्यापन का एकमात्र बिंदु है। इसके अलावा कीस्ट्रोक लॉगिंग से बचने के लिए एक वर्चुअल कीबोर्ड का उपयोग करें।

* **सार्वजनिक वाई-फाई:** असुरक्षित नेटवर्क या सार्वजनिक वाई-फाई का उपयोग करने से बचना चाहिए क्योंकि ये ऑनलाइन लेनदेन में पहचान की चोरी के मामलों के लिए आसान लक्ष्य हैं ।

* **अलर्ट के लिए पंजीकरण करें:** यह एक बहुत ही महत्वपूर्ण कदम है क्योंकि बैंक आपको किसी भी ऑनलाइन कार्ड लेनदेन या एटीएम से निकासी की सूचना **एसएमएस के द्वारा देता है। यदि आपका मोबाईल नंबर बदल गया है तो बैंक के पास** अपना मोबाइल नंबर अपडेट करना भी याद रखें।

* **लॉग आउट करें:** हमेशा सोशल मीडिया साइटों और अन्य ऑनलाइन खातों से डेटा सुरक्षा सुनिश्चित करने के लिए लॉग आउट करें और अपने मोबाइल फोन पर गोपनीय पासवर्डों को संग्रहीत करने से बचें क्योंकि इनका उपयोग धोखेबाजों द्वारा किया जा सकता है।

* **पासवर्ड बदलें:** पहचान की चोरी की संभावना को कम करने के लिए समय-समय पर अपने पासवर्ड बदलते रहें।

* **वर्चुअल कार्ड:** यह एक सीमित डेबिट कार्ड है जो व्यापारी को प्राथमिक कार्ड की जानकारी प्रदान नहीं करता है और एक दिन या 48 घंटे के बाद समाप्त हो जाता है।

ऑफ़लाइन निवारक उपाय

यहां कुछ अतिरिक्त सावधानियां बताई गई हैं जिनसे आप यह सुनिश्चित कर सकते हैं कि आपका कार्ड सुरक्षित है।

* **विवरण न बताएं:** कभी भी अपना पिन, सीवीवी या पासवर्ड किसी को भी न बताएं। सुनिश्चित करें कि ई-मेल या एसएमएस का जवाब न दें जो महत्वपूर्ण व्यक्तिगत या कार्ड से संबंधित विवरणों के लिए पूछते हैं। कोई भी बैंक या क्रेडिट कार्ड फर्म मेल या फोन के जरिए ग्राहकों से कार्ड का विवरण लेने के लिए अधिकृत नहीं है।

* **चेक स्टेटमेंट्स:** नियमित रूप से अपने बैंक या क्रेडिट कार्ड स्टेटमेंट्स पर जाएं ताकि आप पहचान की चोरी के माध्यम से किसी भी अनधिकृत लेनदेन का पता लगा सकें और बैंक को तुरंत अलर्ट कर सकें।

* **व्यापारी और पीओएस:** दुकानों या पेट्रोल पंपों पर सुनिश्चित करें कि विक्रेता द्वारा कार्ड किसी दूरस्थ स्थान पर नहीं ले जाया जाता है जहां आप इसे नहीं देख सकते क्योंकि कार्ड की जानकारी आसानी से कॉपी और चोरी हो सकती है। इसके अलावा, उन विक्रेताओं के साथ खरीदारी करें जो चिप-सक्षम कार्ड रीडर का उपयोग करते हैं। हालांकि प्रत्येक व्यापारी के पास ऐसे चिप-सक्षम कार्ड रीडर नहीं हैं, लेकिन यह प्रावधान कार्ड धोखाधड़ी के जोखिम को महत्वपूर्ण रूप से कम करने में मदद कर सकता है।

कार्ड पहचान की चोरी या धोखाधड़ी या ऑफ़लाइन लेनदेन के मामले में, बैंक या कार्ड प्रदाता को तुरंत नुकसान की रिपोर्ट करें और कार्ड को अवरुद्ध कर दें। इसके लिए, सुनिश्चित करें कि आपके पास अपने बैंक का **कस्टमर केयर** नंबर है। **बैंक को** एक पत्र या ई-मेल **भेजकर धोखाधडी की सूचना दे तथा** जल्द से जल्द एफआईआर दर्ज करने की भी सलाह दी जाती है।

यदि बैंक एक सप्ताह के भीतर जवाब नहीं देता है, तो नोडल अधिकारी से संपर्क करें। यदि 30 दिनों के भीतर बैंक से कोई प्रतिक्रिया नहीं होती है, तो RBI द्वारा नियुक्त बैंकिंग लोकपाल से संपर्क करें (https: /www.rbi। Org.in/commonman/English/Scripts/Against-BankABO.aspx)। यदि यह उपाय बहुत विफल हो जाता है, तो निवारण के लिए न्यायालय का दरवाजा खटखटाएं।

INFORMATION TECHNOLOGY ACT 2000

सूचना तकनीक अधिनियम (इनफार्मेशन टेक्नोलॉजी एक्ट- 2000) भारतीय संसद द्वारा पारित एक अधिनियम है जो 17 अक्टूबर 2000 को पारित हुआ। 27 अक्टूबर 2009 को एक घोषणा द्वारा इसे संशोधित किया गया। सूचना तकनीक कानून 9 जनवरी 2000 को पेश किया गया था। 30 जनवरी 1997 को संयुक्त राष्ट्र की जनरल एसेंबली में प्रस्ताव संख्या 51/162 द्वारा सूचना तकनीक की आदर्श नियमावली (जिसे यूनाइटेड नेशंस कमीशन ऑफ इंटरनेशनल ट्रेड लॉ के नाम से जाना जाता है) पेश किए जाने के बाद सूचना तकनीक कानून, 2000 को पेश करना अनिवार्य हो गया था। संयुक्त राष्ट्र की इस नियमावली में संवाद के आदान-प्रदान के लिए सूचना तकनीक या कागज के इस्तेमाल को एक समान महत्व दिया गया है और सभी देशों से इसे मानने की अपील की गई है। सूचना तकनीक कानून, 2000 की प्रस्तावना में ही हर ऐसे लेनदेन को क़ानूनी मान्यता देने की बात उल्लिखित है, जो इलेक्ट्रॉनिक कॉमर्स के दायरे में आता है और जिसमें सूचनाओं के आदान-प्रदान के लिए सूचना तकनीक का इस्तेमाल हुआ हो। इलेक्ट्रॉनिक कॉमर्स सूचना के आदान-प्रदान और उसके संग्रहण के लिए कागज आधारित माध्यमों के विकल्प के रूप में इलेक्ट्रॉनिक माध्यम का इस्तेमाल करता है। इससे सरकारी संस्थानों में भी इलेक्ट्रॉनिक माध्यम से दस्तावेजों का आदान-प्रदान संभव हो सकता है और इंडियन पेनल कोड, इंडियन एविडेंस एक्ट 1872, बैंकर्स बुक्स एविडेंस एक्ट 1891 और रिज़र्व बैंक ऑफ इंडिया एक्ट 1934 अथवा इससे प्रत्यक्ष या परोक्ष रूप से जुड़े किसी भी कानून में संशोधन में भी इन दस्तावेज़ों का उपयोग हो सकता है।

संयुक्त राष्ट्र की जनरल एसेंबली ने 30 जनवरी 1997 को प्रस्ताव संख्या ए/आरइएस/51/162 के तहत यूनाइटेड नेशंस कमीशन ऑन इंटरनेशनल ट्रेड लॉ द्वारा अनुमोदित मॉडल लॉ ऑन इलेक्ट्रॉनिक कॉमर्स (इलेक्ट्रॉनिक कॉमर्स से संबंधित आदर्श कानून) को अपनी मान्यता दे दी। इस कानून में सभी देशों से यह अपेक्षा की जाती है कि सूचना के आदान-प्रदान और उसके संग्रहण के लिए कागज आधारित माध्यमों के विकल्प के रूप में इस्तेमाल की जा रहीं तकनीकों से संबंधित कोई भी कानून बनाने या उसे संशोधित करते समय वे इसके प्रावधानों का ध्यान रखेंगे, ताकि सभी देशों के में एकरूपता बनी रहे। सूचना तकनीक कानून 2000 17 अक्टूबर 2000 को अस्तित्व में आया। इसमें 13 अध्यायों में विभक्त कुल 94 धाराएं हैं। 27 अक्टूबर 2008 को इस कानून को एक घोषणा द्वारा संशोधित किया गया। इसे 5 फ़रवरी 2009 को फिर से संशोधित किया गया, जिसके तहत अध्याय 2 की धारा 3 में इलेक्ट्रॉनिक हस्ताक्षर की जगह डिजिटल हस्ताक्षर को जगह दी गई। इसके लिए धारा 2 में उपखंड (एच) के साथ उपखंड (एचए) को जोड़ा गया, जो सूचना के माध्यम की व्याख्या करता है। इसके अनुसार, सूचना के माध्यम से तात्पर्य मोबाइल फोन, किसी भी तरह का व्यक्तिगत डिजिटल माध्यम या फिर दोनों हो सकते हैं, जिनके माध्यम से किसी भी तरह की लिखित सामग्री, वीडियो, ऑडियो या तस्वीरों को प्रचारित, प्रसारित या एक से दूसरे स्थान तक भेजा जा सकता है।

परिचय

आधुनिक कानून की शब्दावली में साइबर कानून का संबंध कंप्यूटर और इंटरनेट से है। विस्तृत संदर्भ में कहा जाए तो यह कंप्यूटर आधारित सभी तकनीकों से संबद्ध है। साइबर आतंकवाद के मामलों में दंड विधान के लिए सूचना तकनीक कानून, 2000 में धारा 66-एफ को जगह दी गई है।

66-एफ : साइबर आतंकवाद के लिए दंड का प्रावधान

1 .यदि कोई-

- भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए-

क) किसी अधिकृत व्यक्ति को कंप्यूटर के इस्तेमाल से रोकता है या रोकने का कारण बनता है।
ख) बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कंप्यूटर के इस्तेमाल की कोशिश करता है।
ग) कंप्यूटर में वायरस जैसी कोई ऐसी चीज डालता है या डालने की कोशिश करता है, जिससे लोगों की जान को खतरा पैदा होने की आशंका हो या संपत्ति के नुक़सान का ख़तरा हो या जीवन के लिए आवश्यक सेवाओं में जानबूझ कर खलल डालने की कोशिश करता हो या धारा 70 के तहत संवेदनशील जानकारियों पर बुरा असर पड़ने की आशंका हो या-

- अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझ कर किसी कंप्यूटर से ऐसी सूचनाएं हासिल करने में कामयाब होता है, जो देश की सुरक्षा या अन्य देशों के साथ उसके संबंधों के नज़रिए से संवेदनशील हैं या कोई भी गोपनीय सूचना इस इरादे के साथ हासिल करता है, जिससे भारत की सुरक्षा, एकता, अखंडता एवं संप्रभुता, अन्य देशों के साथ इसके संबंध, सार्वजनिक जीवन या नैतिकता पर बुरा असर पड़ता हो या ऐसा होने की आशंका हो, देश की अदालतों की अवमानना अथवा मानहानि होती हो या ऐसा होने की आशंका हो, किसी अपराध को बढ़ावा मिलता हो या इसकी आशंका हो, किसी विदेशी राष्ट्र अथवा व्यक्तियों के समूह अथवा किसी अन्य को ऐसी सूचना से फायदा पहुंचता हो, तो उसे साइबर आतंकवाद का आरोपी माना जा सकता है।

2 . यदि कोई व्यक्ति साइबर आतंकवाद फैलाता है या ऐसा करने की किसी साजिश में शामिल होता है तो उसे आजीवन कारावास की सजा सुनाई जा सकती है।

2005 में प्रकाशित एडवांस्ड लॉ लेक्सिकॉन के तीसरे संस्करण में साइबरस्पेस शब्द को भी इसी तर्ज पर परिभाषित किया गया है। इसमें इलेक्ट्रॉनिक माध्यमों में फ्लोटिंग शब्द पर खासा जोर दिया गया है, क्योंकि दुनिया के किसी भी हिस्से से इस तक पहुंच बनाई जा सकती है। लेखक ने आगे इसमें साइबर थेफ्ट (साइबर चोरी) शब्द को ऑनलाइन कंप्यूटर सेवाओं के इस्तेमाल के परिप्रेक्ष्य में परिभाषित किया है। इस शब्दकोश में साइबर कानून की इस

तरह व्याख्या की है, कानून का वह क्षेत्र, जो कंप्यूटर और इंटरनेट से संबंधित है और उसके दायरे में इंटेलेक्चुअल प्रॉपर्टी राइट्स, अभिव्यक्ति की स्वतंत्रता और सूचनाओं तक निर्बाध पहुंच आदि आते हैं।

सूचना तकनीक कानून में कुछ और चीजों को परिभाषित किया गया है, जो इस प्रकार हैं, कंप्यूटर से तात्पर्य किसी भी ऐसे इलेक्ट्रॉनिक, मैग्नेटिक, ऑप्टिकल या तेज़ गति से डाटा का आदान-प्रदान करने वाले किसी भी ऐसे यंत्र से है, जो विभिन्न तकनीकों की मदद से गणितीय, तार्किक या संग्रहणीय कार्य करने में सक्षम है। इसमें किसी कंप्यूटर तंत्र से जुड़ा या संबंधित हर प्रोग्राम और सॉफ्टवेयर शामिल है।

सूचना तकनीक कानून, 2000 की धारा 1 (2) के अनुसार, उल्लिखित अपवादों को छोड़कर इस कानून के प्रावधान पूरे देश में प्रभावी हैं। साथ ही उपरोक्त उल्लिखित प्रावधानों के अंतर्गत देश की सीमा से बाहर किए गए किसी अपराध की हालत में भी उक्त प्रावधान प्रभावी होंगे।

अधिनियम के उद्देश्य

सूचना प्रौद्योगिकी अधिनियम, 2000 डेटा के इलेक्ट्रॉनिक एक्सचेंज और संचार के अन्य इलेक्ट्रॉनिक माध्यमों या इलेक्ट्रॉनिक कॉमर्स लेनदेन के माध्यम से किए गए लेनदेन को कानूनी मान्यता प्रदान करता है। इसमें सरकारी एजेंसियों के साथ दस्तावेजों की इलेक्ट्रॉनिक फाइलिंग की सुविधा के लिए संचार और सूचना भंडारण की कागज-आधारित पद्धति के विकल्पों का उपयोग भी शामिल है।

इसके अलावा, इस अधिनियम ने भारतीय दंड संहिता 1860, भारतीय साक्ष्य अधिनियम 1872, बैंकर्स पुस्तक साक्ष्य अधिनियम 1891 और भारतीय रिजर्व बैंक अधिनियम 1934 में संशोधन किया।

अधिनियम के उद्देश्य इस प्रकार हैं:

1. संचार के पुराने पेपर-आधारित तरीके के स्थान पर डेटा के इलेक्ट्रॉनिक एक्सचेंज या संचार के अन्य इलेक्ट्रॉनिक माध्यमों या ई-कॉमर्स के माध्यम से किए गए सभी लेनदेन को कानूनी मान्यता प्रदान करना ।
2. किसी भी जानकारी या कानूनी प्रमाणीकरण की आवश्यकता वाले मामलों के प्रमाणीकरण के लिए डिजिटल हस्ताक्षर को कानूनी मान्यता प्रदान करना ।
3. सरकारी एजेंसियों और विभागों के साथ दस्तावेजों की इलेक्ट्रॉनिक फाइलिंग की सुविधा प्रदान करना
4. डेटा के इलेक्ट्रॉनिक भंडारण की सुविधा प्रदान करना ।
5. बैंकों और वित्तीय संस्थानों के बीच धन के इलेक्ट्रॉनिक हस्तांतरण की सुविधा और कानूनी स्वीकृति प्रदान करना ।

6 खातों की पुस्तकों को इलेक्ट्रॉनिक रूप में रखने के लिए साक्ष्य अधिनियम, 1891 और भारतीय रिजर्व बैंक अधिनियम, 1934 के तहत बैंकरों को कानूनी मान्यता प्रदान करना ।

सूचना तकनीक कानून, 2000 के अंतर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान

मानव समाज के विकास के नज़रिए से सूचना और संचार तकनीकों की खोज को बीसवीं शताब्दी का सबसे महत्वपूर्ण अविष्कार माना जा सकता है। सामाजिक विकास के विभिन्न क्षेत्रों, ख़ासकर न्यायिक प्रक्रिया में इसके इस्तेमाल की महत्ता को कम करके नहीं आंका जा सकता, क्योंकि इसकी तेज़ गति, कई छोटी-मोटी दिक्क़तों से छुटकारा, मानवीय गलतियों की कमी, कम ख़र्चीला होना जैसे गुणों के चलते यह न्यायिक प्रक्रिया को विश्वसनीय बनाने में अहम भूमिका निभा सकती है। इतना ही नहीं, ऐसे मामलों के निष्पादन में, जहां सभी संबद्ध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प सिद्ध हो सकता है। सूचना तकनीक कानून के अंतर्गत उल्लिखित आरोपों की सूची निम्नवत है-

- कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश-धारा 65
- कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश-धारा 66
- संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान-धारा 66 ए
- कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को ग़लत तरीके से हासिल करने के लिए दंड का प्रावधान-धारा 66 बी
- किसी की पहचान चोरी करने के लिए दंड का प्रावधान-धारा 66 सी
- अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंच बनाने के लिए दंड का प्रावधान- धारा 66 डी
- किसी की निजता भंग करने के लिए दंड का प्रावधान-धारा 66 इ
- साइबर आतंकवाद के लिए दंड का प्रावधान-धारा 66 एफ
- आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधान-धारा 67
- इलेक्ट्रॉनिक माध्यमों से सेक्स या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान-धारा 67 ए
- इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो-धारा 67 बी
- मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान-धारा 67 सी
- सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान-धारा 70
- डाटा या आंकड़ों को ग़लत तरीक़े से पेश करना-धारा 71
- आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान-धारा 72 ए
- कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान-धारा 72 ए
- फर्ज़ी डिजिटल हस्ताक्षर का प्रकाशन-धारा 73

सूचना तकनीक कानून की धारा 78 में इंस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों में जांच का अधिकार हासिल है।

- भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान
- ईमेल के माध्यम से धमकी भरे संदेश भेजना-आईपीसी की धारा 503
- ईमेल के माध्यम से ऐसे संदेश भेजना, जिससे मानहानि होती हो-आईपीसी की धारा 499
- फर्ज़ी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल-आईपीसी की धारा 463
- फर्ज़ी वेबसाइट्स या साइबर फ्रॉड-आईपीसी की धारा 420
- चोरी-छुपे किसी के ईमेल पर नज़र रखना-आईपीसी की धारा 463
- वेब जैकिंग-आईपीसी की धारा 383
- ईमेल का ग़लत इस्तेमाल-आईपीसी की धारा 500
- दवाओं को ऑनलाइन बेचना-एनडीपीएस एक्ट
- हथियारों की ऑनलाइन ख़रीद-बिक्री-आर्म्स एक्ट

सूचना तकनीक कानून**, 2000** में संशोधन

17 अक्टूबर, 2000 को इंफॉर्मेशन टेक्नोलॉजी एक्ट, 2000 (सूचना तकनीक कानून, 2000) अस्तित्व में आया 27 अक्टूबर, 2009 को एक घोषणा द्वारा इसे संशोधित किया गया। संशोधित कानून में परिभाषाएं निम्नवत हैं -

सूचना तकनीक कानून, 2000 की प्रस्तावना में ही हर ऐसे लेनदेन को कानूनी मान्यता देने की बात उल्लिखित है, जो इलेक्ट्रॉनिक कॉमर्स के दायरे में आता है और जिसमें सूचनाओं के आदान-प्रदान के लिए सूचना तकनीक का इस्तेमाल हुआ हो।

1. यहां कानून से तात्पर्य सूचना तकनीक कानून, 2000 से है।
2. संवाद (कम्युनिकेशन) का मतलब किसी भी तरह की जानकारी या संकेत के प्रचार, प्रसार या उसे एक स्थान से दूसरे स्थान तक ले जाना है। यह प्रत्यक्ष या अप्रत्यक्ष, किसी भी तरह का हो सकता है।
3. संवाद सूत्र (कम्युनिकेशन लिंक) का अर्थ कंप्यूटरों को आपस में एक-दूसरे से जोड़ने के लिए प्रयुक्त होने वाले सैटेलाइट, माइक्रोवेव, रेडियो, ज़मीन के अंदर स्थित कोई माध्यम, तार, बेतार या संचार का कोई अन्य साधन हो सकता है।

सूचना तकनीक कानून 9 जनवरी, 2000 को पेश किया गया था। 30 जनवरी, 1997 को संयुक्त राष्ट्र की जनरल एसेंबली में प्रस्ताव संख्या 51/162 द्वारा सूचना तकनीक की आदर्श नियमावली (जिसे यूनाइटेड नेशंस कमीशन ऑफ इंटरनेशनल ट्रेड लॉ के नाम से जाना जाता है) पेश किए जाने के बाद सूचना तकनीक कानून, 2000 को पेश करना अनिवार्य हो गया था। संयुक्त राष्ट्र की इस नियमावली में संवाद के आदान-प्रदान के लिए सूचना तकनीक या कागज के इस्तेमाल को एक समान महत्व दिया गया है और सभी देशों से इसे मानने की अपील की गई है। सूचना

तकनीक कानून, 2000 की प्रस्तावना में ही हर ऐसे लेनदेन को कानूनी मान्यता देने की बात उल्लिखित है, जो इलेक्ट्रॉनिक कॉमर्स के दायरे में आता है और जिसमें सूचनाओं के आदान-प्रदान के लिए सूचना तकनीक का इस्तेमाल हुआ हो। इलेक्ट्रॉनिक कॉमर्स सूचना के आदान-प्रदान और उसके संग्रहण के लिए कागज आधारित माध्यमों के विकल्प के रूप में इलेक्ट्रॉनिक माध्यम का इस्तेमाल करता है। इससे सरकारी संस्थानों में भी इलेक्ट्रॉनिक माध्यम से दस्तावेज़ों का आदान-प्रदान संभव हो सकता है और इंडियन पेनल कोड, इंडियन एविडेंस एक्ट 1872, बैंकर्स बुक्स एविडेंस एक्ट 1891 और रिज़र्व बैंक ऑफ इंडिया एक्ट 1934 अथवा इससे प्रत्यक्ष या परोक्ष रूप से जुड़े किसी भी कानून में संशोधन में भी इन दस्तावेज़ों का उपयोग हो सकता है।

संयुक्त राष्ट्र की जनरल एसेंबली ने 30 जनवरी, 1997 को प्रस्ताव संख्या ए/आरइएस/51/162 के तहत यूनाइटेड नेशंस कमीशन ऑन इंटरनेशनल ट्रेड लॉ द्वारा अनुमोदित मॉडल लॉ ऑन इलेक्ट्रॉनिक कॉमर्स (इलेक्ट्रॉनिक कॉमर्स से संबंधित आदर्श कानून) को अपनी मान्यता दे दी। इस कानून में सभी देशों से यह अपेक्षा की जाती है कि सूचना के आदान-प्रदान और उसके संग्रहण के लिए कागज आधारित माध्यमों के विकल्प के रूप में इस्तेमाल की जा रहीं तकनीकों से संबंधित कोई भी कानून बनाने या उसे संशोधित करते समय वे इसके प्रावधानों का ध्यान रखेंगे, ताकि सभी देशों के में एकरूपता बनी रहे। सूचना तकनीक कानून 2000 17 अक्टूबर, 2000 को अस्तित्व में आया। इसमें 13 अध्यायों में विभक्त कुल 94 धाराएं हैं। 27 अक्टूबर, 2009 को इस कानून को एक घोषणा द्वारा संशोधित किया गया। इसे 5 फरवरी, 2009 को फिर से संशोधित किया गया, जिसके तहत अध्याय 2 की धारा 3 में इलेक्ट्रॉनिक हस्ताक्षर की जगह डिजिटल हस्ताक्षर को जगह दी गई। इसके लिए धारा 2 में उपखंड (एच) के साथ उपखंड (एचए) को जोड़ा गया, जो सूचना के माध्यम की व्याख्या करता है। इसके अनुसार, सूचना के माध्यम से तात्पर्य मोबाइल फोन, किसी भी तरह का व्यक्तिगत डिजिटल माध्यम या फिर दोनों हो सकते हैं, जिनके माध्यम से किसी भी तरह की लिखित सामग्री, वीडियो, ऑडियो या तस्वीरों को प्रचारित, प्रसारित या एक से दूसरे स्थान तक भेजा जा सकता है।

आधुनिक कानून की शब्दावली में साइबर कानून का संबंध कंप्यूटर और इंटरनेट से है। विस्तृत संदर्भ में कहा जाए तो यह कंप्यूटर आधारित सभी तकनीकों से संबद्ध है। साइबर आतंकवाद के मामलों में दंड विधान के लिए सूचना तकनीक कानून, 2000 में धारा 66-एफ को जगह दी गई है।

HIGHLIGHTS OF THE AMENDMENT ACT, 2008

- It focuses on privacy issues.
- It focuses on Information Security.
- It came with surveillance on Cyber Cases.
- The Concept of Digital Signature was elaborated.
- It clarified reasonable security practices for corporate.
- Role of Intermediaries were focuses.
- It came with the Indian Computer Emergency Response Team.
- New faces of Cyber Crime were added.
- Powers were given to Inspector to investigate cyber crimes as against only to DSP.
- Severe Punishments and fine were added.

The table 1 briefly enumerates the cyber offences as laid under the IT Act, 2000 (Amendment 2008) with the punishments and penalties.

Table 1: Cyber Offences and Penalties and Punishments

S.no.	Section	Offence	Punishment
1.	65	Tampering with computer source documents	Imprisonment upto 3 years or fine upto Rs 2 lakh or both
2.	66	Computer related offences	Imprisonment upto 3 years or fine upto Rs 5 lakh or both
3.	66B	Dishonestly receiving the stolen computer resource and communication device	Imprisonment upto 3 years or fine upto Rs. 1 lakh
4.	65C	Theft of identity	Imprisonment upto 3 years
5.	66 D	Cheating by personation by using computer resource or communication device	Imprisonment upto 3 years and fine upto Rs. 1 lakh
6.	66E	Violation of Privacy	Imprisonment upto 3 years or fine upto Rs. 2 lakh or both
7.	66F	Cyber Terrorism	Life Imprisonment
8.	67	Publishing or transmitting obscene material in e-form	Upon 1st conviction with imprisonment upto 3 years and fine upto Rs 5 lakh; and upon 2nd or subsequent conviction with imprisonment upto 5 years and fine upto Rs 10 lakh.
9.	67A	Publishing or transmitting material containing sexually explicit act in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or

ePathshala पाठशाला A Gateway to All Post Graduate Courses

			subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
10.	67B	Publishing or transmitting material depicting children in sexually explicit act etc. in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
11.	67C	Violating the directions to preserve and retain the information by intermediaries	Imprisonment upto 3 years and fine
12.	68	Violating the directions of Controller by Certifying Authority or his employee	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
13.	69	Violating the directions of the Central Government or State Government to a subscriber to extend facilities to decrypt information	Imprisonment upto 7 years and fine
14.	69A	Violating the directions to block any information for access by the public	Imprisonment upto 7 years and fine
15.	69B	Violating the directions to monitor and collect traffic data or information	Imprisonment upto 3 years and fine
16.	70	Unauthorized access to a computer	Imprisonment upto 10 years and fine

e-Pathshala ई-पाठशाला A Gateway to All Post Graduate Courses

	70A	system	
17.	70B	Violating the directions of the Indian Computer Emergency Response Team (CERT-IN)	Imprisonment upto 1 years or fine upto Rs 1 lakh or both
18.	71	Penalty for misrepresentation	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
19.	72	Penalty for breach of confidentiality and privacy	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
20.	72A	Disclosure of information in breach of lawful contract	Imprisonment upto 3 years or fine upto Rs 5 lakh or bo Upto 5 lakh.
21.	73	Penalty for publishing electronic signature certificate false in certain particulars	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
22.	74	Publication for fraudulent purpose	Imprisonment upto 2 years or fine upto Rs 1 lakh or both

epathshala पाठशाला Gateway to All Post Graduate Courses

LIABILITY OF SERVICE PROVIDERS UNDER IT ACT

ISP क्या है? (What is ISP)

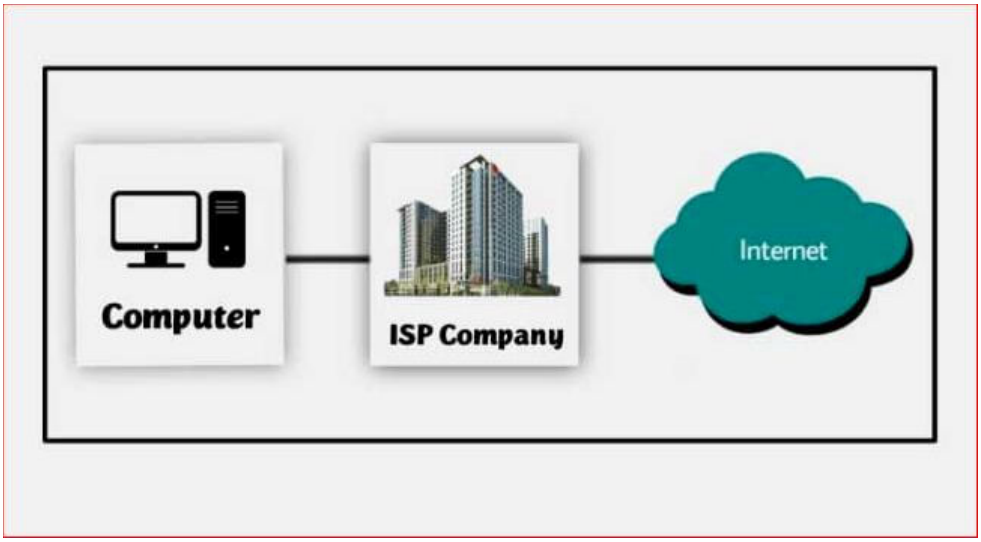
समान्यतः ISP, यूजर को जो भी सेवाएं प्रदान करते है, उसके लिये एक तय शुल्क (Fee) यूजर से लिया जाता है। यदि आपके पास एक कंप्यूटर और मॉडेम है, लेकिन इंटरनेट सर्विस प्रोवाइडर की सदस्यता (ISP subscription) नही है, तो आप इंटरनेट एक्सेस नही कर पाएंगे।

डिवाइस को इंटरनेट से कनेक्ट करने के लिये ISP एक प्रवेश द्वार (gateway) की तरह है। इस द्वार को पार करने के बाद ही आप कई ऑनलाइन एक्टिविटी, जैसे कि गूगल पर जानकारी खोजना, यूट्यूब पर वीडियो देखना, फेसबुक या दूसरे मैसेंजर ऐप के माध्यम से लोगों से संवाद करना और ऑनलाइन शॉपिंग इत्यादि कर पाते है।

सन 1984 में फर्स्ट इंटरनेट सर्विस प्रोवाइडर कंपनी (The World) संयुक्त राज्य अमेरिका (USA) में स्थापित की गई थी। भारत मे पहली सार्वजनिक रूप से उपलब्ध इंटरनेट सेवा 15 अगस्त 1995 में विदेश संचार निगम लिमिटेड (VSNL) द्वारा शुरू की गई।

कुल मिलाकर ISP का मुख्य कार्य इंटरनेट एक्सेस प्रदान करना है। भारत के कुछ प्रमुख क्षेत्रीय प्रदाताओं (regional providers) में Jio, Airtel, Vodafone, Idea, और BSNL शामिल है।

इंटरनेट सर्विस प्रोवाइडर की आवश्यकता क्यों है?



इंटरनेट एक विशाल नेटवर्क है, जो दुनियाभर में मौजूद कम्प्यूटरों को आपस मे जोड़ता है।

गूगल का सर्वर आपसे कई हजारों किलोमीटर दूर यूनाइटेड स्टेट में है। लेकिन जब आप Google.com खोलते है, तो उनकी साइट कुछ ही सेकंड में आपके डिवाइस पर खुल जाती है। ये सब इसलिए होता है, क्योंकि गूगल का सर्वर और आपकी डिवाइस एक ही नेटवर्क पर इंटरकनेक्ट है।

गूगल के सर्वर और आपकी डिवाइस के बीच कनेक्टिविटी बनाने का काम ISP का होता है। ये करने के लिये ISP द्वारा फाइबर ऑप्टिक केबल, टेलीफोन टॉवर और सेटेलाइट इत्यादि का उपयोग किया जाता है।

Internet से कनेक्ट करने के लिये कई विशेष telecommunications, Networking, और Routing उपकरणों की जरुरत पड़ती है। अब एक आम व्यक्ति तो इस तरह के उपकरणों की व्यवस्थता नही कर सकता इसलिये ISP उन्हें इंटरनेट कनेक्टिविटी प्रदान करने के लिये अपना नेटवर्क किराये (Rent) पर देते है।

ISPs यूजर को इंटरनेट से कैसे जोड़ते है?

इसके लिये सबसे पहले आप एक सर्विस प्रोवाइड की सदस्यता (ISP subscription) लेते है। जिसके बाद वो आपको अपने नेटवर्क से कनेक्ट करने की अनुमति देते है। एक बार आपकी डिवाइस इंटरनेट सर्विस प्रोवाइडर के नेटवर्क से कनेक्ट हो जाये फिर वो आपकी डिवाइस को एक IP address देते है।

ये एक यूनिक नंबर होता है, जो इंटरनेट जैसे विशाल नेटवर्क पर कंप्यूटरों को उनकी एक पहचान देता है। बिना IP address कोई भी कंप्यूटर, नेटवर्क पर दूसरे कंप्यूटर के साथ डेटा का आदान-प्रदान नही कर पायेगा।

जब आप गूगल की साइट खोलते है, तो आपका ब्राउज़र आपके ISP को ये रिक्वेस्ट भेजता है, कि इस आईपी एड्रेस वाली डिवाइस को ये वेब पेज चाहिये। जिसके बाद आपका सर्विस प्रोवाइडर गूगल के सर्वर को वह रिक्वेस्ट भेजता है, जिसके बाद गूगल के सर्वर द्वारा वो वेबपेज आपको भेज दिया जाता है।

ISP Liability under the Information Technology Act, 2000

भारत में आईएसपी से संबंधित प्रावधान विशेष रूप से आईटी अधिनियम, 2000 में रखे गए हैं, जहां एक इंटरनेट सेवा प्रदाता को नेटवर्क सेवा प्रदाता और स्पष्टीकरण (ए) से एस के रूप में संदर्भित किया जाता है। 79 इसे परिभाषित करता है:

"नेटवर्क सेवा प्रदाता" का अर्थ है एक मध्यस्थ।

मध्यस्थ को फिर से धारा 2 (डब्ल्यू) के तहत परिभाषित किया गया है:

किसी विशेष इलेक्ट्रॉनिक संदेश के संबंध में "मध्यस्थ" का अर्थ है कि कोई भी व्यक्ति जो किसी अन्य व्यक्ति की ओर से प्राप्त करता है या उस संदेश को प्रसारित करता है या उस संदेश के संबंध में कोई सेवा प्रदान करता है।

इसके अलावा अधिनियम में धारा 79 में एक खंड शामिल है जो कुछ परिस्थितियों में आईएसपी के दायित्व को सीमित करता है:

आईटी अधिनियम की धारा 79 के अनुसार

संदेह को दूर करने के लिए, यह घोषित किया गया है कि नेटवर्क सेवा प्रदाता के रूप में कोई भी सेवा प्रदान करने वाला कोई भी व्यक्ति इस अधिनियम के तहत उत्तरदायी नहीं होगा, यदि किसी तीसरे पक्ष के लिए बनाए गए नियम या कानून या उसके द्वारा उपलब्ध कराई गई जानकारी या डेटा के लिए वह साबित करता है कि अपराध या उल्लंघन उसकी जानकारी के बिना किया गया था या इस तरह के अपराध या उल्लंघन को रोकने के लिए उन्होंने सभी उचित परिश्रम का प्रयोग किया था।

यह अनुभाग कुछ मामलों में नेटवर्क सेवा प्रदाता की देनदारियों को प्रतिबंधित करना चाहता है। आइए पहले "नेटवर्क सेवा प्रदाता" (NSP) शब्द को समझें। धारा 79 कहती है कि एक एनएसपी एक मध्यस्थ है। आईटी अधिनियम ने "मध्यस्थ" शब्द को परिभाषित किया है।

आईटी अधिनियम की धारा 2 (1) (डब्ल्यू) के अनुसार-

''किसी विशेष इलेक्ट्रॉनिक संदेश के संबंध में "मध्यस्थ" का अर्थ है कि कोई भी व्यक्ति जो किसी अन्य व्यक्ति की ओर से उस संदेश को प्राप्त करता है, संग्रहीत करता है या प्रसारित करता है या उस संदेश के संबंध में कोई सेवा प्रदान करता है।''

इसलिए एक NSP की, एक विशेष इलेक्ट्रॉनिक संदेश के संबंध में, निम्नलिखित विशेषताएं हैं:

1. यह किसी अन्य व्यक्ति की ओर से संदेश प्राप्त करता है, या

2. यह किसी अन्य व्यक्ति की ओर से संदेश संग्रहीत करता है, या

3. यह दूसरे व्यक्ति की ओर से संदेश प्रसारित करता है, या

4. यह उस संदेश के संबंध में कोई सेवा प्रदान करता है।

"इलेक्ट्रॉनिक संदेश" शब्द को आईटी अधिनियम में परिभाषित नहीं किया गया है।

ई-कॉमर्स पर UNCITRAL मॉडल कानून एक डेटा संदेश को परिभाषित करता है जैसे -

अगर सूचनाऐं इलेक्ट्रॉनिक, ऑप्टिकल या इसी तरह की तकनीकी का प्रयोग करते हुये उत्पन्न, भेजी, प्राप्त या संग्रहीत की जाती है, इलेक्ट्रॉनिक संदेश कहलाता है"।

आईटी अधिनियम ने भारतीय साक्ष्य अधिनियम में धारा 88 ए डाला है। यह अनुभाग एक इलेक्ट्रॉनिक मेल सर्वर के माध्यम से अग्रेषित एक इलेक्ट्रॉनिक संदेश से संबंधित है।

UNCITRAL मॉडल कानून के तहत डेटा संदेश की परिभाषा और भारतीय साक्ष्य अधिनियम की धारा 88 ए के तहत इलेक्ट्रॉनिक संदेश के संदर्भ पर विचार करने के बाद, यह निष्कर्ष निकाला जा सकता है कि एनएसपी शब्द एक संकीर्ण शब्द है जो केवल इलेक्ट्रॉनिक संदेश सेवा प्रदाताओं से संबंधित है (जैसे ईमेल सेवा प्रदाता)। यह अन्य सेवा प्रदाताओं जैसे खोज इंजन, नीलामी वेबसाइटों आदि पर लागू नहीं होता है। यहां तक कि इंटरनेट सेवा प्रदाताओं (आईएसपी) के लिए, इस खंड का लाभ केवल ईमेल, ध्वनि मेल, टेलीफोनी आदि सेवाओं तक ही पहुंचेगा, जो उनके द्वारा प्रदान की गई हैं और नहीं उनके द्वारा दी जाने वाली इंटरनेट कनेक्शन सेवाएं।

हालांकि, इस खंड को आईटी अधिनियम की धारा 85 के साथ संयोजन के रूप में पढ़ा जाना चाहिए जो कंपनियों की देनदारियों से संबंधित है।

एक एनएसपी किसी तीसरे पक्ष की जानकारी या उसके द्वारा उपलब्ध कराए गए डेटा के लिए उत्तरदायी नहीं है यदि:

1. एनएसपी साबित करता है कि अपराध या उल्लंघन उसकी जानकारी के बिना किया गया था, या
2. एनएसपी यह साबित करता है कि इस तरह के अपराध या उल्लंघन को रोकने के लिए उसने पूरी लगन से अभ्यास किया था।

भारत में आईएसपी की देयता

भारत में आईएसपी के संबंध में, दिनांक 24 अगस्त 2007 के License for Internet Services दिशा निर्देशों के आधार पर उनकी देनदारियों का भी निर्धारण किया जाता है

इस लाइसेंस के खंड 33 के अनुसार:

1. ISPs को गैरकानूनी सामग्री, संदेश या संचार को उनके नेटवर्क पर ले जाने से रोकना चाहिए। इसमें आपत्तिजनक, अश्लील, अनधिकृत और अन्य सामग्री शामिल है।

2. प्रवर्तन एजेंसियों द्वारा ISP को ऐसी सामग्री के विशिष्ट उदाहरण बताए जाने के बाद, उन्हें अपने नेटवर्क पर ऐसी सामग्री को तुरंत रोकना चाहिए।

3. आईएसपी को यह सुनिश्चित करना चाहिए कि उनके द्वारा की गई सामग्री "अंतर्राष्ट्रीय और घरेलू साइबर कानूनों" का उल्लंघन न करे।

4. राष्ट्र विरोधी गतिविधियों के लिए आईएसपी नेटवर्क का उपयोग किया जाता है तो भारतीय दंड संहिता या अन्य कानूनों के तहत अपराध माना जाएगा।

5. आईटी अधिनियम प्रावधानों के अनुपालन के लिए आईएसपी जिम्मेदार होता है।

6. आईएसपी को यह सुनिश्चित करना चाहिए कि उनके नेटवर्क का उपयोग खतरे में डालने या नेटवर्क के बुनियादी ढांचे को कमजोर करने के लिए नहीं किया जा सकता है।

7. आईएसपी को यह सुनिश्चित करना चाहिए कि उनकी सेवाओं का उपयोग भारतीय नेटवर्क को तोड़ने या तोड़ने का प्रयास करने के लिए नहीं किया जाता है।

8. ISPs को बिना किसी देरी के, उपद्रव, अप्रिय या दुर्भावनापूर्ण कॉल, संदेश या संचार को उनके उपकरण और नेटवर्क के माध्यम से ले जाने के लिए सभी ट्रेसिंग सुविधाएं प्रदान करनी चाहिए। ये ट्रेसिंग सुविधाएं भारत सरकार के अधिकृत अधिकारियों सहित पुलिस, सीमा शुल्क, उत्पाद शुल्क, खुफिया विभाग के अधिकारियों आदि को प्रदान की जानी हैं।

9. आईएसपी को सरकार को जासूसी, विध्वंसक कार्य, तोड़फोड़ या किसी अन्य गैरकानूनी गतिविधि का मुकाबला करने के लिए आवश्यक सुविधाएं प्रदान करनी चाहिए।

इस लाइसेंस के खंड 34 के अनुसार:

1. सरकार आईएसपी नेटवर्क में दूरसंचार यातायात की निगरानी कर सकती है। आईएसपी को इस निगरानी के लिए आवश्यक हार्डवेयर और सॉफ्टवेयर के लिए भुगतान करना पड़ता है।

2. आईएसपी को जुड़े हुए सभी उपयोगकर्ताओं और उनके द्वारा उपयोग की जाने वाली सेवा (मेल, टेलनेट, http इत्यादि) का लॉग बनाए रखना चाहिए।

3. ISPs को अपने कंप्यूटर के माध्यम से हर जावक लॉगिन या टेलनेट को भी लॉग इन करना होगा। ये लॉग, साथ ही आईएसपी उपकरण से उत्पन्न सभी पैकेटों की प्रतियां, वास्तविक समय में दूरसंचार प्राधिकरण को उपलब्ध होनी चाहिए।

4. आईएसपी को अपने नेटवर्क पर संचार की गोपनीयता सुनिश्चित करनी चाहिए।

5. आईएसपी को यह सुनिश्चित करना चाहिए कि संदेशों का अनधिकृत अवरोधन उनके नेटवर्क पर न हो।

6. सरकार आपातकाल, युद्ध आदि के मामले में आईएसपी की सेवा, उपकरण और नेटवर्क को अधिग्रहण कर सकती है।

7. ISP के ग्राहकों की पूरी और अद्यतन सूची ISP की वेबसाइट के पासवर्ड संरक्षित हिस्से में उपलब्ध होनी चाहिए। यह अधिकृत इंटेलिजेंस एजेंसियों के उपयोग के लिए है।

8. **लीज** लाइन ग्राहकों के मामले में, आईएसपी को निम्नलिखित प्रारूप में लॉग बनाए रखना चाहिए:

Customer name	**IP Address allotted**	**Bandwidth provided**	**Address of Installation**	**Date of Installation / Commissioning**	**Contact person with Phone / email**

9. तकनीकी नेटवर्क संचालन का मुख्य अधिकारी-प्रभारी और आईएसपी का मुख्य सुरक्षा अधिकारी भारतीय नागरिक होना चाहिए।

10. आईएसपी को यह सुनिश्चित करना चाहिए कि ग्राहकों द्वारा लेनदेन की गई जानकारी सुरक्षित और संरक्षित हो।

11. संदेशों के वैध अवरोधन से निपटने वाले आईएसपी अधिकारियों को भारतीय नागरिक होना चाहिए।

12. आईएसपी के बोर्ड में बहुमत निदेशक भारतीय नागरिक होने चाहिए।

INVESTIGATION OF CYBER CRIMES

साइबर अपराधों की जांच

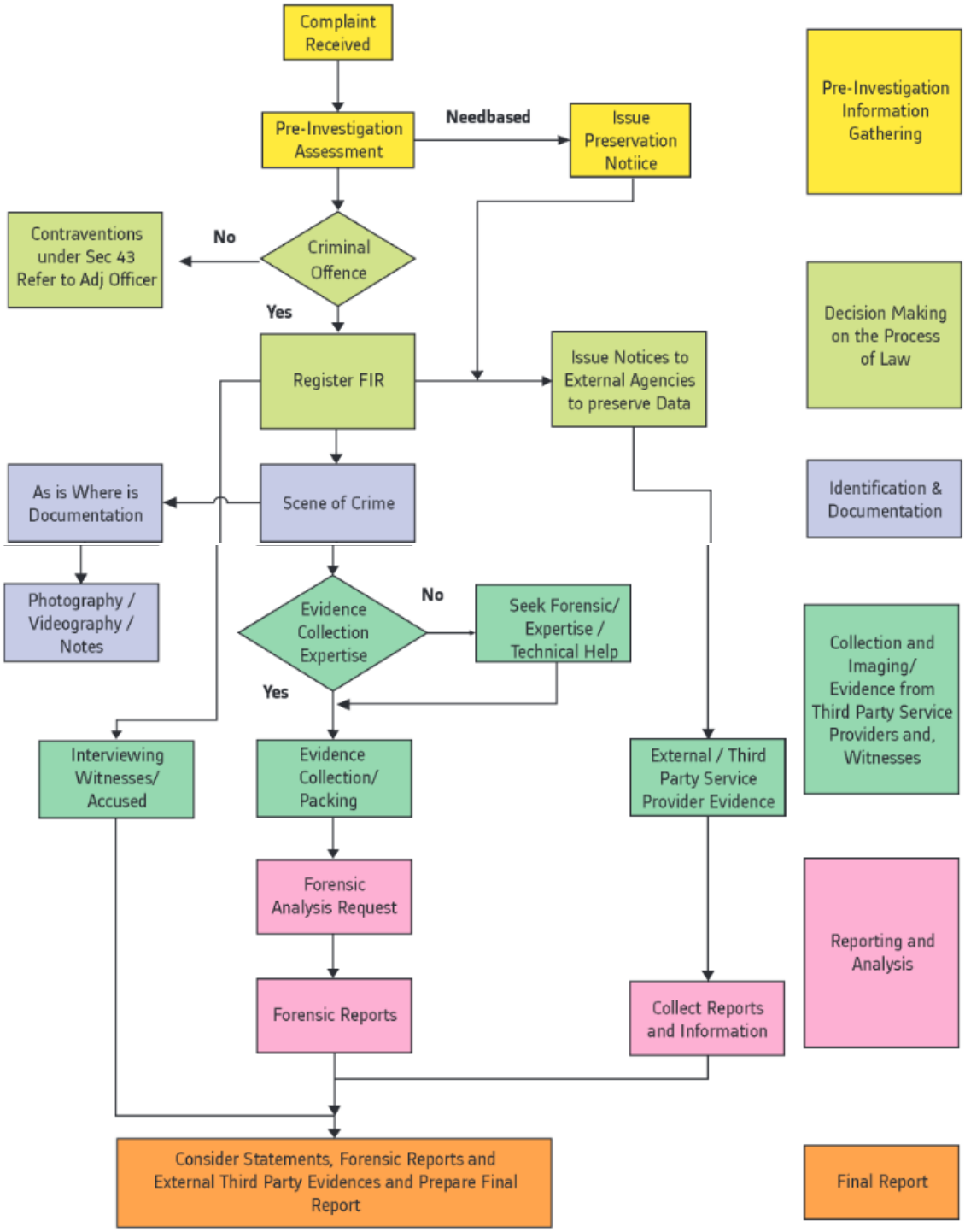
SOPs हमें जांच प्रक्रिया को विकसित करने के लिए निर्देशित करते हैं, जब तक कि चार्जशीट दाखिल न हो जाए और सबूतों को अदालत में शामिल नहीं किया जाता है । डिजिटल साक्ष्य की प्रकृति और वैधता के कारण, यह स्पष्ट है कि स्वचालित वातावरण में जांच के लिए निम्नलिखित मुख्य मानक तरीकों और प्रक्रियाओं की आवश्यकता होती है:

1- साक्ष्य को एक तरह से इकट्ठा किया जाना चाहिए जिसे अदालत द्वारा स्वीकार किया जाएगा। यदि मानक प्रक्रियाएँ तैयार की जाती हैं और उनका पालन किया जाता है तो यह आसान होगा। इससे अंतर्विभागीय और अंतर्राष्ट्रीय प्रभाव वाले मामलों में साक्ष्य के आदान-प्रदान की सुविधा भी होगी, खासकर, अगर सभी विभागों और देशों के जांचकर्ता एक समान तरीके से साक्ष्य एकत्र करते हैं।

2- हर उस चीज़ से बचने के लिए सावधानी बरतनी चाहिए जो डेटा को दूषित कर सकती है या किसी अन्य प्रकार की क्षति का कारण बन सकती है। मानक तरीकों और प्रक्रियाओं का उपयोग दुर्घटनावश क्षति के इस जोखिम को कम करता है। कुछ मामलों में, यह अपरिहार्य है कि परीक्षा प्रक्रिया के दौरान कुछ डेटा को बदल दिया जाएगा। इस प्रकार प्रौद्योगिकी की गहन समझ की आवश्यकता है, जिसका उपयोग परीक्षा के लिए किया जा रहा है और इसके दस्तावेज़ीकरण की भी आवश्यकता है ताकि बाद में न्यायालय में इसके कारणों / प्रभावों के बारे में बताया जा सके।

3- अनुचित साक्ष्य संग्रह के कुछ सबसे महत्वपूर्ण कारण खराब लिखित नीतियां, योजना की कमी, घटना प्रतिक्रिया प्रशिक्षण हैं।

5.2. Standard Operating Procedures – A Flow Chart



Flow chart for digital crime investigation under ITAA 2008

जांच की बुनियादी आवश्यकताएं:

(1) कंप्यूटर / मोबाइल फोन / लैपटॉप / अन्य इलेक्ट्रॉनिक मीडिया का उपयोग की जानकारी।
(2) ई-मेल संदेश भेजना और प्राप्त करना।
(3) आईपी एड्रेस के बारे में ज्ञान, मेल हेडर से आईपी एड्रेस का पता लगाना।
(4) आईएसपी (इंटरनेट सेवा प्रदाता) और एमएसपी (मोबाइल सेवा प्रदाता) के बारे में ज्ञान।
(५) मोबाइल फोन की सीडीआर से जानकारी पढ़ने और एकत्र करने का ज्ञान।
(6) ऑनलाइन व्यापार लेनदेन की प्रक्रिया के बारे में ज्ञान।
(7) ऑनलाइन व्यापार की दुनिया में काम कर रहे भुगतान गेटवे के बारे में ज्ञान।
(8) खाते **जांच** के विवरण को पढ़ने के बारे में ज्ञान।
(9) कुछ ऑनलाइन टूल के उपयोग के बारे में ज्ञान: जैसे कि what is my IP Address, whois my domain, ip2tools, IP address Tracer tools, Trace bhartiya mobile.com, India trace .com, nobbi.com
(10) टूल किट, और पैकिंग सामग्री।
(11) कानूनी वर्गों का उचित ज्ञान ।

A. बैंकिंग धोखाधड़ी :

बैंक भारतीय अर्थव्यवस्था का एक अनिवार्य हिस्सा हैं। धोखाधड़ी को रोकने के लिए प्राथमिक ज़िम्मेदारी स्वयं बैंकों के पास है। बैंक जनता के पैसे की उचित देखभाल करते है। धोखाधड़ी की रोकथाम के लिए आरबीआई बैंकों को की सलाह देता रहता है। बैंकों जैसी संस्थाओं पर धोखाधड़ी का प्रभाव और धोखाधड़ी की आर्थिक लागत, बैंकिंग प्रणाली में विश्वास और अर्थव्यवस्था की अखंडता और स्थिरता को नुकसान पहुंचा सकती है। यह बैंकों को नीचे ला सकता है, केंद्रीय बैंक की पर्यवेक्षी भूमिका को कम कर सकता है और सामाजिक अशांति, असंतोष और राजनीतिक उथल-पुथल भी पैदा कर सकता है। तकनीकी प्रगति से बैंकिंग धोखाधड़ी हाल के दिनों में बढ़ी है। जांच एजेंसियों के समक्ष चुनौती क्षमता निर्माण, जांच की गुणवत्ता, विशेषज्ञों से समर्थन के रूप में है।

बैंकिंग धोखाधड़ी की जांच :

(i) पीड़ित के बैंक खाते का विवरण प्राप्त करें।
(ii) लाभार्थियों के बैंक खाते का विवरण प्राप्त करें।
(iii) लाभार्थियों के बैंक खाता, केवाईसी और आईडीए के साथ खाता खोलने का फॉर्म प्राप्त करें।
(iv) यदि ऑनलाइन लेनदेन में फंड का उपयोग किया गया था, तो बैंक से ट्रांजेक्शन ट्रेल प्राप्त करें।
(v) भुगतान गेटवे कंपनी, (बिलडेस्क, पेटीएम, फ्लिपकार्ट, स्नैप डील, ईबे इंडिया) से धन के वास्तविक उपयोगकर्ता के बारे में जानकारी प्राप्त करें।
(vi) कंपनी से प्राप्त जानकारी पर आरोपी को खोजें।
(vii) शॉपिंग सेंटर और अन्य स्थानों से सीसीटीवी फुटेज प्राप्त करें।
(viii) उस मोबाइल नंबर को सत्यापित करें जिस पर लेन-देन एसएमएस लाभार्थी खाते के उपयोगकर्ता को भेज रहा था।
(ix) लाभार्थी के खाते के बैंक स्टेटमेंट को ध्यान से पढ़ें, आपको अन्य डेबिट / क्रेडिट लेनदेन के बारे में अच्छी तरह से जानकारी मिल जाएगी जिससे आप वास्तविक अपराधी तक पहुंच सकते हैं।
(x) अभियुक्तों की गिरफ्तारी के बाद, बैंक खातों के दस्तावेजों की तुलना करने के लिए नमूना हस्ताक्षर / लेखन करें।
(xi) अपने सर्वर से बैंक द्वारा उपलब्ध कराए गए अभिलेखों के संबंध में भारतीय साक्ष्य अधिनियम का प्रमाण पत्र ६५ लेना न भूलें।

(xii) यदि एटीएम से राशि निकाली जाए तो विशेष रूप से एटीएम के सीसीटीवी फुटेज प्राप्त करें।
(xiii) पीड़ित से जानकारी प्राप्त करने के लिए उपयोग किए जाने पर संदिग्ध मोबाइल फोन की सीडीआर, सीएएफ प्राप्त करें।
(xiv) क्रेडिट कार्ड के माध्यम से किए गए लेनदेन के बारे में पूरी जानकारी संबंधित क्रेडिट कार्ड कंपनी से प्राप्त करें।
(xv) कार्ड कंपनी द्वारा दी गई जानकारी पर अपराधी को ट्रेस करें।
(xvi) Issue notices u/s 91 Cr. P. C. to get information/ records
(xvii) फेसबुक, सर्च इंजन / आईएसपी, एमएसपी / बैंक / पेमेंट गेट तरीके / साइबर कैफे आदि जैसे चिंताजनक इलेक्ट्रॉनिक डेटा प्रदाता को संरक्षण नोटिस जारी करना।

POLICE NOTICE

(Under section 91 of Code of Criminal Procedure 1973)

To,

Sir/Madam,

Sub: Request to provide details with respect to *** bank
Credit /Debit card/ Account/ No:
Ref: (name of police station e.g. Ashok nagar, JP Nagar) Police Station CR No *******

*****

Brief facts about the case

Sample details requested from the bank

1. Account details from dd-mm-yy to dd-mm-yy
2. Access logs of the suspected account
3. Transaction details of debit/credit cards
4. CCTV clippings of ATM cameras from dd-mm-yy to dd-mm-yy

Yours truly,

(Signature, Name of IO & seal)

B. सोशल साइट्स से संबंधित अपराध :

Social Networking एक "**Network of individuals**" है जो पारस्परिक संबंधो जैसे दोस्त, सम्बंधी, ग्राहक और सहकर्मी से मिलकर बनता है। उदाहरण के लिए Social Media एक social networking service है जहाँ आप अपनी प्रोफाइल बनाकर लोगो से जुड़ते है और आपस मे communicate और information exchange करते है।

ये "Social Networks" आपको लोगो से जुड़ने और सामाजिक relationship बनाने में काफी help करते है। Facebook, LinkedIn, Twitter और Instagram आज के सबसे **popular social sites** में से है। ये एक ऐसी Social Networking है, जहाँ आप virtual community बनाते है और online आपस में सूचना का आदान-प्रदान करते है।

Social Networking sites के online risk इस प्रकार है:

1) आप scam के शिकार हो सकते है. आपका account hack किया जा सकता है ये आपकी profile का misuse करके scam links को post करते है, जिससे आपके दोस्तों को नुकसान हो सकता है।
2) इन social networks पर किसी भी Third party app को download न करे. ये एप्लीकेशन की शक्ल में Malicious app, spyware, या virus भी हो सकता है, इससे hackers आपके phone का access प्राप्त करने में कामयाब होते है।
3) ये Social Networks अपने users को **communicative convenience** तो जरूर provide करते है, लेकिन privacy और security का आपको खुद ध्यान रखना चाहिये। किसी भी sensitive information को इन platform में share न करे या फिर उन्हें private रखे।
4) अपनी profile और post की privacy को change करे इनकी visibility को अपने friends तक ही रखे। ये समस्या देखने मे आती है कि आपके data का उपयोग करके fake id बनाई जाती है। जिसका गलत तरह से उपयोग हो सकता है।
5) Unknown friend request को बस ऐसे ही accept न कर ले। ये आपको झांसा दे सकते है और message के जरिये malicious link आपको send करके आपको नुकसान पहुंचा सकते है।

सोशल साइट्स से संबंधित मामलों की जांच:

(i) अश्लील सामग्री / तस्वीर / वीडियो की प्रिंट स्क्रीन कॉपी प्राप्त करें, जो ई-मेल / एमएमएस / एसएमएस / सोशल साइट्स के माध्यम से पीड़ित को भेजी गई थी।

(ii) संदर्भ के लिए संदिग्ध पोस्ट के "URL" लें।

(iii) उपरोक्त संदिग्ध सामग्रियों की भी हार्ड कॉपी प्राप्त करें।

(iv) आईएसपी / मोबाइल कंपनी से प्रेषक का विवरण प्राप्त करें।

(v) मेल भेजने वाले / सामाजिक साइटों के उपयोगकर्ता प्रोफ़ाइल की गतिविधियों और उपयोगकर्ता प्रोफ़ाइल प्राप्त करें।

(vi) मोबाइल कंपनी से CDR और CAF प्राप्त करें यदि मोबाइल का उपयोग अपराध में किया जाता है।

(vii) घटना के समय आईपी एड्रेस के वास्तविक उपयोगकर्ता के बारे में जानकारी प्राप्त करें और अपराधी को ट्रेस करें।

(viii) संदिग्ध व्यक्ति की सीडीआर का विश्लेषण करें और आरोपी का पता लगाएं।

(ix) Issue notices u/s 91 Cr. P. C. to get information/ records

(x) इलेक्ट्रॉनिक डेटा प्रदाता जैसे फ़ेसबुक, सर्च इंजन / आईएसपी, एमएसपी / बैंक / पेमेंट गेट तरीके / साइबर कैफे आदि के लिए नोटिस जारी करना।

NOTICE U/S 91

OFFICE OF THE ADDITIONAL DIRECTOR OF POLICE, STATE CRIME RECORD BUREAU,JAIPUR, RAJASTHAN, INDIA

No. 487 Date :-05-10-13

To,
Legal department
Facebook.com

Sub: To get login activities U/s 91 of Criminal Procedure Code, India.
Ref.: Case No. 07/2013; U/s 67 IT Act 2000 and 292 Indian penal code Police station Cyber crime jaipur, Rajastha (INDIA).

Sir,

We have registered a complaint against a fake Facebook profile. Someone has created a fake Facebook profile to harass the victim. Whereas the above profile now seems to be deactivated. During the investigation some information regarding following URL are required. Please manage the point wise information for the below URL at our email id pscyber@rajpolice.gov.in

URL: https://www.facebook.com/Deepika.batra.900

1. When and from where (complete IP address details with date and time) this Face book account was created.
2. Login Activity details(statement) (Complete IP address detail with date and time) of this Accounts from activation date to till today.
3. All identifying particulars of the subscriber who has created Facebok account.
4. Verified mobile number for this account.

CYBER CRIME POLICE STATION JAIPUR RAJ.

Police Inspector
Cyber Crime Police Station
Rajasthan Police Academy road,
Panipech Nehru Nagar
Jaipur , Rajasthan,(INDIA)
PIN – 302016
Phone no. +91141-2309547
Email-pscyber@rajpolice.gov.in

REPLY FROM FACEBOOK

farget 100006652687390 (Generated 2013-12-10 07:22:36 UTC)
Range 2001-01-01 08:00:00 UTC to 2013-10-26 07:00:00 UTC
Name First Deepika
Middle
Last Batra

stered deepika.batra.900@facebook.com
Email deepikaraand89@gmail.com
resses

Name deepika.batra.900

tration 2013-09-16 14:49:41 UTC
Date

ccount Account Still false
e Date Active
Time 2013-11-22 14:22:17 UTC

Phone
umbers

t Cards

Sessions
tivities IP Address 106.219.24.124
Time 2013-10-20 02:56:10 UTC

IP Address 106.219.24.124
Time 2013-10-20 02:56:10 UTC

IP Address 106.219.24.124
Time 2013-10-20 02:56:10 UTC

IP Address 106.219.24.124
Time 2013-10-20 02:55:15 UTC

IP Address 106.219.7.53
Time 2013-10-19 15:02:10 UTC

IP Address 106.219.7.53
Time 2013-10-19 15:02:09 UTC

IP Address 106.219.7.53
Time 2013-10-19 15:02:09 UTC

IP Address 106.219.7.53
Time 2013-10-19 14:58:43 UTC

IP Address 106.219.48.244
Time 2013-10-19 08:02:40 UTC

IP Address 106.219.48.244
Time 2013-10-19 08:02:40 UTC

IP Address 106.219.48.244

FIR no 7/13
शामिल पत्रावली

1 cr
C&PS

REPLY FROM AIRTEL

Subject: **RE: REGRADING NAME , ADDRESS & CDR IN REFERENCE FIR NO.07/13 U/S 66A , 66D IT ACT IPC ps cyber crime police station jaipur**
To: ccps-raj@nic.in <ccps-raj@nic.in>
Date: 26/05/14 04:04 PM
From: rajasthan nodaldesk <rajasthan.nodaldesk@aircel.co.in>

919636204700.xls (53kB)

Find enclosed

9636204700 JITIN SONI S/O YOGESH SONI RAINI MOHALLA KISHANGARH BAS Alwar

WITH REGARDS
Nodaldesk Rajasthan, AIRCEL LTD. 1st Floor, Dainik Navjyoti, Amrapali Circle, C-Block, Vaishali Nagar-302021, Land line 91-9782500208, [M] 91-9782000561, [F] 0141-5105158.
Kindly note:- Data provided to you, is as per electronic system maintained by AIRCEL LTD. and be deemed authenticated only after duly sealed & signed by Authorized Nodal Officer for evidence before court of law.

From: ccps-raj@nic.in [mailto:ccps-raj@nic.in]
Sent: Monday, May 26, 2014 3:43 PM
To: rajasthan nodaldesk
Subject: REGRADING NAME , ADDRESS & CDR IN REFERENCE FIR NO.07/13 U/S 66A , 66D IT ACT IPC ps cyber crime police station jaipur

DEAR NODAL OFFICER ,

PLEASE PROVIDE NAME , ADDRESS & CDR OF MOBILE NUMBER 9636204700 (**PORTED IN AIRCEL**)FROM 20-05-14 TO TILL DATE IN REFERENCE FIR NO.07/13 U/S 66A ,66D IT ACT B IPC ps cyber crime police station jaipur rajasthan

SHO
cyber crime police station
Jaipur Rajasthan

This e-mail message and its attachments are for the sole use of the intended recipients. It may contain proprietary, confidential, privileged information or other information subject to legal restrictions. If you are not the intended recipient of this message, please do not read, copy, use or disclose this message or its attachments. Please notify the sender immediately and destroy all copies of this message and any attachments.
WARNING: This e-mail message including attachment(s), if any, is believed to be free of any virus. However, it is the responsibility of the recipient to ensure for absence of viruses. Aircel shall not be held responsible nor does it accept any liability for any damage arising in any way from its use.

C ई-मेल :

Electronic Mail को शार्ट में Email कहते है। कोई भी मैसेज या मेल जब इलेक्ट्रॉनिक माध्यम से भेजा जाता है, तो हम उसे "E-mail" कहेंगे। अगर इसकी परिभाषा देखे तो "इलेक्ट्रॉनिक मेल या ईमेल इलेक्ट्रॉनिक डिवाइस का उपयोग करने वाले लोगों के बीच संदेशों का आदान-प्रदान करने की एक विधि है"।

Email को एक कंप्यूटर से दूसरे कंप्यूटर में भेजने के लिये कंप्यूटर नेटवर्क जैसे Internet का उपयोग होता है। प्रत्येक व्यक्ति का एक यूनिक ***E-mail Address*** होता है। अगर आप किसी व्यक्ति को ऑनलाइन मेल भेजना चाहते है, तो आपको उसका ईमेल एड्रेस पता होना चाहिये।

Email का उपयोग मुख्य रूप से टेक्स्ट, इमेज, डॉक्यूमेंट या किसी दूसरे तरह के फाइल्स को भेजने और प्राप्त करने के लिए किया जाता है।

भारत मे कुछ लोकप्रिय ईमेल सर्विस प्रोवाइडर जिनकी लिस्ट नीचे दी गयी है:

1. Gmail (www.gmail.com)
2. Yahoo! Mail (https://login.yahoo.com/)
3. AOL Mail (https://login.aol.com/)
4. Mail (https://www.mail.com/int/)
5. iCloud (https://www.icloud.com/mail)
6. Rediff Mail (https://mail.rediff.com/)
7. Yandex (https://mail.yandex.com/)

E-mail Address:

एक E-mail Address किसी ईमेल अकॉउंट का पता होता है। इसका उपयोग कर आप Email भेज व प्राप्त कर सकते है। ये एड्रेस हर अकॉउंट के लिये अलग होता है।

उदाहरण के लिए – ptsjdr@gmail.com

- Email का जो पहला हिस्सा होता है यानी '@' सिंबल से पहले वाला भाग वो Username होता है। अर्थात इस हिस्से पर उस व्यक्ति का नाम, कंपनी का नाम, संस्था का नाम या किसी समूह का नाम आ सकता है। जैसे ptsjdr
- अगला हिस्सा '@' (at sign) जो Username और Domain name को अलग करता है।
- अंतिम हिस्सा Domain name होता है। जो ये बताता है कि किस कंपनी के Mail server का उपयोग किया जा रहा है। हमारे मामले में हम Gmail.com का उपयोग कर रहे है ऑनलाइन मेल भेजने और प्राप्त करने के लिए।

ई-मेल संदेशों की जांच:

1. Yahoo.com, gmail.com, hotmail.com, redifmail.com जैसे मेल डोमेन की पहचान करें।

2. संदिग्ध ई-मेल आईडी की निम्नलिखित जानकारी / रिकॉर्ड मांगने के लिए ई-मेल सर्वर वेबसाइट पर नोटिस u/s 91 भेजें:

i संदिग्ध ई-मेल आईडी की उपयोगकर्ता प्रोफ़ाइल

ii विशेष अवधि के लॉगिन विवरण

iii संदिग्ध ई-मेल आईडी कब और कहाँ से बनाई गई?

iv यदि पीड़ित ई-मेल आईडी की हैकिंग से संबंधित है, तो पीड़ित के ई-मेल आईडी के हटाए गए डेटा को पुनर्स्थापित करें और पीड़ितों के मोबाइल पर एक नया पासवर्ड भेजें।

v संदिग्ध सामग्री / तस्वीरों / वीडियो के सभी URL से संबंधित प्रतियां संलग्न करें।

vi अपने अनुरोध में घटना का सार भी लिखें कि आपको जानकारी / रिकॉर्ड की आवश्यकता है।

3. मेल हेडर ट्रेसिंग वेबसाइटों (iptrackeronline.com, my ip.com, e-mailheadertracer.com, ip2location.com) के माध्यम से ई-मेल हेडर से आई पी एड्रेस ट्रेस करना।

4. मेल सर्वर से आईपी एड्रेस प्राप्त करने या मेल हेडर से आईपी एड्रेस ट्रेस करने के बाद whatismyipaddress.com से विशेष रूप से आईपी एड्रेस की ISP ट्रेसिंग करें।

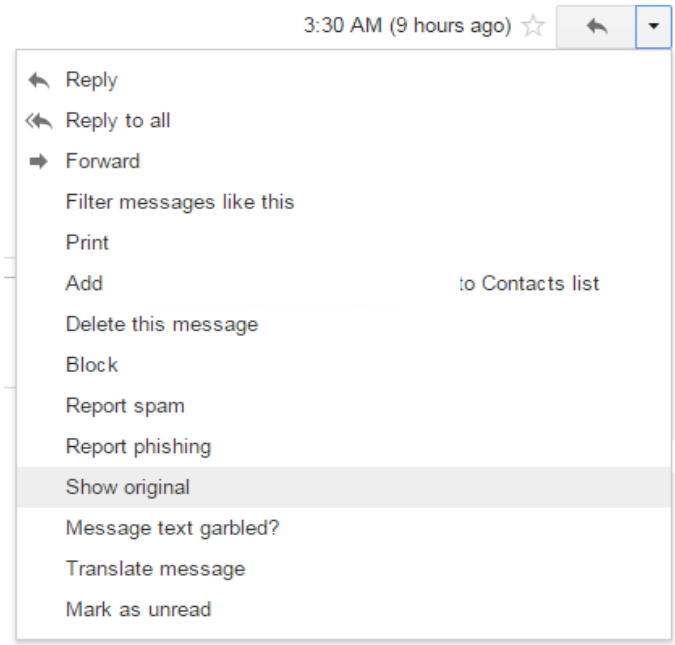
5. Send a notice u/s 91 Cr. P.C. to concern ISP to provide the complete profile of user,

6. दिए गए पते पर संदिग्ध व्यक्ति को खोजें।

7. अंतराष्ट्रीय वेबसाईट्स से लॉगिन डिटेल UTC टाईम जोन में मिलती है अतः सही टाईम की जानकारी के लिये UTC+5.30 Hrs करके टाईम फाईनल किया जाना चाहिये।

ईमेल की लोकेशन और एड्रेस का पता:

आपको जीमेल पर जिस भी ईमेल से मेल आया है उसे ओपन करें। फिर राइट साइड में टाइम के बराबर में दिख रहे बटन पर टैप करें। इसके बाद **SHOW ORIGINAL** पर टैप करें।



Original Message

Message ID	<CAOrU-hsx_6OCmnR8efcA1ca_ELMd50a21yDqQ=QFcyrtn4ehXQ@mail.gmail.com>
Created at:	Thu, Feb 18, 2021 at 9:19 PM (Delivered after 12 seconds)
From:	Surya Prakash [redacted]policeuniversity.ac.in>
To:	Kapil Pareek [redacted]@policeuniversity.ac.in>
Subject:	
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain policeuniversity-ac-in.20150623.gappssmtp.com Learn more

Download Original

Copy to clipboard

हेडर से क्या मिला

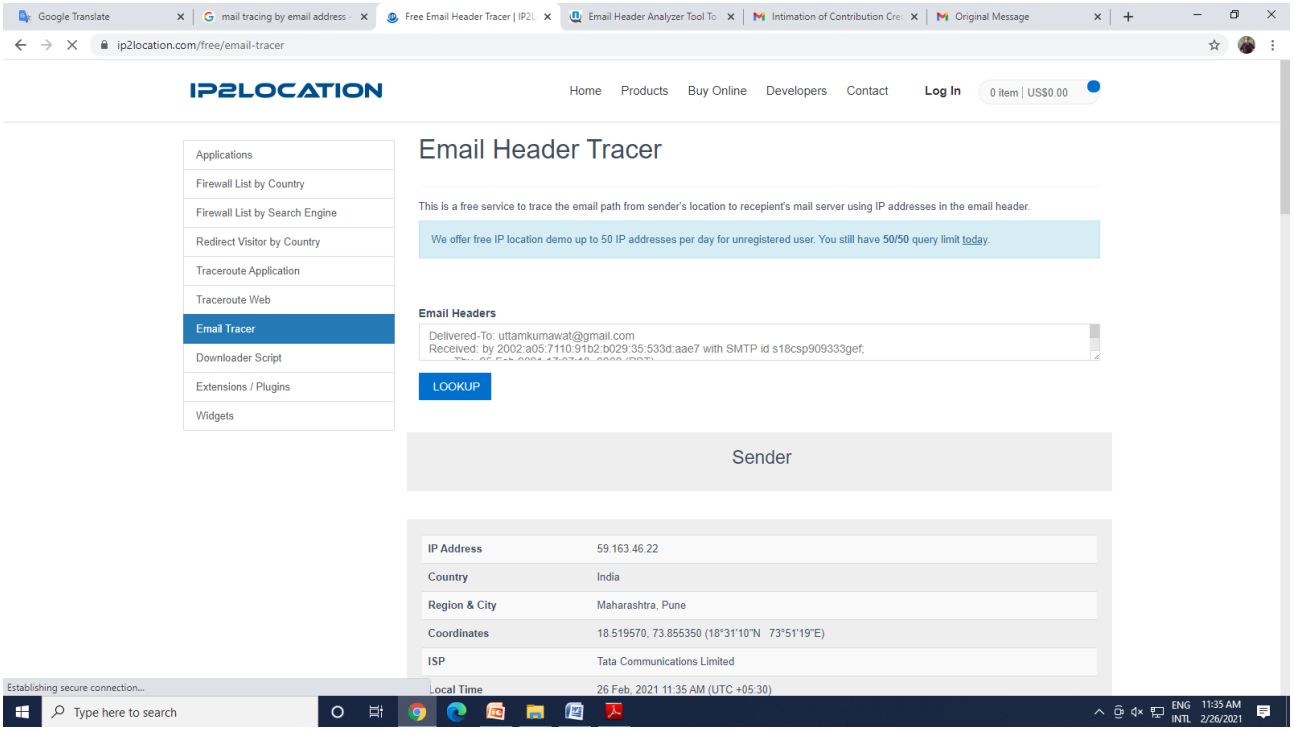
- किसने भेजा
- किसको भेजा
- सोर्स
- टाइम
- यूजर की आइडेंटिटी
- डोमेन
- IP

इस जानकारी से क्या कर सकते हे

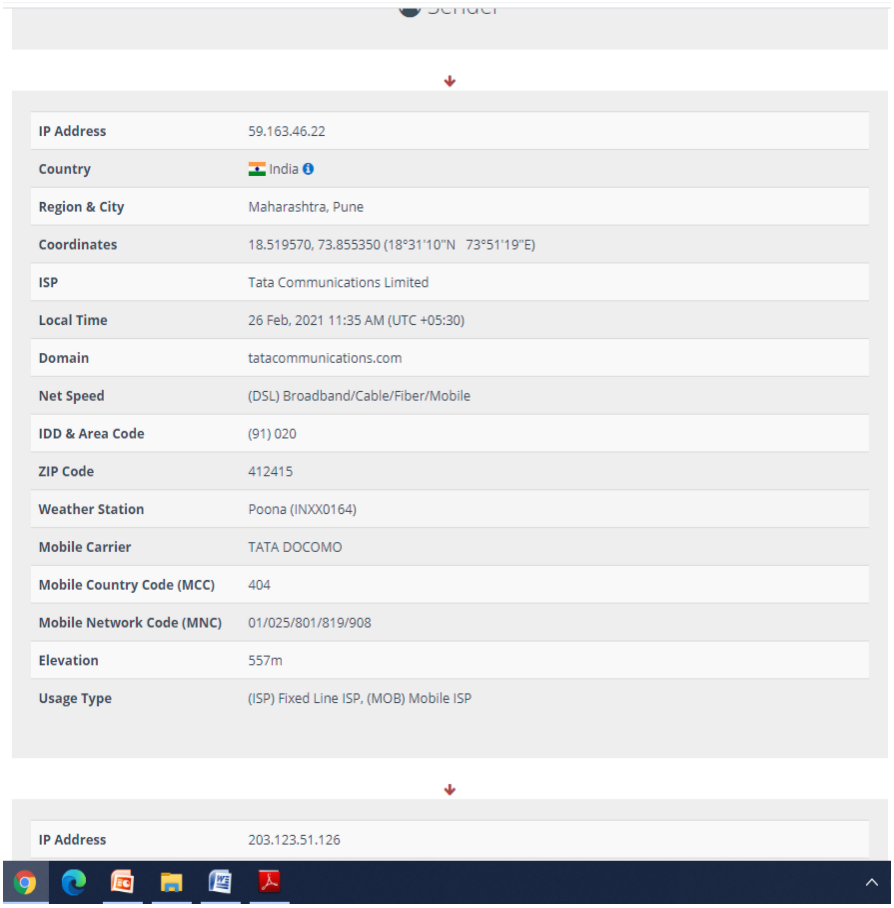
- डोमेन प्रोवाइडर को कॉन्टेक्ट कर सकते हे|
- डोमेन नाम से आईडिया लगा सकते हे|
- IP के की मदद से डिवाइस का पता लगा सकते हे|
- हेडर को कॉपी करें, फिर ट्रेस ईमेल एनालाइज़र में पेस्ट करें |

```
Return-path: <user@example.com>
Received: from mac.com ([10.13.11.252])
  by ms031.mac.com (Sun Java System Messaging Server 6.2-8.04 (built Feb 28
  2007)) with ESMTP id <0JMI007ZN7PETGC0@ms031.mac.com> for user@example.com; Thu,
  09 Aug 2007 04:24:50 -0700 (PDT)
Received: from mail.dsis.net (mail.dsis.net [70.183.59.5])
  by mac.com (Xserve/smtpin22/MantshX 4.0) with ESMTP id l79BOnNS000101
  for <user@example.com>; Thu, 09 Aug 2007 04:24:49 -0700 (PDT)
Received: from [192.168.2.77] (70.183.59.6) by mail.dsis.net with ESMTP
  (EIMS X 3.3.2) for <user@example.com>; Thu, 09 Aug 2007 04:24:49 -0700
Date: Thu, 09 Aug 2007 04:24:57 -0700
From: Frank Sender <sender@example.com>
Subject: Test
To: Joe User <user@example.com>
Message-id: <61086DBD-252B-46D2-A54C-263FE5E02B41@example.com>
MIME-version: 1.0 (Apple Message framework v752.2)
X-Mailer: Apple Mail (2.752.2)
Content-type: text/plain; charset=US-ASCII; format=flowed
Content-transfer-encoding: 7bit
```

- **Get Source** / LOOKUP/Analyze बटन दबाएं



ईमेल एनालाईजर द्वारा प्राप्त सूचना



IP Address	59.163.46.22
Country	India
Region & City	Maharashtra, Pune
Coordinates	18.519570, 73.855350 (18°31'10"N 73°51'19"E)
ISP	Tata Communications Limited
Local Time	26 Feb, 2021 11:35 AM (UTC +05:30)
Domain	tatacommunications.com
Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
IDD & Area Code	(91) 020
ZIP Code	412415
Weather Station	Poona (INXX0164)
Mobile Carrier	TATA DOCOMO
Mobile Country Code (MCC)	404
Mobile Network Code (MNC)	01/025/801/819/908
Elevation	557m
Usage Type	(ISP) Fixed Line ISP, (MOB) Mobile ISP

IP Address	203.123.51.126

D. IP Address

IP का Full Form है **Internet Protocol होता है। IP address,** network hardware का identifying number होता है। IP address एक device को IP-based network में दुसरे devices के साथ communicate करने के लिए allow करता है।

IP address, को simply हम "**IP**" भी कह सकते हैं। यह एक unique address होता है जिससे एक device को Internet या एक local network में आसानी से identify किया जा सकता है। यह एक system को दुसरे system के द्वारा recognize होने के लिए allow करता है जो की via Internet protocol connected होते हैं। दो primary types के IP address formats होते हैं — **IPv4** और **IPv6**.

Use of IP Address

एक IP address किसी भी एक networked device को एक identity प्रदान करता है। जैसे की एक घर या business office को पहचानने के लिए उनकी एक specific physical location होती है, ठीक उसी प्रकार एक network में अलग अलग devices को IP Addresses के माध्यम से differentiate किया जाता है।

उदाहरण के लिए. अगर मुझे एक package भेजना है अपने दोस्त को जो की एक दुसरे ही देश में रहता है तब इसके लिए मुझे उसकी **exact destination location** ज्ञात होना आवश्यक है। केवल receiver का नाम ही काफी नहीं होता है, साथ में उसकी एक specific address भी होनी चाहिए, जो की उस package में लिखा जाता है या attach किया जाता है, जिससे वह package उस तक आसानी से पहुँच सकते हैं। इसी प्रकार किसी नेटवर्क में एक कम्प्यूटर से डाटा जब दूसरे कम्प्यूटर को भेजा जाता है तो डाटा पैकेट के साथ IP address, attach करके भेजा जाता है ताकि वो डाटा पैकेट सही कम्प्यूटर पर पहुंच सके।

IP Versions (IPv4 vs IPv6)

IPv4 पुराना version हैं वहीँ IPv6 उसका upgraded IP version होता है। IPv6 को IPv4 के स्थान पर इसलिये लाया गया क्योंकि IPv6, IPv4 की तुलना में ज्यादा number की IP Addresses प्रदान करती है।

IPv4 addresses हमें केवल 4 billion unique IP Addresses (2^{32}) ही प्रदान कर सकता है। ये भी बहुत ज्यादा addresses है, लेकिन आज के modern world के लिए ये काफी नहीं है क्यूँ किआज प्रत्येक user के पास एक से ज्यादा अलग अलग devices है जो की internet का इस्तमाल करते हैं।

अगर हम practically सोचें तब दुनियाभर में 7 billion people से ज्यादा लोग हैं। अगर प्रत्येक लोग एक भी device का इस्तमाल करें तब भी IPv4 उन्हें sufficient IP address प्रदान करने में सक्षम नहीं है।

वहीँ दूसरी तरफ IPv6, करीब 340 trillion, trillion, trillion addresses (2^{128}) को support करता है जो होता है 340 और उसके साथ **12 zeroes**! इसका मतलब की अगर पृथ्वी का प्रत्येक इन्सान भी लाखों devices को internet के साथ connect कर सकता है तब भी IP Addresses की कोई कमी नहीं होगी।

ज्यादा IP Addresses को supply करने के साथ साथ IPv6 और भी बहुत ही benefit प्रदान करते हैं जैसे की-

- IP address collisions नहीं होंगे जो की private addresses, auto-configuration से होते हैं साथ में Network Address Translation (NAT) करने की भी जरुरत नहीं है।
- ये efficient routing प्रदान करती है।

- साथ में easier administration भी प्रदान करती है।
- ये built-in privacy भी प्रदान करती है।

IPv4 addresses 32-bit numerical number जो की एक decimal format में लिखे हुए होते हैं, जैसे की 203.278.148.81 या 192.138.0.1. वहीँ **IPv6** में trillions की तादाद में addresses होती है, इसलिए उन्हें hexadecimal के format में display किया जाता है, जैसे की **3fge:1800:4545:3:100:l8ff:ee21:97cf.**

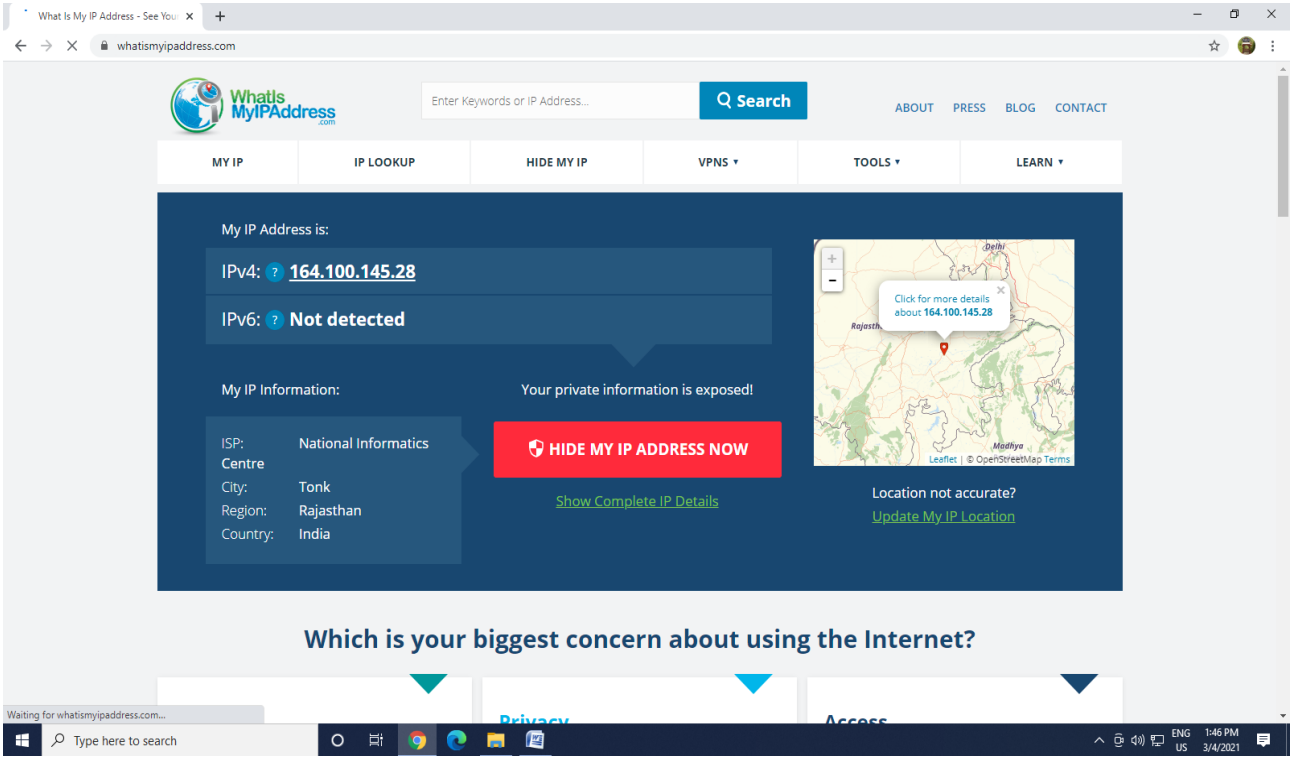
IP Address कैसे पता करे

कोई भी आई.पी. एड्रेस दो प्रकार के हो सकते है–

1- Public IP Address

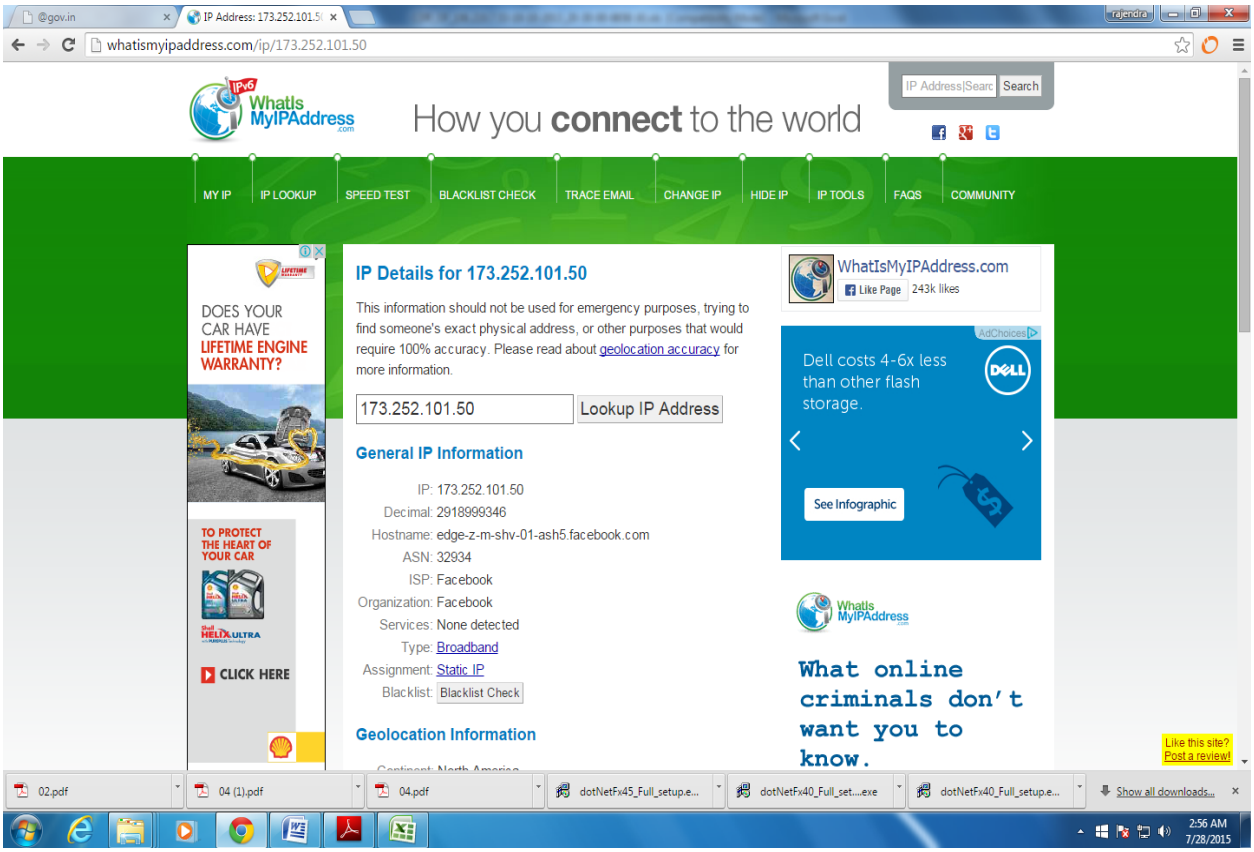
स्वयं का IP Address पता करना–

आपके Router के IP Address को ढूंढना बहुत ही आसान होता है, जिसके लिए आप WhatsMyIP.org, या WhatIsMyIPAddress.com का इस्तमाल कर सकते हैं। ये sites उन सभी network-connected device के साथ काम कर सकती हैं जो की एक web browser को support करती है, जैसे smartphone, iPod, laptop, desktop, tablet, इत्यादि.



किसी अन्य आई.पी. एड्रेस के बारे में जानकारी पता करना–

किसी अन्य का आई.पी. एड्रेस का IP Lookup में प्रयोग कर प्राप्त सूचना से यह पता लगा सकते है कि वह आई.पी. एड्रेस किस संगठन का है, किस देश का है, किस प्रकार का है इत्यादि। इसके लिये निम्न प्रकार whatismyipaddress.com की स्क्रीन पर दिये गये टेक्स्ट बॉक्स में आई. पी. एड्रेस लिखकर सामने दिये गये Lookup IP Address बटन पर क्लिक करेंगे जिससे उस आई. पी. एड्रेस से संबंधित जानकारी नीचे डिस्प्ले हो जायेगी।



इस टूल के साथ आपको क्या मिलेगा-

- आईएसपी और संगठन का नाम
- IP का होस्ट नाम
- वह जिस देश में है
- क्षेत्र / राज्य
- शहर
- स्थान का अक्षांश और देशांतर
- उस क्षेत्र का क्षेत्र कोड
- उस IP पर चलने वाली कोई भी ज्ञात सेवा

2- Private IP Address

वैसे किसी specific device की private IP address को जानना इतना आसान नहीं होता है.

Windows में, आप अपने device की IP address का पता via Command Prompt कर सकते हैं, जिसके लिए आपको बस ipconfig command का ही इस्तमाल करना पड़ेगा.

Linux users को इसके लिए अपने system में एक terminal window को launch करना होता है और enter करें command hostname – I(जिसमें capital "i" का इस्तमाल होता है) ifconfig, या ip addr show.

वहीँ **macOS,** में आप command ifconfig का उपयोग कर सकते हैं आपकी local IP address को पाने के लिए.

iPhone, iPad, और iPod touch devices में आप private IP address को देख सकते हैं Wi-Fi Menu में Settings app के द्वारा. इसे देखने के लिए, आपको tap करना होगा small "i" button को जो की network जिससे आप connected हों उसके next में होता है.

Android Devices में आप अपना local IP address देखने के लिए ***Settings > Wi-Fi, या Settings > Wireless Controls > Wi-Fi settings*** का steps पालन करना होगा. आपको पर उस network के ऊपर tap करना होता है जिसपर आप होते हैं, जिससे आपको network की सभी information दिखाई पड़ जाती है जिसमें private IP address भी होता है.

CRIME SCENE, FIR AND CHARGESHEET

साइबर अपराध सीन प्रबंधन

अपराध **सीन** प्रबंधन पर, आईओ को चाहिए कि-

1. एक विशेषज्ञ के साथ एक उचित टीम का चयन करें।

2. टीम के प्रत्येक सदस्य को विशिष्ट जिम्मेदारी सौंपें।

3. कैमरा / वीडियो कैमरा के साथ जांच बॉक्स के साथ एक फोरेंसिक टूल किट रखें।

4. हार्ड वेयर (कंप्यूटर / प्रिंटर / मॉडेम और कंप्यूटर / लैपटॉप / और जुड़े अन्य उपकरणों) की भौतिक स्थिति को परिवर्तित न करें।

5. काम करने की स्थिति में तय किए गए सिस्टम की तस्वीरें / वीडियोग्राफी करें।

6. Crime scene का एक स्केच ड्रा करें और सभी हार्ड-वेयर और कनेक्टेड मीडिया को कनेक्टेड केबल स्थान के साथ दिखाएं।

7. Crime scene का समग्र नियंत्रण रखना ताकि कोई भी वर्तमान सिस्टम से डेटा को हटा / हटा नहीं सके।

8. विभिन्न उपकरणों के शिकायतकर्ता / मालिक को पहचानें और विवरण, उपयोगकर्ता नाम, सेवा प्रदाताओं के विवरण प्राप्त करें। आईओ को यह सुनिश्चित करना चाहिए कि ये व्यक्ति गवाहों की उपस्थिति में विभिन्न पासवर्ड संरक्षित / सुरक्षित जानकारी प्राप्त करने के लिए खोज और जब्ती टीम के साथ उपलब्ध हों।

9. ऑफ-साइट डेटा स्टोरेज, डेटा सेंटर और संगठन की आपदा वसूली नीतियों या बैक-अप योजनाओं आदि सहित सभी सुरक्षा प्रणालियों पर दी गई जानकारी इकट्ठा करें।

10. उन लोगों की सूची की पहचान करें जो नेटवर्क की पहचान कर सकते हैं। नेटवर्क का एक योजनाबद्ध आरेख साक्षात्कार के दौरान तैयार करने के लिए उपयोगी होगा।

पूर्व-जांच तकनीकी मूल्यांकन

पूर्व-जांच मूल्यांकन को सभी सही और प्रासंगिक जानकारी को प्राप्त कर शुरू किया जाना चाहिए जो आईओ को घटना / अपराध के बारे में पूर्ण जानकारी दे। पूर्व-जांच मूल्यांकन प्रश्नावली आईओ को प्रश्नों का एक सेट देता है, प्रत्येक आईओ को यह ध्यान रखना होगा कि अपराध / अपराध की स्थिति के आधार पर इस सूची को और विस्तारित किया जा सकता है।

सीन ऑफ ऑफेंस: साइबर कैफे

i) साइबर कैफे में मौजूद कंप्यूटर सिस्टम की संख्या की पहचान करें।

ii) इंटरनेट से जुड़े कंप्यूटर सिस्टम की संख्या की पहचान करना।

iii) नेटवर्क टोपोलॉजी और आर्किटेक्चर (क्लाइंट - सर्वर) के बारे में विवरण प्राप्त करें।

iv) सीसीटीवी / वेब कैमरा क्लिपिंग प्राप्त करें, यदि कोई हो।

v) क्या साइबर कैफे मालिक द्वारा किसी भी उपयोगकर्ता प्रबंधन सॉफ्टवेयर का उपयोग किया जाता है?

vi) प्रासंगिक अवधि के लिए इंटरनेट उपयोगकर्ताओं के लॉग रजिस्टर को प्राप्त करें।

vii) साइबर कैफे के मालिक द्वारा अपनाई गई स्टोरेज डिवाइस पॉलिसी के प्रारूपण की जाँच करें।

viii) साइबर कैफे के मालिक द्वारा किए गए हार्डवेयर प्रतिस्थापन की जाँच करें।

ix) साइबर कैफे प्रणालियों पर मीडिया के उपयोग को हटाने के बारे में नीति की जाँच करें।

अपराध का सीन: घर

i) कनेक्शन के प्रकार (वाई-फाई / ईथरनेट) की पहचान करें।

ii) इंटरनेट कनेक्शन के लिए कितने कंप्यूटर सिस्टम का उपयोग किया जाता है?

iii) प्रणाली का स्थान और सिस्टम तक पहुंच वाले व्यक्तियों का विवरण।

iv) उपयोगकर्ता द्वारा उपयोग / स्वामित्व वाली हटाने योग्य भंडारण मीडिया (बाहरी हार्ड डिस्क सहित) के बारे में विवरण प्राप्त करें।

v) नेटवर्क टोपोलॉजी और आर्किटेक्चर (क्लाइंट - सर्वर) के बारे में विवरण प्राप्त करें, यदि कोई हो।

vi) अन्य कंप्यूटर बाह्य उपकरणों (प्रिंटर / स्कैनर / मॉडेम, आदि) के बारे में विवरण प्राप्त करें।

अपराध का सीन: कॉर्पोरेट पर्यावरण

i) अपराध के लिए प्रश्नावली जिसमें कंप्यूटर को साधन / साधन या भंडार के रूप में उपयोग किया जाता है: यह प्रश्नावली जांच अधिकारी को उन मूलभूत जानकारी को इकट्ठा करने में मदद करती है जहां अपराध कंप्यूटर सिस्टम का उपयोग करके किया जाता है।

ii) कंप्यूटर सिस्टम को क्राइम करने के लिए प्रश्नावली: यह प्रश्नावली संबंधित कार्यालय को उन प्रासंगिक सूचनाओं को इकट्ठा करने में मदद करती है, जहां अपराध को लक्षित किया जाता है,

पूर्व-जांच मूल्यांकन के लिए उपर्युक्त प्रारूप IO को समग्रता में घटना को समझने में मदद करेगा। पूर्व-जांच मूल्यांकन के अंत में, IO निर्दिष्ट / अधिकृत व्यक्तियों के लिए संरक्षण नोटिस जारी करने में सक्षम होगा । इसी तरह, यह आईओ को अपेक्षित सबूत हासिल करने के लिए आवश्यक तकनीकी सहायता के प्रकार पर निर्णय लेने में सहायता देगा। इन सबसे ऊपर, जांच अधिकारी तय कर **सकेगा** कि जांच कैसे आगे बढ़नी चाहिए।

साइबर अपराधों की एफआईआर तैयार करना

पीड़ित, आरोपी, गवाहों, दस्तावेजी साक्ष्य और कालानुक्रमिक घटना में घटना के बारे में पूरी जानकारी के बारे में अधिक जानकारी रखने वाली एक प्राथमिकी। / O के लिए मामले को समझने और जांच करने के साथ-साथ साक्ष्य मूल्य के लिए महत्वपूर्ण है। एफआईआर में शामिल तथ्यों को प्राथमिक साक्ष्य माना जाता है। इसलिए पुलिस अधिकारियों को एक आदर्श एफआईआर दर्ज करने में पीड़ितों की मदद करने की आवश्यकता है।

1. पीड़ित और संदिग्ध व्यक्ति के बारे में जानकारी: पीड़ित और संदिग्ध व्यक्ति के बारे में विवरण को एक प्राथमिकी में शामिल किया जाना चाहिए

(i) घटना के बारे में पहली सूचना रिपोर्ट वर्णनात्मक होनी चाहिए,

(ii) दुर्घटनाओं को कालानुक्रम में लिखा जाना चाहिए,

(iii) घटना से संबंधित विभिन्न चीजों के बारे में सही विवरण का उल्लेख किया जाना चाहिए मोबाइल नंबर, ई-मेल पता, वेबसाइट का पता, एसएमएस / एमएमएस सॉफ्ट और हार्ड कॉपी, ऑडियो / सीडी / मेमोरी कार्ड, बैंक खातों में वीडियो क्लिपिंग, वेबसाइटों पर पोस्टिंग / सामग्री (ऑडियो / वीडियो / तस्वीरें) बातचीत / ईमेल की तिथि और समय, पृष्ठों के URL, व्यक्तियों और उनके सहयोगियों के बारे में अन्य जानकारी,

(iv) उचित कानूनों के उचित वर्गों को लागू करना।

साइबर अपराध की शिकायत दर्ज करने के लिए कदम

1. साइबर अपराध की शिकायत दर्ज करने का पहला कदम यह है कि वर्तमान में शहर के साइबर क्राइम सेल के पास लिखित शिकायत दर्ज हो।

आईटी अधिनियम के अनुसार, एक साइबर अपराध वैश्विक अधिकार क्षेत्र के दायरे में आता है। इसका मतलब यह है कि साइबर क्राइम की शिकायत भारत में किसी भी साइबर सेल में दर्ज की जा सकती है, चाहे वह मूल रूप से उस स्थान पर ही क्यों न हो।

वर्तमान में, भारत के अधिकांश शहरों में समर्पित साइबर क्राइम सेल है।

2. साइबर अपराध की शिकायत दर्ज करते समय, आपको मेल करने के लिए अपना नाम, संपर्क विवरण और पता प्रदान करना होगा। आपको शहर के साइबर अपराध सेल के प्रमुख को लिखित शिकायत को संबोधित करने की आवश्यकता है जहां आप साइबर अपराध की शिकायत दर्ज कर रहे हैं।

3. यदि आप ऑनलाइन उत्पीड़न के शिकार हैं, तो पुलिस स्टेशन में रिपोर्ट करने के लिए आपकी सहायता के लिए एक कानूनी वकील से संपर्क किया जा सकता है। इसके अतिरिक्त, आपको शिकायत के साथ कुछ दस्तावेज प्रदान करने के लिए कहा जा सकता है। हालाँकि, यह अपराध की प्रकृति पर निर्भर करेगा।

4. साइबर अपराध की प्राथमिकी दर्ज करें: यदि आपके पास भारत में किसी भी साइबर सेल तक पहुंच नहीं है, तो आप स्थानीय पुलिस स्टेशन में पहली सूचना रिपोर्ट (एफआईआर) दर्ज कर सकते हैं। यदि आपकी शिकायत वहाँ स्वीकार नहीं की जाती है, तो आप आयुक्त या शहर के न्यायिक मजिस्ट्रेट से संपर्क कर सकते हैं।

5. कुछ साइबर अपराध अपराध भारतीय दंड संहिता के तहत आते हैं। आप उन्हें रिपोर्ट करने के लिए निकटतम स्थानीय पुलिस स्टेशन में साइबर अपराध की प्राथमिकी दर्ज कर सकते हैं।

यह धारा **154** के तहत अनिवार्य है**,** दंड प्रक्रिया संहिता**,** प्रत्येक पुलिस अधिकारी के लिए अपराध की जानकारी के बावजूद **/** अपराध की शिकायत दर्ज करने के लिए**,** जिसमें अपराध किया गया था।

6. भारतीय दंड संहिता के अंतर्गत आने वाले अधिकांश साइबर अपराधों को संज्ञेय अपराधों के रूप में वर्गीकृत किया जाता है। एक संज्ञेय अपराध वह है जिसमें गिरफ्तारी या जांच के लिए वारंट की आवश्यकता नहीं होती है।

इस मामले में**,** एक पुलिस अधिकारी शिकायतकर्ता से शून्य प्राथमिकी दर्ज करने के लिए बाध्य है। उसके बाद उसे उस स्थान के अधिकार क्षेत्र में पुलिस स्टेशन में भेजना चाहिए**,** जहां अपराध किया गया था।

7. ज़ीरो एफआईआर उन मामलों के पीड़ितों को कुछ सांत्वना प्रदान करती है**,** जिन पर तुरंत ध्यान देने **/** जांच की आवश्यकता होती है क्योंकि यह पुलिस रिकॉर्ड पर अपराध को लागू करने में समय बर्बाद करने से बचता है।

साइबर अपराध मामलों की चार्जशीट तैयार करना:

डिजिटल / इलेक्ट्रॉनिक साक्ष्य साइबर अपराध जांच का मुख्य हिस्सा हैं।। / O को चार्जशीट में जांच के दौरान एकत्रित डिजिटल / इलेक्ट्रॉनिक साक्ष्य शामिल होना चाहिए।

डिजिटल साक्ष्य:

1. संदेश / अश्लील सामग्री / एमएमएस और वीडियो की स्क्रीन प्रिंट तस्वीरें, सॉफ्ट कॉपी और हार्ड कॉपी में भी।

2. संदिग्ध आईडी के स्क्रीन प्रिंट / खाता जैसे फेस बुक, ट्विटर अकाउंट मेल इनबॉक्स / व्हाट्सएप अकाउंट / वेब पेज, वेब पेजों का यूआरएल।

3. हार्ड डिस्क और मोबाइल फोन के मामले में साइबर फोरेंसिक टूल द्वारा उत्पन्न हैश मूल्य के साथ इमेजिंग और डेटा विश्लेषण रिपोर्ट।

4. सीडीआर / डाटा सॉफ्ट कॉपी, (केवल संदिग्ध तारीख के लिए), सीएएफ ।

5. सोशल साइट्स पेमेंट गेटवे, साइबर कैफे और अन्य वेबसाइटों से सॉफ्ट कॉपी में मिली जानकारी।

6. सॉफ्ट और हार्ड कॉपी में आईएसपी / एमएसपी से प्राप्त जानकारी।

7. नोटिस यू / एस 91 सीआरपीसी की सॉफ्ट और हार्ड प्रतियां। को आईएसपी / एमएसपी / सोशल साइट्स पर भेजा गया।

हार्ड कॉपी:

1. सभी डिजिटल साक्ष्यों की हार्ड कॉपी।

2. डिजिटल साक्ष्य संग्रह फॉर्म और chain of custody

3. सभी प्रदर्शनों के साथ एफएसएल विशेषज्ञ की राय।

4. हार्ड कॉपी में सभी पारंपरिक रिकॉर्ड जैसे मूल एफआईआर, गवाहों के बयान, जब्ती ज्ञापन, अपराध के दृश्य की रिपोर्ट, के रिकॉर्ड।

5. भारतीय साक्ष्य अधिनियम का प्रमाणपत्र u/s 65-B को चार्जशीट के साथ संलग्न करना अनिवार्य है, जो एमएसपी / बैंकों / आईएसपी / भुगतान गेट से मांगे गए थे।

6.न्यायालय में सीडी / डीवीडी में इलेक्ट्रॉनिक साक्ष्य प्रस्तुत किए जाने चाहिए।

चार्जशीट तैयार करने के लिए दिशा-निर्देश

1-जांच / एफआईआर दर्ज करने के दौरान शिकायतकर्ताओं द्वारा साझा की गई सभी प्रासंगिक जानकारी को चार्जशीट में शामिल किया जाना चाहिए।

2-कृपया सुनिश्चित करें कि एफआईआर में उल्लिखित अनुभाग अभी भी मामले के लिए लागू हैं या उचित ITAA 2008 और अन्य सहायक आईपीसी, विशेष और स्थानीय कानूनों सहित मामले से पहले अनुभागों को बदलने की सलाह दी जाती है। (ऐसे कई केसेज है जिनमे आई ओ ने आईटी एक्ट की गलत धाराओं के तहत चार्जशीट भरी)

3-सुनिश्चित करें कि chain of custody और DEC फॉर्म के साथ खोज और जब्ती प्रक्रिया चार्जशीट में शामिल है।

4-सुनिश्चित करें कि साइबर अपराध की प्रकृति और एफएसएल या फोरेंसिक परीक्षक से अनुरोधित आवश्यक जानकारी / विश्लेषण को चार्जशीट में ठीक से शामिल किया गया है।

5- क्राईम सीन तथा क्राईम में प्रयोग किये गये सिस्टम को पहचानने की प्रक्रिया से संबंधित पूरी जानकारी आई ओ द्वारा उपलब्ध कराई जानी चाहिये।

6-कृपया उन सभी तकनीकी व्यक्तियों को शामिल करें जिन्होंने मामले में गवाह के रूप में डिजिटल पहचान, उत्पादन और विश्लेषण किया।

7-कृपया निष्कर्ष के साथ अपराध को स्थापित करने के लिए कालक्रम में घटित घटनाओं को शामिल करें।

8-कृपया एक खाली सीडी-आर में जांच के दौरान एकत्र किए गए डिजिटल साक्ष्य स्टोर करें ।

9-कृपया एक सीडी में डिजिटल साक्ष्य की अलग सूची बनाएं।

10-जांच के दौरान जब्त सीडी और अन्य हार्डवेयर पर एफआईआर नंबर और चार्जशीट नंबर का उल्लेख करना न भूलें।

SEARCH AND SEIZURE OF DIGITAL DEVICES

हार्डवेयर / कंप्यूटर / लैपटॉप / मोबाइल फोन की जब्ती:

Chain of Custody यह प्रमाणित करने की प्रक्रिया है कि किसी साक्ष्य को किस तरह से इकट्ठा किया गया है, ट्रैक किया गया है और अदालत में पेश करने तक कैसे उसकी सुरक्षा की जाती है। हर बार जब भी सबसे अच्छा सबूत दिया जाता है, **Chain of Custody** फॉर्म को अद्यतन करने की आवश्यकता होती है, आपको यह बताना होगा कि यह क्या है , यह कहां से आया है और यह कहां गया है, और कोई अंतर नहीं हो सकता है। किसी भी कंप्यूटर फोरेंसिक जांच का महत्वपूर्ण हिस्सा उचित सबूत संग्रह और एकत्र किए गए सबूतों की **Chain of Custody** का उचित रखरखाव सुनिश्चित करना होता है (जैसे कंप्यूटर सिस्टम, हार्ड ड्राइव और बैकअप कॉपी)। आपको यह सुनिश्चित करने की आवश्यकता है कि आप जाँच के दौरान कौन, क्या, कब और कहाँ के प्रत्येक साक्ष्य या सामग्री को पहचान सकते हैं:

1. सबूतों को किसने संभाला? (आई / ओ और उनकी टीम का नाम)
2. सबूतों पर कौन सी प्रक्रियाएँ की गईं और क्या कब्जे में ली गईं? (जब्ती मेमो और अपराध के दृश्य का मेमो, अगर किसी भी उपकरण का उपयोग किया जाता है, जब्त हार्डवेयर और डिजिटल साक्ष्य का विवरण)
3. साक्ष्य कब एकत्र और / या किसी अन्य पार्टी को हस्तांतरित किया गया था? (पूरी जानकारी)
4. सबूत कहाँ एकत्र और संग्रहीत किए गए थे? (जब्ती और जब्त किए गए नामों के स्थान का वर्णन करें)

प्रक्रिया–

1. यदि जब्ती के समय चालू है, तो सिस्टम को स्विच ऑफ न करें।
2. गर्मी और पानी से दूर रखें।
3. विभिन्न कोणों से फोटो ग्राफ / वीडियो ग्राफ लें ।
4. कनेक्टिंग इलेक्ट्रिक केबल और चार्जर को जब्त करना न भूलें।
5. जब्त इलेक्ट्रॉनिक हार्ड वेयर का उपयोग न करें।
6. जब्त वस्तुओं से आवश्यक जानकारी प्राप्त करने के लिए उन्हें बिना किसी देरी के विशेषज्ञ के पास भेजें।
7. सुरक्षा के लिए उचित पैकिंग सामग्री का उपयोग करें।
8. हार्ड डिस्क / लैपटॉप / यूएसबी की जब्ती के दौरान राइट ब्लॉकिंग किट का उपयोग करके हैश वैल्यू लें।
9. कंप्यूटर / लैपटॉप की बड़ी जब्ती होने पर विशेषज्ञ की मदद लें।
10. जब्त वस्तु का पूर्ण विवरण लिखे।
11. मोबाइल फोन जब्ती में IMEI no लिखना न भूलें। किसी भी मोबाइल फोन का आईएमईआई नंबर प्राप्त करने के लिए टाइप करें - * # 06 #
12. जब्ती ज्ञापन स्वतंत्र गवाहों की उपस्थिति में तैयार किया जाना चाहिए और जिस व्यक्ति से संपत्ति जब्त की गई है, जब्ती ज्ञापन पर हस्ताक्षर आवश्यक है।
13. जब्ती के सामान्य सिद्धांत का पालन करें।
14. मेमो ऑफ एसओसी एंड डीईसी (डिजिटल एविडेंस कलेक्शन फॉर्म) फॉर्म में सभी जब्त की गई वस्तुओं को जमा करें।
15. उपयोगकर्ता / संदिग्ध व्यक्ति से पासवर्ड के बारे में पूछें।
16. मेमोरी स्टिक्स, कॉम्पैक्ट फ्लैश / यूएसबी, सीडी कैमरा, डायरी आदि जैसे अतिरिक्त भंडारण मीडिया को जब्त करना न भूलें।

17. जब्त की गई सामग्री को सावधानी से परिवहन करें।
18. तलाशी, जब्ती और पैकिंग के दौरान अभियुक्तों से सहायता न लें।
19. यदि इंटरनेट डेटा कार्ड (डोंगल) जब्त कर लिया गया है, तो सब्सक्राइबर आईएसपी कंपनी से जीपीआरएस सीडीआर लें।
20. CCTV फुटेज के विश्लेषण के मामले में संदिग्ध DVR (डिजिटल वीडियो रिकॉर्डर) प्रणाली को जब्त करना न भूलें।

मोबाइल फोन के बारे में जांच

मोबाइल फोन से साक्ष्य प्राप्त करने की प्रक्रिया:

(I) यदि उपकरण बंद है, तो चालू न करें।

(II) डिवाइस और स्क्रीन डिस्प्ले फोटोग्राफ ।

(III) डिवाइस के साथ सभी केबलों (बिजली की आपूर्ति सहित) को इकट्ठा करें।

(IV) अतिरिक्त संग्रहण मीडिया (मेमोरी कार्ड, मेमोरी स्टिक) को जब्त करें।

(V) जब्त मोबाइल फोन रखने के लिए फैराडे बैग का उपयोग करें।

(VI) सूखी और ठंडी जगह पर स्टोर करें।

FARADAY BAG

एक फैराडे एक बैग है, जहां एक सेल फोन रखा जाता है, ताकि यह कोई संकेत प्राप्त न कर सके। यह किसी भी परिवर्तन को रोकता है जो सिग्नल प्राप्त करके फोन में हो सकता है।

फैराडे बैग एक बहु-स्तरित (multi-layered) प्रवाहकीय जाल(conductive mesh) द्वारा निर्मित एक संलग्नक है, जिसे rip-stop नायलॉन (सामग्री जिसे पैराशूट बनाया जाता है), से लेपित किया जाता है, फिर उत्पाद को मजबूत और उद्देश्य के लिए फिट करने के लिए एक पॉलीयुरेथेन बाहरी त्वचा में कवर किया जाता है। ।

मोबाइल सीडीआर विश्लेषण:

हम विशेष मोबाइल नंबरों की सीडीआर से कई प्रकार की जानकारी प्राप्त कर सकते हैं।

(i) कॉल दिनांक, समय और अवधि,

(ii) उपयोगकर्ता का स्थान,

(iii) किस नंबर पर अधिकतम कॉल

(iv) बाहर जाने / आने वाले कॉल के अनुसार दिनांक और समय,

(v) उपयोगकर्ता का IMEI नंबर,

(vi) उपयोगकर्ता संख्या पर कितने IMEI नंबर का उपयोग किया जाता है,

(vii) विशेष तिथि और समय पर उपयोगकर्ता द्वारा कितनी एसएमएस / एमएमएस प्राप्त / भेजे जाते हैं,

(viii) टॉवर सीडीआर विश्लेषण (टॉवर डंप)

(ix) सेवा एसएमएस से जानकारी: बैंक खाते, क्रेडिट कार्ड, बीमा, क्लब के सदस्य, बैंक ऋण,

(x) वीओआइपी कॉल (जीपीआरएस) सीडीआर से आईपी पता,

(xi) प्रयुक्त परिवहन,

(xii) संदिग्ध द्वारा प्रयुक्त रूट,

(xiii) अन्य मोबाइल नग। IMEI खोज से,

(xiv) बिलिंग रिकॉर्ड।

मोबाइल सेवा प्रदाताओं से जानकारी

(I) संदिग्ध / पीड़ित मोबाइल नंबरों के मोबाइल सीडीआर और जीपीआरएस सीडीआर,

(II) सीएएफ ग्राहक अधिग्रहण प्रपत्र,

(III) टॉवर डंपिंग डेटा,

(IV) ऑनलाइन फंड ट्रांसफर / अन्य लेनदेन पर

(I) मेमोरी कार्ड का विवरण,

(II) एमएनपी मोबाइल नंबर पोर्टेबिलिटी,

(III) बिलिंग नाम और भुगतान गेटवे,

(IV) उपयोगकर्ता नाम (यदि उपयोगकर्ता सिम धारक के अलावा अन्य है)।

मोबाइल फोन से जानकारी:

(i) मॉडल ,

(ii) मोबाइल नंबर,

(iii) IMEI नंबर: (* # 06 # दबाकर),

(iv) मेमोरी कार्ड का विवरण,

(v) एसएमएस / एमएमएस,

(vi) वीडियो / तस्वीरें,

(vii) संपर्क सूची,

(viii) इनकमिंग / आउटगोइंग / मिस्ड कॉल के बारे में कॉल लॉग

(ix) नोट्स / डायरी से व्यक्तिगत जानकारी।

ANNEXURE-A

CHAIN OF CUSTODY FORM FOR SEIZED COMPUTER/ LAPTOP/ HD AND OTHER REMOVABLE DISKS

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE			
CRIME NUMBER …… DATE OF SEIZURE ……..			
NAME OF THE I.O …….. TIME …….			
P.F. NUMBER ……...			
TECHINAL INFORMATION			
MANUFACTURE	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY					
REASON/ACTION	**RECEIVED FROM**	**RECEIVED BY**	**DATE**	**TIME**	**REMARKS**

REASON/ACTION: IO SHALL ENSURE DOCUMENTATION OF THE TRANSFERRING THE SEIZED EVIDENCE TO OTHER CUSTODIANS IN CHRONOLOGICAL ORDER.

DIGITAL EVIDENCE COLLECTION FORM

DIGITAL EVIDENCE COLLECTION FORM			
CRIME NUMBER :		DATE :	
PS/CIRCLE/SDPO:		TIME:	
IO NAME		ITEM NUMBER:	
LOCATION		CUSTODIAN/SUSPECT NAME	

COMPUTER INFORMATION			
☐ LAPTOP	☐ DESKTOP	MANUFACTURER	
☐ HDD ONLY	☐ EXTERNAL HDD	MODEL NUMBER	
☐ OHERS		SERIAL NUMBER	
TIME ZONE		ASSET TAG	
BIOS DATE AND TIME		ACTUAL DATE AND TIME	

EVIDENCE DRIVE			
ACQUIRED BY		DATE OF ACQUISITION	
SIGNATURE OF I.O.		TIME OF ACQUISITION	

ACQUISITION INFORMATION			
☐ IDE	☐ SCSI	MANUFACTURER	
☐ SATA	☐ OTHER	MODEL NUMBER	
		SERIAL NUMBER	
		HDD SIZE	

COLLECTION DETAILS		DESTINATION DRIVE DETAILS	
SOFTWARE USED		MANUFACTURER	
VERSION		MODEL NUMBER	
WRITE PROTECT DEVICE USED		SERIAL NUMBER	
VERIFIED BY		HDD SIZE	
IMAGE FILE NAME			
NOTES			

ANNEXURE- B

REQUISITION LETTER TO FSL:

FORWARDING NOTE:

(IN ALL CASES WHERE EXAMINATION OF ANY MATERIAL IS REQUIRED AT THE LABORATORY, A COPY OF THIS FORM DULY FILLED IN SHOULD ACCOMPANY THE EXHIBITS.

CASE NO.	POLICE STATION
SECTION OF LAW	DISTT.
DATE- / /	STATE

I. NATURE OF CRIME

NATURE OF CRIME

……...

……..

BRIEF HISTORY

…….....

……..

ANY OTHER RELEVANT

DETAILS……

II. LIST OF EXHIBITS FOR EXAMINATION

SR. NO./ BARCODE	DESCRIPTION OF EXHIBITS	HOW, WHEN, AND BY WHOM FOUND	SOURCE OF EXHIBITS	REMARKS

III. NATURE OF EXAMINATION REQUIRED

SR. NO./ BARCODE	DESCRIPTION OF EXHIBITS	NATURE OF EXAMINATION REQUIRED	DATE OR ANY KEYWORD OR FILTER	REMARKS

I/O`S ARE ADVISED TO PAY ADDITIONAL ATTENTION TO THIS SECTION, AS THIS PLAYS A CRITICAL COMPONENT IN THE INVESTIGATION. APART FROM REQUESTING THE INFORMATION REQUIRED FOR INVESTIGATION LIKE FILES, DELETED INFORMATION, ETC., FROM THE DIGITAL EVIDENCE, LOT OF OTHER INFORMATION, WHICH CAN BE DEVELOPED AS SUPPORTING (SECONDARY) EVIDENCE IN THE INVESTIGATION LIKE LOGIN TIME, USERS LIST, VARIOUS APPLICATION INSTALLED, IP ADDRESS, PRINTERS CONNECTED, ETC.

I/O `S ARE SUGGESTED TO CONTACT THE FORENSIC LAB PROFESSIONAL TO UNDERSTAND WHAT KIND OF INFORMATION CAN BE RETRIEVED FROM THESE DIGITAL MEDIA WHICH CAN BE VITAL EVIDENCE.

SR. NO.	FULL NAME	OCCUPATION	SEX	DATE AND TIME OF ARREST	WHETHER BAILED, JC OR IN POLICE CUSTODY

SEAL	RANK AND SIGN OF THE I.O.
O/W NO. -…….	DATE- …….
FORWARDED TO THE DIRECTOR …….	
SPECIMEN SEAL/S IMPRESSION ON EXHIBITS OR PARCEL/S	SIGN AND DESIGNATION OF FORWARDING OFFICER

CERTIFICATE OF AUTHORITY

CERTIFIED THAT THE DIRECTOR…….HAS THE AUTHORITY TO EXAMINE THE EXHIBITS SENT TO HIM IN CONNECTION WITH CASE NO. …….. U/S …… POLICE STATION……DISTT.

DATE :	
PLASE :	SIGN AND DESIGNATION OF FORWARDING AUTHORITY

DIGITAL FORENSIC AND DIGITAL EVIDENCE

डिजिटल फोरेंसिक का परिचय

जैसे-जैसे दुनिया का डिजिटलीकरण होता जा रहा है, सार्वजनिक और निजी दोनों क्षेत्रों में व्यवसाय करने के लिए प्रौद्योगिकी पर निर्भरता बढ़ेगी। आज की सूचना युग में, संगठन उत्पादकता बढ़ाने, आंतरिक और बाह्य परिचालन लागत बचाने, डेटा सुरक्षा बढ़ाने और व्यावसायिक क्षमताओं का विस्तार करने के लिए प्रौद्योगिकी का उपयोग करते हैं। इन लाभों को प्राप्त करने के लिए मुख्य कुंजी सभी काम के पहलुओं के डिजिटल परिवर्तन को लागू करना है और विशेष रूप से डेटा को कागजी फ़ाइलों के प्रतिस्थापन के रूप में डिजिटल रूप से संग्रहीत करना है। व्यक्ति भी अपने दैनिक जीवन में प्रौद्योगिकी पर बहुत निर्भर हो गए हैं, लगभग सभी लोग किसी न किसी तरीके से प्रौद्योगिकी को अपने जीवन में शामिल कर रहे हैं।

डिजिटल युग में तेजी से बदलाव के साथ साइबर अपराधों में वृद्धि हुई थी। साइबर क्राइम 2021 तक सालाना 6 ट्रिलियन डॉलर तक पहुंच जाएगा। इसी अध्ययन में भविष्यवाणी की गई है कि 2022 तक 6 बिलियन इंटरनेट उपयोगकर्ता होंगे (8 बिलियन की अनुमानित विश्व जनसंख्या का 75%), फलस्वरूप, डिजिटल डिवाइस हर सेकंड में बड़ी मात्रा में डिजिटल डेटा उत्पन्न करेंगे।

डिजिटल फोरेंसिक किसी भी प्रकार के कंप्यूटिंग डिवाइस (जैसे कंप्यूटर, सर्वर, लैपटॉप, सेल फोन, टैबलेट, डिजिटल कैमरा, नेटवर्किंग डिवाइस या किसी भी प्रकार का डेटा स्टोरेज डिवाइस) का उपयोग करके किए गए अपराधों की जांच करने की प्रक्रिया है। डिजिटल फोरेंसिक के अंतर्गत रैंसमवेयर, फ़िशिंग, डिनाईल ऑफ सर्विस (DoS) हमलों, डेटा ब्रीच और किसी भी प्रकार के साइबर हमले से उत्पन्न होने वाली समस्याओं की जांच भी की जाती है। डिजिटल फोरेंसिक जांच का अंतिम लक्ष्य डिजिटल साक्ष्य को संरक्षित करना, पहचान करना, हासिल करना और दस्तावेज को अदालत में इस्तेमाल किया जाना है।

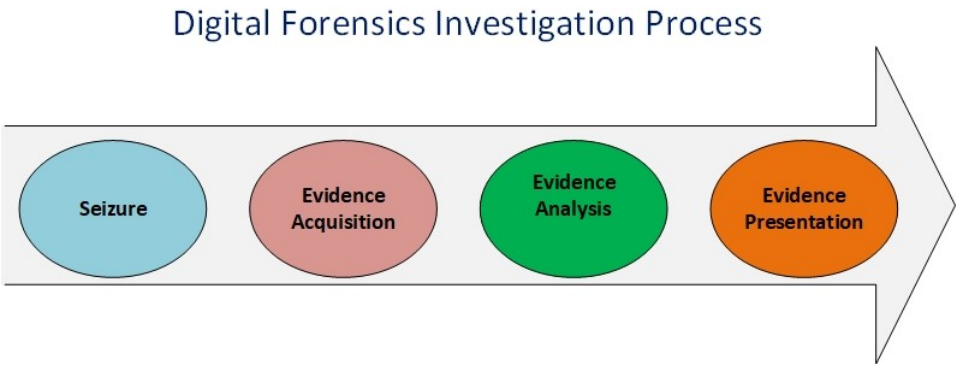
इस परिभाषा के तहत, डिजिटल फोरेंसिक का उपयोग किसी भी अपराध की जांच करने के लिए किया जाता है, जिसमें इलेक्ट्रॉनिक उपकरणों का उपयोग करना शामिल है, चाहे इन उपकरणों का उपयोग अपराध करने के लिए किया गया हो या अपराध के लक्ष्य के रूप में। आधुनिक फोरेंसिक क्षमता होने के कारण आधुनिक संगठनों के लिए आंतरिक नीति के उल्लंघन और उनके कम्प्यूटरीकृत सिस्टम के खिलाफ बाहरी हमलों की जांच करना बहुत महत्वपूर्ण हो जाता है, उदाहरण के लिए, बड़े निगमों में पहले से ही ऐसी क्षमता है जो कई सरकारी पुलिस विभागों की क्षमता से अधिक है।

डिजिटल फोरेंसिक के उद्देश्य :-

1-यह कंप्यूटर और संबंधित सामग्रियों को इस तरह से पुनर्प्राप्त, विश्लेषण और संरक्षित करने में मदद करता है कि यह जांच एजेंसी को उन्हें अदालत में सबूत के रूप में पेश करने में मदद करता है।
2-यह अपराध के पीछे के मकसद और मुख्य अपराधी की पहचान को अंजाम देने में मदद करता है।
3-अपराध स्थल पर डिजाइनिंग प्रक्रियाएं आपको यह सुनिश्चित करने में मदद करती हैं कि प्राप्त डिजिटल सबूत दूषित नहीं हैं।
4-डेटा अधिग्रहण: सबूत निकालने और उन्हें मान्य करने के लिए डिजिटल मीडिया से हटाए गए फ़ाइलों और हटाए गए विभाजन को पुनर्प्राप्त करना।
5-आपको सबूतों को जल्दी से पहचानने में मदद करता है, और आपको पीड़ित पर दुर्भावनापूर्ण गतिविधि के संभावित प्रभाव का अनुमान लगाने में भी मदद करता है
6-एक कंप्यूटर फोरेंसिक रिपोर्ट का उत्पादन जो जांच प्रक्रिया पर एक पूरी रिपोर्ट प्रदान करता है।
7-Chain of Custody का पालन करके साक्ष्य को संरक्षित करना।

डिजिटल फोरेंसिक प्रक्रिया

डिजिटल फोरेंसिक जांच के संचालन के लिए कई तरीके या सुझाई गई प्रक्रियाएं हैं, जिनमे निम्न 4 चरण मुख्य रूप से अपनाये जाते है–



Seizure (सीजर)

इस चरण में, संदिग्ध डिजिटल डिवाइस को जब्त कर लिया जाता है और ठीक से पैक करके डिजिटल फोरेंसिक लैब में ले जाया जाता है। इसके लिये एक अन्वेषक के पास अदालत से एक आधिकारिक खोज वारंट होना चाहिए और उसे संदिग्ध उपकरण को जब्त करने की उचित अनुमति होनी चाहिए।

डिजिटल डिवाइस किसी भी प्रकार का कंप्यूटिंग डिवाइस हो सकता है जैसे कि डेस्कटॉप कंप्यूटर, सर्वर, लैपटॉप, टैबलेट, स्मार्टफोन, एक्सटर्नल हार्ड ड्राइव, यूएसबी स्टिक या बैकअप मीडिया, इंटरनेट ऑफ थिंग्स (IoT) डिवाइस।

अपराध स्थल पर पहुंचने पर, यदि संदिग्ध डिवाइस अभी भी चल रहा था, तो डिवाइस को बंद करने से पहले अस्थिर मेमोरी को पहले (यदि संभव हो) प्राप्त किया जाना चाहिए। volatile मेमोरी में वर्तमान जांच के लिए महत्वपूर्ण जानकारी हो सकती है, जैसे पासवर्ड, आईएम चैट लॉग, इंटरनेट ब्राउज़िंग इतिहास, रनिंग प्रोग्राम और क्लिपबोर्ड सामग्री।

कुछ मामलों में, क्षेत्राधिकार संबंधी चुनौतियां उत्पन्न हो सकती हैं और फोरेंसिक जांचकर्ताओं को संदिग्ध डिजिटल उपकरणों को जब्त करने से रोक सकती हैं। उदाहरण के लिए, यदि अपराध इंटरनेट के माध्यम से किया गया था और संदिग्ध मशीन या सर्वर दूसरे देश में स्थित था, तो ऐसे मामले में सबूत कैसे हासिल किए जा सकते हैं? अंतर्राष्ट्रीय खोज वारंट का होना कठिन और समय लेने वाला है और सभी मामलों में लागू नहीं हो सकता है।

Evidence Acquisition साक्ष्य प्राप्ति

इस चरण में, एक पेशेवर कंप्यूटर फोरेंसिक तकनीशियन द्वारा संदिग्ध डिवाइस हार्ड ड्राइव -और RAM की डुप्लिकेट कॉपी बनवाई जायेगी (जिसे बिट-टू-बिट छवि भी कहा जाता है)। एक से अधिक डुप्लिकेट कॉपी रखना बेहतर होगा क्योंकि प्रयोगशाला में इन प्रतियों पर जांच की जाएगी ताकि मूल कॉपी में कोई समस्या न हो।

फोरेंसिक जांचकर्ता आमतौर पर प्रक्रियाओं के एक मानक सेट का पालन करते हैं: यह सुनिश्चित करने के लिए कि यह गलती से दूषित नहीं हो, डिवाइस को भौतिक रूप से अलग करने के बाद, जांचकर्ता डिवाइस के स्टोरेज

मीडिया की डिजिटल कॉपी बनाते हैं। एक बार मूल मीडिया की प्रतिलिपि बना लेने के बाद, यह अपनी प्राचीन स्थिति को बनाए रखने के लिए सुरक्षित है। सारी जांच डिजिटल कॉपी पर की जाती है।

Evidence Analysis साक्ष्य विश्लेषण

इस चरण में, अधिग्रहित फोरेंसिक छवि का विश्लेषण विभिन्न उपकरणों और तकनीकों का उपयोग करके किया जाता है ताकि उपयोगी लीड फॉर्म को प्राप्त किया जा सके जैसे: हटाई गई फ़ाइलों और ईमेलों को पुनर्प्राप्त करना, छिपे हुए डेटा की खोज करना, चैट और वेब ब्राउज़र इतिहास को पुनः प्राप्त करना। फोरेंसिक छवि का विश्लेषण करने के लिए उपयोग किए जाने वाले फोरेंसिक उपकरण को अदालत द्वारा स्वीकार किया जाना चाहिए। कुछ लोकप्रिय कोर्ट द्वारा स्वीकार किए गए टूल में निम्नलिखित शामिल हैं:

EnCase (https://www.guidancesoftware.com/encase-forensic), Sleuth Kit (https://www.sleuthkit.org/autopsy), AccessData (https://accessdata.com) RAM मेमोरी को कैप्चर करने के लिए (volatilityfoundation.org)

Evidence Presentation साक्ष्य प्रस्तुति

अंतिम चरण में, फोरेंसिक जांचकर्ता एक व्यापक रिपोर्ट तैयार करेगा जिसमें उसके निष्कर्षों का विवरण होगा। रिपोर्ट लिखने के लिए इस्तेमाल की जाने वाली भाषा को गैर-तकनीकी लोगों जैसे कि वकीलों, न्यायाधीशों द्वारा अच्छी तरह से समझा जाना चाहिए।

जांचकर्ता कॉपी की जांच करने के लिए कई तरह की तकनीकों और फोरेंसिक एप्लिकेशन का उपयोग करते हैं, छिपे हुए फ़ोल्डरों की खोज करते हैं और हटाए गए, एन्क्रिप्ट किए गए या क्षतिग्रस्त फ़ाइलों की प्रतियों को खोजते हैं। डिजिटल कॉपी पर पाए जाने वाले किसी भी साक्ष्य को सावधानीपूर्वक "खोज रिपोर्ट" में प्रलेखित किया जाता है और कानूनी कार्यवाही की तैयारी में मूल के साथ सत्यापित किया जाता है।

फोरेंसिक पद्धति

इंटरनेशनल एसोसिएशन ऑफ कंप्यूटर इन्वेस्टिगेटिव स्पेशलिस्ट्स (IACIS) ने एक फोरेंसिक कार्यप्रणाली विकसित की है जिसे निम्नानुसार संक्षेप में प्रस्तुत किया जा सकता है:

1- Crime scene की रक्षा करना, कंप्यूटर के लिए बिजली बंद करना और हार्डवेयर का दस्तावेजीकरण करना और कंप्यूटर सिस्टम को सुरक्षित स्थान पर पहुंचाना

2- डिजिटल मीडिया के बिट स्ट्रीम बैकअप, सभी भंडारण उपकरणों पर डेटा को प्रमाणित करने और सिस्टम की तारीख और समय का दस्तावेजीकरण करने के लिए हैश एल्गोरिदम का उपयोग करना

3- कीवर्ड खोजें और फ़ाइल प्रबंधन की जाँच करें

4- कार्यक्रम की कार्यक्षमता, दस्तावेज़ निष्कर्षों / परिणामों का मूल्यांकन करें और सॉफ़्टवेयर की प्रतियां बनाए रखें।

Digital Forensic Tools

फोरेंसिक टूल का मुख्य उद्देश्य डिजिटल साक्ष्य निकालना है जो अदालत में स्वीकार्य हो सकता है। इलेक्ट्रॉनिक साक्ष्य साइबर अपराध में महत्वपूर्ण भूमिका निभा रहे हैं। डिजिटल मीडिया में data को खोजने के लिए कंप्यूटर फोरेंसिक टूल का उपयोग किया जाता है।

The best computer forensics tools

Digital evidence can exist on a number of different platforms and in many different forms. Forensic investigation often includes analysis of files, emails, network activity and other potential artifacts and sources of clues to the scope, impact and attribution of an incident.

Due to the wide variety of potential data sources, digital forensics tools often have different specialties. This list outlines some of the most common and widely used tools for accomplishing different parts of a computer forensics investigation.

1. Disk analysis: Autopsy/the Sleuth Kit

Autopsy and the Sleuth Kit are likely the most well-known forensics toolkits in existence. The Sleuth Kit is a command-line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI-based system that uses The Sleuth Kit behind the scenes.

The tools are designed with a modular and plug-in architecture that makes it possible for users to easily incorporate additional functionality. Both tools are free and open-source, but commercial support and training are available as well.

2. Image creation: FTK imager

Autopsy and The Sleuth Kit are designed to examine disk images of hard drives, smart phones and so on. The benefit of analyzing an image (rather than a live drive) is that the use of an image allows the investigator to prove that they have not made any modifications to the drive that could affect the forensic results.

Autopsy does not have image creation functionality, so another tool needs to be used. While the majority of the AccessData Forensics Toolkit items are paid tools, its FTK Imager is a free product. This can be used to create disk images that can then be analyzed using Autopsy/The Sleuth Kit.

3. Memory forensics: volatility

Tools like The Sleuth Kit focus on the hard drive, but this is not the only place where forensic data and artifacts can be stored on a machine. Important forensic information can be stored in RAM, and this volatile memory must be collected quickly and carefully to be forensically valid and useful.

Volatility is the most well-known and popular tool for analysis of volatile memory. Like The Sleuth Kit, Volatility is free, open-source and supports third-party plugins. In fact, the Volatility Foundation holds an annual contest for users to develop the most useful and innovative extension to the framework.

4. Windows registry analysis: Registry recon

The windows registry acts as a database of configuration information for the Windows OS and the applications running on it. These applications can store a variety of different data in the registry, and the registry is one of the common locations where malware deploys persistence mechanisms.

It is possible to open and view the Windows registry via the built-in Windows application regedit, and registry analysis is built into some forensics platforms. However, specialized tools like Registry Recon are available as well. Registry Recon is a commercial tool that is designed to rebuild Windows

registries from a forensic image and includes the ability to rebuild deleted parts of the registry based upon analysis of unallocated memory space.

5. Mobile forensics: Cellebrite UFED

Mobile adoption is constantly growing, and many organizations allow employees to use these devices at work either via BYOD programs or corporate-owned devices. Additionally, these devices are a growing target of cyberattacks, such as phishing, making them a likely source of valuable forensic information.

With the growing importance of mobile forensics, a mobile-focused forensics tool might be a useful acquisition. Cellebrite UFED is widely regarded as the best commercial tool for mobile forensics. It supports a number of different platforms (not just mobile devices) and boasts exclusive methods and tools for mobile device analysis.

6. Network analysis: Wireshark

Many forensics tools focus on the endpoint, but this is not the only source of useful data in a forensics investigation. Most cyberattacks occur over the network, and analysis of network traffic captures can help with the identification of malware and provide access to data that may have already been deleted and overwritten on the endpoint.

For network traffic analysis, Wireshark is the most popular and widely-used tool. Wireshark is free and open-source, offers dissectors for many different types of network traffic, has a clear and easy-to-use GUI for traffic analysis and includes a wide range of functionality under the hood. It supports live traffic capture or can ingest network capture files for analysis.

7. Linux distributions: CAINE

Many of the tools presented here (and many other digital forensics tools besides them) are free and open-source. While this makes them easy to acquire, installation and configuration can be complex. To simplify this process, a number of different Linux digital forensics distributions are available as virtual machines. These VMs include a number of tools pre-installed and preconfigured.

The Computer Aided Investigative Environment (CAINE) is one example of such a tool. This Linux distribution includes many of the most widely used computer forensics tools and may include third-party plugins for tools like Autopsy.

These seven tools don't even scratch the surface of the tools available for digital forensics. Offerings range from free and open-source scripts designed to accomplish a single task to massive, commercial forensics platforms.

Due to the wide range of potential tools, a good starting point is trying out a Linux forensics distribution like CAINE. This provides access to a range of free tools without requiring any purchases or configuration.

डिजिटल साक्ष्य (DIGITAL EVIDENCE)

"इलेक्ट्रॉनिक साक्ष्य" की अवधारणा सूचना प्रौद्योगिकी अधिनियम, 2000 ("आईटी अधिनियम") और साक्ष्य अधिनियम, 1872 ("साक्ष्य अधिनियम") और भारतीय दंड संहिता, 1860 ("आईपीसी") में संबंधित संशोधनों के माध्यम से पेश की गई है। आईटी अधिनियम और इसका संशोधन इलेक्ट्रॉनिक व्यापार पर संयुक्त राष्ट्र आयोग (अंतर्राष्ट्रीय व्यापार कानून ("UNCITRAL") मॉडल कानून पर आधारित हैं। आईटी अधिनियम की धारा 2 (1) (टी) के अनुसार, "इलेक्ट्रॉनिक रिकॉर्ड" शब्द का अर्थ डेटा, stored रिकॉर्ड या डेटा generated छवि या ध्वनि , इलेक्ट्रॉनिक रूप में या माइक्रो-फिल्म या कंप्यूटर-जनित माइक्रो फिश में प्राप्त या भेजा जाता है। आईटी अधिनियम की धारा 4 स्पष्ट रूप से सामान्य कागज-आधारित अभिलेखों के स्थान पर इलेक्ट्रॉनिक अभिलेखों की वैधता और उपयोग को मान्यता देती है।

आईटी अधिनियम की धारा 92 के आधार पर साक्ष्य अधिनियम में संशोधन किया गया और "इलेक्ट्रॉनिक रिकॉर्ड" को शामिल करने के लिए "सबूत" शब्द में संशोधन किया गया, जिससे डिजिटल साक्ष्य को स्वीकार करने की अनुमति मिली। इलेक्ट्रॉनिक साक्ष्य के लिए दी गई कानूनी मान्यता से पहले, साक्ष्य 63 और 65 के साक्ष्य अधिनियम ने इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता के लिए शर्तों के साथ प्रमुखता से पेश किया और प्रदान किया। इन प्रावधानों के अनुसार, साइबर फोरेंसिक को लागू करके विभिन्न माध्यमों से एकत्र किए गए इलेक्ट्रॉनिक साक्ष्य को "दस्तावेज़" माना जाता था और मुद्रित प्रतिकृतियों को द्वितीयक साक्ष्य माना जाता था, जिसके लिए एक सक्षम हस्ताक्षरकर्ता से प्रामाणिकता के प्रमाणीकरण की आवश्यकता होती थी।

डिजिटल साक्ष्य या इलेक्ट्रॉनिक साक्ष्य डिजिटल रूप में संग्रहीत या प्रेषित की जाने वाली कोई भी संभावित जानकारी है जिसे एक पक्ष किसी अदालत के मुकदमे में इस्तेमाल कर सकता है। डिजिटल साक्ष्य स्वीकार करने से पहले एक अदालत यह निर्धारित करेगी कि क्या साक्ष्य प्रासंगिक है, क्या यह प्रामाणिक है, यदि यह सुनवाई योग्य है और क्या एक प्रति स्वीकार्य है या मूल की आवश्यकता है।

पिछले कुछ दशकों में डिजिटल साक्ष्यों का उपयोग बढ़ा है क्योंकि अदालतों ने ई-मेल, डिजिटल फोटोग्राफ, एटीएम लेनदेन लॉग, वर्ड प्रोसेसिंग दस्तावेज, इंस्टेंट मैसेज हिस्ट्रीज़, अकाउंटिंग प्रोग्राम्स, स्प्रेडशीट, इंटरनेट ब्राउज़र हिस्टरीज़ से बचाई गई फाइलों, डेटाबेस, कंप्यूटर मेमोरी की सामग्री, कंप्यूटर बैकअप, कंप्यूटर प्रिंटआउट, ग्लोबल पोजिशनिंग सिस्टम के उपयोग की अनुमति दी है।

डिजिटल सबूत अधिक अस्थिर, नष्ट करने के लिए और अधिक कठिन, आसानी से संशोधित, आसानी से नकल, संभवतः अधिक अभिव्यंजक, और अधिक आसानी से उपलब्ध हो जाता है। दिसंबर 2006 में, इलेक्ट्रानिक संग्रहित साक्ष्य के संरक्षण और प्रकटीकरण की आवश्यकता के लिए प्रक्रिया के नए सख्त नियम बनाए गए। डिजिटल साक्ष्य के कारण इसकी प्रामाणिकता के लिए अक्सर हमला किया जाता है, जिसके साथ इसे संशोधित किया जा सकता है, हालांकि अदालतें इस तर्क को छेड़छाड़ के सबूत के बिना अस्वीकार करने लगी हैं।

किसी भी डिजिटल फोरेंसिक जांच का मुख्य कार्य न्यायालय में उपयोग किए जाने वाले डिजिटल सबूतों का अधिग्रहण, संरक्षण, जांच और प्रस्तुत करना है।

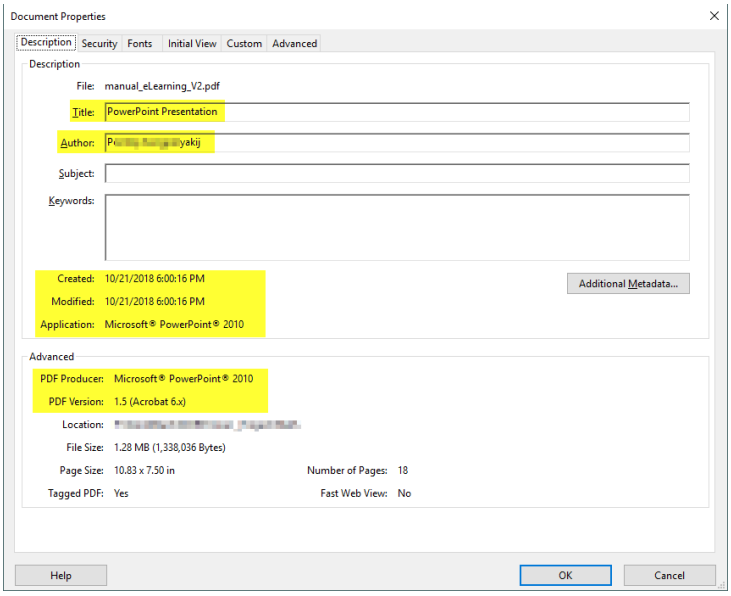
डिजिटल साक्ष्य (जिसे इलेक्ट्रॉनिक साक्ष्य के रूप में भी जाना जाता है) किसी भी जानकारी को डिजिटल प्रारूप में संग्रहीत या प्रेषित किया जाता है, इसमें कंप्यूटर, लैपटॉप, सेल फोन, टैबलेट, पीडीए हार्ड ड्राइव और विभिन्न स्टोरेज डिवाइस मीडिया जैसे यूएसबी अंगूठे का उपयोग करके संग्रहीत सभी डेटा शामिल हैं। ड्राइव, एसडी कार्ड, बाहरी हार्ड ड्राइव, सीडी / डीवीडी। कंप्यूटर नेटवर्क के माध्यम से प्रेषित डेटा को ऑपरेटिंग सिस्टम और डेटाबेस लॉग के अलावा डिजिटल सबूत का एक हिस्सा भी माना जाता है।

डिजिटल साक्ष्य को फॉरेंसिक साउंड तरीके से हासिल किया जाना चाहिए। "फॉरेंसिकली साउंड" एक शब्द है जिसका उपयोग डिजिटल फोरेंसिक परीक्षकों द्वारा अदालत में स्वीकार्य होने के लिए अपनी अखंडता को संरक्षित करते हुए डिजिटल साक्ष्य प्राप्त करने की प्रक्रिया का वर्णन करने के लिए किया जाता है।

डिजिटल साक्ष्य में निम्नलिखित शामिल हैं **-**

1. ईमेल संदेश और अनुलग्नक
2. दोनों ऑनलाइन खातों (क्लाउड स्टोरेज, सोशल मीडिया) और स्थानीय कंप्यूटर खातों के लिए उपयोगकर्ता खाता जानकारी (उपयोगकर्ता नाम, पासवर्ड, व्यक्तिगत चित्र आदि)।
3. डिजिटल फोटो, ऑडियो और वीडियो
4. आईएम वार्तालाप इतिहास
5. वेब ब्राउज़िंग इतिहास
6. लेखांकन कार्यक्रमों द्वारा उत्पन्न फाइलें
7. सभी प्रकार की इलेक्ट्रॉनिक फाइलें (MS Office फाइलें, डेटाबेस, स्प्रेडशीट, बुकमार्क··· आदि)।
8. अस्थिर मेमोरी में डेटा (RAM)
9. रजिस्ट्री जानकारी (विंडोज आधारित प्रणालियों में)
10. कंप्यूटर बैकअप
11. नेटवर्किंग डिवाइस रिकॉर्ड (राउटर, स्विच, प्रॉक्सी सर्वर, फ़ायरवॉल)
12. प्रिंटर स्पूलर फाइलें
13. एटीएम लेनदेन लॉग
14. फैक्स और कॉपियर मशीनें लॉग करती हैं
15. इलेक्ट्रॉनिक दरवाजा लॉग दिखता है
16. GPS ट्रैक लॉग्स
17. घरेलू उपकरणों (स्मार्ट टीवी, स्मार्ट रेफ्रिजरेटर) से निकाला गया डिजिटल डेटा
18. निगरानी वीडियो रिकॉर्डिंग
19. एन्क्रिप्टेड और छिपी हुई फाइलें
20. और डिजिटल प्रारूप में संग्रहीत कोई भी डेटा और सबूत के रूप में कानून की अदालत में इस्तेमाल किया जा सकता है।

हमें ध्यान देना चाहिए कि अधिकांश डिजिटल फ़ाइल प्रकारों में मेटाडेटा जुड़ा हुआ है, उदाहरण के लिए, मेटाडेटा डेटा के बारे में डेटा है, कुछ स्वचालित रूप से एप्लिकेशन द्वारा बनाई गई हैं (जैसे फ़ाइल निर्माण और परिवर्तन तिथि / समय, एप्लिकेशन संस्करण जानकारी) और अन्य को उपयोगकर्ता द्वारा सेट किया जा सकता है (जैसे फ़ाइल का लेखक का नाम, टिप्पणी और ईमेल पता)।



पीडीएफ फाइल मेटाडेटा

इलेक्ट्रॉनिक रिकॉर्ड की अनुकूलता

साक्ष्य अधिनियम की धारा 65 ए यह प्रदान करती है कि इलेक्ट्रॉनिक रिकॉर्ड की सामग्री साक्ष्य अधिनियम की धारा 65 बी के प्रावधानों के अनुसार साबित हो सकती है। इस प्रकार, इलेक्ट्रॉनिक रिकॉर्ड के माध्यम से किसी भी दस्तावेजी सबूत को साक्ष्य अधिनियम की धारा 65 बी के तहत निर्धारित प्रक्रिया के अनुसार ही साबित किया जा सकता है। एविडेंस एक्ट की धारा 65 बी इस बात को स्पष्ट करती है कि, कोई भी जानकारी इलेक्ट्रॉनिक रिकॉर्ड में निहित है, चाहे वह किसी कागज पर छपे दस्तावेज या संचार की सामग्री हो, या ऑप्टिकल या मैग्नेटिक मीडिया में कॉपी या रिकॉर्ड की गई हो। कंप्यूटर द्वारा निर्मित, इसे एक दस्तावेज माना जाता है और मूल उत्पादन के सबूत के बिना प्रमाण में स्वीकार्य है, जो साक्ष्य अधिनियम की धारा 65 बी (2) - (5) में निर्धारित शर्तों की संतुष्टि के अधीन है।

तकनीकी स्थिति और गैर-तकनीकी आधार

साक्ष्य अधिनियम की धारा 65 बी इलेक्ट्रॉनिक सबूतों की स्वीकार्यता के लिए तकनीकी स्थितियों और गैर-तकनीकी दोनों आधारों के लिए प्रदान करती है। साक्ष्य अधिनियम की धारा 65 बी की उप-धारा (2) उन तकनीकी परिस्थितियों को सूचीबद्ध करती है जिन पर एक मूल इलेक्ट्रॉनिक रिकॉर्ड की डुप्लीकेट कॉपी (प्रिंट-आउट सहित) का उपयोग किया जा सकता है। ये:

a) इलेक्ट्रॉनिक रिकॉर्ड के निर्माण के समय, इसका उत्पादन करने वाला कंप्यूटर नियमित उपयोग में रहा हो

बी) इलेक्ट्रॉनिक रिकॉर्ड में निहित जानकारी नियमित और सामान्य रूप से कंप्यूटर में फीड की जाती रहनी चाहिए

ग) कंप्यूटर ठीक से काम कर रहा था; तथा

डी) डुप्लिकेट कॉपी मूल इलेक्ट्रॉनिक रिकॉर्ड का ही प्रतिरूप होना चाहिए।

जैसा कि अनुमान लगाया जा सकता है उपरोक्त शर्तें डेटा की सत्यता से संबंधित हैं। शर्तों का दो गुना प्रभाव है क्योंकि वे i) यह सुनिश्चित करते हैं कि डेटा का कोई अनधिकृत उपयोग नहीं हुआ है; (ii) डिवाइस ठीक से काम कर रहा था, जिससे पुन: प्रस्तुत डेटा की सटीकता और वास्तविकता सुनिश्चित होती है।

प्रामाणिक होने का प्रमाण पत्र

साक्ष्य अधिनियम की धारा 65 बी (4) गैर तकनीकी परिस्थितियों के लिए प्रामाणिकता प्रमाण पत्र की आवश्यकता के लिए प्रदान करती है। प्रमाण पत्र का उद्देश्य साक्ष्य अधिनियम की धारा 65B की पूर्ववर्ती उपधारा (2) द्वारा निर्धारित शर्तों को पूरा करना है। प्रमाण पत्र को उस व्यक्ति द्वारा निष्पादित / हस्ताक्षरित किया जाना है जो उस उपकरण के संबंध में एक जिम्मेदार पद पर है जिसके माध्यम से डेटा का उत्पादन किया गया है। प्रमाण पत्र में विवरण सहित इलेक्ट्रॉनिक रिकॉर्ड की पहचान करनी चाहिए, जिस तरीके से इसका उत्पादन किया गया था और इलेक्ट्रॉनिक रिकॉर्ड के उत्पादन में शामिल किसी भी उपकरण के ऐसे विवरण दें जो इलेक्ट्रॉनिक रिकॉर्ड के उत्पादन के लिए उपयुक्त हो। प्रमाण पत्र के पीछे पूरा विचार स्रोत की अखंडता और डेटा की प्रामाणिकता सुनिश्चित करने के लिए भी है, ताकि अदालत उस पर निर्भरता रखने में सक्षम हो सके। यह महत्वपूर्ण है क्योंकि इलेक्ट्रॉनिक डेटा में छेड़छाड़ और परिवर्तन का खतरा अधिक है।

प्रासंगिकता, वास्तविकता, इलेक्ट्रॉनिक रिकॉर्ड की सत्यता और विश्वसनीयता

जबकि इलेक्ट्रॉनिक रिकॉर्ड की प्रासंगिकता प्रत्येक मामले के तथ्यों और परिस्थितियों के लिए विशिष्ट है, डिजिटल साक्ष्य की सत्यता और विश्वसनीयता सबसे बड़ी चुनौतियों में से एक है जो अदालतों को इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता पर भरोसा करते हुए निपटना है। इसलिए, यह महत्वपूर्ण हो जाता है कि न्यायालय यह सुनिश्चित करें कि रिकॉर्ड इकट्ठा करते समय रिकॉर्ड में बिना हेरफेर, परिवर्तन या क्षतिग्रस्त करें न्यायालय में प्रस्तुत किया गया है।

साक्ष्य अधिनियम के तहत अनुमान

साक्ष्य अधिनियम भी इलेक्ट्रॉनिक रिकॉर्ड के उपयोग को सुविधाजनक बनाने के लिए कुछ अनुमानों के लिए प्रदान करता है। साक्ष्य अधिनियम की धारा 85 ए के मद्देनजर, अदालत यह मान लेगी कि हर इलेक्ट्रॉनिक रिकॉर्ड का एक अनुबंध (पक्षों के इलेक्ट्रॉनिक हस्ताक्षर युक्त) होने के कारण पार्टियों के इलेक्ट्रॉनिक हस्ताक्षर के साथ **निष्कर्ष निकाला गया था। इसी प्रकार, साक्ष्य अधिनियम की धारा 85B न्यायालयों को यह मानने की अनुमति देती है कि सुरक्षित इलेक्ट्रॉनिक रिकॉर्ड को उस समय के विशिष्ट बिंदु से परिवर्तित नहीं किया गया है जो सुरक्षित स्थिति से संबंधित है, जब तक कि इसके विपरीत साबित न हो जाए। इसके अलावा, साक्ष्य अधिनियम की धारा 85C इलेक्ट्रॉनिक हस्ताक्षर प्रमाण पत्र में निहित जानकारी की सटीकता के रूप में अनुमान के लिए प्रदान करता है, जबकि साक्ष्य अधिनियम की धारा 81A इलेक्ट्रॉनिक रूपों में राजपत्र के संबंध में इस तरह के अनुमान के लिए प्रदान करता है।**

न्यायिक कार्यवाहियों में इलेक्ट्रॉनिक मीडिया का उपयोग

साक्ष्य में इलेक्ट्रॉनिक रिकॉर्ड के अलावा, न्यायिक कार्यवाही में अन्य उद्देश्यों के लिए इलेक्ट्रॉनिक मीडिया पर निर्भरता में वृद्धि हुई है। ईमेल, व्हाट्सएप संदेशों आदि जैसे इलेक्ट्रॉनिक मीडिया के लाभ को पहचानते हुए, सुप्रीम कोर्ट ने वाणिज्यिक मुकदमेबाजी और मुकदमेबाजी में सेवा के सामान्य तरीकों के अलावा, ई-मेल के माध्यम से काउंटर पार्टी की सेवा के लिए पक्षकारों / उनके अधिवक्ताओं को प्रोत्साहित किया है। इसी तरह का दृश्य माननीय बॉम्बे हाई कोर्ट ने भी लिया है। हाल के दिनों में, माननीय दिल्ली उच्च न्यायालय और माननीय बॉम्बे हाई कोर्ट द्वारा भी व्हाट्सएप के माध्यम से सेवा को मान्यता दी गई है।

AIRCEL

Certificate

(U/s 65 B (4) (c) of the evidence Act 1872)

Reference: - Notice No. 138 dated 19.01.2015 & email dated 20th January'2015 in respect of providing certified copy of CDR's & CAF under FIR no. 38/2014 U/S 66C,66D IT Act and 419,420 & 120B IPC Police station Cyber Crime Jaipur Rajasthan.

IT IS CERTIFIED that Call Detail Record (C.D.R.) of the following MSISDN Nos. 8013773743, 8013773818 & 002348108299419 for the search periods from 5th October'2014 till 30th October'2014, 10th October'2014 till 30th October'2014 & 1st October'2014 till 25th November'2014 respectively, have been generated from our Computer System and provided to the Deputy Superintendent of Police, Cyber Crime Police Station, Jaipur.

IT IS ALSO CERTIFIED that the CDR containing the information attached/ given under this case has been produced by the computer, regularly used to store or process the information pertaining to CDR's. The activity to store CDR's is an automated process that electronically incorporates the data received from Telecom Switches into database; hence no manual intervention is involved.

IT IS ALSO CERTIFIED that the information containing CDR is derived / produced from the information / data automatically incorporated into the computer database during the ordinary course of the activities.

IT IS ALSO CERTIFIED that condition laid down in section 65B (2) (a) to 65B (2) (d) of the Evidence Act, 1872 regarding the admissibility of data generated as computer output and the computer in question are fully satisfied in all aspects.

IT IS ALSO CERTIFIED that the information/ electronic record/ computer output containing the CDR, attached/ given under this case has been produced from the server, using appropriate electronic device and the contents thereof are true reproduction of its original to the best of my Knowledge and belief.

Thanking you.

Yours sincerely,

For **Aircel Limited**

Nodal Officer

Rajasthan Service Area

Aircel Limited
Jaipur Office : 1st & 2nd Floor, Navajyoti, Amrapali Circle, C-Block, Vaishali Nagar, Jaipur - 302021 Ph.+91-9782500201
Registered Office
Aircel Limited : 5th Floor, Spencer Plaza, 769, Anna Salai, Chennai - 600 002
CIN-U32201TN1994PLC026608 Phone : 91 - 44 - 28490849 Fax : 91- 44 - 42280155
E-mail: rajasthan.al@aircel.co.in, Website: www.aircel.com

CERTIFICATE U/S 65B OF EVIDENCE ACT 1872

I/O SHOULD OBTAIN A CERTIFICATE U/S 65B OF EVIDENCE ACT REGARDING THE ELECTRONIC/ DIGITAL INFORMATION COLLECTED DURING INVESTIGATION FROM BANKS, MSP, ISP AND OTHERS.

SAMPLE CERTIFICATE U/S 65-B OF INDIAN EVIDENCE ACT

1. ISSUED BY HDFC BANK

CERTIFICATE U/S 2A OF BANKER'S BOOKS OF EVIDENCE ACT,1891

Reg: Investigation of fir 38/2014 66-C, 66D IT Act and 420,419,467,468,120-B of Indian penal code.

It is certified that the above information is a true extract in printed form of the relevant data created in the usual and ordinary course of business and stored on the hard disk of the computer systems installed at branch of the bank.

It is further certified:-

That the Access to the Computer System and the data stored thereon is controlled by defined authorized roles exercised through unique user id and the associated passwords. Only the concerned user knows the password and use of ID with password establishes his identity and accountability. Changes to the data are controlled through application level checks and controls.

That physical access to the computers/ server room is prevented by locking the server room and the branch after office hours. Detection of any unauthorized changes in the data after day end and before day; begin activity is carried through check – Sum procedures which built into the application program. Unauthorized changes in the data during regular working hours are prevented/ detected through verification of outputs with authorized inputs.

That in case of system failure the data is retrieved from the back up kept on tape/ floppy/ cartridge/ hard disk which is under the control of system Administration/ designated employee of the branch;

That back-up is verified by; the system during the process of transfer data to backup media.

That physical and logical label identifies the data storage media.

That back up devices and media is kept under lock and key which are in the custody of a designated staff member and that physical and logical access controls are in place as safeguards against tampering of the systems.

It is further certified that to the best of our knowledge and belief the Computer system that generated and stored this information operated properly at the time of such generation/ storage of the data and the printout represent correctly the relevant data.

For HDFC Bank Ltd.

Branch Manager cum Systems Administrator

INTERNATIONAL CYBERCRIME

अंतर्राष्ट्रीय साईबर अपराध

यद्यपि अंतर्राष्ट्रीय साइबर अपराध की कोई सार्वभौमिक रूप से स्वीकृत परिभाषा नहीं है, यह आमतौर पर अवैध इंटरनेट वाली गतिविधियों के रूप संदर्भित किया जाता है जो अक्सर वैश्विक इलेक्ट्रॉनिक नेटवर्क में होती हैं। साइबर अपराध विभिन्न श्रेणियों के हैं, लेकिन इन सभी अपराधों के बीच एक सामान्य विशेषता है, और वह है अंतर्राष्ट्रीय कानून की प्रभावशीलता और राष्ट्रों के बीच सहयोग को चुनौती देना।

अंतर्राष्ट्रीय साइबर अपराध के प्रकार :–

अंतर्राष्ट्रीय साइबर अपराध आमतौर पर कई ब्रॉडहेड में वर्गीकृत किए जाते हैं। वे इस प्रकार हैं:

- **एक व्यक्ति के खिलाफ अपराध:** इसमें कोई भी साइबर अपराध शामिल है जो किसी व्यक्ति के व्यक्तित्व को प्रभावित करता है। इसमें गतिरोध, मानहानि, हैकिंग, ई-मेल और एसएमएस स्पूफिंग आदि जैसे अपराध शामिल हैं।
- **संपत्ति के खिलाफ अपराध:** यह तब होता है जब किसी व्यक्ति की संपत्ति किसी तरह खतरे में होती है। इसमें आमतौर पर बौद्धिक संपदा, साइबर बर्बरता, साइबर हमले, कंप्यूटर प्रणाली की हैकिंग आदि के खिलाफ अपराध शामिल हैं।
- **सरकार के खिलाफ अपराध:** यह साइबर अपराध का एक बहुत खतरनाक रूप है जो अंतर्राष्ट्रीय शांति और सुरक्षा के लिए भी खतरा है। इसमें साइबर आतंकवाद और युद्ध शामिल है।
- **समाज के खिलाफ अपराध:** समाज के खिलाफ अपराध उन साइबर गतिविधियों को इंगित करता है जो बड़ी संख्या में लोगों को नुकसान पहुंचा रहे हैं जिसमें साइबर तस्करी, जालसाजी, साइबर जुआ आदि शामिल हैं।

अंतरराष्ट्रीय साइबर अपराध जांच की प्रक्रिया

अंतरराष्ट्रीय साइबर अपराध जांच की प्रक्रिया देशों में भिन्न होती है। एक बेहतर दृष्टिकोण यह देखना होगा कि साइबर अपराधों से राज्य, राष्ट्रीय और अंतर्राष्ट्रीय कानून प्रवर्तन एजेंसियां कैसे निपटती हैं।

पुलिस की कार्रवाई

जैसे ही किसी व्यक्ति को साइबर अपराध का मामला सामने आता है, उसे अपने नजदीकी पुलिस स्टेशन में रेफर या शिकायत करनी चाहिए। यह सारहीन है कि इसमें साइबर सेल है या नहीं। यह सलाह दी जाती है कि वह अपनी शिकायत को प्रथम दृष्टया विश्वसनीय बनाने के लिए पर्याप्त सबूत इकट्ठा करे। शिकायत मिलने पर मामले को देखने वाली पुलिस इसे आपराधिक या सिविल या कुछ मामलों में आपराधिक और सिविल दोनों में वर्गीकृत करेगी:

- मामला दर्ज करने के लिए पर्याप्त सबूत इकट्ठा करें।
- एक अदालत के क्षेत्रीय या विषयगत अधिकार क्षेत्र का फैसला करें और बाद में दंड प्रक्रिया संहिता की धारा 177 से 179 के तहत मामला दर्ज करें।

केंद्रीय जांच ब्यूरो

सीबीआई एक विशेष संरचना के माध्यम से साइबर अपराध की जांच करती है। यह इस प्रकार है-

1. साइबर अपराध अनुसंधान और विकास इकाई (CCRDU): यह निकाय निम्नलिखित कार्य के साथ शामिल है:

- राज्य पुलिस बलों के साथ संपर्क करना और साइबर अपराध के मामलों की जानकारी एकत्र करना
- उन मामलों की पहचान करने के लिए सॉफ्टवेयर विशेषज्ञों के साथ संपर्क करना, जिन्हें अपराधों की रोकथाम और पहचान के लिए राज्य पुलिस बलों के ध्यान की आवश्यकता है।
- अन्य देशों में रिपोर्ट किए गए नवीनतम मामलों पर जानकारी का एक संग्रह।
- मासिक साइबर क्राइम डाइजेस्ट की तैयारी।
- आईटी मंत्रालय, भारत सरकार और संगठनों और संस्थानों और इंटरपोल मुख्यालय के साथ तालमेल का रखरखाव।

2. साइबर अपराध जांच सेल (CCIC):

- इस सेल के पास अखिल भारतीय अधिकार क्षेत्र है और सूचना प्रौद्योगिकी अधिनियम 2000 के तहत आपराधिक अपराधों की जांच करता है।

3. साइबर फोरेंसिक प्रयोगशाला (सीएफएल): साइबर फोरेंसिक प्रयोगशाला के निम्नलिखित कार्य हैं-

- विशेषज्ञ गवाही प्रदान करता है
- साइबर फोरेंसिक में अनुसंधान और विकास
- कंप्यूटर खोज और जब्ती के लिए साइट पर सहायता प्रदान करें
- आपराधिक जांच के समर्थन में मीडिया विश्लेषण प्रदान करें
- जांच पर परामर्श प्रदान करता है

4. नेटवर्क मॉनिटरिंग सेंटर:

नेटवर्क मॉनिटरिंग सेंटर इंटरनेट की निगरानी और किसी भी असामान्य गतिविधियों की खोज के लिए नेटवर्क मॉनिटरिंग टूल का उपयोग करता है।

इंटरपोल

इंटरपोल दुनिया का सबसे बड़ा पुलिस संगठन है। जब अंतरराष्ट्रीय साइबर अपराध की जांच की बात आती है तो यह एजेंसी विभिन्न देशों की कानून प्रवर्तन एजेंसियों के पूर्ण सहयोग को सुनिश्चित करने में एक लंबा रास्ता तय कर सकती है। इंटरपोल अंतर्राष्ट्रीय साइबर अपराध जांच की जांच करने में मदद करता है:

- कानून प्रवर्तन एजेंसियों को परिचालन और खोजी समर्थन प्रदान करना
- साइबर खुफिया और विश्लेषण
- डिजिटल फोरेंसिक
- नवाचार और अनुसंधान
- क्षमता निर्माण और
- प्राकृतिक साइबर समीक्षाएँ

कई अन्य एजेंसियां और यूनियनें हैं जो इस वैश्विक मुद्दे से निपटने में सहयोग करती हैं:

- **एशिया-प्रशांत आर्थिक सहयोग (APEC):** एशिया-प्रशांत क्षेत्र में, APEC साइबर सुरक्षा को बढ़ावा देकर साइबर अपराध से निपटने के लिए 21 सदस्य अर्थव्यवस्थाओं का समन्वय करता है।

- **यूरोप की परिषद (EOC):** यूरोप की परिषद ने सार्वजनिक और निजी दोनों क्षेत्रों में व्यक्तिगत डेटा की सुरक्षा के लिए कई सम्मेलनों को लागू किया।
- **संयुक्त राष्ट्र:** संयुक्त राष्ट्र के पास कई संकल्प हैं जो अंतर्राष्ट्रीय साइबर अपराध की बेहतर जांच को बढ़ावा देने में मदद करते हैं। उदाहरण के लिए, संकल्प 56/121 ने राज्यों को राष्ट्रीय कानून, नीति विकसित करने पर व्यापक कार्य पर विचार करने के लिए आमंत्रित किया और साइबर अपराध को रोकने के लिए अभ्यास किया।
- **राष्ट्रमंडल राष्ट्र:** राष्ट्रमंडल सचिवालय ने "मॉडल ऑन कंप्यूटर एंड कंप्यूटर संबंधित अपराध" तैयार किया, जो 53 सदस्य देशों के घरेलू कानूनों में काफी बदलाव लाया गया।

इनमें से कुछ के नाम थे, कई अन्य संगठन हैं जो अंतर्राष्ट्रीय सहयोग सुनिश्चित करने के लिए एक लंबा रास्ता तय करते हैं और इस तरह अंतर्राष्ट्रीय साइबर अपराध की बेहतर जांच करते हैं।

The challenges faced in cases of International Cyber Crime

जब यह अंतर्राष्ट्रीय साइबर अपराध की बात आती है, तो यह कुछ चुनौतियों से भरा है:

- अंतरराष्ट्रीय साइबर अपराध के तहत आने वाली विविधता का अपराधीकरण करने के लिए पर्याप्त कानून नहीं हैं।
- अक्सर जांच में शामिल देश पर्याप्त व्यक्तिगत संसाधनों का निवेश करने में विफल होते हैं।
- अपराधी का पता लगाने में असमर्थता एक और बाधा है; इस मामले में, अपराध के भौतिक स्रोत का पता नहीं लगाया गया है।
- अंतरराष्ट्रीय स्तर पर सबूतों का संग्रह और साझाकरण सुचारू नहीं है।

जांच की प्रक्रिया में बाधाओं पर काबू पाने का साधन एक व्यापक और व्यापक विषय है। लेकिन निम्नलिखित कुछ मूल बातें हैं जिनका पालन करना आवश्यक है:

- सभी प्रकार के साइबर अपराधों और अपराधों के अपराधीकरण के लिए बेहतर कानून होने चाहिए, इस मामले में, विभिन्न देशों की सरकार द्वारा किया जाता है।
- जांच में शामिल एजेंसियों को साइबर आपातकाल का सामना करने के लिए तकनीकी रूप से सुसज्जित होना चाहिए। एक टीम को हमेशा तकनीकी सहायता के लिए तैयार रखा जाना चाहिए
- साइबर संसाधनों का उपयोग करने वाले लोगों को जागरूक किया जाना चाहिए।
- साइबर अपराध जांच में शामिल देशों को संसाधनों और सूचनाओं को साझा करने के लिए तैयार रहना चाहिए।

साइबर क्राइम भी बढ़ रहा है, और पीड़ितों की संख्या हर सेकंड बढ़ रही है। साइबर अपराध में वैश्विक रुझानों के बाद सतर्क रहना जितना महत्वपूर्ण है क्योंकि आप कभी नहीं जानते कि अगला शिकार कौन होगा।

CYBER CRIME AGAINST WOME

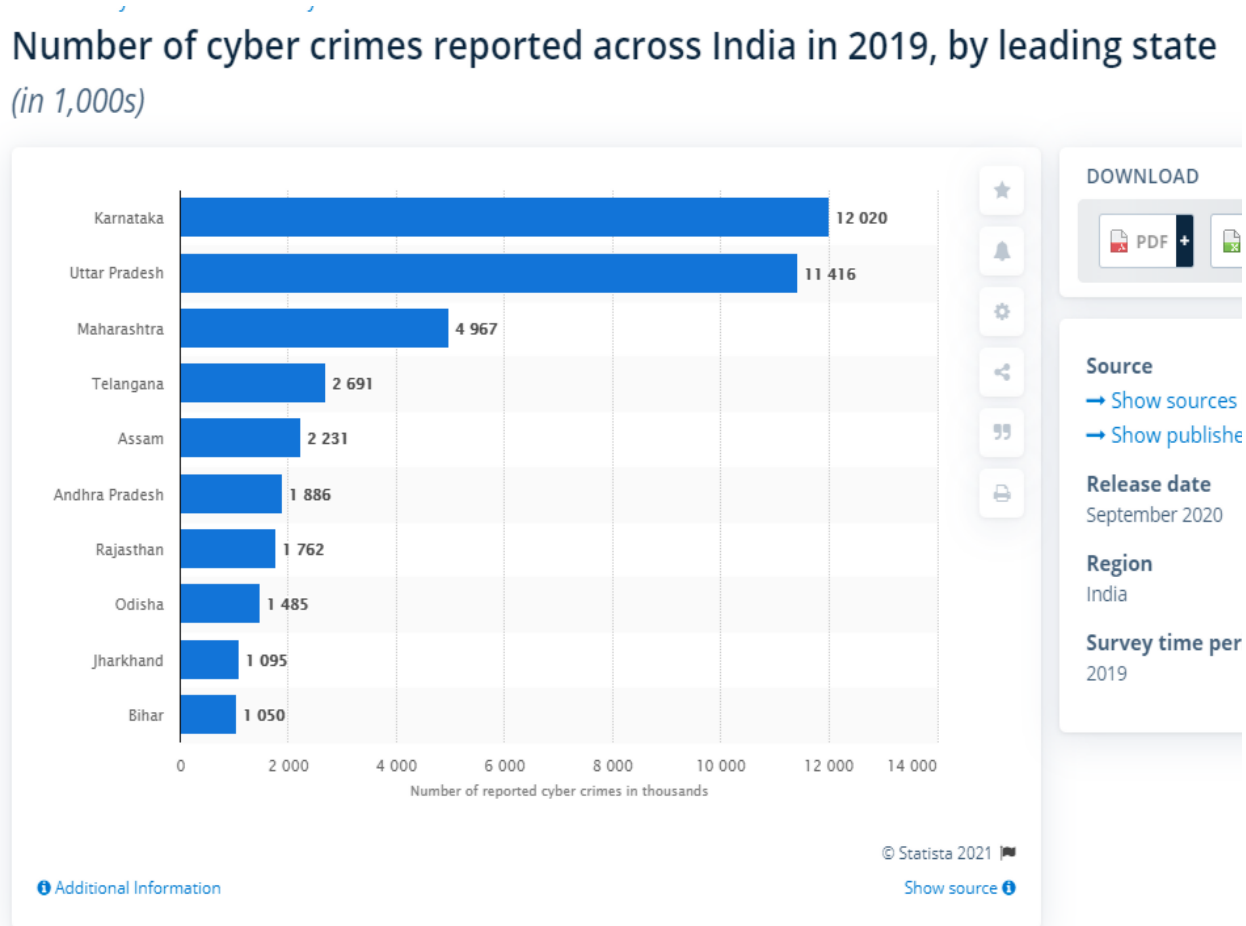
महिलाओं के विरूद्ध साईबर अपराध

भारत में हर दूसरे सेकंड, एक महिला साइबर क्राइम (cyber crime) का शिकार होती है और ऑनलाइन प्लेटफॉर्म अब एक नया मंच है, जहां हर पल एक महिला सुरक्षा को चुनौती दी जा रही है। ट्रोलिंग, गाली-गलौज, धमकी देना, घूरना, बदनाम करना, पीछा करना, बदला लेना और अश्लील बातें करना जैसे साइबर क्राइम (cyber crime) दुनिया में मौजूद हैं। महिलाओं के खिलाफ साइबर क्राइम (cyber crime) में प्रभाव शारीरिक से अधिक मानसिक होता है जबकि महिलाओं की सुरक्षा सुनिश्चित करने वाले कानूनों का ध्यान मानसिक नुकसान की तुलना में शारीरिक तोर पर अधिक है।

कुछ प्रमुख प्रसिद्ध साइबर क्राइम ने हजारों महिलाओं को डिप्रेशन, उच्च रक्तचाप जैसे विभिन्न स्वास्थ्य मुद्दों में डाल दिया है और ई-उत्पीड़न (e – assualt) के कारण महिलाएं चिंता, हृदय रोग और थायरॉयड जैसी बीमारियों से पीड़ित हैं।

देश में जिस तेजी से सोशल मीडिया यूजर्स बढ़े हैं, उतनी ही तेजी से महिलाओं के प्रति साइबर अपराध भी बढ़ा है। राष्ट्रीय महिला आयोग के पास आने वाली शिकायतों के आंकड़ों से यह खुलासा हुआ है।

राष्ट्रीय महिला आयोग के पास अप्रैल 2017 से मार्च 2018 में साइबर अपराध से संबंधित आने वाली शिकायतों की संख्या 339 थीं, जो अप्रैल 2018 से मार्च 2019 में बढ़कर 402 हो गई। इस तरह एक ही साल में साइबर अपराध की शिकायतों में 18% से अधिक की वृद्धि हुई है।



प्रमुख साइबर क्राइम :

- **साइबरस्टॉकिंग:** महिलाओं के प्रति साइबरस्टॉकिंग की घटनाये बढ़ रही है । साइबरस्टॉकिंग ऑनलाइन उत्पीड़न और ऑनलाइन दुरुपयोग के लिए किसी को परेशान करने के लिए इंटरनेट का उपयोग करने का एक तरीका है। किसी को बार-बार टेक्स्ट मैसेज भेजना, फ्रेंड रिक्वेस्ट भेजना, स्टेटस अपडेट पर नजर रखना और इंटरनेट मॉनिटरिंग इस अपराध की श्रेणी में आते हैं। आईपीसी की धारा 354 डी के तहत यह दंडनीय अपराध है। एक साइबर स्टॉकर पीड़ित को सीधे शारीरिक खतरे में नहीं डालता है, लेकिन जानकारी इकट्ठा करने के लिए पीड़ित की ऑनलाइन गतिविधि का ध्यान रखता है, विभिन्न रूपों से धमकी देता है।
- **मानहानि:** साइबर मानहानि में मानहानि और मानसिक तनाव दोनों ही शामिल हैं। इसमें एक वेबसाइट पर व्यक्ति के बारे में बदनाम करने वाली जानकारी प्रकाशित करना या पीड़ितों या संगठन के सामाजिक और दोस्तों के बीच इसे प्रसारित करना शामिल है, जो उनकी मानसिक पीड़ा और दर्द का कारण बनकर किसी महिला की प्रतिष्ठा को बर्बाद करने का एक आसान तरीका है।

- **ई-मेल स्पूफिंग:** यह एक ईमेल को दर्शाता है जो निकलता किसी नाम से है लेकिन भेजने वाला कोई और होता है । यह मौद्रिक क्षति का कारण बन सकता है।

- **फ़िशिंग:** फ़िशिंग संवेदनशील जानकारी जैसे उपयोगकर्ता का नाम और पासवर्ड प्राप्त करने और व्यक्तिगत जानकारी प्राप्त करने का प्रयास है।

- **साइबर स्पाइंग-** आईटी एक्ट की धारा 66 ई के अंतर्गत यह दंडनीय अपराध है, इसमें चेजिंग रूम, लेडीज वॉशरूम, होटल के कमरे और बाथरूम जैसी जगहों पर रिकॉर्डिंग डिवाइस लगाए जाते हैं।

- **साइबर पॉर्नोग्राफी-** इसके तहत महिलाओं के अश्लील फोटो या वीडियो हासिल कर उन्हें ऑनलाइन पोस्ट कर दिया जाता है। अधिकांश मामलों में अपराधी फोटो के साथ छेड़छाड़ करते हैं और बदनाम करने, परेशान और ब्लैकमेल करने के लिए उनका इस्तेमाल करता है। इस तरह के अपराधों में आईटी एक्ट की धारा 67 और 67ए के अंतर्गत आते हैं।

- **साइबर बुलिंग-** इसमें साइबर अपराधी पहले महिलाओं या लड़कियों से दोस्ती बनाते हैं और फिर उन्हें विश्वास में लेकर नजदीकियां बढ़ाने के बाद महिला या लड़की के निजी फोटो हासिल कर लेते हैं। इसके बाद पीड़िता से मनचाहे काम करवाने के लिए ब्लैकमेल करते हैं।

साइबर कानून

सूचना और प्रौद्योगिकी अधिनियम, 2000 के तहत, किसीकी गोपनीयता भंग करने के लिए कई धाराओं के तहत साइबर अपराधियों पर मामला दर्ज किया जा सकता है:।

- धारा 67 इलेक्ट्रॉनिक सामग्री में अश्लील सामग्री को प्रकाशित या प्रसारित करने से संबंधित है। आई..टी.ए में पहले के खंड को बाद में आई.टी.ए .ए 2008 के अनुसार बढ़ा दिया गया था जिसमें बाल पोर्नोग्राफी और किसी और के द्वारा रिकॉर्डों को बनाए रखना सभी शामिल थे।
- धारा 66 ए: संचार सेवा के माध्यम से आपत्तिजनक संदेश भेजना, झुंझलाहट आदि के कारण ऐसे संदेश की उत्पत्ति के बारे में प्राप्तकर्ता को परेशान करना या धोखा देने के लिए ईमेल भेजना (आमतौर पर आईपी या ईमेल स्पूफिंग के रूप में जाना जाता है) यह सभी यहां शामिल हैं। इन कृत्यों के लिए सजा तीन साल तक की कैद या जुर्माना है।
- धारा 66 बी: बेईमानी से चुराए गए कंप्यूटर संसाधन या संचार उपकरण को तीन साल तक की सजा या एक लाख रुपये जुर्माना या दोनों।

- धारा 66 सी; इलेक्ट्रॉनिक हस्ताक्षर या अन्य पहचान दस्तावेज़ की चोरी जैसे दूसरों के पासवर्ड या इलेक्ट्रॉनिक हस्ताक्षर आदि का उपयोग बिना उसकी जानकारी के करना।
- धारा 66D: कंप्यूटर संसाधन या संचार उपकरण का उपयोग करने वाले व्यक्ति द्वारा धोखा देने पर या तो जेल की सजा से दंडित किया जाएगा, जो तीन साल तक का होता है और जुर्माना के लिए भी उत्तरदायी होगा जो एक लाख रुपये तक हो सकता है।
- धारा 66 ई: गोपनीयता का उल्लंघन – किसी व्यक्ति के गोपनीय क्षेत्र को उसकी सहमति के बिना प्रकाशित करना या प्रसारित करना।इसके लिए तीन साल की सजा या दो लाख रुपये का जुर्माना या दोनों हो सकता है।
- धारा 66 एफ: साइबर आतंकवाद – राष्ट्र की एकता, अखंडता, या सुरक्षा को खतरे में डालने और कंप्यूटर संसाधन तक पहुंचने के लिए अधिकृत किसी भी व्यक्ति को इनकार करना या प्राधिकरण के बिना कंप्यूटर संसाधन में घुसने या प्रवेश करने का प्रयास करने का इरादा रखना।
- धारा 72: गोपनीयता और गोपनीयता भंग करने के लिए सजा।
- धारा 72A: कानूनन कॉन्ट्रैक्ट के दौरान सूचना का खुलासा करने के लिए सजा।
- धारा 441; आईपीसी: यह धारा आपराधिक अत्याचार से संबंधित है।
- धारा 354डी: यह खंड गतिरोध से संबंधित है। यह स्टाकर को एक पुरुष के रूप में परिभाषित करता है जो एक महिला का पीछा करता है और उस महिला से संपर्क करने की कोशिश करता है, डिजिटल मीडिया का उपयोग करते समय महिला द्वारा की गई हर गतिविधि पर नज़र रखता है।

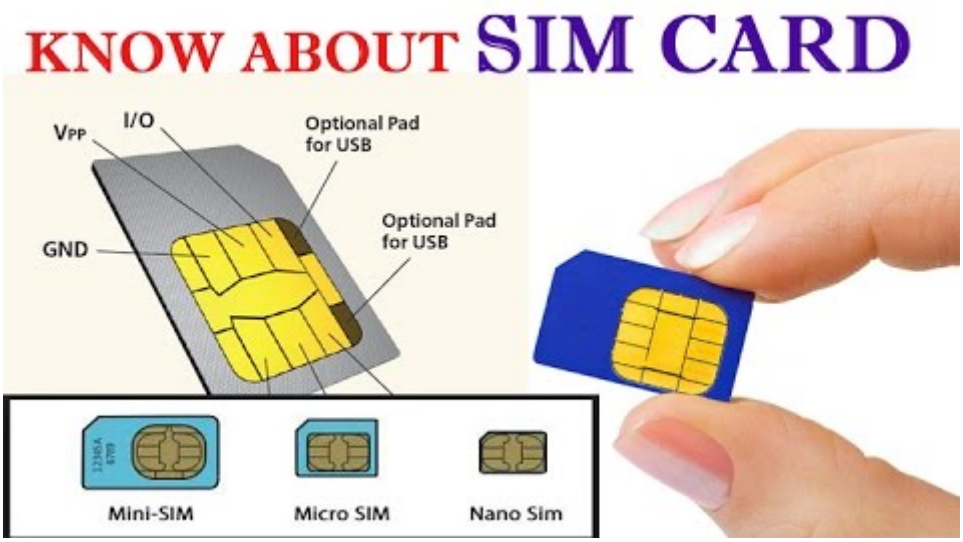
आजकल की टेक्नोलॉजी की दुनिया में जहाँ इंटरनेट हमारे लिए वरदान है वही ऐसे बहुत -से क्षेत्र है जहाँ यह एक श्राप का रूप भी ले लेता है। हमे आजकल की इस सोशल मीडिया की दुनिया में बहुत संभलकर कदम उठाने चाहिए

CELL PHONE TECHNOLOGY

SIM (Subscriber Identity Module)

एक सिम कार्ड, जिसे ग्राहक पहचान मॉड्यूल के रूप में भी जाना जाता है, एक स्मार्ट कार्ड है जो GSM सेलुलर टेलीफोन ग्राहकों के लिए डेटा संग्रहीत करता है। इस तरह के डेटा में यूजर्स की पहचान, स्थान और फोन नंबर, नेटवर्क ऑथराइज़ेशन डेटा, पर्सनल सेक्युरिटी किज, कौन्टेक्ट लिस्ट और टेक्स्ट मैसेजेज शामिल हैं। सेक्युरिटी फीचर्स में डेटा की सुरक्षा और ईव्सड्रॉपिंग को रोकने के लिए प्रमाणीकरण और एन्क्रिप्शन शामिल हैं। सिम कार्ड में थोड़ी मात्रा में मेमोरी भी होती है जो 250 संपर्कों, कुछ एसएमएस संदेशों और कार्ड की आपूर्ति करने वाले वाहक द्वारा उपयोग की जाने वाली अन्य जानकारी को संग्रहीत कर सकती है।

सिम कार्ड कैसा दिखता है?



एक सिम कार्ड सिर्फ प्लास्टिक के एक छोटे टुकड़े जैसा दिखता है। महत्वपूर्ण हिस्सा एक छोटी इंटिग्रेडेट चिप है जिसे उस मोबाइल डिवाइस द्वारा पढ़ा जा सकता है जिसे इसमें डाला गया है, और इसमें एक विशिष्ट आइडेंटिफिकेशन नंबर, फोन नंबर और यूजर के लिए विशिष्ट अन्य डेटा शामिल है, जो इसके लिए रजिस्टर है।

GSM तथा CDMA

GSM यानि ग्लोबल सिस्टम फॉर मोबाइल कम्युनिकेशंस, यह विश्व में सबसे ज्यादा प्रयोग किया जाना वाला मोबाइल नेटवर्क है। यहॉ तक कि अाप भी इसे ही यूज कर रहे होगें। इसका पता करना बहुत आसान है कि अपका फोन CDMA है या GSM, आपके फोन में सिम कार्ड पड़ता है या नहीं अगर सिम कार्ड पड़ता है तो यह GSM है और अगर नहीं तो अपका फोन CDMA है

CDMA यानि कोड डिवीजन मल्टीपल एक्सेस, इस प्रकार के नेकवर्क पर जो फोन काम करते हैं, उन मोबाइल फोन में सिम कार्ड नहीं पडता है, अगर पडता भी है तो केवल उसी मोबाइल नेटवर्क कंपनी को पडता है जिस मोबाइल नेटवर्क कंपनी का आपने फोन खरीदा है, यहॉ हम मोबाइल नेटवर्क कंपनी की बात कर रहे हैं जैसे आयडिया, एयरटेल, बीएसएनएल, डोकोमो आदि। इस प्रकार के फोन में केवल उसी कंपनी का ही सिम कार्ड काम

करता है किसी दूसरी कंपनी का नहीं। आपका फोन एक बार में केवल एक नेटवर्क को सपोर्ट करेगा, CDMA या फिर GSM।

- एक GSM के phone में एक specialized card चाहिए जिसे की SIM (Subscriber Identity Module) भी कहा जाता है. ये SIM carrier specific होते हैं और इन्हें एक phone से दुसरे में बदला जा सकता है बिना किसी data के loss हुए.
- CDMA device में SIM cards की जरुरत नहीं है बल्कि वो ESNs (Electronic Serial Numbers) पर निर्भर करते हैं.
- CDMA phone में अगर आपको phone को activate करना है तब user को अपने Carrier को call करना पड़ेगा अथवा online system का इस्तमाल करना पड़ेगा 'ESN' change के लिए. यहाँ SIM card के न होने के कारण device swapping बहुत ही कठिन है.
- GSM ज्यादा flexible हैं CDMA की तुलना में. यहाँ SIM card को आसानी से एक मोबाइल से दुसरे मोबाइल में बदला जा सकता है. वहीँ CDMA तभी काम करेगा अगर ESN database में registered हो तब.
- अगर CDMA phone बंद हो गया तब आपको नया phone खरीदना होगा, वहीँ GSM में ऐसा करने की कोई जरुरत नहीं है.
- CDMA technology में ज्यादा security प्राण की जाती है GSM की तुलना में क्यूंकि encryption CDMA में inbuilt होती है. इसीलिए GSM की तुलना में CDMA phone calls बहुत ही ज्यादा secure हैं.

Next-Generation SIM Technology(eSIM):

नेक्स्ट-जनरेशन की सिम टेक्नोलॉजी को Embedded-SIM (eSIM) कहा जाता है। इस चिप को बदला नहीं जा सकता और यह सीधे आपके डिवाइस के सर्किट बोर्ड पर टिकी होती है और इसमें "Remote SIM Provisioning," होती है, जिसे कस्टमर अपने डिवाइसेस पर लगे ई-सिम को रिमोटली एक्टिवेट कर सकते है। अभी, Google के Pixel 2 और Apple Watch 3 (कुछ कारों के साथ), केवल वास्तविक उपभोक्ता टेक्नोलॉजी हैं जो eSIM का उपयोग कर रहे हैं, लेकिन यह जल्दी बदलने की उम्मीद है।

ICCID (Integrated Circuit Card ID) Number

प्रत्येक सक्रिय सिम कार्ड का अपना सिम कार्ड नंबर होता है, जिसका उपयोग व्यक्तिगत रूप से कार्ड को असाइन करने और पहचान करने के लिए किया जाता है। इन नंबरों को सीधे कार्ड पर मुद्रित किया जाता है या कार्ड वाहक या संलग्न पत्र पर दर्ज किया जाता है। इस संख्या के लिए तकनीकी शब्द **ICCID (Integrated Circuit Card ID)** है। ICCID में 19 से 20 अंक होते हैं

यह IMEI नंबर के साथ भ्रमित नहीं होना चाहिए। IMEI मोबाइल फोन की पहचान संख्या है, जबकि ICCID सिम कार्ड की संख्या है।

एक प्रदाता के साथ संचार करते समय, सिम कार्ड नंबर अक्सर महत्वपूर्ण होता है क्योंकि यह एकमात्र जानकारी है जो वास्तविक सिम कार्ड को संदर्भित करता है। यदि आप कई प्रीपेड कार्डों का उपयोग करते हैं, तो यह जानना महत्वपूर्ण है कि कौन सा मोबाइल फोन कार्ड, एक रद्दीकरण से संबंधित है। इसलिए, ICCID भी अक्सर अनुरोध किया जाता है।

कई पहचानकर्ता सेलुलर प्रौद्योगिकी के लिए मौजूद हैं जिनके लिए ICCID संख्याओं की आवश्यकता होती है, जिससे यह निर्धारित होता है कि किस उपभोक्ता को किस नेटवर्क से कनेक्ट करना चाहिए

यह इस तरह काम करता है:

- आपने अपने डिवाइस में एक सिम कार्ड डाला है।
- डिवाइस उपलब्ध सेलुलर नेटवर्क के लिए खोज करता है, डिवाइस ऑपरेटर को पहचान कोड अग्रेषित करता है।
- सिम कार्ड पहचान कोड उत्पन्न करने के लिए ICCID कोड का उपयोग करता है।
- मोबाइल ऑपरेटर द्वारा पहचान कोड प्राप्त करने के बाद, वे निर्धारित करते हैं कि ग्राहक के पास नेटवर्क में काम करने के अधिकार हैं या नहीं।

यह विशेष रूप से देशों में उपयोग किए जाने वाले एल्गोरिदम के साथ अलग तरीके से काम करता है: यदि सिम कार्ड नेटवर्क पर नहीं है, लेकिन सिम कार्ड ऑपरेटर उसी देश में है, तो ग्राहक को एक सीमित सेवा प्रदान की जाती है, उदाहरण के लिए, यदि आपका डिवाइस एक मोबाइल है , तो केवल आपातकालीन सेवाओं को कॉल करने की क्षमता। यदि सब्सक्राइबर का ICCID सेलुलर नेटवर्क से मेल खाता है, तो ऑपरेटर कॉल, इंटरनेट आदि की पहुंच खोलता है।

What Do the Numbers Mean?

For example, consider the ICCID code: 8901260234814455936F

- 89 - is an industry code, a product for telecommunications networks.
- 012 - is usually the same as the country code.
- 60 - is the area code of the mobile operator in a particular country.
- 234814455936F – The SIM card number not only has a meaning but acts as an individual operator.

I.M.S.I.—(International Mobile Subscriber Identification Number)

एक **standard IMSI number 15 digit** का होता है जिसका उपयोग सेलुलर नेटवर्क के उपयोगकर्ता की पहचान करने के लिए किया जाता है और यह सभी सेल्युलर नेटवर्क से जुड़ी एक विशिष्ट पहचान है। IMSI फोन के अंदर सब्सक्राइबर आइडेंटिटी मॉड्यूल (सिम) में स्टोर होता है और इसे फोन द्वारा उपयुक्त मोबाइल नेटवर्क पर भेजा जाता है। इसे 64 बिट फ़ील्ड के रूप में संग्रहीत किया जाता है। इसका उपयोग एचएलआर में मोबाइल के अन्य विवरण प्राप्त करने या स्थानीय रूप से आगंतुक रजिस्टर में स्थानीय रूप से कॉपी किए जाने के लिए भी किया जाता है।

I.M.E.I - International Mobile Equipment Identity

IMEI का full form है **International Mobile Equipment Identity**. ये एक ऐसा number हैं जो की प्रत्येक mobile का किसी दुसरे mobile से अलग होता है।

एक **standard IMEI number 15 digit** का होता है, साथ में कुछ additional check number भी जोड़ा जाता है। दूसरा **IMEI/SV (SV means Software Version) 16 digit** का होता है, लेकिन ये केवल नए Mobile Phones में ही होता है। IMEI number अब केवल phone की पहचान तक ही सिमित नहीं रह गया है, इससे तो कोई device को block भी किया जा सकता है। यदि आपका Mobile Phone चोरी हो गया है तो इस number के जरिये आप अपने local Service Provider को सूचित कर अपने number को block भी कर सकते है। इस number का इस्तमाल ज्यादातर Police चोरी किये गए phones का पता लगा ने के लिए करती है।

सन **2004** से अभी के format कुछ इस प्रकार से है AA-BBBBBB-CCCCCC-D. इसमें पहले दो भाग labelled A और B को कहा जाता है Type **Allocation Code(TAC)**, और ये directly Manufacturer और Phone के Model से संभंधित है। उदहारण के रूप में iPhone5 का TAC है **01-332700** और Samsung Galaxy S2 का है **35-853704**. दूसरा भाग labelled C एक serial number है जो की unique होता है सभी handset के लिए और ये तय करता है उस mobile का manufacturer और last digit एक checksum होता है, जिसका इस्तमाल पूरी string को verify करने के लिए होती है।

Use of IMEI Number

देखा जाये तो IMEI Number का मुख्य काम है Mobile को identify करना. लेकिन उसके दुसरे भी फायदे हैं जैसे की Mobile Phone की चोरी को रोकना और मोबाइल ट्रेकिंग में police की मदद करना. जैसे की सभी mobile का unique IMEI Number होता है तो उसे बदला नहीं जा सकता, यदि वो चोर दूसरा SIM भी इस्तमाल करे तब भी वो Mobile Phone को इस्तमाल नहीं कर सकता यदि उसे block कर दिया गया हो. **IMEI Number** को device hardware में अच्छी तरह Hard Coded किया गया होता है, जिस कारण इसे remove करना इतना आसान नहीं है बिना mobile को खराब किये.

यदि हमारा Mobile Phone कभी चोरी हो गया हो और अगर हमने complain दे दिया तब हमारे service provider के पास option होता है की वो उस Mobile Phone को IMEI Number के द्वारा Blacklist कर सकते हैं और उसका सही location भी ट्रैक कर सकते हैं.

How to Find IMEI Number)

Maximum Mobile में *#06# **enter करने से आपका IMEI Number दिखा देता है.**

चेक अंकों का निर्धारण तीन चरणों में किया जाता है:

I.M.E.I. नम्बर–490154203237518 अंतिम Digit चैक Digit होता है जिसका इस्तमाल पूरी string को verify करने के लिए किया जाता है। यह अंक CDR मे 0 Display होता है तो यह कैसे पता करें कि लास्ट एक डिजिट क्या होगा।

चैक Digit का उदाहरण–

I.M.E.I. Check Digit Formula

IMEI	4	9	0	1	5	4	2	0	3	2	3	7	5	1	?
Double every other	4	18	0	2	5	8	2	0	3	4	3	14	5	2	?
Sum digits	4 + (1 + 8) + 0 + 2 + 5 + 8 + 2 + 0 + 3 + 4 + 3 + (1 + 4) + 5 + 2 + ? = 52 + ?														

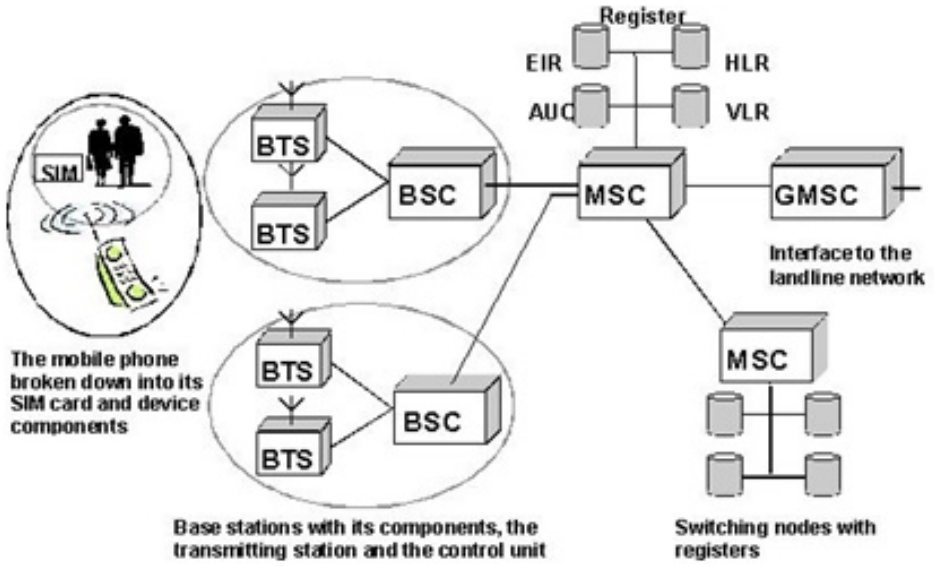
Sum Divisble By 10 We Need =8

Check Digit =8

Last Digit =8

GSM Architecture

The GSM architecture consists of three major interconnected subsystems that interact with themselves and with users through certain network interface. The subsystems are Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Operational Support Subsystem (OSS). Mobile Station (MS) is also a subsystem but it is considered as a part of BSS.



1. Mobile Station (MS): Mobile Station is made up of two entities.

A. Mobile equipment (ME):

- It is a portable, vehicle mounted, hand held device.
- It is uniquely identified by an IMEI number.
- It is used for voice and data transmission. It also monitors power and signal quality of surrounding cells foe optimum handover. 160 characters long SMS can also be sent using Mobile Equipment.

B. Subscriber Identity module (SIM):

- It is a smart card that contains the International Mobile Subscriber Identity (IMSI) number.
- It allows users to send and receive calls and receive other subscriber services. - It is protected by password or PIN.
- It contains encoded network identification details. it has key information to activate the phone.
- It can be moved from one mobile to another.

2. Base Station Subsystem (BSS): It is also known as radio subsystem, provides and manages radio transmission paths between the mobile station and the Mobile Switching Centre (MSC). BSS also manages interface between the mobile station and all other subsystems of GSM. It consists of two parts.

A. Base Transceiver Station (BTS):

- It encodes, encrypts, multiplexes, modulates and feeds the RF signal to the antenna.
- It consists of transceiver units.

- It communicates with mobile stations via radio air interface and also communicates with BSC via Abis interface.

B. Base Station Controller (BSC):

- It manages radio resources for BTS. It assigns frequency and time slots for all mobile stations in its area.
- It handles call set up, transcoding and adaptation functionality handover for each MS radio power control.
- It communicates with MSC via A interface and also with BTS.

3. Network Switching Subsystem (NSS): it manages the switching functions of the system and allows MSCs to communicate with other networks such as PSTN and ISDN. It consist of

A. Mobile switching Centre:

- It is a heart of the network. It manages communication between GSM and other networks.
- It manages call set up function, routing and basic switching.
- It performs mobility management including registration, location updating and inter BSS and inter MSC call handoff.
- It provides billing information.
- MSC does gateway function while its customers roam to other network by using HLR/VLR.

B. Home Location Registers (HLR): - It is a permanent database about mobile subscriber in a large service area. - Its database contains IMSI, IMSISDN, prepaid/post-paid, roaming restrictions, supplementary services.

C. Visitor Location Registers (VLR): - It is a temporary database which updates whenever new MS enters its area by HLR database. - It controls mobiles roaming in its area. It reduces number of queries to HLR. - Its database contains IMSI, TMSI, IMSISDN, MSRN, location, area authentication key.

D. Authentication Centre: - It provides protection against intruders in air interface. - It maintains authentication keys and algorithms and provides security triplets (RAND, SRES, Ki).

E. Equipment Identity Registry (EIR):

- It is a database that is used to track handset using the IMEI number.
- It is made up of three sub classes- the white list, the black list and the gray list.

4. Operational Support Subsystem (OSS): It supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose and troubleshoot all aspects of GSM system. It supports one or more Operation Maintenance Centres (OMC) which are used to monitor the performance of each MS, Bs, BSC and MSC within a GSM system. It has three main functions:

- To maintain all telecommunication hardware and network operations with a particular market.
- To manage all charging and billing procedures
- To manage all mobile equipment in the system.

Interfaces used for GSM network :
1)UM Interface –Used to communicate between BTS with MS
2)Abis Interface— Used to communicate BSC TO BTS
3)A Interface-- Used to communicate BSC and MSC
4) Singling protocol (SS 7)- Used to communicate MSC with other network .

Common Mobile Forensics Tools and Techniques

Data acquisition is the process of gathering information from mobile devices and their associated media. This process reduces the chances of data loss due to damage or battery depletion during storage and transportation. Mobile device identification is necessary at the beginning of the forensic examination. The identification process includes understanding of the type of cell phone, its OS, and other essential characteristics to create a legal copy of the mobile device's content.

There are many tools and techniques available in mobile forensics. However, the selection of tools and techniques during an investigation depends on the type of mobile device and its associated media.

Gather Data from Mobile Devices

The data can be gathered from mobile devices in two ways, namely, physical acquisition and logical acquisition.

Physical Acquisition, also known as a physical memory dump, is a technique for capturing all the data from flash memory chips on the mobile device. It allows the forensic tool to collect remnants of deleted data. Initially, the received data is in raw format and cannot be read. Later on, some methods are applied to convert that data into a human readable form.

Logical Acquisition, or logical extraction, is a technique for extracting the files and folders without any of the deleted data from a mobile device. However, some vendors describe logical extraction narrowly as the ability to gather a particular data type, such as pictures, call history, text messages, calendar, videos, and ringtones. A software tool is used to make a copy of the files. For example, iTunes backup is used to make a logical image of an iPhone or iPad.

Data Types Can Collect from a Mobile Device

Students should understand data types before the collection of data from a mobile device. The common data types include contacts list, call log, SMS, images, audio, video, GPS data, and apps data. Also, both current and deleted data types can be extracted from a mobile device.

Call Detail Records (CDRs): Service providers frequently use CDRs to improve network performance. However, they can provide useful information to investigators, as well. CDRs can show:

- Call started and ended date/time
- The terminating and originating towers
- Whether the call was outgoing or incoming
- Call time duration
- Who was called and who made the call

Almost all service providers retain these important records for a certain time. The forensic specialist can collect these records if he requires. However, the collection of this information depends on the policies of the concerned state. Every state has different laws in this regard.

Global Positioning System (GPS): GPS data is an excellent source of empirical evidence. If the suspect has an active mobile device at the crime scene, GPS can pinpoint his location as well as his criminal acts. GPS also locates the movements of the suspect from a crime scene to the hideout. Furthermore, it helps in finding phone call logs, images, and SMS messages. Presently, a GPS system includes 27 satellites in operation.

App Data: Many apps store and access data the user is not aware of. In fact, many apps seek permission during the installation process to access these data. For example, photo or video editing

apps request permission to access media files, camera, and GPS for navigation. This data can be a primary source of evidence to the court.

SMS: Text messaging is a widely used way of communication. Text messages leave electronic records of dialogue that can be presented in the court as evidence. They include the relevant information such as:

- Date/time of each message
- Phone number of sender and receiver

Photos and Videos as Evidence: They can be a tremendous source of evidence, but their relevance to crime and authentication is crucial.

Tools & Techniques Used in Mobile Forensics

Forensic software tools are continually developing new techniques for the extraction of data from several cellular devices. The two most common techniques are physical and logical extraction. Physical extraction is done through JTAG or cable connection, whereas logical extraction occurs via Bluetooth, infrared, or cable connection.

There are various types of tools available for mobile forensic purposes. They can be categorized as open source, commercial, and non-forensic tools. Both non-forensic and forensic tools frequently use the same techniques and protocols to interact with a mobile device.

Tools Classification System: Forensic analysts must understand the several types of forensic tools. The tools classification system offers a framework for forensic analysts to compare the acquisition techniques used by different forensic tools to capture data. Figure 1 shows the system:

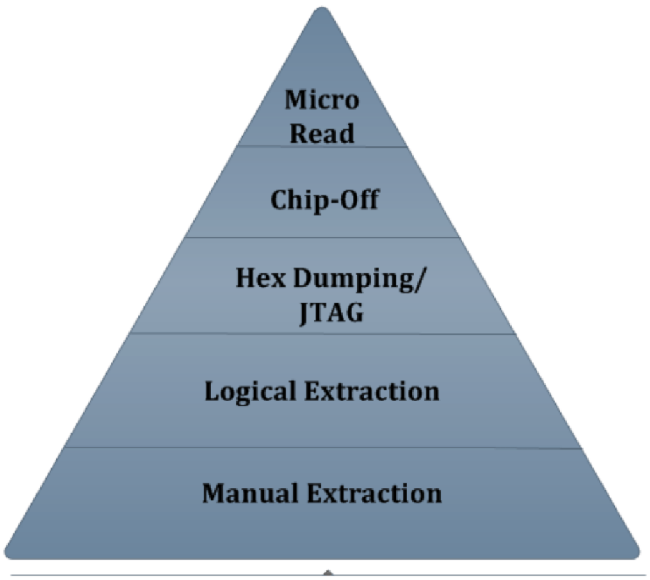


Figure 1: Mobile Device Tool Classification System

Manual Extraction

The manual extraction technique allows investigators to extract and view data through the device's touchscreen or keypad. At a later stage, this data is documented photographically. Furthermore, manual extraction is time-consuming and involves a great probability of human error. For example, the data may be accidentally deleted or modified during the examination.

Popular tools for manual extractions include:

- Project-A-Phone
- Fernico ZRT
- EDEC Eclipse

Logical Extraction

In this technique, the investigators connect the cellular device to a forensic workstation or hardware via Bluetooth, Infrared, RJ-45 cable, or USB cable. The computer—using a logical extraction tool—sends a series of commands to the mobile device. As a result, the required data is collected from the phone's memory and sent back to the forensic workstation for analysis purposes. The tools used for logical extraction include:

- XRY Logical
- Oxygen Forensic Suite
- Lantern

Hex Dump

A hex dump, also called physical extraction, extracts the raw image in binary format from the mobile device. The forensic specialist connects the device to a forensic workstation and pushes the boot-loader into the device, which instructs the device to dump its memory to the computer. This process is cost-effective and supplies more information to the investigators, including the recovery of phone's deleted files and unallocated space. The common tools used for hex dump include:

- XACT
- Cellebrite UFED Physical Analyzer
- Pandora's Box

Chip-Off

The chip-off technique allows the examiners to extract data directly from the flash memory of the cellular device. They remove the phone's memory chip and create its binary image. This process is costly and requires an ample knowledge of hardware. Improper handling may cause physical damage to the chip and renders the data impossible to retrieve. The popular tools and equipment used for chip-off include:

- iSeasamo Phone Opening Tool
- Xytronic 988D Solder Rework Station
- FEITA Digital inspection station
- Chip Epoxy Glue Remover
- Circuit Board Holder

Micro Read

This process involves interpreting and viewing data on memory chips. The investigators use a high-powered electron microscope to analyze the physical gates on the chips and then convert the gate level into 1's and 0's to discover the resulting ASCII code. This process is expensive and time-consuming. Also, it requires an ample knowledge of hardware and file systems. There is no tool available for micro read.

CALL DETAIL RECORD (CDR) AND ANALYSIS

सीडीआर विवरण कई विविध उद्देश्यों की पूर्ति कर सकता है। इसका प्रयोग प्रवर्तन एजेंसियों द्वारा किसी विशेष मामले को सुलझाने के लिए, अदालत में सबूत के रूप में, व्यक्तिगत उपयोग के लिए, आवश्यक जानकारी का ट्रैक रखने के लिए, लापता व्यक्तियों को ट्रेस करने के लिए, खोए या चोरी हुए मोबाइल फोन आदि को पुनः प्राप्त के लिए किया जाता है। वर्षों से सीडीआर विवरणों के कानूनी निष्कर्षण ने कई मामलों को सुलझाने में मदद की है।

बिजनेस स्टैंडर्ड के अनुसार, हिमाचल प्रदेश पुलिस की अपराध जांच प्रभाग (CID) शाखा ने मोबाइल फोरेंसिक सहायता के माध्यम से एक वर्ष में 203 मामलों को हल किया। इसमें CDR (कॉल डिटेल रिकॉर्ड्स), IMEI (इंटरनेशनल मोबाइल इक्विपमेंट आइडेंटिटी), टॉवर लोकेशन, CAF (कस्टमर एप्लिकेशन फॉर्म) आदि जैसे डेटा शामिल हैं, CID की उक्त शाखा की तकनीकी सेल की रिपोर्ट है कि इसे जांच एजेंटों से एक दिन में लगभग 100 अनुरोध मिलते हैं और 12 घंटे के भीतर आवश्यक जानकारी प्रदान कर देते है, क्योंकि वे तुरंत अनुरोध दूरसंचार कंपनियों को आगे बढ़ाते हैं। इससे हमें अनुमान लगाता है कि उपयुक्त एजेंसियों के माध्यम से कॉल विवरण रिकॉर्ड को प्राप्त करने के लिए 12 घंटे से अधिक नहीं है।

सीडीआर कब तक स्टोर किया जाता है

टेलीकॉम कंपनियों द्वारा कॉल डेटा को 6 महीने की अवधि के लिए सरकारी दिशानिर्देशों के अनुसार संग्रहित किया जाता है। डेटा की उच्च भंडारण लागत के कारण (लगभग प्रति वर्ष कई पेटाबाइट्स के लिए, टेलीकॉम कंपनियां केवल सीमित मात्रा में डेटा स्टोर करने का विकल्प चुनती हैं, जो छह महीने या एक वर्ष है और बाकी को टेप पर संग्रहीत करके रख लिया जाता है। इन अभिलेखों को उन स्थितियों को छोड़कर आसानी से प्राप्त नहीं किया जा सकता है जहां सरकारी दबाव है, उदाहरण के लिए, उच्च प्रोफ़ाइल मामलों या उन मामलों में जिनमें राष्ट्रीय सुरक्षा के लिए तत्काल खतरा है।

Unified Access Services License (UASL)

वर्तमान में भारत में 22 सेवा क्षेत्र हैं, जिन्हें 4 महानगरों में वर्गीकृत किया गया है: ए, बी, सी, डी। दिल्ली, मुंबई, कोलकाता और चेन्नई चार महानगर हैं। भारत में चार वायरलेस नेटवर्क हैं:

1. एयरटेल इंडिया
2. रिलायंस (Jio)
3. वोडाफोन + आइडिया (विलय)
4. बीएसएनएल + एमटीएनएल

पहले तीन निजी स्वामित्व में हैं, जबकि चौथा राज्य का स्वामित्व है। ये सभी लाइसेंस प्राप्त ऑपरेटर हैं और अपने राजस्व शेयर के आधार पर कुछ लाइसेंस शुल्क का भुगतान करते है। लाइसेंस समझौते के अनुसार, ये सेलुलर ऑपरेटर जब तक प्रासंगिक ITU (अंतर्राष्ट्रीय दूरसंचार मानक) को पूरा करते हैं, तब तक कई मोबाइल सेवाएँ प्रदान कर सकते हैं जैसे वॉयस मैसेज, नॉन वॉयस मैसेज, डेटा सर्विसेज आदि।

लाइसेंस समझौते के के अनुसार, "भारत में संचालित नेटवर्क से संबंधित रिमोट एक्सेस गतिविधियों का पूरा ऑडिट ट्रेल छह महीने की अवधि के लिए बनाए रखा जाना चाहिए और लाइसेंसकर्ता या किसी अन्य एजेंसी द्वारा अनुरोध पर प्रदान किया जाना चाहिए।"

इस लाइसेंस समझौते के अनुसार, उपरोक्त सेवा प्रदाताओं को दूरसंचार यातायात की निगरानी के लिए आवश्यक व्यवस्था करने और राज्य या केंद्र सरकार को इससे संबंधित सभी आंकड़ों को प्रकट करने की

आवश्यकता है। क्लॉज में निर्दिष्ट आवश्यकता सात सुरक्षा एजेंसियों के लिए कम से कम 210 कॉल की एक साथ निर्बाध निगरानी की है। इसके साथ ही, निम्नलिखित डेटा को भी बनाए रखना आवश्यक है:

- दोनों पक्षों के मोबाइल नंबर / पीएसटीएन नंबर (कॉलर और रिसीवर)
- समय, तिथि और अवरोधन(interception) की अवधि
- Target Subscriber की लोकेशन (सेल आईडी के साथ)
- कॉल.फ़ॉरवर्डिंग के मामले में टेलीफोन नंबर जिस पर सक्रिय है
- असफल कॉल प्रयासों के डेटा रिकॉर्ड
- रोमिंग ग्राहक की सीडीआर

कंपनियों को किसी भी एक दिये गये समय के लिये, नेटवर्क के उपयोगकर्ता के सटीक भौगोलिक स्थान (बीटीएस लोकेशन) की जानकारी भी प्रदान करने की आवश्यकता होती है ।

यह जानकारी एक पीडित पार्टी के लिए उपयोग की जा सकती है क्योंकि कभी.कभी एक सेवा प्रदाता एक निश्चित अवधि के सीडीआर की आपूर्ति करने से इनकार कर सकता है, क्योंकि यह बहुत पुरानी या प्राप्त होने लायक नहीं हो। ऐसे मामलों में सेवा प्रदाता से पूछताछ की जा सकती है और लाइसेंस समझौते को संदर्भित किया जा सकता है।

कौन अधिकारी सीडीआर निकाल सकते हैं-

प्रारंभ में, अधिकांश कानून प्रवर्तन एजेंसियां सीडीआर निकाल सकती थीं। इनमें से कुछ थे:

- एसीपी (अतिरिक्त पुलिस आयुक्त)
- डीसीपी (पुलिस उपायुक्त)
- CID (अपराध जांच विभाग)
- सीबीआई (केंद्रीय जांच ब्यूरो)
- एनआईए (राष्ट्रीय जांच एजेंसी)
- एटीएस (आतंकवाद विरोधी दस्ते)
- सेबी (भारतीय प्रतिभूति और विनिमय बोर्ड)
- आईटीडी (आयकर विभाग), आदि।

लेकिन सरकार ने सीडीआर के निष्कर्षण के बारे में दिशानिर्देशों को फिर से जारी किया है। नए दिशानिर्देशों के अनुसार, **पुलिस अधीक्षक** से कम रैंक वाला कोई भी अधिकारी दूरसंचार कंपनियों से सीडीआर प्राप्त नहीं कर सकता है।

संशोधित दिशा निर्देश हैं:

- सबसे पहले, जैसा कि ऊपर उल्लेख किया गया है, सीडीआर विवरण किसी भी अधिकारी द्वारा एसपी से कम रैंक के साथ एक्सेस नहीं किया जा सकता है।
- संबंधित अधिकारी को प्राप्त रिकॉर्ड की एक निर्देशिका बनाने और उसे हर महीने जिला मजिस्ट्रेट को प्रस्तुत करने की आवश्यकता होती है।
- डीएम को संबंधित मुख्य सचिव को विवरण भेजने की आवश्यकता होती है ताकि एक राज्य-व्यापी रिकॉर्ड को प्रभावी ढंग से बनाए रखा जा सके।

तदनुसार, प्रत्येक अतिरिक्त पुलिस आयुक्त (एसीपी) या जिले के पुलिस उपायुक्त (डीसीपी), अपराध शाखा, आर्थिक विंग, विशेष सेल, आईजी एयरपोर्ट एसीपी और विशेष सेल, अपराध शाखा को सीडीआर प्राप्त करने के लिए अधिकृत किया गया है।

सीडीआर निकालने की प्रक्रिया में कितना समय लगता है?

हालांकि इस बात का कोई नियम नहीं है कि कंपनियों को डेटा कितनी तेजी से देना चाहिए, जैसा कि ऊपर बताया गया है, अगर मामला अत्यावश्यक है, यानी अपराध या आतंकवादी गतिविधि जैसे गंभीर मुद्दे से संबंधित है, और जानकारी की मांग की गई है एक प्रासंगिक प्राधिकरण, सूचना दूरसंचार कंपनियों द्वारा कुछ घंटों में दी जाती है। अन्यथा, यह कई सप्ताह भी हो सकता है।

सीडीआर एक साक्ष्य के रूप में –

सीडीआर अदालत में द्वितीयक साक्ष्य के रूप में स्वीकार्य है। प्रौद्योगिकी के विकास के साथ, अदालतें इन दिनों सबूत के रूप में विभिन्न इलेक्ट्रॉनिक और डिजिटल डेटा की अधिक ग्रहणशील हैं। इससे पहले, सीडीआर के लिए भारतीय साक्ष्य अधिनियम, 1872 की धारा 65 बी (4) के तहत निर्धारित प्रमाणपत्र के साथ होना आवश्यक था। हाल ही में, अधिनियम की धारा 65 बी की व्याख्या करते हुए, सर्वोच्च न्यायालय ने फैसला किया है कि न्याय के हित में ऐसा कोई प्रमाण पत्र प्रस्तुत करना अनिवार्य नहीं है। इसके अलावा, अगर इस तरह के प्रमाण पत्र की अदालत द्वारा पूरी तरह से आवश्यकता होती है, तो इसे चार्जशीट दाखिल होने के बाद प्रस्तुत किया जा सकता है।

CDR DATA AND ANALYSIS

कॉल डेटा रिकॉर्ड (सीडीआर) एसएमएस और कॉल का एक विस्तृत रिकॉर्ड है जो किसी सेवा प्रदाता के ग्राहक द्वारा भेजा और प्राप्त किया जाता है। यह वो सारी जानकारी प्रदान करता है जो किसी संदिग्ध की दिन की स्थिति, रात का स्थान, हैंडसेट का विवरण, अधिकतम संपर्क नंबर, तिथि, समय, टॉवर स्थान आदि की पहचान करने में मदद कर सकता है।

निम्नलिखित विवरण एमएसपी से प्राप्त किया जा सकता है-

- कॉल डिटेल रिकॉर्ड (CDR)
- सबस्क्राइबर डिटेल रिकॉर्ड (SDR)
- ग्राहक आवेदन पत्र (CAF)

CDR formats

- Text (plain text)
- Html (hypertext markup Lang)
- .xls (Excel file format)
- .csv (comma-separated value)- flat file
- .pdf (portable document format)

ऊपर उल्लेखित प्रारूप बहुत असंगत हैं क्योंकि किसी भी सेवा प्रदाता के पास कोई दिशानिर्देश नहीं है कि किस प्रारूप में अनुरोधकर्ता को दिया जाना है। ये सभी प्रारूप सेवा प्रदाताओं द्वारा सिस्टम द्वारा ऑटो-जनरेट किए जाते हैं और इन्हें उस विशेष मोबाइल सेवा प्रदाता (MSP) की नोडल एजेंसी / अधिकारी द्वारा ईमेल किया जा सकता है।

कई जांच डेटा हैं जो सेवा प्रदाता से प्राप्त किए जा सकते हैं जैसे:

- सेल फोन विवरण
- टॉवर जानकारी (TDR)
- लैंडलाइन कॉल विवरण
- अंतर्राष्ट्रीय कॉल विवरण (गेटवे के माध्यम से कॉल रूट)
- सदस्य का विवरण
- सेल फोन फोरेंसिक उपकरण
- सिम कार्ड डेटा निष्कर्षण
- टेलीफोन अवरोधन रिकॉर्ड

CDR FORMAT -

Calling (A) Party	Called (B) Party	Date	Time	Duration	First Cell ID	Last Cell ID	Call Type	IMEI	IMSI
919819194961	919920641598	27-08-2014	06:52:59	900	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	919920641598	27 08 2014	07:14:57	356	404 20 11 34273	404 20 11 34273	Call Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	08:47:13	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	09:49:01	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27 08 2014	13:15:45	0	404 20 11 34273	N/A	SMS In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:15:53	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:15:57	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:17:54	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:29:06	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:33:38	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	LM-HDFCSL	27-08-2014	19:33:33	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	918692842502	27-08-2014	20:00:52	92	404-20-11-34271	404-20-11-34271	Call-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	20:08:21				SMS-Out	911240902779740	40420305264
919819194961	919920641598	27-08-2014	21:09:20			1	Call-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	21:13:09		0 404-20-11-30021	N/A	SMS-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	21:13:34		0 404-20-11-37591	N/A	SMS-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	21:23:53		0 404-20-11-37591	N/A	SMS-Out	911240902779740	40420305264
919819194961	307691970262759 0	27-08-2014	21:24:38	269	404-20-11-37591	404-20-11-30021	Call-Out	911240902779740	40420305264
919819194961	9950467770	27-08-2014	21:35:10	10	404-20-11-30021	404-20-11-30021	Call-Out	911240902779740	40420305264
919819194961	919221209134	27 08 2014	21:36:09	82	404 20 11 37591	404 20 11 30021	Call Out	911240902779740	40420305264
919819194961	919702627596	27 08 2014	21:47:44	189	404 20 11 37591	404 20 11 30021	Call In	911240902779740	40420305264
919819194961	919702627596	27-08-2014	22:19:50	66	404-20-11-30252	404-20-11-33441	Call-In	911240902779740	40420305264
919819194961	7738015760	27-08-2014	22:21:53	51	404-20-11-30252	404-20-11-30252	Call-Out	911240902779740	40420305264
919819194961	919702724492	27 08 2014	22:35:25	22	404 20 11 34271	404 20 11 34274	Call In	911240902779740	40420305264
919819194961	919221919141	27-08-2014	22:45:49	8	404-20-11-34271	404-20-11-34271	Call-In	911240902779740	40420305264
919819194961	919920641598	27-08-2014	23:01:51	24	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	307691860284250 0	27 08 2014	23:10:42	34	404 20 11 34271	404 20 11 34271	Call Out	911240902779740	40420305264
919819194961	307691860284250 0	27-08-2014	23:13:21	125	404-20-11-34272	404-20-11-34271	Call-Out	911240902779740	40420305264
919819194961	307691970262759 0	27-08-2014	23:14:23	10	404-20-11-34272	404-20-11-34271	Call-Out	911240902779740	40420305264
919819194961	307691970262759 0	27 08 2014	23:15:01	79	404 20 11 34272	404 20 11 34271	Call Out	911240902779740	40420305264

Normal CDR

Total colums:-	Words Shown In CDR
CALLING PARTY NO CALLED PARTY NO START DATE CALL TIME BILL DURATION FIRST_CELL_ID LAST_CELL_ID CALL DIRECTION ESN_or_IMEI_NO MIN_or_IMSI_NO TYPE OF CONNECTION SMS CENTRE ROAMING DETAILS BTS_ADDRESS	MO = Outgoing, MT = Incoming, SO = SMS Out, ST = SMS In, CF = Call Forwarding, PP = Prepaid, PO = Postpaid, N/A = Not Available in CDR, 2G:- 2G-Voice Call 2G-SMS, 3G:- 3G-Voice Call 3G-SMS, 3GV:- 3G-Video Call

Calling (A) Party	Called (B) Party	Date	Time	Duration	First Cell ID	Last Cell ID	Call Type	IMEI	IMSI
919819194961	919920641598	27-08-2014	06:52:53	900	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	919920641598	27-08-2014	07:14:57	356	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	08:47:13	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	08:49:01	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:15:45	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	13:15:53	0	404-20-11-34273	N/A	SMS-In	911240902779740	40420305264
9198					273	N/A	SMS-In	911240902779740	40420305264
9198					273	N/A	SMS-In	911240902779740	40420305264
9198					273	N/A	SMS-In	911240902779740	40420305264
9198					273	N/A	SMS-In	911240902779740	40420305264
9198					271	404-20-11-34271	Call-In	911240902779740	40420305264
919819194961	919867458394	27-08-2014	20:08:21	0	404-20-19-30293	N/A	SMS-Out	911240902779740	40420305264
919819194961	919920641598	27-08-2014	21:09:20	145	404-20-11-37591	404-20-11-30021	Call-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	21:13:09	0	404-20-11-30021	N/A	SMS-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	21:13:34	0	404-20-11-37591	N/A	SMS-Out	911240902779740	40420305264
919819194961	919867458394	27-08-2014	21:23:53	0	404-20-11-37591	N/A	SMS-Out	911240902779740	40420305264
919819194961	3076919702627590	27-08-2014	21:24:38	269	404-20-11-37591	404-20-11-30021	Call-Out	911240902779740	40420305264
919819194961	9930467773	27-08-2014	21:35:18	18	404-20-11-30021	404-20-11-30021	Call-Out	911240902779740	40420305264
919819194961	919221299134	27-08-2014	21:36:09	82	404-20-11-37591	404-20-11-30021	Call-Out	911240902779740	40420305264
919819194961	919702627596	27-08-2014	21:47:44	169	404-20-11-37591	404-20-11-30021	Call-In	911240902779740	40420305264
919819194961	919702627596	27-08-2014	22:19:58	66	404-20-11-30252	404-20-11-33441	Call-In	911240902779740	40420305264
919819194961	7738015750	27-08-2014	22:21:53	51	404-20-11-30252	404-20-11-30252	Call-Out	911240902779740	40420305264
919819194961	919702724492	27-08-2014	22:35:25	22	404-20-11-34271	404-20-11-34274	Call-In	911240902779740	40420305264
919819194961	919221919141	27-08-2014	22:45:49	8	404-20-11-34271	404-20-11-34271	Call-In	911240902779740	40420305264
919819194961	919920641598	27-08-2014	23:01:51	24	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	3076918692842500	27-08-2014	23:10:42	34	404-20-11-34271	404-20-11-34271	Call-Out	911240902779740	40420305264
919819194961	3076918692842500	27-08-2014	23:13:21	125	404-20-11-34272	404-20-11-34271	Call-Out	911240902779740	40420305264
919819194961	3076919702627590	27-08-2014	23:14:23	10	404-20-11-34272	404-20-11-34271	Call-Out	911240902779740	40420305264
919819194961	3076919702627590	27-08-2014	23:15:01	79	404-20-11-34272	404-20-11-34271	Call-Out	911240902779740	40420305264

Ending Tower Location Cell-ID or BTS

(Base Transceiver Station)

Calling (A) Party	Called (B) Party	Date	Time	Duration	First Cell ID	Last Cell ID	Call Type	IMEI	IMSI
919819194961	919920641598	27-08-2014	06:52:53	900	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	919920641598	27-08-2014	07:14:57	356	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	3076919702627590	27-08-2014	23:15:01	79	404-20-11-34272	404-20-11-34271	Call-Out	911240902779740	40420305264

404-20-11-34273

Cell ID (CID)

A **GSM Cell ID (CID)** is a generally unique number used to identify each **Base transceiver station (BTS)** or sector of a BTS within a Location area code (LAC) if not within a GSM network. The last digit of CID represents cells' **Sector ID**

Value 0 is used for omnidirectional antenna.
Value 1, 2, 3 are used to identify sectors of trisector or bisector antennas.

Calling (A) Party	Called (B) Party	Date	Time	Duration	First Cell ID	Last Cell ID	Call Type	IMEI	IMSI
919819194961	919920641598	27-08-2014	06:52:53	900	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	919920641598	27-08-2014	07:14:57	356	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264

404-20-11-34273

Mobile Network Code (MNC)

404-20 – Vodafone – Mumbai
404-05 – Vodafone – Gujarat

405-799 – Idea – Mumbai
405-24 – Idea – Gujarat

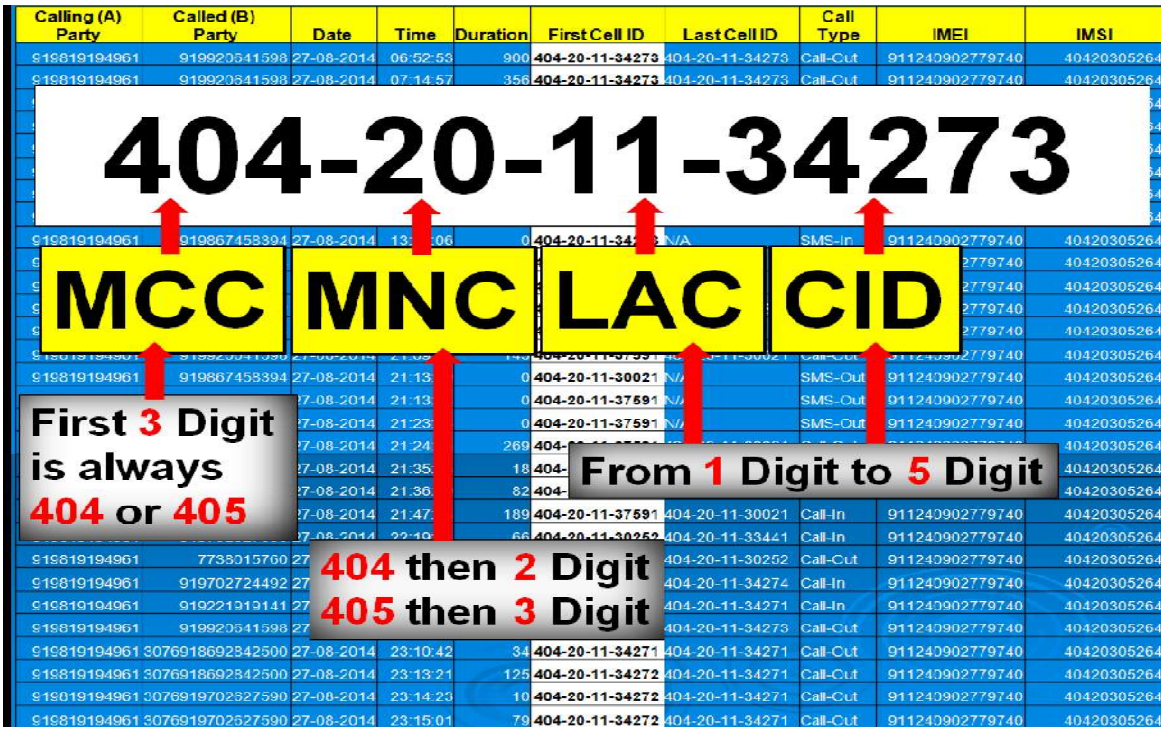
404-92 – Airtel – Mumbai
404-98 – Airtel – Gujarat

Calling (A) Party	Called (B) Party	Date	Time	Duration	First Cell ID	Last Cell ID	Call Type	IMEI	IMSI
919819194961	919920641598	27-08-2014	06:52:53	900	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264
919819194961	919920641598	27-08-2014	07:14:57	356	404-20-11-34273	404-20-11-34273	Call-Out	911240902779740	40420305264

404-20-11-34273

Location Area Code (LAC)

The served area of a cellular radio network is usually divided into location areas. Location areas are comprised of one or several radio cells. Each location area is given an unique number within the network, the Location Area Code (LAC). This code is used as a unique reference for the location of a mobile subscriber. This code is necessary to address the subscriber in the case of an incoming call.

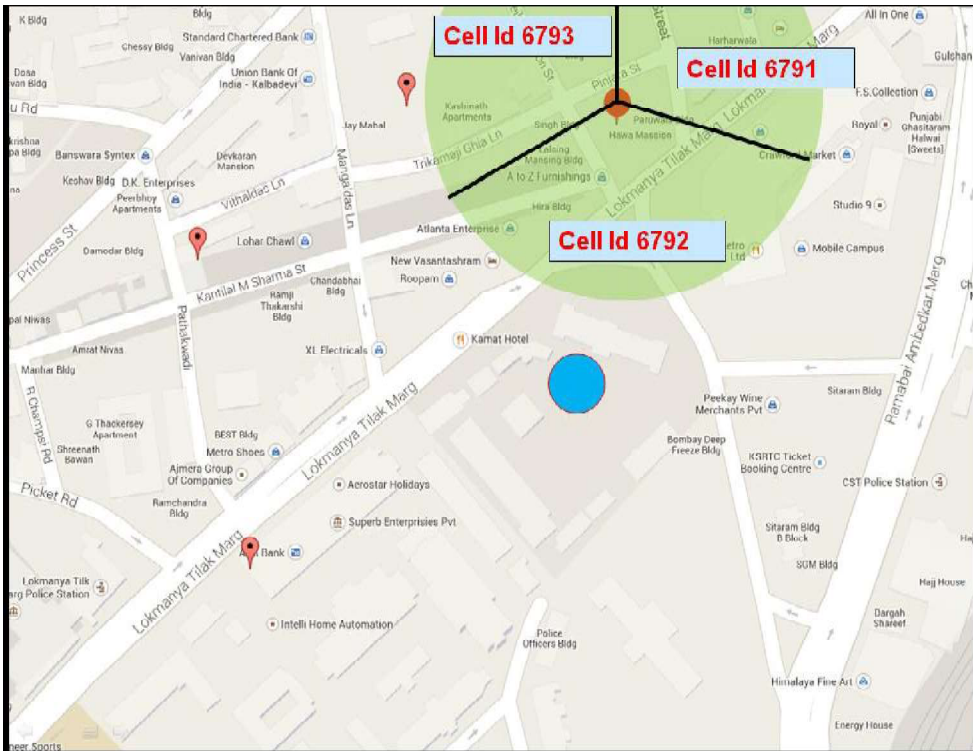


MCC (Mobile Country Code)

MNC (Mobile Network Code)

LAC (Location Area Code)

CID (Cell ID)



किसी भी मोबाईल कंपनी से निम्न विभिन्न प्रकार की सूचनाऐं मंगवाई जा सकती है–

CDR File

- Contains all the details corresponding to a particular mobile number for a fixed period.
- The details incorporated in this CDR file are
- cell number,
- call type whether the call is incoming, outgoing,
- whether the text message is sent, received,
- IMEI number,
- IMSI number,
- call date, call time, call duration,
- cell, cell last etc.

Tower CDR File

- Tower CDR File refer to call evidence document corresponding to any tower used by any mobile number
- Contains all the communication made using a particular tower.
- The details incorporated in this CDR file are
- Called number,
- Calling number,
- Call flow direction,
- Id of the tower,
- Duration etc

SDR File

- SDR(Subscriber Data Record) file contains different details of the subscriber or customer.
- Contains:
- Mobile Number,
- Permanent address,
- Present address,
- Customer name and other customer related details

Cell ID File

- Cell ID File is maintained by different service provider to hold the tower related information.
- The file contain information's like :
- Location of the different tower available,
- Latitude, Longitude,

- Address of the located tower,
- Tower ID in different formats like full CGI or part of the tower ID

NOTE:-

1- ALL INFORMATION/ RECORDS SHOULD BE OBTAINED THROUGH ISSUING A NOTICE U/S 91 Cr. P. C TO CONCERN AUTHORITY.

2- NOTICES TO ISP, MSP & SOCIAL SITES U/S 91 Cr. P. C. WILL BE ISSUED BY THE SIGNATURE OF DISTRICT SUPERINTENDENT OF POLICE/ CONCERN DCP.

3- NOTICES TO BANKS AND OTHER AUTHORITIES MAY BE ISSUED BY THE I.O/ S.H.O. OF CONCERN POLICE STATION.

ANNEXURES

	NAME OF WEBSITES	TYPE OF INFORMATION/ RECORDS
1	http://www.whatismyip.com/ http://ip-lookup.net/ http://www.iplocation.net/	Access about ISP of IP Address.
2	http://www.whoishostingthis.com/ https://www.whois.net/ http://www.ip2location.com	Search about the registration and profile details of a website.
3	http://www.indiatrace.com/ http://trace.bharatiyamobile.com/	Information about the name of mobile number`s company and their related state.
4	http://www.nobbi.com/imeicheck.php	It provides the name of mobile company & its model number from IMEI number of mobile phones.
5	Ipconfig/all	For MAC address of HDD.
6	https://shtuff.it/ http://hwaddress.com/	To know about the name of manufacture /Company MAC address.
7	http://www.ip-tracker.org/ http://www.cyberforensics.in/ http://www.iptrackeronline.com/	To get IP address from email header.

IMPORTANT MAIL ADDRESSES OF ISP, MSP, PAYMENT GATEWAY AND OTHERS.

S.NO.	Name	E-mail Addresses
1	Facebook	records@fb.com
2	Yahoo	In-legalpoc@yahoo-inc.com
3	Google/Gmail	Lis-apac@google.com
4	Rediff Mail	legal@rediff.com
5	Microsoft	leportal@microsoft.com
6	Bill Desk	nrevani@billdek.com support@billdesk.com
7	Mobikwik	partners@mobikwik.com
8	EBay India	inathani@ebay.com
9	Flip kart	sachin@flipkart.com
10	Snap deal	Id=info@snapdeal.com Id=help@snapdeal.com
11	Pay tm	care@paytm.com info@customercarenumber.co.in
12	Aircel	Rajasthan.nodeldesk@aircel.co.in
13	Airtel	Rajcircle.nodelofficer@in.airtel.com
14	BSNL	Bsnl_mou@yahoo.co.in
15	Idea	Inodel.raj@idea.adityabirla.com
16	Vodafone	Nodeldd.rajasthan@vodafone.com
17	Reliance	Vinay.k.sharma@relianceada.com
18	MTS	Rajcircle.nodelofficer@mtsindia.in
19	TATA	Securitywing.rajasthan@tatatel.co.in

SAMPLE OF A NOTICE U/S 91 CrPC

Office of Dy. Superintendent of Police,
Cyber Crime Police Station, Jaipur, Rajasthan (India)

No. Date :-

Notice u/sec. 91 of Cr.P.C.

To,

The Manger (IT)
Tata Internet Services,
India.

Whereas, a criminal case has been registered at…… Police Station on----------, vide F.I.R. No…….. u/sec. in which investigation is being carried out by the undersigned.

Whereas, I have reasons to believe that the following documents and information, are your custody, and are required for investigation of the aforesaid case, you are directed to produce the following documents and provide information on following points, on or before----------, either in person or through your representative with the print-outs related to following information which are certified and the soft copy which is properly sealed.

1- *All identifying particulars related to your Internet Access subscriber who was allocated the following I.P. Addresses on the date and time mentioned each of them*
1. *I.P. Address*
2. *Date*
3. *Time*

2- *All the Internet access logs related to the above I.P. Address allocation on the date and time mentioned against each of them*

SIGNATURE WITH SEAL OF
INVESTIGATION OFFICER

Provisions of 91 Criminal Procedure Code :-

91. Summons to produce document or other thing.-

(l) Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it. or to produce it. at the time and place stated in the summons or order.

(2) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document 01' thing to be produced instead of attending personally to produce the same.

Annexure 5-8: Sample Letter to the Service Provider

From: Name of the Investigating Officer or Supervisory Officer (Police Inspector or above) Provide Full address, phone number and Official Mail ID.		Place Date

NOTICE UNDER SECTION 91 CrPC

To,

The Manager
ABC Company
ISP Division, Mumbai.

Sub: Request to furnish the details about the IP address.
Ref: Crime Number: xxxxxxxxxx u/s xxxxxxxxx of ITAA2008 of xxxxxxxx Police Station, xxxxxxxx City / District

With reference to the above cited subject, the undersigned is investigating officer of the criminal case mentioned above. For the purposes of investigation, details of the subscriber and his/her physical address details are required as per below mentioned IP addresses.

203.94.218.220 on 07 Feb 2008 at 05:01:24 pm GMT (22:31:24 in IST)

Please treat the matter as most urgent.

Official Seal	(Signature of the Investigating Officer or Supervisory Officer Demanding Information)

Annexure 5-6: FSL Requisition-Information to be Furnished

Information needs to be furnished to forensic examiner and request for specific information based on the type of crime:

- Questions and information common to most of the cases/incidents
  - Brief facts of the case
  - Details/description of the objects
  - Date and time of collection of the objects
  - Status of the objects when collected (powered on and powered off)
  - Seized from – person, organization, location, etc.
  - Seized by – person and organization
  - Please recover all the deleted folders and files from the system
  - Please provide the list of all files and folders from the system
- Questions to be asked in case of "Computer as a target" cyber crime
  - What type of operating system has been installed in the computer?
  - When was the operating system installed?
  - Please provide the user names/users present in the system
  - What programs or software is installed in the computer?
  - What is the IP address assigned to the system, if any?
  - What is the MAC address of the system?
  - Are there any information relating e-mail addresses present in the computer system?
  - Are there any chat messenger software installed. If so, are there any chat IDs/profiles?
  - Any suspicious or malicious software installed?
  - Please provide the Internet history of the computer (Web sites accessed, files uploaded, downloaded, etc.)?
  - Are there any firewall logs available in the system?
- Questions to be asked in case of "sending threatening e-mail"
  - Whether sender's e-mail address is present in the seized hard disk.
  - Whether receiver's e-mail address is present in the seized hard disk.
  - Whether the contents of the e-mail message (subject mail of case) is present in the hard disk.
  - Any information relating to the IP addresses are available?
- Questions to be asked in case of "Creation of obscene profile/hosting of obscene videos"
  - Whether the obscene information (subject in the case) is present in the seized hard disk
  - Whether any e-mail ID relating to the hosting of the obscene profile is present
- Questions to be asked in case of "Computer as an Instrument/Repository"
  - What is the operating system of the computer?
  - Which are the user accounts that are present in the computer?
  - What financial applications/software applications are installed in the system?
  - Are there any logs available for these applications?
  - Please provide the list of files/filenames that were recently accessed
  - What external devices (like thumb drives/external hard drives) were connected to the computer?
  - Are there any databases and excel spread sheets available in active or deleted state?
  - Are there any accounting packages/software installed?
  - Are there any encrypted or password-protected files available? If so, please extract the content from them?
  - Are there any pornographic images/videos present in the computer system?
  - Was the system date and time changed at any point of time?

GUIDELINES TO PREPARE CHARGE SHEET

- All the relevant information shared by the complainants during registering the FIR/course of investigation should be included in the charge sheet.
- Please make sure the sections mentioned in FIR are still applicable for the case or it advised to file a requisition to change of sections before the case including appropriate ITAA 2008 and other supportive IPC, special and local laws. (there are number of incidents, IO filling the charge sheet under wrong sections of IT Act)
- Make sure the search and seizure procedure along with chain of custody and DEC form are included in the charge sheet.
- Make sure the nature of cyber crime and the necessary information/analysis requested from FSL or forensic examiner are incorporated properly in charge sheet.
- Please provide the detailed information about the crime scene and the process IO followed to identify the systems used/ affected in the crime.
- Please include all the technical persons who identified, produced and analyzed the digital in the case as witness.
- Please include the incidents occurred in the chronological order of time to establish the crime along with findings.
- Please burn (store/Image) on the digital evidence collected during the investigation in a blank CD-R.
- Please create separate list of digital evidence in a CD. That will be presented exhibits having list of all digital evidences in chronological order at submitted along with charge sheet.
- Do not forget to mention FIR number and charge sheet number on CD and other hardware seized during investigation.

This document was created with the Win2PDF “print to PDF” printer available at
http://www.win2pdf.com

This version of Win2PDF 10 is for evaluation and non-commercial use only.

This page will not be added after purchasing Win2PDF.

http://www.win2pdf.com/purchase/