

**2ND SEMESTER 2021/2022 ACADEMIC YEAR**

**MID TRIMESTER EXAMINATION ANSWER BOOKLET**

THE FOLLOWING DETAILS MUST BE COMPLETED BY THE STUDENT

400

ADS19B00208Y

STUDENT’S ID NUMBER­­­­­­­­­­: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ LEVEL:\_\_\_\_\_\_\_\_\_\_

IT454

COMPUTER FORENSICS

COURSE COD**E: \_\_\_\_\_\_\_\_\_** COURSE TITLE:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EMMANUEL ADOTEY PAPPOE

LECTURER’S NAME: (Refer to the Question Paper) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**QUESTION NUMBER: (e.g., Q1) \_\_\_\_\_\_\_\_SUB-QUESTION (e.g., 1(a))\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PART A**

**QUESTION 2**

1. Forensic Soundness takes place when the Electronically Stored Information (ESI) as digital evidence, stays complete and materially unaltered which is because of using a methodology or technology. It is also an application of a transparent digital forensics process which preserves the initial meaning of data for production in a law court.

The four principles include:

MINIMALLY HANDLING THE ORIGINAL: A forensic image of electronically stored information should be taken and used to carry out investigative processes and techniques. Digital forensic process should be minimally applied to original data sources.

ACCOUNTING FOR ANY CHANGE: In some cases, digital evidence can change from its original state. When this happens, it would be documented to note the extent, nature, and reason for the change.

COMPLY WITH THE RULES OF EVIDENCE: Applicable rules of evidence should be considered throughout an investigation.

AVOID EXCEEDING ONE’S KNOWLEDGE: Avoid any activity which is beyond one’s current level of skill and knowledge.

1. The chain of custody is used to show the transfer of ownership over digital evidence between entities and it can also be used to validate the integrity of evidence which is been presented in a court of law.

The guidelines which are required in the chain of custody process includes:

COLLECTION OF DATA: This is the first stage which involves identification, recording, labeling and acquisition of data from all relevant sources which preserves the integrity of the data and the evidence collected.

EXAMINATION: the chain of custody is documented during this process, and it outlines the forensic process undertaken. It is necessary to take screenshots all through the process to show the tasks which are completed, and the evidence uncovered.

ANALYSIS: This is the examination stage result. Legally justifiable methods and techniques are used to get useful information to address questions posed in a particular case.

REPORTING: This stage includes the statement regarding chain of custody; the detailing of the various tools used; the description of the analysis of different data sources; identifying issues and vulnerabilities; recommending additional forensics measures which can be taken.

1. Ethics outlines the ethical principles which governs behavior and decisions in a company. Ethics in computer forensics has to do with a set of moral principles which regulates the use of computers.

The importance of ethics in computer Forensics include:

In professional ethics, it provides individuals openness and disclosure, due diligence, and duty of care.

In computer ethics, it sets a standard to guide and instruct people in the ethical use of computer system.

In business ethics, it aids organizations to conduct themselves ethically to exist in a competitive global landscape.

1. Data acquisition has to do with the process of copying data. While in computer forensics, it’s the collection of digital evidence.

Types of acquisitions include:

Static acquisition

Live acquisition.

The 2 methods for determining the best data acquisition includes:

The collection of large evidence from a large drive can take hours, if a time is limited, then the following should be considered:

LOGICAL ACQUISITION DISK-TO-DISK OR DISK-TO-DATA FILE: This captures only the specific types of files of interest to the case. This method is used when you do not need to examine the whole drive.

SPARSE ACQUISITION: This is quite like logical acquisition; it gathers fragments of deleted or unallocated data and this method is used when you do not need to examine the entire drive.

**QUESTION 3**

A) Personal Ethics has to do with an individual’s personal morals and code of conduct. These ethics are instilled in the individual by their parents, family, and friends at the very beginning. Without personal ethics, the life of a human being is shallow and incomplete. For example, an individual’s honesty, openness, sense of responsibility and so on can be put into consideration. An individual’s personal ethics are revealed in a professional situation through their behavior.

Professional Ethics has to do with an individual’s values and principles which are introduced to an individual in a professional organization.

Every employee in a company must follow certain rules and do not have any choice. These ethics are necessary to import in the professional world because it brings in a sense of disciple into the individual’s life and maintain the decorum in the company. For example, transparency, confidentiality, fairness and so on falls under professional ethics.

Computer ethics are a set of moral standards which govern the use of computers. It is society’s views about the use of computers, both software and hardware.

B) RAW FORMAT (OPEN-SOURCE FORMAT): This is a bit-by-bit copy of the drive to a file (Linux dd command). It allows for fast data transfers. It can also ignore minor data read errors on source drives and some computer forensics tools can read raw format.

Some of its cons include needing as much storage space as original disk or data. Not all data is collected. Some raw format tools or freeware versions night does not gather marginal/bad sectors on the source drive.

PROPRIETARY FORMATS: some commercial computer forensics tools have their own formats for the collection of digital evidence. It offers features not available with Raw like; this gives an option whether to compress image files and can split an image into smaller segmented files. It also integrates metadata into the image file.

Some of its cons includes the inability to share an image between several vendors’ computer forensics analysis tools. The proprietary file formats simply means that you will convert from one format to another making use of multiple tools. The conversion between these formats may corrupt data if the formats are not understood properly.

There is a file size limitation for each segmented volume.

ADVANCED FORENSICS FORMAT (AFF): Its design goals include providing compressed or uncompressed image files. There are no size barriers for disk-to-image files. It provides space in the image file or the segmented files for metadata. It’s a simple design with extensibility and an open source for several platforms and OSs. It is an open source.

C) Maintaining the highest level of objectivity in all forensic examinations

and present the facts involved accurately.

◾ Examine and analyze the evidence in a case thoroughly

◾ Examinations based upon established, validated principles should be conducted

◾ Give opinions having a basis that is demonstratively reasonable

◾ Not withholding any findings, be it inculpatory or exculpatory, which

would cause the facts of a case to be misrepresented

◾ On no account should you misrepresent credentials, education, training, and experience or

membership status

1. - An organization should be ethical to protect the interests of themselves, the public interest, and the business community at large.

* To meet the expectations and grow trust with stakeholders, the investors, and shareholders.
* To create an environment where staff can act consistently with the organization’s principles and values.

**PART B**

**QUESTION 4**

1. PERSONAL ETHICS: are values that individuals regard as desirable and are usually applied to behaviors of people. An example of personal ethics includes; Showing concern and respect for the well-being of others.

PROFESSIONAL ETHICS: Has to do with a person or people who carries out a specific activity like digital forensics within a business environment. An example would be: loyalty to professional responsibilities.

COMPUTER ETHICS: is a set of standards to direct and instruct people in the ethical use of computers. An example would be; It is society’s views about the use of computers, both software and hardware.

BUSINESS ETHICS: Is the application of the general principles which was discussed above to behavior within a business environment. An example would be: to protect the interests of themselves, the public interest and the business community in general.

IMPARTIALITY AND OBJECTIVITY: one of the main importance for carrying out an investigation is to establish factual conclusions which are based on credible evidence. There are times when the subject is known or familiar with the practitioner and it is their responsibility to maintain the utmost fairness while the investigation is ongoing to draw conclusions based on factual and credible evidence.

OPENNESS AND DISCLOSURE: while analyzing evidence, practitioners may encounter certain findings which need to be assessed further before factual conclusions can be made like paying attention to inculpatory or exculpatory evidence.

CCONFIDENTIALITY AND TRUST: a digital forensic practitioner’s work comes with high level of trust. They can come across highly sensitive and confidential information which needs to be kept a secret and communicated on a need-to-know basis.

DUE DILIGENCE AND DUTY OF CARE: Informed decision-making during an investigation must be made according to the applicable laws, regulations and standards to avoid potential consequences. A practitioner must constantly demonstrate their behavior and conduct is done honestly and in compliance with laws and professional norms.

1. Three critical questions to be answered would include:

- what items are physically located within the crime scene?

- where are these items/evidence physically located within the crime scene?

- what condition are these items/evidence currently in?

C) Locard’s Exchange Principle: Anyone or anything entering a crime scene carries something in with them and leaves something behind as they leave.

The Locard’s Exchange Principle states that with contact between entities, there will be an exchange. In the realistic world, an instance of this exchange can happen where a perpetrator might inadvertently leave their fingerprints or traces of blood at the crime scene.

In the digital world, evidence always exists in a logical state which is intangible in comparison to physical evidence. An example would be an email communication and web browsing are how these exchanges can occur within the digital world.

D) The rules of evidence to be followed include:

- the Digital evidence integrity must be preserved to be admissible in the court of law.

- if evidence is contaminated, it cannot be decontaminated.

- The digital evidence must be reliable: Authentic evidence, clear and easy to understand, and believable by a jury.

- the digital evidence must be complete: exculpatory evidence for alternative suspects.

**QUESTION 5**

A) The standardized international principles for the recovery of digital evidence are governed by the following attributes:

◾ Consistency with all legal systems

◾ The use of a common language

◾ Durability

◾ The ability to cross international boundaries

◾ The ability to instill confidence in the integrity of evidence

◾ Applicability to every forensic evidence

◾ Applicability at every level, which includes that of individual and agency

B) Best practices when shooting video or taking photographs to document a crime scene include:

◾ Providing a complete view of the physical environment, which includes floor-to-

ceiling and wall-to-wall

◾ Capturing individual perspectives of dedicated work areas (as needed), such

as cabinets, shelves, garbage cans

◾ Showing wired connections between computer systems and peripherals or

other devices, such as printers or switches

◾ Recording ports, slots, and plugs on the computer systems that are open,

empty, or unused

◾ Picturing processes, documents, etc., that are actively visible on the monitor.

It is important not to press any keys or buttons that could result in triggering

the system to perform some action (i.e., logic bomb4).

In addition to photographs and videos, details about the crime scene must also be

documented in a notebook. A dedicated notebook, or logbook, should be used by

every digital forensic practitioner as a means of maintaining an accurate record of

events, actions taken, and interactions involving their investigations. Like how

law enforcement agencies document their interactions in a logbook, forensic prac-

titioners need to write down their efforts on the presumption that the investigation

could eventually end up in court

C) From a technical perspective,

there are times when digital evidence cannot be compared to its original state.

such as with random access memory (RAM) that is constantly in a state of change.

For these occurrences, point- in-time snapshots are taken that demonstrate the state

of the technology at that moment. From a legal perspective, authentication means

satisfying the legal systems that the:

◾ Content of the record has remained unchanged

◾ Information in the record does in fact originate from its original source

◾ Extraneous information about the record is accurate (i.e., timestamp)

Supporting the need to establish authenticity, the goal for maintaining the integrity

of digital evidence is to demonstrate that it has not been changed since the time it was first gathered. In digital forensics, verifying integrity involves comparing the

digital fingerprint of digital evidence when it is first gathered and subsequently

throughout its lifecycle.

D) Digital forensics is the application of science to law and must follow established and scientifically proven principles, methodologies, and techniques required to legally admit evidence in a court of law.

**QUESTION NUMBER: (e.g., Q2) \_\_\_\_\_\_\_\_SUB-QUESTION (e.g., 2(a))\_\_\_\_\_\_\_\_\_\_\_\_\_**