UNIVERSITY OF GHANA

BSc COMPUTER SCIENCE

FIRST SEMESTER EXAMINATIONS: 2017/2018

CSIT425: COMPUTER CRIME, FORENSICS AND AUDITING

MARKING SCHEME

INSRUCTIONS

ANSWER ANY THREE OF THE QUESTIONS FOR 20 MARKS EACH

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

[60 MARKS TOTAL]

Q1a Define computer forensics and with the aid of a diagram, briefly explain the five phases that are used in digital forensic investigation process? [5MARKS]

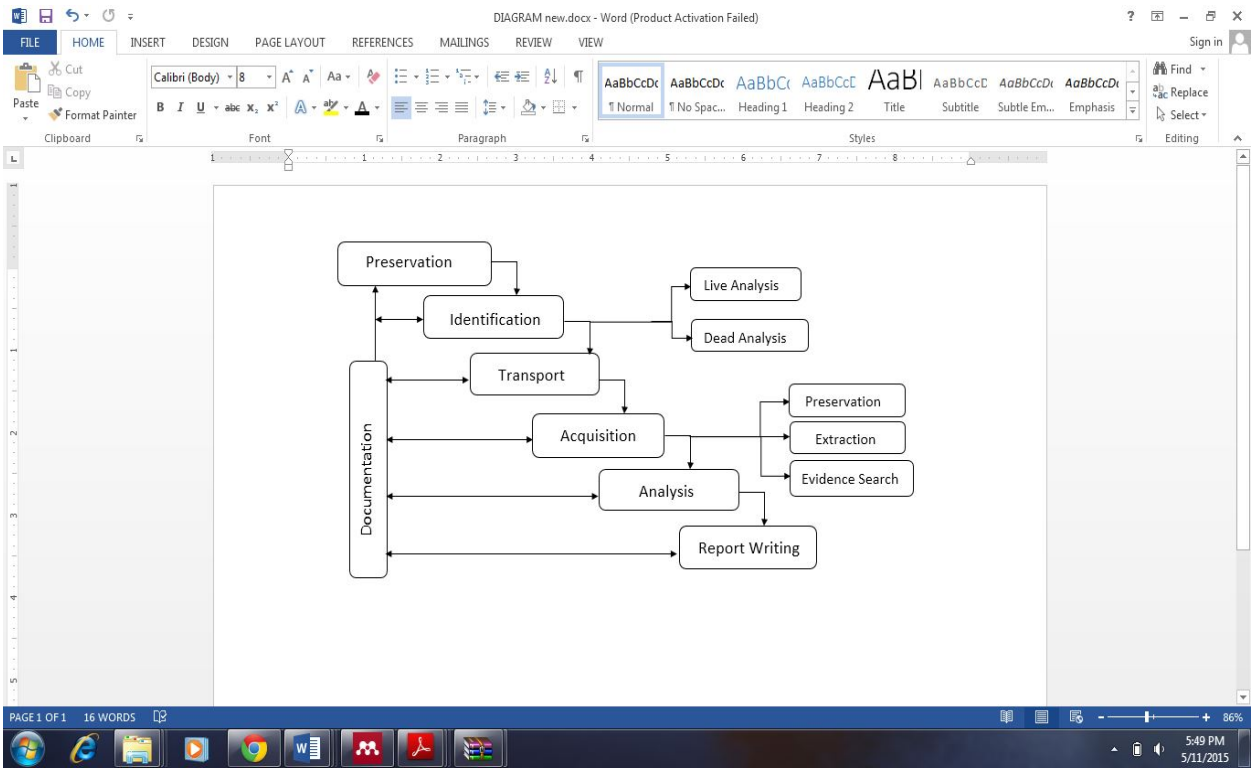
Q1b. Using the EOCO-vrs-GFA 2013 case study, explain why Computer evidence must be Au thentic, Accurate, Complete and Convincing to juror and in conformity with common law and legislative rules and admissible at court? [5MARKS]

Q1c. Explain the theory behind the searching process in the evidence searching phase? [5MAR KS]

Q1d. After you have taken steps to preserve the data, explain search techniques in acquisition phase? [5MARKS]

ANSWER1A

Computer Forensics 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

1b.

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.

1c. 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.

1d.
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.

Q2. Computer Forensics students must understand the laws and regulatory Frameworks with their particular jurisdiction. State and Brief explain the following Legal Acts and who they are aimed at? [20 MARKS]

Q2a. Section 1 of the Computer Misuse Act 1990

Q2b. Electronic Transactions Act 2008

Q2c. The Fraud Act 2006

Q2d. Section 1 of the Theft Act 1968

Q2e. Sale of Goods Act 1979

Q2f. Supply of Goods and Services Act 1982

ANSWER 2

Section 1 of the Computer Misuse Act 1990.

Is aimed directly at hackers who gain access to computer programs or data without any further intention to carry out any other act.

- It says that a person is guilty of an offence if:

- he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
- the access he intends to secure is unauthorized; and
- he knows at the time when he causes the computer to perform the function that this is the case.

The offence of theft is defined under section 1 of the Theft Act 1968 as

- If a person carries out a fraud which results in that person obtaining property, including money or a bank credit, the offence of theft may have been committed.
- A section in the Theft Act 1968 states that:
- A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it . . .
- a dishonest appropriation of property belonging to another with the intention to permanently deprive the other of it.
- If a person gains access to a computer system without permission and then makes a printout of some information contained therein, has he committed theft?
- The fact that the owner of the information has not been deprived of it, because the hacker has only made a copy, is fatal to any charge of theft.

Electronic Transaction Act 2008

Act 7.1: The Admissibility of an electronic record shall not be denied as evidence in legal proceedings except as provided in the Act.

In assessing the evidential weight of an electronic record the Court shall have regard to:

a) The reliability of the manner in which the electronic records was generated, displayed, stored and communicated.

b) The reliability of the manner in which the integrity of the information was stored

c) The mana in which its originator was identified,

d) Any other facts that the Courts may consider relevant

The Fraud Act 2006

- A person is guilty of fraud if he is in breach of any of
    - fraud by false representation;
    - fraud by failing to disclose information; and

- fraud by abuse of position.

Sale of Goods Act 1979

Sale of Goods Act 1979 refers to Computer equipment (hardware) that may be purchased outright or hired.

- If purchased then the Sale of Goods Act 1979 will apply
- Computer hardware, if it is sold, will be subject to the Sale of Goods Act
- If the supplier goes beyond the mere supply of the equipment and carries out some work such as assembling and installing the equipment, the Supply of Goods and Services Act 1982 will apply

Supply of Goods and Services Act 1982

An agreement to write software will be within the scope of the Supply of Goods and Services Act 1982

- If the contract is for the hire of the equipment, then the Supply of Goods and Services Act 1982 will apply, whether or not installation or other services are also provided by the supplier.
- Contracts for hardware and software are governed by different legal rules.
- This simple distinction is not always easy to apply in practice
- The suggested approach is to look at the predominant purpose of the transaction.
- In other words, did the person acquiring the subject matter think that he was obtaining hardware or software?

Q3a. Use any case studies such as the Roman Case study, Two Nigerians Verses Ghana Arm Forces cases as examples to answer the questions:

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. Use the PICL guidelines to carry out digital forensic investigations process?

d. A Cryptographic Hash should be calculated on data saved during a dead or live analysis. Explain why.

ANSWER 3a

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.

3b.

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 cybercrime 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.

3c.

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. Isolate 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.

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.

L**og 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.

3d. 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.

Q4a. In Relation to Information Technology Contracts, define TERMS OF CONTRACT and with examples, explain the concepts of implicit and explicit terms. [5MARKS]

Q4b. In relation to Computer Misuse Act 1990, briefly explain with examples the Latin name: mens rea and actus reus of the offences. [5MARKS]

ANSWER 4A

Terms of Contract

Contractual terms in an agreement that exist between two parties. When there is a contract, it is important to know precisely what the terms of the contract are. Even where the contract is wholly in writing, things are not necessarily that straightforward and the law may insert additional terms (implied terms) into the contract or strike out some of the terms apparently agreed upon by the parties to the contract.

Implied Terms:

- A particular problem is where the contract is not in writing or is only partly in writing. An example is where a signed note or memorandum indicates that a contract exists but clearly does not contain all the terms on the face of it.
- On its own such a note would be unenforceable because it lacks certainty.
- In relation to oral contracts and contracts partly in writing, it will be a matter of submitting evidence of the other terms to give the contract sufficient certainty.

- To overcome some of these difficulties, the law may imply terms into the contract.

Express Term

- The first task is to look at what has been expressly agreed by the parties.
- The express terms, whether oral or in writing, may be the only terms of the contract.
- In many cases, the law will imply terms into the contract
    - a result of legislation.
    - on the basis of common law.
- An unexpressed term can be implied if and only if the court finds that the parties must have intended that the term forms part of their contract.

[5MARKS]

ANSWER 4B

In relation to Computer Misuse Act 1990, briefly explain with examples the Latin name:

mens rea and actus reus of the offences.

ANSWER

- The mens rea of the offence is an intention to secure access to any program or data and concurrent knowledge that the access is unauthorized.
- **mens rea** (roughly equating to a guilty mind) and
- The actus reus is causing a computer to perform any function and the fact that the intended access is unauthorized.
- the prohibited acts or omissions, known as the **actus reus** of the offence.

[5MARKS]