भारतीय संस्कृति, शिक्षा और दर्शन

विभिन्न संकल्पनाएं

सम्पादक : डॉ. दिनेश चन्द्र शर्मा

भारतीय संस्कृति, शिक्षा और दर्शन

विभिन्न संकल्पनाएँ

सम्पादक :

डॉ. दिनेश चंद्र शर्मा

Ph.D., D.Lit. (Sub.)

निदेशक, कॉम्पिटिशन प्लस ग्रुप ऑफ इन्स्टीट्यूशन,
अजमेर

Books n Books

51/1509, आचमन, वेदविहार,
लोहाखान, अजमेर-305001

प्रकाशक :
पुष्पा शर्मा
Books n Books
51/1509, आचमन, वेदविहार,
लोहाखान, अजमेर-305001
ई-मेल : bnbajmer@gmail.com

संस्करण
प्रथम 2025

ISBN : 978 - 81 - 993854 - 7 - 4

मूल्य - 300/-

रचना -
भारतीय संस्कृति, शिक्षा और दर्शन विभिन्न संकल्पनाएँ

सम्पादक -
डॉ. दिनेश चंद्र शर्मा

आवरण -
श्रीनिवास प्रिन्टोग्राफिक्स, अजमेर

मुद्रक -
श्री श्याम ऑफसेट, किशनगढ़

Cyber Security

Gourav Palasia
Assistant Professor (Deptt. of Science and Technology)
Hukumchand Noble Institute of Science and Technology

Cyber Security Introduction : Cyber Security सबसे अधिक चिंतित मामला है क्योंकि साइबर खतरे और हमले बढ़ रहे हैं। सिस्टम को लक्षित करने के लिए हमलावर अब अधिक परिष्कृत तकनीकों का उपयोग कर रहे हैं। व्यक्ति, छोटे पैमाने के व्यवसाय या बड़े संगठन, सभी प्रभावित हो रहे हैं तो ये सभी फर्में चाहे आईटी या गैर-आईटी फर्मों ने साइबर सुरक्षा के महत्व को समझा है और अपनाने पर ध्यान केंद्रित किया है साइबर खतरों से निपटने के लिए हर संभव उपाय करें।

What is cyber security?

''साइबर सुरक्षा मुख्य रूप से लोगों, प्रक्रियाओं और प्रौद्योगिकियों के बारे में है जो एक साथ काम कर रहे हैं खतरे में कमी, भेद्यता में कमी, निरोध की पूरी श्रृंखला को शामिल करें, अंतर्राष्ट्रीय संगठन, घटना प्रतिक्रिया, लचीलापन, और पुनर्प्राप्ति नीतियां और गतिविधियां, जिनमें शामिल हैं कंप्यूटर नेटवर्क संचालन, सूचना आश्वासन, कानून प्रवर्तन, आदि।''

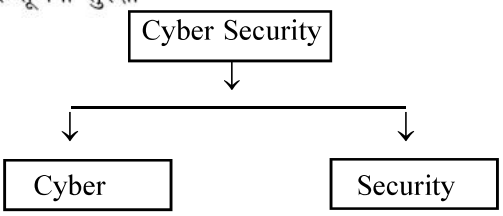
- साइबर सुरक्षा सुरक्षा के लिए डिजाइन की गई तकनीकों, प्रक्रियाओं और प्रथाओं का निकाय है नेटवर्क, कंप्यूटर, प्रोग्राम और डेटा हमले, क्षति या अनधिकृत पहुंच से।
- साइबर सुरक्षा शब्द डिजिटल की सुरक्षा के लिए डिजाइन की गई तकनीकों और प्रथाओं की जानकारी संदर्भित करता है।
- डेटा जो एक सूचना प्रणाली पर संग्रहीत, प्रेषित या उपयोग किया जाता है।

साइबर सुरक्षा इंटरनेट से जुड़े सिस्टम की सुरक्षा है, जिसमें हार्डवेयर, सॉफ्टवेयर और साइबर हमलों से डेटा। यह दो शब्दों से मिलकर बना है एक साइबर और दूसरा सुरक्षा।

साइबर उस तकनीक से संबंधित है जिसमें सिस्टम, नेटवर्क और प्रोग्राम शामिल हैं या जानकारी।

जबकि सुरक्षा से संबंधित सुरक्षा जिसमें सिस्टम सुरक्षा, नेटवर्क शामिल है सुरक्षा

और आवेदन और सूचना सुरक्षा



- Computer System
- Network
- Programs x Data

- System Security
- Network Security
- Program x Data Security

Needs of Cyber Security :-

- To protect private data.
- To protect intellectual data.
- To protect banking x finance data.
- National Security.
- Global Economy.
- Protect Sensitive data.

History of Cyber Security :-

1. 1969 UCLA के प्रोफेसर ने Standard Research Institute को संदेश (Message) भेजा।

2. 1970 रॉबर्ट ने पहला वायरस नाम "CREPER" बनाया।

3. 1986 रूसियों ने साइबर शक्ति को हथियार के रूप में इस्तेमाल किया।

4. 1988 अमेरिकी वैज्ञानिक ने इंटरनेट के आकार (Size) की जांच के लिए प्रोग्राम बनाया।

Cyber Security Goals:- (CIA) : C = Confidentiality
I = Integrity
A = Availability

Confidentiality : Confidentiality Unauthorized person को डेटा के प्रकटीकरण (Disclosure) को रोकने के बारे में है।

इसका मतलब Data को साझा करने और रखने में शामिल nauthorized person की पहचान को निजी (Private) और गुमनाम (Anonymous) रखने की कोशिश करना भी है। अक्सर खराब Encrypted Data , Man-In-Middle (MITM) Attacks, Sensitive Data का खुलासा करके Confidentiality से समझौता किया जाता है।

Confidentiality स्थापित करने के Standard Measures में शामिल हैं:

• Data encryption
• Two-factor authentication
• Biometric verification
• Security tokens

Integrity :- Integrity से तात्पर्य सूचना को Nauthorized Person द्वारा Modified किए जाने से बचाने से है।

Integrity की गारंटी के लिए Standard Measures में शामिल हैं:

• क्रिप्टोग्राफिक चेकसम (Cryptographic Checksums)
• Using file permissions (फाइल अनुमतियों का उपयोग करना)
• निर्बाध बिजली आपूर्ति (Uninterrupted Power Supplies)
• डेटा बैकअप (Data Backups)

Availability :- Availability सुनिश्चित कर रही है कि Nauthorized Person जरूरत पड़ने पर Information तक पहुंचने में सक्षम हैं।

Availability की गारंटी के लिए Standard Measures में शामिल हैं :-

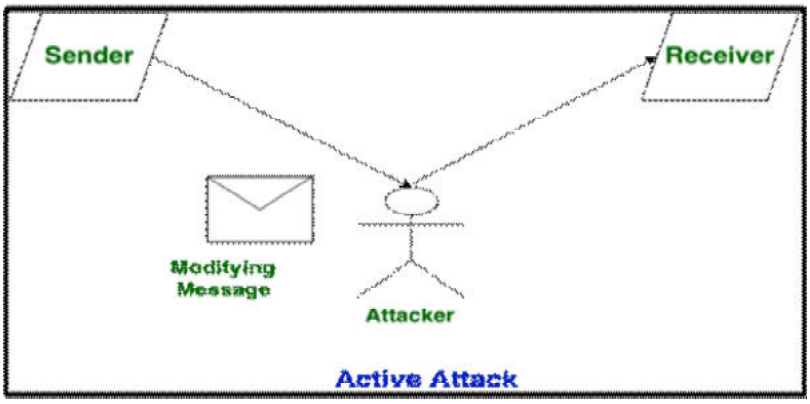
• Backing up data to external drives
• Implementing firewalls
• Having backup power supplies
• Data redundancy

Attack :- Cyber Attack Damage पहुंचाने के इरादे (intent) से computer, computing system or computer network तक unauthorized access हासिल करने का कोई भी प्रयास है। Cyber attacks का उद्देश्य computer systems को destroy करना, बाधित करना, नष्ट करना या नियंत्रित करना या इन systems के भीतर रखे data को बदलना, block करना, हटाना, हेरफेर करना या चोरी करना है।

Two Types के Attacks हैं जो security से संबंधित हैं

1. Active Attacks
2. Passive Attacks

1. Active Attacks : Active attacks ऐसे attacks हैं जिनमें attacker messages की सामग्री (content) को change or modify करने का प्रयास करता है। Active attacks Integrity के साथ-साथ availability के लिए भी खतरा है। Active attacks के कारण system हमेशा क्षतिग्रस्त (damaged) होता है और System resources को बदला जा सकता है। सबसे महत्वपूर्ण बात यह है कि, Active attacks में, पीड़ित को attacks के बारे में सूचित किया जाता है।



Types of active attacks are as following:

2. Masquerade – Masquerade attack एक ऐसे attack को संदर्भित करता है जो valid access identity के माध्यम से personal computer information तक unauthorized access प्राप्त करने के लिए fake identity का उपयोग करता है। सामान्य user behavior से महत्वपूर्ण विचलन का पता लगाकर कभी-कभी नकाबपोशों की Automatic discovery (खोज) की जाती है

3. Modification of messages – इसका अर्थ है कि किसी message के कुछ हिस्से को बदल दिया गया है या उस message को unauthorized effect उत्पन्न करने के लिए विलंबित (delayed) या पुन: व्यवस्थित किया गया है। Modification original data की integrity पर attack है। इसका मूल रूप से मतलब है कि unauthorized पक्ष न केवल data तक पहुंच प्राप्त करते हैं, बल्कि सेवा से इनकार करने वाले हमलों को triggering करके data को धोखा देते हैं, जैसे कि प्रेषित data पैकेट को बदलना या नकली data के साथ नेटवर्क में बाढ़ आना। विनिर्माण (Manufacturing) प्रमाणीकरण (authentication) पर attack है।

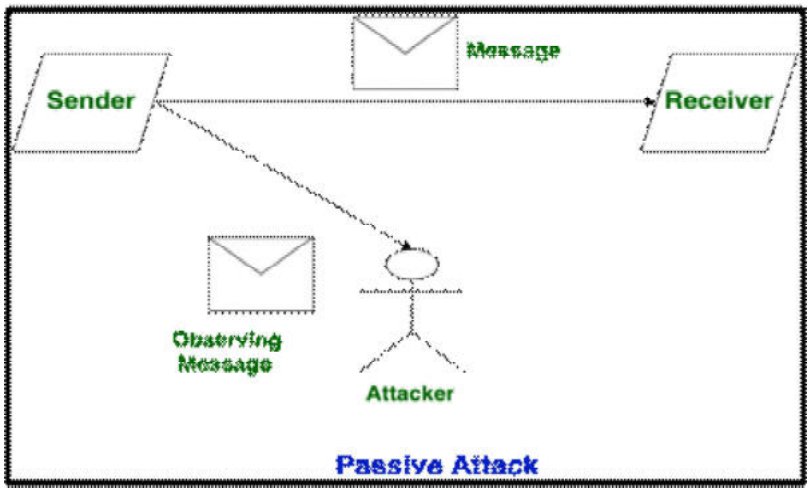
4. Repudiation – यह attack तब होता है जब network पूरी तरह से secured नहीं होता है या login control से छेड़छाड़ की जाती है। इस attack के साथ, e-mail messages के spoofing के समान, दूसरों की ओर से data के सामान्य हेरफेर तक, log files में false data को बचाने के लिए malicious user के कार्यों द्वारा author's की information को बदला जा सकता है।

5. Replay – इसमें एक authorized effect उत्पन्न करने के लिए एक message का passive capture और उसके बाद के प्रसारण शामिल हैं। इस attack में, attacker का मूल उद्देश्य उस particular network पर मूल रूप से मौजूद

data की एक save copy है और बाद में इस data को personal uses के लिए उपयोग करना है। एक बार data corrupted or leaked हो जाने के बाद यह users के लिए insecure and unsafe होता है।

6. Denial of Service – यह communication facilities के normal use को रोकता है। इस attack का एक विशिष्ट लक्ष्य (specific target) हो सकता है। For example, एक निकाय किसी विशेष गंतव्य (particular destination) के लिए निर्देशित सभी messages को दबा सकता है। service denial करने का एक अन्य रूप पूरे network को या तो network को अक्षम (disabled) करके या messages के साथ overloading करके performance को कम करने के लिए व्यवधान है।

Passive Attacks :- Passive Attacks उस प्रकार के attacks होते हैं जिनमें, attacker messages की content को देखता है या messages की content की प्रतिलिपि बनाता है। Passive Attacks गोपनीयता (Confidentiality) के लिए danger है। Passive Attacks के कारण system को कोई नुकसान नहीं होता है। सबसे खास बात यह है कि Passive Attacks में Victim को attacks की Information नहीं होती है।



Types of Passive attacks are as follows :-

1. The release of message content :– Telephonic conversation, electronic mail message, या transferred file में sensitive or confidential information हो सकती है। हम एक opponent को इन प्रसारणों की con-

tents को सीखने से रोकना चाहते हैं।

2. Traffic analysis :- मान लीजिए कि हमारे पास information को encryption करने का एक तरीका था, ताकि attacker भले ही message पर कब्जा कर ले, message से कोई information नहीं निकाल सके। opponent मेजबान के communicating के location or identity का निर्धारण कर सकता है और आदान-प्रदान किए जा रहे messages की frequency और length check कर सकता है। यह information हो रही communication की nature का अनुमान लगाने में useful हो सकती है। traffic analysis के विरुद्ध सबसे उपयोगी सुरक्षा SIP traffic का encryption है। ऐसा करने के लिए, एक attacker को यह निर्धारित करने के लिए SIP proxy (या उसके call log) तक पहुंचना होगा कि call किसने किया।

Background and current scenario of information security :- पूर्व में सूचना की सुरक्षा को बनाए रखना कठिन था।

• **1960's :-** पासवर्ड सुरक्षा (Password Protection) यह 1960 के दशक के दौरान था जब संगठन ने पहली बार अपने कम्प्यूटर के लिए अधिक सुरक्षात्मक (Protective) बनना शुरू किया। इस समय के दौरान इतनी सुरक्षा के बारे में चिंता करने के लिए कोई इंटरनेट नेटवर्क नहीं था जो बड़े पैमाने पर केंद्रित या अधिक भौतिक माप और कम्प्यूटर पर काम करने के बारे में पर्याप्त ज्ञान वाले लोगों तक पहुंच को रोकने के लिए, ऐसा करने के लिए, कभी भी डिवाइस में पासवर्ड जोड़ा गया।

• **1970's :-** क्रीपर (CREEPER) से रीपर (REAPER) तक Cyber Security की शुरुआत 1970 के दशक के दौरान एक Research Project के साथ हुई, जिसे उस समय ARPANET के नाम से जाना जाता था। एक शोधकर्ता ने एक कंप्यूटर प्रोग्राम बनाया जो ARPANET के नेटवर्क को स्थानांतरित करने में सक्षम था। उन्होंने प्रोग्राम का नाम क्रीपर रखा क्योंकि नेटवर्क पर यात्रा करते समय जो मुद्रित संदेश छोड़ दिया गया था "I'm the creeper : CATCH ME IF YOU CAN" बाद में एक प्रोग्राम तैयार किया गया। जो क्रीपर को अगले स्तर तक ले गया, जिससे यह स्व-प्रतिकृति (self-Replicating) और अब तक का पहला computer worm बन गया। सौभाग्य से उन्होंने रीपर नामक एक और प्रोग्राम लिखा, जिसने Wrote का पीछा किया और एंटीवायरस सॉफ्टवेयर का पहला उदाहरण प्रदान करते हुए इसे हटा दिया

• **1990's :-** वर्ष के दौरान कंप्यूटर से जुड़े, computer viruses अधिक उन्नत हो गए और सूचना सुरक्षा प्रणाली नहीं चल सकी। हालाँकि, इसकी self

replicated की क्षमता इसका पतन होगी, जिसे worm ने इतनी आक्रामक रूप से दोहराया कि इसने कंप्यूटर को संचालन योग्य बना दिया और इंटरनेट को रेंगने की गति को धीमा कर दिया। यह पूरे नेटवर्क में तेजी से फैल गया और अनकही क्षति हुई। Robert Merries computer fraud और misuse act के तहत सफलतापूर्वक आरोपित होने वाले पहले व्यक्ति बने।

• **1980's :-** Firewalls का उदय इंटरनेट, जनता के लिए उपलब्ध होने के साथ ही अधिक से अधिक लोगों ने अपनी personal information ऑनलाइन डालना शुरू कर दिया, इस वजह से अपराधियों ने Web द्वारा people × government से Data चोरी करने के लिए कहा। जनता की सुरक्षा के लिए बड़े पैमाने पर Firewalls and anti virus programs तैयार किए जाने थे।

In 2014 :- Yahoo एक और biggest data branch का experience करता है। इस attack में कुल 500 million Yahoo user से समझौता (compromised) किया गया था

In 2015 :- Messaging app service Snap chat उजागर हुई थी। Hackers ने 4.6 मिलियन अकाउंट का यूजरनेम, phone number and location पोस्ट किया।

In 2017 :- Hackers ने उन लोगों के 50 मिलियन Name, home address, mobile phone numbers and emails चुरा लिया, जिन्होंने ber and the drivering license और 70 लाख ड्राइवरों की अन्य जानकारी का इस्तेमाल किया था।

In 2020 :- Ministry of Information and Technology ने Tiktok and pubg mobile समेत 118 Chinese mobile app पर प्रतिबंध लगा दिया है। IT mystery started हुआ Chinese app को information technology Act की धारा 69 ए के तहत प्रतिबंधित कर दिया गया है। IT industry को विभिन्न स्रोतों से कई complaints मिली हैं कि android and IOS platform पर उपलब्ध कुछ मोबाइल ऐप के दुरुपयोग के बारे में उपयोगकर्ताओं के Data को चोरी और प्रसारित करने के लिए IT industry को कई शिकायतें मिली हैं। सेवा के लिए unauthorized तरीके से भारत के बाहर स्थान है।

Cyber Attacks:-

1. Virus 2. Adware 3. Trojan Horse 4. Ransomwar
5. Phishing

A. Virus(Vital Information Resources Under Siege) :- computer virus एक malicious टुकड़ा है device से फैलने के लिए designed

किया गया कम्प्यूटर कोड यंत्र को। मैलवेयर का एक उपसमुच्चय, इन self copy-ing खतरों को आमतौर पर नुकसान पहुंचाने के लिए designed किया गया है डिवाइस या डेटा चोरी। एक computer virus बहुत हद तक जैविक के समान है वाइरस। लगातार दोहराने के लिए डिजाइन किया गया, कंप्यूटर वायरस आपके programs and files को संक्रमित करते हैं, अपने कंप्यूटर के काम करने के तरीके में बदलाव करें या इसे पूरी तरह से काम करने से बंद करें।

Creeper program, जिसे अक्सर पहला virus माना जाता है, 1971 में Bob Thomas Creeper द्वारा बनाया गया था, वास्तव में यह देखने के लिए एक secu-rity test के रूप में designed किया गया था कि क्या एक self-replicating program संभव था। infected प्रत्येक नई hard drive के साथ, Creeper खुद को पिछले host से हटाने का प्रयास करेगा। Creeper का कोई malicious इरादा नहीं था और उसने केवल एक simple message प्रदर्शित किया: "I'M THE CREEPER. CATCH ME IF YOU CAN!"

कंप्यूटर वायरस क्या करता है?

कुछ वायरस कंप्यूटर को नुकसान पहुंचाने के लिए प्रोग्राम किया जाता है आपके कंप्यूटर को प्रोग्रामों को नुकसान पहुंचाकर, हटाकर फाइलें या हार्ड ड्राइव को पुन: स्वरूपित करना। अन्य बस खुद को दोहराएं या नेटवर्क यातायात को बढ़ा दें, जिससे इंटरनेट गतिविधि मे कोई भी प्रदर्शन करना असंभव हो जाता है। इससे भी कम हानिकारक कंप्यूटर वायरस आपके सिस्टम को महत्वपूर्ण प्रदर्शन रूप से बाधित कर सकते हैं, कंप्यूटर मेमोरी को कम करना और बार-बार कंप्यूटर crashes होने का कारण

Different types of computer viruses :-

1. Resident Virus : Resident virus एक प्रकार का computer vi-rus है जो computer memory में खुद को छुपाता (hides) है और store करता है, जो तब virus' programming के आधार पर computer द्वारा चलाई जाने वाली किसी भी file को infect करने की अनुमति देता है।

इसे Terminate and Stay Resident (TSR) के रूप में भी जाना जाता है, यह computer RAM में load करने का एक तरीका ढूंढता है और फिर कुछ शर्तों के पूरा होने पर user द्वारा खोली गई executable योग्य files को infects करता है। इस तरह के virus के कुछ examples Jerusalem Virus, Onehalf virus, Magistr, Junkie, Satanbug etc.

2. Direct Action Virus : जब कोई virus खुद को सीधे .exe या .com file से जोड़ता है और device में प्रवेश करता है, जबकि इसके execution को

Direct Action Virus कहा जाता है। यदि यह memory में स्थापित हो जाता है, तो यह स्वयं को hidden कर रखता है। इसे Non-Resident virus के रूप में भी जाना जाता है।

3. Boot sector virus : boot sector virus एक प्रकार का malware है जो system's boot partition या hard disk के Master Boot Record (MBR) को infects करता है। startup के दौरान और security software को executed करने से पहले, virus malicious code executes करता है।

4. Multipartite Virus : एक virus जो पहले से infected computer के boot sector और executable files दोनों पर attack कर सकता है, उसे multipartite virus कहा जाता है। यदि एक multipartite virus आपके system पर attacks करता है, तो आपको cyber threat का risk है।

5. Overwrite Virus :- Most harmful viruses में से एक, overwrite virus मौजूदा program को पूरी तरह से remove सकता है और इसे overwrite करके malicious code से बदल सकता है। धीरे-धीरे यह पूरी तरह से host's programming code को harmful code से बदल सकता है।

6. Polymorphic Virus :- spam and infected websites के माध्यम से फैले, polymorphic virus file infectors होते हैं जो complex होते हैं और इनका पता लगाना कठिन होता है। वे existing program का एक modified or morphed version बनाते हैं और system को infect करते हैं और original code को बनाए रखते हैं।

7. File Infector Virus : जैसा कि नाम से पता चलता है, यह पहले एक file को infects करता है और फिर बाद में other executable योग्य files और programs में फैल (spreads) जाता है। इस virus का main source games and word processors हैं।

8. Spacefiller Virus : यह एक rare type का virus है जो किसी fills के empty spaces को virus से भर देता है , इसे cavity virus के नाम से जाना जाता है। यह न तो file के size को प्रभावित (affect) करेगा और न ही आसानी से पता लगाया जा सकता है।

9. Macro Virus : एक virus उसी macro language में लिखा गया है जो software program में उपयोग किया जाता है और यदि कोई word processor file खोली जाती है तो computer को infects करता है। मुख्य रूप से ऐसे viruses का source emails के माध्यम से होता है।

B. Adware : (Adware or Advertising supported software) यह

एक software है जो आपके कंप्यूटर पर विज्ञापन अवांछित प्रदर्शित (unwanted displays) करता है। Adware आपको इकट्ठा करने के लिए ब्राउजर का उपयोग करता है, 'लक्षित (target)' करने के लिए web browsing history विज्ञापन जो आपके अनुरूप लगते हैं।

C. Trojan Horse : Trojan Horse Virus एक प्रकार का malware है जो एक legitimate program के रूप में प्रच्छन्न कंप्यूटर (computer disguised) पर download होता है। वितरण पद्धति (delivery method) में आम तौर पर एक attacker को वैध software. के hide malicious code को छिपाने के लिए social engineering का उपयोग करते हुए देखा जाता है ताकि users को अपने Software के साथ system access प्राप्त करने का प्रयास किया जा सके।

D. Ransomware :- Ransomware एक प्रकार का malicious software है जो एक computer को संक्रमित करता है और users की पहुंच को प्रतिबंधित करता है यह तब तक है जब तक इसे unlock करने के लिए फिरौती का भुगतान नहीं किया जाता है। Ransomware variants कई सालों से देखे गए हैं और अक्सर पीड़ितों से पैसे निकालने का प्रयास करते हैं on-screen alert प्रदर्शित करना।

E. Phishing :- Phishing attacks भेजने की प्रथा है कपटपूर्ण संचार (fraudulent communications) जो प्रतीत होते हैं एक प्रतिष्ठित स्रोत (reputable source) से आते हैं। यह आमतौर पर है email के माध्यम से किया जाता हैं। लक्ष्य चोरी (goal steal) करना है credit card और login जैसे sensitive data information या install malware करने के लिए।

Computer Forensics

Computer forensics technology का एक क्षेत्र (field) है जो computer device से साक्ष्य की identify करने और store करने के लिए investigative techniques का उपयोग करता है। अक्सर, Computer forensics का उपयोग उन सबूतों को उजागर करने के लिए किया जाता है जिनका उपयोग अदालत में किया जा सकता है। Computer forensics investigations के बाहर के क्षेत्रों को भी शामिल करता है।

Computer forensics इकट्ठा करने के लिए investigation and analysis techniques का अनुप्रयोग है और सबूत सुरक्षित रखें। Forensic आमतौर पर personal computers, laptops, personal digital से data का विश्लेषण करते हैं सहायक, cell phones, servers, tapes, और किसी भी अन्य प्रकार के media।

इस process में शामिल हो सकते हैं encryption को breaking से लेकर कानून प्रवर्तन टीम (law enforcement team) के साथ search warrants

निष्पादित करने तक कुछ भी, hard drives से Files को पुनर्प्राप्त करने और उनका विश्लेषण करने के लिए जो सबसे महत्वपूर्ण सबूत होंगे गंभीर दीवानी (most serious civil) और फौजदारी मामले (criminal cases)। computers, and data storage media की Forensic जांच एक complicated and highly specialized process है। Forensic examinations के परिणाम संकलित और reports में शामिल किए जाते हैं। कई मामलों में, examiners अपने निष्कर्षों की गवाही देते हैं, जहां उनके skills और abilities को रखा जाता है अंतिम जांच के लिए।

DIGITAL FORENSICS : Digital Forensics को संरक्षण (preservation), पहचान (identification), निष्कर्षण (extraction) और process के रूप में परिभाषित किया गया है। Computer evidence का documentation जिसका उपयोग न्यायालय द्वारा किया जा सकता है। यह एक science है computer, mobile phone, server, or network जैसे digital media से सबूत ढूंढना। यह complicated digital संबंधित मामलों को solve करने के लिए forensic team को सर्वोत्तम तकनीक और उपकरण प्रदान करता है। डिजिटल फोरेंसिक forensic team को analyzes, inspect, identifies, and preserve करने में मदद करता है विभिन्न प्रकार के electronic devices पर रहने वाले digital evidence Digital forensic science की एक शाखा है जो पुनर्प्राप्ति पर केंद्रित है और cybercrime से जुड़े digital devices में मिली सामग्री की जांच gksrh gSaA Some common techniques include the following:

- Reverse steganography. Steganography is a common tactic used to hide data inside any type of digital file, message or data stream
- Stochastic forensics
- Cross-drive analysis
- Live analysis
- Deleted file recovery

FORENSICS INVESTIGATION :- Forensics एक crime को solve के लिए इस्तेमाल की जाने वाली वैज्ञानिक विधियाँ (scientific methods) हैं। Forensics investigation एक संदिग्ध (suspicious) के बारे में analysis पर आने के लिए crime से संबंधित सभी physical evidence का संग्रह (gathering) और विश्लेषण (analysis) है। crime कैसे हुआ, यह स्थापित (Established) करने के लिए Investigators blood, तरल पदार्थ (fluid) या fingerprints, अवशेष (residue), hard drives, computers, or other technology

को देखेंगे। हालांकि, यह एक सामान्य परिभाषा है, क्योंकि कई प्रकार के Forensics हैं।

TYPES OF FORENSICS INVESTIGATION :-

- Forensic Accounting / Auditing
- Computer or Cyber Forensics
- Crime Scene Forensics
- Forensic Archaeology
- Forensic Dentistry
- Forensic Entomology
- Forensic Graphology
- Forensic Pathology
- Forensic Psychology
- Forensic Science
- Forensic Toxicology

Processing steps of conducting of investigation.

Step :-1. Acquisition : उचित hardware and software tools का उपयोग करके crime scene से सामग्री (materials) का अधिग्रहण (Acquisition) प्राप्त data को legal evidence बनाता है।

Step :-2. Data Acquisition : Data acquisition वह Data प्राप्त करने के लिए continuous world information का नमूना है जिसे computer द्वारा हेरफेर किया जाएगा।

Step :-3. Data Recovery : Forensic data recovery क्षतिग्रस्त साक्ष्य (damaged evidence) sources से forensically रूप से sound तरीके से data की निकासी है।

Step :- 4. Forensics Analysis : Forensic digital analysis electronically रूप से stored information (ESI) का depth analysis और examination है।

Step :- 5. Presentation : Digital analysis की presentation में relevant information की पहचान पर एक formal written report शामिल है।

❑❑❑