UNIT-4 Computer Forensics

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Understand the functions and objectives of computer forensics ✓ Discuss computer forensics policy and procedure development ✓ Document and report key findings in detail

Unit 4

Computer Forensics

If you manage or administer information systems and networks, you should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word forensics means "to bring to the court.") Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive. Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal "scientific" discipline. We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

Cyber forensic is a branch of science which deals with tools and techniques for investigation of digital data to find evidences against a crime which can be produced in the court of law. It is a practice of preserving, extracting, analyzing and documenting evidence from digital devices such as computers, digital storage media, smartphones, etc. so that they can be used to make expert opinion in legal/administrative matters.

Why is Computer Forensics Important?

Adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure. You can help your organization if you consider computer forensics as a new basic element in what is known as a "defense-in-depth approach to network and computer security. For instance, understanding the legal and technical aspects of computer forensics will help you capture vital information if your network is compromised and will help you prosecute the case if the intruder is caught.

What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected. Recent legislation makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data.

Computer forensics is also important because it can save your organization money. Many managers are allocating a greater portion of their information technology budgets for computer and network security. In increasing numbers, organizations are deploying network security devices such as intrusion detection systems (IDS), firewalls, proxies, and the like, which all report on the security status of networks. From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

What are some typical aspects of a computer forensics investigation? First, those who investigate computers have to understand the kind of potential evidence they are looking for in order to structure their search. Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property.

Second, the investigator must pick the appropriate tools to use. Files may have been deleted, damaged, or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process. Two basic types of data are collected in computer forensics. Persistent data is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off.

Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it. System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

Legal Aspects of Computer Forensics Anyone overseeing network security must be aware of the legal implications of forensic activity. Security professionals need to consider their policy decisions and technical actions in the context of existing laws. For instance, you must have authorization before you monitor and collect information related to a computer intrusion. There are also legal ramifications to using security monitoring tools.

Computer forensics is a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux. The important point for forensics investigators is that evidence must be collected in a way that is legally admissible in a court case. Increasingly, laws are being passed that require organizations to safeguard the privacy of personal data. It is becoming necessary to prove that your organization is complying with computer security best practices.

If there is an incident that affects critical data, for instance, the organization that has added a computer forensics capability to its arsenal will be able to show that it followed a sound security policy and potentially avoid lawsuits or regulatory audits.

In large organization, as soon as a cyber-crime is detected by the incident handling team, which is responsible for monitoring and detection of security event on a computer or computer network, initial incident management processes are followed. This is an in-house process. It follows following steps:

1. **Preparation:** The organization prepares guidelines for incident response and assigns roles and the responsibilities of each member of the incident response team. Most of the large organizations earn a reputation in the market and any negative sentiment may negatively affect the emotions of the shareholders. Therefore, an effective communication is required to declare the incident. Hence, assigning the roles based on the skill-set of a member is important.
2. **Identification:** based on the traits the incident response team verifies whether an event had actually occurred. One of the most common procedures to verify the event is examining the logs. Once the occurrence of the event is verified, the impact of the attack is to be assessed.
3. **Containment:** based on the feedback from the assessment team, the future course of action to respond to the incident is planned in this step.
4. **Eradication:** In this step, the strategy for the eradication or mitigate of the cause of the threat is planned and executed.
5. **Recovery:** it is the process of returning to the normal operational state after eradication of the problem.
6. **Lesson Learned:** if a new type of incident is encounter, it is documented so that this knowledge can be used to handle such situations in future.

The second step in the process is forensic investigation is carried out to find the evidence of the crime, which is mostly performed by 3rd party companies. The computer forensic investigation involves following steps:

1. **Identify incident and evidence:** this is the first step performed by the system administrator where he tries to gather as much information as possible about the incident. Based on this information the scope and severity of the attack is assessed. Once the evidence of the attack is discovered, the backup of the same is taken for the investigation purpose. The forensic investigation is never performed on the original machine but on the data that is restored from the backup.

2. **Collect and preserve evidence:** Various tools like Helix, WinHex, FKT Imager, etc. are used to capture the data. Once the backup of the data is obtained, the custody of the evidence and the backup is taken. MD5(message digest) hash of the backup is calculated and matched with the original one to check the integrity of the data. Other important sources of information like system log, network information, logs generated by Intrusion Detection Systems(IDS), port and process information are also captured.
3. **Investigate:** The image of the disk is restored from the backup and the investigation is performed by reviewing the logs, system files, deleted and updates files, CPU uses and process logs, temporary files, password protected and encrypted files, images, videos and data files for possible stegnographic message, etc.
4. **Summarize and Presentation:** The summery of the incident is presented in chronological order. Based on the investigation, conclusions are drawn and possible cause is explained.

While carrying out the digital forensic investigation, rules and procedure must be applied. Specially while capturing the evidence. It should be ensured that the actions that are taken for capturing the data do not change the evidence. The integrity of the data should be maintained. It must be ensured that the devices used for capturing the backup are free from contamination.

Moreover, all the activities related to seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review[9]. Prevention is always better than cure. It is always recommended to fine tune your intrusion detection system like firewall occasionally perform penetration tests on your network to avoid pray to hacker. Last but not the least, report the crime.

The Role of Forensics within Organisations

When a cyber-security incident occurs the IT staff will often be expected to make an initial assessment to try and identify the exact nature and seriousness of the incident. They will often not have received any kind of computer forensic training. As a result they are not necessarily aware of the issues surrounding the collection of digital data that may have to be relied upon at a later date in court. Vital information such as time and date stamps can be lost making the investigation more difficult. In the worst case scenario vital evidence may be thrown out of court due to the improper handling of the data during the course of the investigation.

Computer forensic investigations require specialist skills which involves not just the preservation and identification of digital evidence but the correct interpretation of that evidence. When confronted with a forensic investigation, organisations initially tend to focus on the costs involved. Yes there is an up- front cost and depending on the complexity of the investigation and the number of computers

involved, it can appear to be expensive. However consider the following: Evidence that can only be obtained by a forensic examination can often prove vital to the successful outcome of the investigation. A forensic investigation can often reduce the need for full legal action to be taken.

A forensic investigation can save time resulting in a saving of money. When formulating an incident response plan, organisations should be building into that plan a forensic response. This may mean providing staff with computer forensic training, identifying computer forensic companies with the skills already that can assist, or a combination of both. Computer forensics is now well established in many countries around the world and is rapidly gaining momentum in many other countries. In the UK they have now even set up an insurance scheme where if the organisation is required to call in a computer forensic company, they can claim it on insurance. Organisations need to embrace forensics and use it as another tool against those who are committing cyber-crime.

An organisation equipped with a well-trained computer forensic capability is able to both reactively and proactively defend against attacks from both inside and outside the organisation.
When looking to establish a forensics expertise within your organisation there a variety of factors that must be considered:

- People – cost of setting up the team in terms of recruitment, initial and ongoing training
- Forensic laboratory – development of a forensic laboratory with sufficient equipment to carry out forensic investigations
- Developing appropriate incident response procedures and understanding their effect and impact upon the organisation
- Organisational policy – modifications to the security policy and employee contracts may be required to permit forensic investigation of employee systems
- Organisational IT infrastructure (optional) – development of the IT infrastructure to facilitate forensic investigations.

For those working in the field, there are five critical steps in computer forensics, all of which contribute to a thorough and revealing investigation.

Policy and Procedure Development

Whether related to malicious cyber activity, criminal conspiracy or the intent to commit a crime, digital evidence can be delicate and highly sensitive. Cybersecurity professionals understand the value of this information and respect the fact that it can be easily compromised if not properly handled and

protected. For this reason, it is critical to establish and follow strict guidelines and procedures for activities related to computer forensic investigations. Such procedures can include detailed instructions about when computer forensics investigators are authorized to recover potential digital evidence, how to properly prepare systems for evidence retrieval, where to store any retrieved evidence, and how to document these activities to help ensure the authenticity of the data.

Law enforcement agencies are becoming increasingly reliant on designated IT departments, which are staffed by seasoned cybersecurity experts who determine proper investigative protocols and develop rigorous training programs to ensure best practices are followed in a responsible manner. In addition to establishing strict procedures for forensic processes, cybersecurity divisions must also set forth rules of governance for all other digital activity within an organization. This is essential to protecting the data infrastructure of law enforcement agencies as well as other organizations.

An integral part of the investigative policies and procedures for law enforcement organizations that utilize computer forensic departments is the codification of a set of explicitly-stated actions regarding what constitutes evidence, where to look for said evidence and how to handle it once it has been retrieved. Prior to any digital investigation, proper steps must be taken to determine the details of the case at hand, as well as to understand all permissible investigative actions in relation to the case; this involves reading case briefs, understanding warrants, and authorizations and obtaining any permissions needed prior to pursuing the case.

Evidence Assessment

A key component of the investigative process involves the assessment of potential evidence in a cyber crime. Central to the effective processing of evidence is a clear understanding of the details of the case at hand and thus, the classification of cyber crime in question.

For instance, if an agency seeks to prove that an individual has committed crimes related to identity theft, computer forensics investigators use sophisticated methods to sift through hard drives, email accounts, social networking sites, and other digital archives to retrieve and assess any information that can serve as viable evidence of the crime.

This is, of course, true for other crimes, such as engaging in online criminal behavior like posting fake products on eBay or Craigslist intended to lure victims into sharing credit card information. Prior to conducting an investigation, the investigator must define the types of evidence sought (including specific platforms and data formats) and have a clear understanding of how to preserve pertinent data. The investigator must then determine the source and integrity of such data before entering it into evidence.

Evidence Acquisition

Perhaps the most critical facet of successful computer forensic investigation is a rigorous, detailed plan for acquiring evidence. Extensive documentation is needed prior to, during, and after the acquisition process; detailed information must be recorded and preserved, including all hardware and software specifications, any systems used in the investigation process, and the systems being investigated. This step is where policies related to preserving the integrity of potential evidence are most applicable. General guidelines for preserving evidence include the physical removal of storage devices, using controlled boot discs to retrieve sensitive data and ensure functionality, and taking appropriate steps to copy and transfer evidence to the investigator's system.

Acquiring evidence must be accomplished in a manner both deliberate and legal. Being able to document and authenticate the chain of evidence is crucial when pursuing a court case, and this is especially true for computer forensics given the complexity of most cybersecurity cases.

Evidence Examination

In order to effectively investigate potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases. Investigators typically examine data from designated archives, using a variety of methods and approaches to analyze information; these could include utilizing analysis software to search massive archives of data for specific keywords or file types, as well as procedures for retrieving files that have been recently deleted. Data tagged with times and dates is particularly useful to investigators, as are suspicious files or programs that have been encrypted or intentionally hidden.

Analyzing file names is also useful, as it can help determine when and where specific data was created, downloaded, or uploaded and can help investigators connect files on storage devices to online data transfers (such as cloud-based storage, email, or other Internet communications). This can also work in reverse order, as file names usually indicate the directory that houses them.

Files located online or on other systems often point to the specific server and computer from which they were uploaded, providing investigators with clues as to where the system is located; matching online filenames to a directory on a suspect's hard drive is one way of verifying digital evidence. At this stage, computer forensic investigators work in close collaboration with criminal investigators, lawyers, and other qualified personnel to ensure a thorough understanding of the nuances of the case, permissible investigative actions, and what types of information can serve as evidence.

Documenting and Reporting

In addition to fully documenting information related to hardware and software specs, computer forensic investigators must keep an accurate record of all activity related to the investigation, including all methods used for testing system functionality and retrieving, copying, and storing data, as well as all actions taken to acquire, examine and assess evidence. Not only does this demonstrate how the integrity of user data has been preserved, but it also ensures proper policies and procedures have been adhered to by all parties. As the purpose of the entire process is to acquire data that can be presented as evidence in a court of law, an investigator's failure to accurately document his or her process could compromise the validity of that evidence and ultimately, the case itself.

Why Should We Report Cyber Crime?

Some of the companies do not report a cyber crime incident because they fear this will harm their reputation amongst its shareholders. Some of the data are very sensitive and its disclosure may impact their business negatively. But, the fact is until and unless a cyber crime incident is reported, the cyber criminals will never be crabbed by the law enforcement agencies. This will further worsen the conditions and encourage the criminals to repeat these types of incidents with the same or the other organizations. So it is very important to identify and prosecute them. This will help not only to identify the existing threats to the economy and the infrastructure but also new threats are identified.

Further Reading:

- ✓ ***Guide to Computer Forensics and Investigations, by Book by Amelia Phillips, Bill Nelson, and Christopher Steuart 2003***
- ✓ ***File system forensic analysis, by Book by Brian Carrier 2005***