FIRST SEMESTER EXAMINATIONS: 2016/2017

CSIT425: COMPUTER CRIME, FORENSICS AND AUDITING

MARKING SCHEME

INSRUCTIONS

ANSWER ANY THREE OF THE QUESTIONS FOR 15 MARKS EACH

TIME ALLOWED: ***TWO AND A HALF (2½) HOURS***

[60 MARKS TOTAL]

]

1. The Principles of Computer Forensics is to recover, analyse, and present computer based material in such a way that it is useable as evidence in a court of law. Therefore it is essential that none of the equipment or procedures used during the examination of the computer prevent this.

a. Define computer forensics and briefly explain the five phases that are used in digital forensic investigation process.

b. Using you understanding explain why Computer evidence must be Authentic, Accurate, Complete and Convincing to juries and in conformity with common law and legislative rules and admissible at court.

c. Explain the theory behind the searching process in the evidence searching phase.

d. Explain the search techniques after you have after you have taken steps to preserve the data?

(20 MARKS)

ANSWER 2

a.

- It is the Process of Investigating computers and its associate's media to determine if it has been used to commit a crime and or used to gain an unauthorized activities.

- Preservation – The preservation of the digital media being investigated. Eg. Secure crime scene, take pictures, packaging and labelling of evidence. Date and time of investigation.
- Identification – Identify all evidences that are evidential to the crime to assist in analysis.
- Extraction – Acquisition or extraction of evidential data from digital media for analysis, use write blocker to protect data from being writing to before Mirror imaging data for analysis

- Documentation of digital evidence - Documentations ensure that there is continuity of evidence, sometimes known as chain of custody. E.g. Record Date, time, questions asked finding, hypothesis.
- Report Writing – Writing your final unambiguous findings of the investigations to whoever authorised the investigation. Eg. To the Police, Corporate Body or an Individual

b.

Authenticity: Does the evidential material come from where it claim to come from.

Accurate: Can the substance of the story the material tells be believed and is it consistent? In the case of computer derived material, are there reasons for doubting the correct working of the comp uter.

Completeness: Is the story that the material claims to tell complete? Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing.

Convincing to jurors: Evidence must be freedom from interference and contamination: Are these evidences and levels acceptable as a result of forensic investigation and other post event handling.

Two Key steps:

- Define the general characteristics of the object for which we are searching and then look for that object in a collection of data. For example, if we want all files with the JPG extension, we will look at each file name and identify the ones that end with the characters ". JPG."
- This process typically starts with a survey of common locations based on the type of incident, if one is known.

d.

- Most searching for evidence is done in a file system and inside files.
- A common search technique is to search for files based on their names or patterns in their names.
- Another common search technique is to search for files based on a keyword in their content.
- Files can be search based on their temporal data, such as the last accessed or written time.
- For example, if we are investigating Web-browsing habits, we will look at the Web browser cache, history file, and bookmarks.
- If we are investigating a Linux intrusion, we may look for signs of a rootkit or new user accounts.
- We can search for known files by comparing the MD5 or SHA-1 hash of a file's content with a hash database. such as the National Software Reference Library

- Hash databases can be used to find files that are known to be bad or good.
- Another common method of searching is to search for files based on signatures in their content. This allows us to find all files of a given type even if someone has changed their name.
- When analysing network data, we may search for all packets from a specific source address or all packets going to a specific port.
- We also may want to find packets that have a certain keyword in them.

1. To effectively combat cybercrime, greater emphasis must be placed in the compute r forensic field of study. Therefore the professional must know who the cyber criminal's pri mary targets are and who can use Computer Forensic Evidence.

a. With your understanding and using examples, explain the four roles the computer can play in a Cybercrime

b. Identify about three groups who require Computer Forensic Evidence and briefly explain what they use them for?

c. Explain the importance of digital forensics Tools

d. Explain the importance of Documenting searches procedures.

(20 MARKS)

ANSWER

a.

- A computer can play one of three roles in a computer crime:
- A computer can be the **target** of the crime
- It can be the **instrument** of the crime
- Or it can serve as an **evidence repository storing valuable information** about the

crime.

b.

- Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.

- Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman’s compensation cases.
- Corporations often hire computer forensics specialists to find evidence relating to:

- Sexual harassment corporations often hire computer forensics specialists to find evidence relating to: Sexual harassment, Embezzlement, Theft or misappropriation of trade secrets, Other internal/confidential information

c.

- The importance of digital forensics tools provides the investigator ability to capture and forensically analyze digital media and multiple computers across your enterprise simultaneously is critical when performing root cause analysis and internal investigations.
- The digital forensics tools enables proactive use of this technology and allows you to detect threats that have circumvented the typical signature-based tools, such as antivirus, intrusion detection and other alerting systems.

d.

- Documentations ensure that there is continuity of evidence, sometimes known as chain of custody. That is, it must be possible to **account for all that has happened to the exhibit between its original collection** and its appearance in court preferably unaltered. It also ensure good record keeping
- When you fail to document something in its present you cant catch up anymore.

Eg Document access log for coming in and out of crime scene secure the areas.

Eg interview staff, managers, suspects, individuals involved in the evidence

- Due diligence must be applied in evidence gathering and document

1. An ethical hacker possesses the skills, mindset and tools of a hacker but is also trustworthy. Ethical hackers perform the hacks as security tests for their systems. Also the intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. Therefore the attacker must have Methods, Opportunity and Motive(MOM)

a. Explain with examples the acronym 'MOM' and why the malicious attacker must have these three things to penetrate a system?

b. Identify and briefly explain the four types of threats that can be used to penetrate a system.

c. Using the acronym 'MOM' explain the differences between a hacker and an ethical hacker.

d. Briefly explain the three main types hackers (crackers) techniques that the hacker can technically commit to network connections.

(20 MARKS)

Answer3

a.

"MOM" - Method, Opportunity and Motive

A malicious attacker must have three things:

- Method: the skills, knowledge, tools, and other things with which to be able to pull off the attack. E.g for the two cyber criminals to hack or penetrate, intercept, modify and fabricate the CID emails, they must have tools e.g. Backtrack or Sluoth Kit to penetrate. They modify, delete, and steal critical information.
- Opportunity: the time and access to accomplish the attack – They must be able to gather and monitor various email address and their contents for
- Motive: a reason to want to perform this attack against this system. They are out for

personal gain: fame, profit, and even revenge. Eg, They were about to cash $13 when arrested.

b.

An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network.

- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.
- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modi fication**. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.
- Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing.

c.

- Hacker - Someone who tries to compromise computers or maliciously breaks with malicious intent into systems for personal gain. They are out for personal gain: fame, profit, and even revenge. Many malicious hackers are electronic thieves. They modify, delete, and steal critical information, often making other people miserable.
- Ethical hackers - perform the hacks as security tests for their systems. Ethical hackers (or good guys) protect computers against illicit entry. An ethical hacker possesses the skills, mind set, and tools of a hacker but is also trustworthy.

d.

Hacking or Cracking techniques on networks include:

- Creating worms - **Computer worms** are malicious software applications designed to spread via computer networks.

- Computer worms are one form of **malware** along with viruses and trojans.
- Initiating denial of service (DoS)attacks - refers to a form of attacking computer systems over a network. DoS is normally a malicious attempt to render a networked system unusable (though often without permanently damaging it).
- Establishing unauthorized *remote access* connections to a device. Such as: **Interruptio n, Interception, Modification and Fabrication**

1. When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role. To ensure this as the digital forensic investigator: Using case studies such as the Roman Assignment Case study, EOCO and GFA case , and the CID verses the two cybercriminal cases as examples for each question:

a. Explain what Life Analysis is and the methodologies used in evidence gathering

b. Explain what Dead Analysis is and the methodologies used in evidence gathering

c. Explain with examples the PICL guidelines in you digital forensic investigations?

d. Why is important that data saved during a dead or live analysis, a cryptographic hash should be calculated.

(20 MARKS)

Answer4

a.

A live analysis occurs when you use the operating system or other resources of the system being investigated to find evidence. Eg. Ebay, Amazon and Banks. This process typically starts with a

survey of common locations based on the type of incident, if one is known.

- For example, if we are investigating Web-browsing habits, we will look at the Web browser cache, history file, and bookmarks.

- For a live analysis, suspect processes can be killed or suspended.
- The network connection can be unplugged (plug the system into an empty hub or switch to prevent log messages about a dead link)
- Network filters can be applied so that the perpetrator cannot connect from a remote system and delete data.

b.

- A dead analysis occurs when you are running trusted applications in a trusted operating system to find evidence. A dead analysis is more ideal because the system is shutdown, but is not possible in all circumstances. Eg. A cyber crime or murder case that has occurred already and the culprits are being investigated.
- The goal of this phase is to reduce the amount of evidence that is overwritten, so that we can limit the number processes that can write to our storage devices.

- For a dead analysis, we will terminate all processes by turning the system off, and we will make duplicate copies of all data. For example, legal requirements may cause you to unplug the system and make a full copy of all data.
- Write blockers can be used to prevent evidence from being overwritten.
- When important data are saved during a dead analysis, a cryptographic hash should be calculated to later show that the data have not changed.

c.

- P**reservation of the system** being investigated. Do not modify any data that could be used as evidence. You do not want to be in a courtroom where the other side tries to convince the jury that you may have overwritten exculpatory evidence.
- This is what we saw in the Preservation Phase of the investigation process.

- Copy important data, put the original in a safe place, and analyze the copy so that you can restore the original if the data is modified.
- Calculate MD5 or SHA hashes of important data so that you can later prove that the data has not changed.
- Use a write-blocking device during procedures that could write to the suspect data.

- **Isolate –** Is the analysis environment from both the suspect data and the outside world. I solate yourself from the suspect data because you do not know what it might do. Running an executable from the suspect system could delete all files on your computer, or it could communicate with a remote system. Running an executable from the suspect system could delete all files on your computer Or it could communicate with a remote system. Eg. Opening an HTML file from the suspect system could cause your Web browser to execute scripts and download files from a remote server.

- Is to ***correlate data*** *with other independent sources. This helps reduce the* risk of forged data. For example, timestamps can easily be changed in most systems. Therefore, if time is very important in your investigation, you should try to find log entries, network traffic, or other events that can confirm the file activity times.
- Is to **log and document** your actions. This helps identify what searches you have not yet conducted and what your results were. When doing a live analysis or performing techniques that will modify data, it is important to document what you do so that you can later document what changes in the system were because of your actions.

d.

- A cryptographic hash should be calculated to later show that the data have not changed.

A cryptographic hash, such as MD5, SHA-1, and SHA-256, is mathematical formula that generates a very big number based on input data. If any bit of the input data changes, the output number changes dramatically.

1. The board of directors of a technical research company demoted the company's founder and chief executive officer CEO. The executive, disgruntled because of his demotion, was later terminated; it was subsequently determined that the executive had planned to quit about the same time he was fired and establish a competitive company. Upon his termination, the executive took home two computers; he returned them to the company four days later, along with another company computer that he had previously used at home. Suspicious that critical information had been taken; the company's attorneys sent the computers to a CFST for examination.

a. Using the acquired evidence generated, discusses the analysis techniques and steps the CFS Team used in their quest to gather the table of information usage?

b. Applying the scientific method to digital forensics analysis, explain the methods involve to objectively and critically assessing digital evidence to gain an understanding of and reach conclusions about the crime.

c. Define what type of analysis this is required and what methodology that should be applied.

d. How do you analyse a server that has been compromised in your digital investigation to supports or refutes a hypothesis.

(20 MARKS)

Gather information and make observations and carryout forensic examination and involves:

- Analysis Techniques will aid Verifying the integrity and authenticity of the evidence, Pe rforming a survey of all evidence to determine how to proceed most effectively, Do some pre-processing to salvage deleted data, handle special files, filter out irrelevant data, and extract embedded metadata.
- Carryout a keyword searching to focus on certain items, and a preliminary review of

system configuration and usage. You need not be limited to digital evidence, and can be augmented by interviews, witness statements, and other materials or intelligence.

b.

- Evaluating the source of digital objects, Exploring unfamiliar file formats to extract usable information. Developing timelines to identify sequences and patterns in time of events Performing functional analysis to ascertain what was possible and impossible, Perform relational analysis to determine the relationships and interaction between components of a crime.

C,

- A dead analysis will be required as the digital media has been given to me by the company. A dead analysis is more ideal because the system is shutdown. Eg. A corporate crime has occurred already and the culprits are being investigated.
- For a dead analysis, we will terminate all processes by turning the system off, and we will make duplicate copies of all data. For example, legal requirements may cause you to unplug the system and make a full copy of all data.
- Write blockers can be used to prevent evidence from being overwritten.

When important data are saved during a dead analysis, a cryptographic hash should be calculated to later show that the data have not changed.

D, Consider a server that has been compromised.

- We start an investigation to determine how it occurred and who did it. During the investigation, we find data that were created by events related to the incident.

- We recover deleted log entries from the server, find attack tools, and find numerous vulnerabilities that existed on the server.

- Using this data, and more, we develop hypotheses about which vulnerability the attacker used to gain access and what she did afterwards. Later, we examine the firewall configuration and

logs and determine that some of the scenarios in our hypotheses are impossible because that type of network traffic could not have existed, and we do not find the necessary log entries.

- Therefore, we have found evidence that refutes one or more hypotheses.