

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

**MID SEMESTER EXAMINATION ANSWER BOOKLET**

THE FOLLOWING DETAILS MUST BE COMPLETED BY THE STUDENT

400

ADS19A00110Y

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

IT454

COMPUTER FORENSICS

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

EMMANUEL ADOTEY PAPPOE

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

**PART A**

**QUESTION NUMBER: (e.g. Q1) \_2\_\_SUB-QUESTION (e.g. 1(a))\_\_2A,B,C,D\_\_**

1. It occurs when the application of a methodology or technology ensures that the Electronically Stored Information (ESI) used as digital evidence remains complete and substantially unchanged. It is also a visible use of digital forensics, preserving data's original meaning for production in court.

The four (4) principles that must be followed to achieve soundness specific to digital evidence are;

* Minimally Handle the Original: Original data sources should only be subjected to minimal digital forensic processing. Instead, a forensic image of the ESI should be captured and used to carry out the procedures and methods of an investigation.
* Take into Account Any Change: Digital evidence occasionally undergoes changes from its initial state. Change should always be recorded in order to describe its nature, scope, and cause.
* Adhere to the Rules of Evidence: When conducting an investigation, the relevant rules of evidence (such as laws and regulations) should be taken into account.
* Refrain from Going Beyond Your Knowledge: Refrain from engaging in any activity or work that is beyond your current degree of expertise.

1. The chain of custody can be utilized to verify the reliability of evidence that has been submitted in court as well as to demonstrate the transfer of ownership of digital evidence between different entities.

The rules that must be followed during the chain of custody process include:

* Data collection: Data must be identified, recorded, labeled, and acquired from all pertinent sources during the first stage of the investigation in order to maintain the validity of the evidence gathered.
* Examination: During this procedure, the chain of custody is recorded and it describes the forensic procedures used. Throughout the procedure, screenshots must be taken to document the tasks that are accomplished and the evidence that has been found.
* Analysis: This is the outcome of the examination stage. In order to gather relevant data for answering the questions raised in a certain case, legally acceptable procedures and techniques are used.
* Report: The chain of custody statement, a description of the tools used, a description of the analysis of the various data sources, the identification of problems and vulnerabilities, and suggestions for additional forensics measures are all included in the reporting stage.

1. Ethics describes the moral standards that guide actions and judgments within an organization. In computer forensics, ethics refers to a set of moral standards that govern how computers should be used.

its importance;

* In professional ethics, it offers people with transparency and disclosure, due diligence, and duty of care, which are all important in computer forensics.
* In computer ethics, a guideline is established to help individuals use computers ethically.
* In terms of business ethics, it helps businesses act morally so they can compete in a global market.

1. It is related to data gathering. While it is the gathering of digital evidence in computer forensics.

A few examples of acquisitions are:

* Indefinite acquisition
* real-time acquisition

The following are the 2 techniques for selecting the best data acquisition:

Obtaining substantial evidence from a sizable disk can take hours; therefore, if time is of the essence, the following should be taken into account:

* Logical arrangement a data file or a disk-to-disk: Only the precise file types relevant to the case are captured in this. When you don't need to look at the entire drive, you employ this technique.
* SPARES Acquisition: Similar to logical acquisition, this method is employed when only a portion of the data needs to be examined. It collects bits of deleted or unallocated data.

**QUESTION NUMBER: (e.g. Q2) \_3\_\_SUB-QUESTION (e.g. 2(a))\_\_3a,b,c,d\_\_**

1. The differences explained;

* Personal ethics pertains to a person's personal principles and standards of behavior. From the early beginning, parents, relatives, and friends implant these morals in the individual. The life of a person is brief and lacking without personal ethics. An individual's integrity, openness, accountability, and other traits, for instance, can be taken into account.
* Computer ethics are a collection of moral principles that guide how computers should be used. It is how the general public feels about using computers, both software and hardware.
* In a professional, a person's behavior reveals their personal ethics. A person's values and principles that are introduced to them in a professional organization are what is meant by professional ethics. Every employee in a corporation is obligated to abide by certain standards and cannot opt out of doing so. The professional world has to adopt these standards since they bring in a maintain the etiquette in the workplace and instill a feeling of discipline in the individual's life. Transparency, confidentiality, impartiality, and other principles are examples of professional ethics.

1. The three formats of digital evidence are;

Raw format (open-source format): This creates a file from a drive's bit-by-bit copy (Linux command (dd)). It enables quick data transfers. Additionally, some computer forensics programs can read raw format, and it can tolerate tiny data read errors on source devices.  Its drawbacks include the need for as much disk or data storage as the original. Not all information is gathered. Some freeware or raw format utilities do not gather marginal or damaged sectors on the source device.

Proprietary formats: Certain professional computer forensics software has its own formats for storing digital data. It has features that Raw lacks, such as the ability to break an image into fewer segmented files and choose whether to compress picture files. It adds metadata to the image file as well. One of its drawbacks is that the computer forensics analysis techniques from different manufacturers cannot share an image. Simply said, using numerous tools to convert from one format to another is what the term "proprietary file formats" refers to. If the formats are not adequately understood, the conversion between these formats may corrupt the data. Each split volume has a file size restriction.

Advanced forensics format (AFF): Its design objectives include offering compressed or uncompressed picture files. Disk-to-image files have no size limitations. It makes room for metadata in the picture file or split files. It has a straightforward design that is extensible and open source for many platforms and operating systems. Being open source.

1. Examining the principles;

* carefully reviewing and analyzing the evidence in a case.
* conducting examinations based on recognized, validated standards.
* You must never give false information about your credentials, training, experience, or membership status.
* Give opinions with a basis that can be proven to be reasonable.
* Not suppressing any information that could lead to a misrepresentation of the facts of a case, whether it be incriminatory or exculpatory.

1. The three-ethics importance in an organization are;

* An organization should act ethically to safeguard their own interests as well as that of the general public and the business sector.
* Always fulfill commitments and increase confidence among shareholders, investors, and stakeholders.
* To foster an atmosphere where employees can operate in accordance with the organization's values and ideals.

**PART B**

**QUESTION NUMBER: (e.g. Q2) \_4\_\_SUB-QUESTION (e.g. 2(a))\_\_4a,b,c,d\_\_**

1. They are;

* Personal ethics pertains to a person's personal principles and standards of behavior. From the early beginning, parents, relatives, and friends implant these morals in the individual. The life of a person is brief and lacking without personal ethics. An individual's integrity, openness, accountability, and other traits, for instance, can be taken into account. These are moral principles that people generally apply to their behavior. An illustration of personal ethics is having regard and concern for others welfare.
* Impartiality and Objectivity: One of the most crucial aspects of doing an inquiry is coming to factual findings that are supported by solid evidence. When the issue is known to or familiar to the practitioner, it is up to them to maintain the highest level of objectivity throughout the course of the investigation in order to develop conclusions based on factual and reliable evidence.
* Professional ethics: Every employee in a corporation is obligated to abide by certain standards and cannot opt out of doing so. The professional world has to adopt these standards since they bring in a maintain the etiquette in the workplace and instill a feeling of discipline in the individual's life. Transparency, confidentiality, impartiality, and other principles are examples of professional ethics. It Concerns an individual or people who do a particular task, like digital forensics, in a professional ethics loyalty to one's obligations as a professional is one example.
* Diligence and duty of care: To minimize potential repercussions, informed decisions throughout an investigation must be taken in accordance with the relevant laws, rules, and standards. An expert must consistently display their behavior and Its conduct is carried out honestly, in accordance with the law, and industry standards.
* Computer Ethics: a collection of moral principles that guide how computers should be used. It is how the general public feels about using computers, both software and hardware. A set of guidelines and instructions for using computers ethically. As an illustration, consider how society sees the use of computers both the hardware and software.
* Business ethics is the application of the broad guidelines that were previously covered to conduct in a professional setting. An illustration might be: to safeguard the interests of individuals, the general corporate community, and the public interest.
* Openness and Disclosure: When examining the evidence, practitioners may come across some facts that require additional evaluation before factual conclusions can be drawn, such as paying attention to incriminating or conclusive evidence.
* Confidentiality and Trust: A great level of trust is placed in the work of a digital forensic specialist. They may appear extremely sensitive and privileged information that should only be shared with those who need to know it.

1. Questions to be answered:

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

1. One of the main goals in conducting a forensic investigation is to establish factual conclusions that are based on credible evidence. Anyone or anything entering a crime scene carries something in with them and leaves something behind as they depart, according to Locard's Exchange Principle.

The Principle also states that, whenever two entities come into contact, there will be an exchange. In the actual world, this exchange might occur and the offender might unintentionally leave their fingerprints or blood evidence at the crime site.

In contrast to physical evidence, which can be seen and touched, evidence in the digital world always exists in a logical state. Email correspondence and web browsing are two examples of how these exchanges can take place in the digital age.

1. The standards of evidence that must be respected include:

* For digital evidence to be admitted into evidence in the court of law, its integrity must be maintained.
* Evidence that has been polluted cannot be cleaned.
* Reliable digital evidence is required: genuine proof that is convincing to a jury that is understandable and unambiguous.
* The digital evidence must be comprehensive, including material that exonerates potential suspects.

**QUESTION NUMBER: (e.g. Q2) \_5\_\_SUB-QUESTION (e.g. 2(a))\_\_5a,b,c,d\_\_**

1. The standard international principles;

* 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

1. When shooting video or taking photographs to document a crime scene, best practices include:

* Providing a full view of the physical environment, including floor-to-ceiling and wall-to-wall.
* Capturing individual perspectives of dedicated work areas (as needed), such as cabinets, shelves, garbage cans
* Displaying connectivity between computer systems and external devices or any other devices, such as printers or switches
* It is critical not to press any keys or buttons that could cause the system to perform some action (i.e., logic bomb4).

Details about the crime scene must be documented in addition to photographs and videos. A committed note pad, or logbook, ought to be utilized by each computerized measurable expert for the purpose of keeping a precise record of occasions, action taken, and associations including their examinations. Like how policing report their cooperation in a logbook, legal practitioners need to record their endeavors on the assumption that the examination could ultimately wind up in court.

1. Three qualities in computer forensics;

The initial state of digital evidence can occasionally not be compared from a technological standpoint.

as with volatile random-access memory (RAM), which is continually changing. Point-in-time snapshots are taken for these occurrences to show the status of the available technology at the time. Legally speaking, authentication entails ensuring that the legal systems:

* The information in the record has not changed.
* The record contains information that was obtained from the original source.
* Unrelated details regarding the record are correct (i.e., timestamp).

Supporting the need to uphold integrity and the urge to establish authenticity of a digital piece of evidence is to show that it hasn't been altered after it was first gathered. Verifying authenticity in digital forensics entails comparing the digital evidence is first acquired and later, it has a digital fingerprint. all the way through its life.

1. It is the process of preserving, identifying, extracting, and documenting digital evidence that can be used in court is known as digital forensics. Finding evidence from digital media, such as a computer, smartphone, server, or network, is a science. It gives the forensic team the best methods and resources to handle challenging digital-related cases. The use of digital forensics by the forensic team facilitates the identification, preservation, and analysis of the digital evidence present on many kinds of electronic devices.

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