FACULTY OF SCIENCE
ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	**IT08X27** COMPUTER FORENSICS
CAMPUS	APK
FINAL SUMMATIVE ASSESSMENT	OCTOBER 2020

DATE	2020-10-27	**SESSION**	08:30–10:30
ASSESSORS		PROF W.S. LEUNG	
EXTERNAL MODERATOR		PROF M.S. OLIVIER *(UNIVERSITY OF PRETORIA)*	
DURATION	*2 Hours*	**MARKS**	100

INSTRUCTIONS

- Length of this question paper (including this cover page): 4 (four) pages.
- ALL Questions must be answered.
- This test must be completed by yourself within the prescribed time limit.
- Submissions must be successfully made to Eve by the cut-off upload time.
- You may NOT copy and paste answers from any source. All answers must be written by yourself during this assessment.
- You are bound by all university regulations. Please take special note of those regarding assessment, plagiarism, and ethical conduct.
- You must complete and submit the "Final Summative Assessment Honesty Declaration" document to EVE. Submissions without an accompanying declaration will NOT be marked.
- Regardless of whether you submit handwritten or typed out answers, please ensure that your submission is (for my continued sanity, please):
  - Clear and legible (it's only fun when I am hiding clues, ok?)
  - Ordered (and each answer is presented in contiguous units i.e. *do not answer a bit of a question here and then continue three pages down the line*)
  - Presented in a single document
- No communication concerning this assessment is permissible during the assessment session except with Prof Leung.

It seemed like the usual slow news Tuesday when the smartphones of staff members at the Circadian Outsider (an independent media house) sound off almost synchronously, prompting them to check their mail. This is followed by a flurry of activity as some staff members stop in their tracks while others rush to their desktop machines to access the link in an email promising explosive evidence that would expose Infinity Mutual Trading, a company registered in South Africa that promises its members a passive income through an Artificial Intelligence trader bot that performs very successfully in Bitcoin trading.

By clicking on the link in the email, individuals were directed to the following message posted on AnonChan*, the bulletin board that thrives on anonymity:*

> #∞MTLeaks Anonymous 27/10/20 08:28:30 No.78074291 [Reply] ▶
> Once bitten, twice shy right? But not for the idiots who are throwing their money (often life savings) at the same scamsters behind the collapsed BitCoinIt scheme. Wake up! Infinity Mutual Trading is nothing more than an illigitimet "financial services provider". There is no magical AI bot making the money. What there is, are the usual group of thieving "founders" skimming millions of rands from the pool of funds kept afloat by gullible new members.
>
> We have obtained proof by acquiring transaction and member data from their website (http://myinfinitycoin.com). Its non-existent security was laughable with zero hacking required. Simple enumeration (iterating the id=? parameter used in the various available URLs) and scraping were all it took to grab all the ∞MT transactions (I didn't even need to authenticate).
>
> - For the TLDR; people: Ponzi and Pals are gutting the fund. Soon there will be <u>NO MORE</u> money. Summary of the Stats in this **PDF**.
> - For everyone else (reporters, members of law enforcement, I'm talking to you), check the data for yourselves at: http://s2mfew43os4nrxvf.onion/

Question 1: The Legal Build-Up [10]

James Ponzi, CEO of Infinity Mutual Trading, has responded to the allegations by saying that the data acquired (illegally) is not an accurate reflection of the true state of finances at ∞MT. Furthermore, he has opened up a case of cybercrime with the local police station, going so far as to suggest that the police investigate Vivi Carney, an individual who he accuses of harassing him and his colleagues at ∞MT by posting defamatory posts on social media.

1.1. According to South African laws currently in place, is Ponzi right that a cybercrime has occured? Based on what the anonymous whistleblower claims to have done, motivate your answer by referring to the pertinent sections of the relevant law. (5)

1.2. A Circadian Outsider journalist corners a member of the National Prosecuting Authority of South Africa and presents the notion of using the available leaked data which contains rather damning evidence of rampant financial fraud to arrest the ringleaders of ∞MT. *"I doubt it,"* the NPA representative responds rather hesitantly, *"Unfortunately, there's the issue of fruit of the poisonous tree."* (5)

Explain what the NPA representative is referring to. Do you agree with their assessment? Motivate your answer.

Question 2: Investigating the Digital Crime Scene [50]

You and your investigative unit have been assigned to the ∞MT case.

2.1. Most investigative processes commonly comprise five stages: preparation, survey/identification, preservation, examination & analysis, and presentation. For each of the five strages, describe the tasks that you and your team intend to be carrying out in your investigation of the suspected digital crime scene (located at ∞MT's Johannesburg satellite offices). (15)

Ponzi doesn't seem pleased to see you on the doorstep of his offices. "Why are you even here? You are wasting your time. Go find Vivi Carney and seize HER computer. She used to be one of the senior members of ∞MT before we had a falling out and we had to kick her out. She is extremely jealous that we continue to make money while she has been cut off. She must have used her insider knowledge to get into our systems." *It takes a bit of convincing, but after some negotiation, Ponzi reluctantly allows you access to the ∞MT office, but insists that you copy only the files that are pertient to the investigation.*

2.2. As an investigator, it is extremely important to avoid preconceived theories. Therefore, despite what you have read as claimed by the whistleblower, and what Ponzi insists, you should come up with your own theory of how the data was acquired. (10)

Do this by coming up with your OWN hypothesis and attempting to either prove or disprove it. Describe the formation and evaluation of your hypothesis using the following five steps: observation, hypothesis, prediction, experimentation/testing, and conclusion.

2.3. As you begin to work with the evidence itself, you quickly discover that ∞MT has no forensic readiness in place. How does this impact your investigation? (4)

2.4. How does Locard's Exchange Principle play a role in your investigation? Describe both the advantages and disadvantages that the principle brings to an investigator. (6)

2.5. If Ponzi is to be believed, what is Carney's motive and behaviour type? Motivate your answer. How does understanding the offender's motive help you with the investigation? (5)

2.6. What are the advantages and disadvantages when it comes to the limited acqusition of digital evidence, as imposed by Ponzi? (5)

Question 3: A Look at the Anonymous Post [20]

The link mentioned at the end of the AnonChan *post appears to be rather perculiar.*

3.1. Of what is the link an example of? (1)

3.2. Briefly explain the technology behind the link and how you would access the resource. (4)

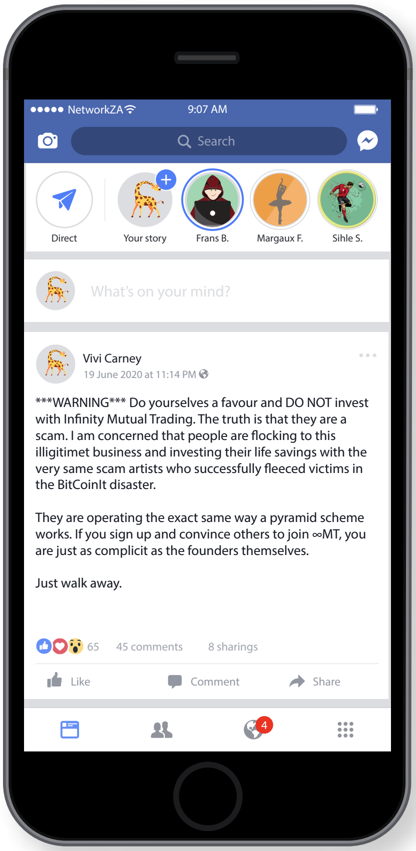
3.3. Describe some of the difficulties and challenges in conducting digital forensic investigations involving the above technology in general. (5)

3.4. How would you classify the certainty of the ∞MT data acquired by the anonymous whistleblower? Motivate your answer *(do not use Casey's Certainty Scale)*. (5)

3.5. It is established that the anonymous whistleblower made use of a VPN service to publish the post on AnonChan. Does this mean that you will have no means of tracing the person behind the post? Explain your answer. (5)

Question 4: The Suspect [20]

As Vivi Carney seems to be a person of interest, you obtain a search warrant to approach her at her home (where she is working from during the COVID-19 lockdown). Carney is quite co-operative. "I get agitated when I see how clueless people can be when it comes to money. Ponzi and his pals first approached me to join them. I responded that I was interested to find out more and once I realised how they operated, I started to post warnings on social media in an attempt to warn people away. See?" She shows you the following post she made on Facebook warning the public away:



(Template from www.freepik.com)

4.1. Carney also shows you her laptop, which has an SSD hard drive. Discuss the technology and considerations that you as an investigator must consider (in comparison to traditional mechanical hard drives). (6)

4.2. Carney's hard drive shows no activity on the day when the ∞MT member website was accessed to create the data dump. Does this serve as sufficient alibi that Carney is not involved? Motivate. (6)

4.3. You notice that Carney has authored a number of PDF documents on the laptop. Explain how analysing these documents, along with the other information you have been presented with in this question paper could be used to find links (these can be direct or circumstantial) between Carney and the anonymous whistleblower on AnonChan. (8)

The End

＼(＾∀＾)メ(＾∀＾)ノ