Cyber Security- Understanding Computer Forensics

1. Define digital forensics and Computer forensics. What is the role of digital forensics?

•Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence.the use of scientifically derived and proven methods toward the preservation, collection, validation, identification,analysis, interpretation, documentation.

•The application of computer for investigating computer-based crime has led to development of a new field called computer forensics. Computer forensics is primarily concerned with the systematic,"identification," "acquisition," "preservation" and "analysis" of digital evidence.

The role of digital forensics is to:

1. Uncover and document evidence and leads.

2. Corroborate evidence discovered in other ways.

3. Assist in showing a pattern of events (data mining has an application here).

4. Connect attack and victim computers.

5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.

6. Extract data that may be hidden, deleted or otherwise not directly available.

2. What is chain of custody? Why is it used? What are the documents that chain of custody must include?

Chain of custody means the chronological documentation trail, etc,that indicates the seizure, custody, control, transfer, analysis and disposition of evidence (physical or electronic).

Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.Chain of custody is particularly important in situations where sampling can identify the existence of contamination and can be used to identify the responsible party.The chain of custody requires that from the moment the evidence is collected, every transfer of evidence from one person to another person should be documented as it helps to prove that nobody else could have accessed that evidence. It is advisable to keep the number of evidence transfers as low as possible.All transactions as well as every succeeding transaction between evidence collection and its appearance in court need to be completely documented chronologically to with stand legal challenges to the authenticity of the evidence.

The documents that chain of custody must include:

• Conditions under which the evidence is collected.

• The identity of all those who handled the evidence.

• Duration of evidence custody.

• Security conditions while handling or Storing the evidence and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs.

• The signatures of persons involved at each step.

3. Define evidence according to the “Indian Evidence Act 1872”.How is digital evidence different from physical evidence?

According to the "Indian Evidence Act 1872," "Evidence" means:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.

2. All documents that are produced for the inspection ofthe court are called documentary evidence.

As compared to the "physical" evidence, "digital evidence" is different in nature because it has some unique characteristics.

• digital evidence is much easier to change/manipulate!

• "perfect" digital copies can be made without harming original.

• At the same time the integrity of digital evidence can be proven.

• Another subtle aspect is that it is usually in the form of the "image"— this means that it is convenient and possible to create a defensible"clone" of storage device.

4. Explain the contexts involved in actually identifying a piece of digital evidence.

The contexts involved in actually identifying a piece of digital evidence are :

• Physical context: It must be definable in its physical form, that is, it should reside on a specific piece of media.

• Logical context: It must be identifiable as to its logical position, that is, where does it reside relative to the file system.

• Legal context: We must place the evidence in the correct context to read its meaning. This may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

5. List any five guidelinesfor the (digital) evidence collection phase.

Following are some guidelines for the (digital) evidence collection phase:

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.

2. Capture a picture of the system as accurately as possible.

3. Keep detailed notes with dates and times. If possible, generate an automatic transcript

4. Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.

5. Minimize changes to the data as you are collecting it. This is not limited to content changes; avoid updating file or directory access times.

6. Explain with an example how an email can be faked.

The sender's E-Mail address can be easily faked and can be hard to detect,

• If the server mentioned in the bottom "received" section does not match the server of the E-Mail address, this suggests that the E-Mail address is a fake one.

• An example is

Received: from infvic.it (adsl-98-201.38-151.net24.it [151.38.201.98])by mail-relay2.bpvi.it (Postfix) with ESMTP id 2887550074 for <redazione@infvic.it>; Mon, 19 Apr 2004 10:41:54 +0200 (CEST)From: sfiorillo@hotmail.com

From the example given ,

•the E-Mail address in the "From"field has "hotmail.com" as the domain for the E-Mail whereas in the received section of the header there is no hotmail server mentioned at all. This is clearly a forged (fake) E-Mail and it is very likely to have a fake "From"address.

• Also note that the time on the received section is Central European Standard Time (CEST), and hotmail.com servers are not in Europe.

7. Give the process model for understanding a seizure and handling of forensics evidence legal framework.

The process model for understanding a seizure and handling of forensics evidence legal framework.

• The cardinal rules to remember are that evidence:

1. is admissible;
2. is authentic;
3. is complete;
4. is reliable;
5. is understandable and believable.

8. List forensics life cycle phases. Explain the first two phases.

The forensics life cycle involves the following phases:

• Preparation and identification;

• collection and recording;

• storing and transporting;

• examination/investigation;

• analysis, interpretation and attribution;

• reporting;

• testifying.

1)Preparing for the Evidence and Identifying the Evidence

• In order to be processed and applied, evidence must first be identified as evidence.

• It can happen that there is an enormous amount of potential evidence available for a legal matter, and it is also possible that the vast majority of the potential evidence may never get identified.

• For Example , every sequence of events within a single computer should be recorded.

•In a networked environment, this extends to all networked devices, potentially all over the world.

•If the evidence cannot be identified as relevant evidence,it may never be collected or processed at all, and it may not even continue to exist in digital form by the time it is discovered to have relevance.

2)Collecting and Recording Digital Evidence

• Digital evidence can be collected from many sources. Obvious sources include computers, cell phones, digital cameras, hard drives, CD-ROM,USB memory devices and so on.

• Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).

• Special care must be taken when handling computer evidence: most digital information is easily changed, and once changed it is usually impossible to detect that a change has taken place.

• For this reason, it is common practice to calculate a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated.

• Collecting volatile data requires special technical skill.

• If a machine is still active, any intelligence that can be gained by examining the applications currently open is recorded.

• If the machine is suspected of being used for illegal communications, not all of this information may be stored on the hard drive.

• If information stored solely in random access memory (RAM) is not recovered before powering down, it may be lost.

• The embedded memory chips makes it a good candidate to be used in every device that interacts with our daily life,the various types of "embedded memories"inside a computer (ROM, PROM, EPROM, EEPROM).

9. Discuss the issues involved in Storing and Transporting Digital Evidence

Issues Involved in Storing and Transporting Digital Evidence

Storage:

Data Integrity: Ensuring the original state of the evidence remains unaltered.

Physical Security: Protecting evidence from environmental factors and physical threats.

Chain of Custody: Maintaining a detailed record of the evidence's handling.

Long-Term Preservation: Implementing strategies for long-term storage.

Transportation:

Data Integrity: Preventing data corruption or alteration during transfer.

Chain of Custody: Documenting the movement of evidence.

Physical Security: Protecting evidence from damage, loss, or theft.

Authentication: Ensuring the authenticity and reliability of the transferred evidence.

Environmental Factors: Avoiding exposure to extreme conditions.

Human Error: Minimizing the risk of errors during transportation and handling, as even minor mistakes can compromise the evidence's integrity and legal admissibility.

10. Explain several types of analysis of digital data in digital forensics

The different analysis types are based on interpretation, or abstraction,layers, which are generally part of the data's design.

1)Media analysis:

• It is analysis of the data from a storage device.

• This analysis does not consider any partitions or other operating system (OS)-specific data structures.

• If the storage device uses a fixed size unit, such as a sector, then it can be used in this analysis.

2)Media management analysis:

• It is analysis of the management system used to organize media.

• This typically involves partitions and may include volume management or redundant array of independent (or inexpensive) disks systems that merge data from multiple storage devices into a single virtual storage device.

3)File system analysis: It is the analysis of the file system data inside a partition or disk. This typically involves processing the data to extract the contents of a file or to recover the contents of a deleted file.

4)Application analysis:

• It is the analysis of the data inside a file.

• Files are created by users and applications.

• The format of the contents is application-specific.

5) Network analysis:

• It is the analysis of data on a communications network.

• Network packets can be examined using the OSI Model to interpret the raw data into an application-level stream.

• Application analysis is a large category of analysis techniques because there are many application types.

6)OS analysis:

This analysis examines the configuration files and output data of the OS to determine what events may have occurred.

7)Executable analysis:

Executables are digital objects that can cause events to occur and they are frequently examined during intrusion investigations because the investigator needs to determine what events the executable could cause.

8)Image analysis:

• Digital images are the target of many digital investigations because some are contraband.

• This type of analysis looks for information about where the picture was taken and who or what is in the picture.

• Image analysis also includes examining images for evidence of steganography

9)Video analysis:

• Digital video is used in security cameras and in personal video cameras and webcams.

• Investigations of online predators can sometimes involve digital video from webcams.

• This type of analysis examines the video for the identification of objects in the video and the location where it was shot.

11. List the elements of digital forensics reporting.

The following are the broad-level elements of the report:

1. Identity of the reporting agency;

2. case identifier or submission number;

3. case investigator;

4. identity of the submitter;

5. date of receipt;

6. date of report;

7. descriptive list of items submitted for examination, including serial number, make and model;

8. identity and signature of the examiner;

9. brief description of steps taken during examination, such as string searches, graphics image searches and recovering erased files;

10. results/conclusions.

12. What does testify in digital forensics involve? When can a witness testify evidence? What are the principles applied to maintain the integrity of digital evidence?

• This phase involves presentation and cross-examination of expert witnesses.

• Depending on the country and legal frameworks in which a cybercrime case is registered,certain standards may apply with regard to the issues of expert witnesses.

• Digital forensics evidence is normally introduced by expert witnesses except in cases where non-experts can bring clarity to non-scientific issues by stating what they observed or did.

• For example, a non-expert who works at a company may introduce the data he/she extracted from a company database and discuss how the database works and how it is normally used from a non-technical standpoint.

• To the extent that the witness is the custodian of the system or its content, he/she can testify to matters related to that custodial role as well.

• Only expert witnesses can address issues based on scientific, technical or other specialized knowledge.

• A witness qualified as an expert by knowledge, skill, experience, training or education may testify in the form of an opinion or otherwise if

(a) the testimony is based on sufficient facts or data

(b) the testimony is the product of reliable principles and methods,

(c) the witness has applied the principles and methods reliably to the facts of the case.

• The expert may in any event be required to disclose the underlying facts or data on cross-examination.

• In order to comply with the need to maintain the integrity of digital evidence, certain rules

must be complied with. In general, the following principles are applicable:

• Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

• Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media that person must be competent to do so and be able to give evidence explaining the relevance and the implications of his/her actions.

• Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

• Principle 4: The person in-charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered

13. List any six security issues that are associated with social networking sites. Give any 3 examples of security measures used by social networking sites.

Security issues that are associated with social networking sites are listed below:

1. Corporate espionage.

2. Viruses and worms.

3. Spear Phishing and social networking specific Phishing.

4. Infiltration of networks leading to data leakage

5. ID theft

6. Bullying, Spam,Stalking.

EXAMPLES:

1. Limiting Code Execution:

Social networking sites often restrict the types of code users can embed on their profiles to mitigate security risks. For instance, MySpace doesn't allow JavaScript code, preventing potential malicious scripts from running. PerfSpot limits the content of HTML code to further restrict data retrieval attempts.

2. User Privacy Controls:

Many social networking sites offer granular privacy settings, empowering users to control their personal information. Facebook and MySpace allow users to specify who can view their profile, posts, and other content. Yahoo!360 provides basic privacy settings to restrict profile visibility.

3. Profile Visitor Tracking and Transparency:

Some social networking sites offer features to monitor profile visitors, increasing user awareness and potentially deterring malicious activity. Friendster, Hi5, Orkut, and PerfSpot allow users to track who visits their profiles. Orkut takes this a step further by requiring users to disclose their own viewing history if they track others, promoting transparency.

14. Discuss the technical challenges in computer forensics

• There are two aspects of the technical challenges faced in digital

forensics investigation

1. one is the "complexity" problem
2. the other is the "quantity" problem involved in a digital forensics investigation.

• A digital forensics investigator often faces the "complexity problem"because acquired data is typically at the lowest and most raw format.Non-technical people may find it too difficult to understand such format.

• For resolving the complexity problem, tools are useful; they translate data through one or more "layers of abstraction" until it can be understood.

• Digital forensics is also challenged by the "quantity problem" — it involves the hugeness of digital forensics to analyze.

• So data reduction techniques need to be used to solve this.

• Data reduction is done by grouping data into one larger event or by removing known data.

• Abstraction of data layers is a core feature in the design of modern digital systems.

• Let us consider fat file system example; "FAT" is a file allocation table. FAT file

system is one of the most basic file systems that is still used in many computers.

• It is broken up into three main areas.

• The first area is the Boot Sector that contains the addresses and sizes of structures in this specific file system.

• The next two areas are the FAT and the Data Area.

• The locations of which are identified in the Boot Sector.

• The Data Area is divided into consecutive sectors called clusters. Clusters store the contents of a file or directory.

• Each cluster has an entry in the FAT that specifies if the cluster is unallocated or which cluster is the next in the file that has allocated it.

• Files are described by a directory entry structure. The directory entry structures are stored in the clusters allocated to the parent directory.

• The structure contains the file name, time, size and starting cluster. The remaining clusters in the file, if any, are identified using the FAT.

• The FAT file system has seven layers of abstraction.

• The first layer uses just the partition image as input, assuming that the

acquisition was done of the raw partition using a tool such as the UNIX "dd"tool.

~Shravya N Bhat -ISE-I~