NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE HONOURS (DIGITAL FORENSICS)	
QUALIFICATION CODE: 08BHDF	**LEVEL:** 8
COURSE: Digital Forensics Management	**COURSE CODE:** DFM811S
DATE: June 2022	**SESSION:** 1
DURATION: 3 hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION MEMORANDUM	
EXAMINER(S)	**MR. ISAAC NHAMU**
MODERATOR:	**DR. AMELIA PHILLIPS**

THIS MEMORANDUM PAPER CONSISTS OF 6 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Please use the memorandum or sample solutions to guide your marking.
2. When marking questions you should be guided by the allocation of marks.
3. Sample answers or solutions appear in bold.
4. Reasonable, in depth or innovative correct solutions provided by the students should be allocated marks even though not provided in this memorandum

Question 1

a. Explain the difference between "live acquisition" and "post-mortem acquisition". [4]

b. What are the advantages and disadvantages of live and post-mortem acquisition? [4]

c. Give an example when "live acquisition" is necessary. [2]

a. In case of live acquisition, the evidence is collected from a system where the microprocessor is running. In case of post-mortem acquisition, the evidence is collected from storage media of a system that is shut down.

b. Post-mortem provides better integrity preservation[1] and does not influence the data[1]. However, volatile data can be lost[1] in the process of shutting down a system. Live acquisition enables the collection of volatile data[1], but also influences the data[1]. It is difficult to implement in most cases because of preparation and things like storage space[1]. Live acquisitions are not reproducible.

c. In case the HD is encrypted, it is better to collect the data from the HD while it is running[2]. Or when a server of a company cannot be shut down.

Question 2

Identify ten challenges that mobile technologies bring to Digital Forensics. [10]

Challenges: To include: fast change in technology[1], conflicts due to different Oss[1], Connection problems due to large variety of data cables[1], proprietary hardware[1], need for isolation from radio signals when analyzing devices[1], volatility[1] and change in data[1], identification of some phones[1], limited tools[1], PIN/password blocking[1] ...
[10 challenges]

Question 3

a. What is confirmation bias? How can it limit the conclusions that can be drawn from digital artifacts? [5]

It is the tendency people have to seek, interpret and remember information that confirms rather than brings into doubt their preconceptions[2]. (It occurs when people give more weight to evidence that supports their hypothesis and undervalue (or ignore) evidence that could disprove it).

- Confirmation bias may result in skewed finding that try to favour the investigator's conscious or subconscious assumptions
- Also, it may result in the interpretation of ambiguous or contradictory evidence in a way that is consistent with the guilt of an already identified suspect or in line with a favoured hypothesis.

b. What are some ways we can limit the influence of forensic confirmation bias? Provide five ways. [5]

i. Apply the ABC of Investigation
   – Assume Nothing[1]
   – Believe Nothing[1]
   – Challenge Everything[1]
ii. Sift through all of the available evidence before you settle on an opinion[1].
iii. Review all available data & evidence, not just that which fits with your hypothesis[1].
iv. Appoint an investigator who has no emotional stake in the outcome[1].
v. Where possible utilise automated digital investigation products[1].

c. Outline in detail any five anti-forensics techniques and highlight how each can be countered. [10]

Students should describe any five from the following anti-forensics techniques and how they can mitigate them.

i. Encryption
ii. Program Packers
iii. Overwriting data
iv. Onion Routing
v. Steganography
vi. Changing Timestamps
vii. Other

Question 4

a. Describe the phases of a contemporary digital investigative process. [5]

b. Outline five challenges that have been presented to the digital investigative process by the current COVI-19 pandemic. [10]

c. Based on the challenges you have identified in b. suggest a modification of the contemporary investigative process described in a. [5]

a. Description of Identification, Preservation, Acquisition, Analysis and presentation.
b. Any five challenges including:
   i. Evidence collection is difficult since there are regulations that may restrict the whole investigation team from entering a location
   ii. Preservation of evidence has been an issue when the data has been collected and the work building is being disinfected and experts tend to take along the evidence to their homes and their kids might end up playing with it.
   iii. Working from home meant household people eavesdropping on confidential conversations with colleagues
   iv. Delays, with the strict law of isolation and less human contact investigations that require physical methods to acquire or extract, resulted in delayed investigation process as some resources or rules such as working in the lab with co-workers to extract information was prohibited.
   v. Remote working, trying to conduct an investigation remotely and transmitting information via the network stood a huge risk as attackers can maliciously tamper with the data or evidence by altering, or wiping data, which will stand the question of integrity in the court of law.
   vi. Cloud computing- The use of cloud computing increases during the pandemic and acquiring evidence from the cloud is difficult as the evidence can be remotely wiped or deleted by those who committed crime.
   vii. **Licensing cost and payment of experts** - due to covid 19 pandemic investigations will take longer to happen as certain companies might have people working in groups/ shifts in order not to spread the covid virus if any employee has it.. this will then force companies to extend their forensic licensing tools as investigations will last longer than usual. Not only tools also forensic experts are hired in order to carry out certain investigations and so on.
c. Any attempt to incorporate changes brought about by COVID-19

Question 5

Case:

Xiaolang Zhang worked as an engineer for Apple's autonomous car division. He had been with the company 2 ½ years when he announced that he would be resigning and returning to China to take care of his elderly mother. He told his manager that he would be working for an electric car manufacturer in China. The conversation left the manager suspicious. Company security started an investigation. They searched Zhang's two work phones and laptop—but were most alarmed when they reviewed Zhang's network activity. The story the network data told was that Zhang's activity had spiked to a two-year high in the days leading up to his resignation. It consisted of "bulk searches and targeted downloading copious pages of information" taken from secret databases he could access. When confronted, Zhang admitted to taking company data. The matter was referred to the Authorities, and Zhang was charged for theft of trade secrets.

Nellis, S. (July 10, 2018). Ex-Apple Worker Charged With Stealing Self-Driving Car Trade Secrets. *Reuters* available at-https://www.reuters.com/article/us-apple-theft/ex-apple-worker-charged-with-stealing-self-driving-car-trade-secrets-idUSKBN1K02RR

Suppose you were tasked to investigate this case and you have been instructed to handle the investigation in a proper manner.

a. Detail how you would initiate the acquisition of evidence for the investigation. [2]
b. Draft a plan as to where and how you might get evidence for this case. [10]
c. Detail two ways by which Xiaolang could have covered up the trails of evidence and how you could still recover the evidence if possible. [4]
d. Outline two proactive measures that Apple could have employed (Or employed) for the speedy recovery of digital evidence in this case. [4]

a. Start with identification i.e. check the nature of the crime and anticipate what tools and methods you are going to use. Image the drives that need to be used for the acquisition of information. Setup network monitoring e.g. using a packet filtering or capturing package like Wireshark.
b. Look for evidence in the following areas: (Any five)
    - The mail server and Email attachments
    - Intrusion detection information
    - Server logs
    - Network logs
    - Firewall logs
    - Router logs
    - Logs for network monitoring software/hardware
c. Any two anti-forensics techniques e.g. Deleting Emails and Internet Browsing History these can be recovered using software like encase, or through Email Address spoofing this would be difficult to uncover.
d. Turn on logging features of their networks and keep these logs for a long period. Install intrusion detection systems to capture malicious traffic.

Question 6

a. Outline four methods of preserving digital evidence that involves mobile phones. [4]

b. Is Locard's exchange principle applicable to Digital Forensics? Give at least four examples from digital forensics that support this principle [4]

a. Preservation:
   i. As a general rule it is recommended that the phone be left in the state it was found. If the phone is on do not turn it off
   ii. If it is on, make every attempt to keep it charged until it is properly evaluated.
   iii. Use bags that prohibit the phone from receiving and transmitting e.g. paraben bags
   iv. Use Radio Isolation Containers
   v. Cellular Network Isolation Techniques

b. Yes (No marks)
   i. Meta data of a picture: We can make use of the time a picture was taken to determine how far the person was from the scene
   ii. Text messages: can be used to see communication of victim and perpetrator
   iii. Browser history can be used. Maybe the perpetrator was googling was to kill a person or searching for flights so they flee
   iv. Contacts can be used to determine who the perpetrator knows and connect dots
   v. Maps application data can be used to determine their geographical movements

c. In 2021, Gartner predicted that three quarters of the personal information in the world would be subject to one or more privacy laws. Privacy laws and regulations will soon affect everything that private enterprises and public organizations are doing almost everywhere and all the time. As more and more regulations go into effect, organisations must lay the technology and process groundwork in place to meet these requirements.

Digital forensics management is no exception to these observations. Outline at least six privacy regulatory and/or privacy technical considerations that are of concern to the digital forensics investigative process. [12]

i. The use of technologies that enforce privacy on information such as encryption and the use of password may act as anti-forensics there by inhibiting the ability of investigators from assessing data.
ii. Limitation of purpose: Investigators may not have the right to view all the information that they want because of the legal and ethical bindings of privacy. The evidence acquired should soley serve for the purpose it was obtained for, this information can not be distributed , viewed or analyzed if its not for the purpose of the investigation.
iii. Integrity: Analysis and evaluations carried out on evidence should not change the evidence itself, investigators should always keep raw data and make a copy of it instead of working on original data.
iv. Responsibility: Investigators in possession responsible for how they handle the evidence and for all actions taken against the evidence thus they are required to show professionalism and accountability.
v. Competence: Persons accessing the original data during the investigation process should be well skilled and competent. He or she should show the right skillset on acquiring, analyzing and handling the evidence, digital forensic tools should be used correctly and this evidence should only be accessed or made available to the right people.
vi. Lawfulness. Consent, contractual need, compliance with legal obligations, protection of essential interests, public interest, and/or legitimate interest should all be considered when collecting and using personal data. Examiners must ask or have consent for personal or corporate data acquisition to ensure acquired data is within the prescribed privacy laws.

<<<<<<<<<END>>>>>>>>>