FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	**IT08X27** COMPUTER FORENSICS
CAMPUS	APK
EXAMINATION	NOVEMBER 2019

DATE	2019-11-07	**TIME**	08:30–10:30
ASSESSORS		PROF WS LEUNG	
MODERATOR		PROF MS OLIVIER (University of Pretoria)	
DURATION	2 Hours	**MARKS**	100

PLEASE READ THROUGH THESE INSTRUCTIONS CAREFULLY AND ADHERE TO THEM

The Academy takes NO responsibility for your ignorance (willful or otherwise) and will NOT grant additional opportunities to students who fail to submit their work correctly

- This question paper comprises 4 (four) pages (including this cover page).
- Answer ALL questions.

- This exam paper contains a case study which appears throughout the question paper. The case study appears in italics to help students differentiate between the case study and the exam's questions.

- Mark each answer correctly and answer entire questions contiguously – if this is not possible, clearly indicate that your answer continues later in the assessment script.
- Write clearly and legibly - marks will not be awarded if the lecturer is unable to make sense of what has been written.
- Keep answers relevant to the course content – note that most questions require that you support your answer with background knowledge (use the mark allocation to determine whether you will need to support your answers).
- Take note of the marks allocated for each question - it is highly advised that a minimum of x facts is provided if the question is out of x marks.

DO NOT TURN OVER THIS QUESTION PAPER UNTIL YOU HAVE BEEN GIVEN INSTRUCTION TO COMMENCE

News of Bertie Warbucks' sudden death in what appears to be a freak accident several days prior is still a topic of discussion around the office coffee machines across the country. The scion of one of the richest families in the country that started the Tomorrow Foundation, Bertie was found dead in the Tomorrow Automobile assembly plant. The police speculate that the nearby assembly robot arm had mistook Bertie for a side vehicle panel, picked him up, and flung him across the room with such force that he was killed on impact.

According to Bertie's fiancée (an IT professional), Bertie had come home with a bruised eye the day before. When questioned on what had happened, Bertie admitted that he had gotten into a fistfight with his brother, Atticus at their parents' home. Bertie, a "Top Cop" who successfully solved numerous cases involving corporations engaged in criminal activities, had accused Atticus, an advocate, of using the Tomorrow Foundation to advance his criminal endeavours. "Bertie said that the world would be extremely disappointed to hear that Atticus wasn't the stand-up pillar of society everyone thought him to be." Bertie's fiancée has now opened a case with the police, claiming that Atticus had set instructions on the robot arm to kill Bertie.

Question 1

Securing a search warrant for the Tomorrow Automobile assembly plant, the investigating officers assigned to the task set to work. The lead officer has indicated that they must conduct a ***reconstructive investigation****.*

What is reconstructive investigation? What does it entail? Explain how it can contribute to the officers' efforts in carrying out a thorough investigation. (10)

[10]

Question 2

The investigating officers regroup and share notes, pooling the following list of evidence that they have identified:

a) Video recording of the interview with Bertie's fiancée recalling Bertie's account of the fight with his brother.
b) Vehicle tracking log which shows Bertie's connected vehicle (it has Internet access) driving from his apartment to the Tomorrow Automobile assembly plant.
c) The desktop machine which controls the robot arm – it acts out any instructions sent to it remotely or locally and is accessible to everyone working on the floor.
d) The SmartScript 1500n, a networked copier, printer and scanner located on the premises – workers on the floor are able to print out job cards on this machine. It has a hard drive that allows it to store jobs.
e) A video of the security camera footage showing Atticus' car pulling up into the Tomorrow Automobile assembly plant's premises on the day of the murder – the video was captured by the investigating officer who recorded it while it was playing out on the security screen using their cellphone.

With reference to the aspects that should be considered when evaluating whether evidence is admissible, assess the admissibility of the five above evidence items (a–e), motivating why they may or may not be admissible in a court of law. (10)

[10]

Question 3

The police are working with the theory that the perpetrator uploaded the killer instructions to the robot arm before Bertie arrived later that evening.

a) Formulate and evaluate a hypothesis regarding how this uploading of killer instructions might have occured. Use the following headings: Observation, Hypothesis, Prediction, Experimentation/Testing, and Conclusion. (5)
b) Explain *(use a diagram to aid you)* how Locard's Exchange Principle means that if the machine had been tampered with, evidence of this tampering will exist. (5)

[10]

Question 4

The investigating officers' investigation into the desktop machine turn up empty. There is no evidence to suggest that it had been maliciously tampered with. However, they also notice that Bertie's laptop and mobile phone cannot be found. This is quite strange as Bertie was never far from his phone in case an informant or colleague needed to get hold of him.

With the assistance of Bertie's fiancée using the "Find my iPhone" feature, an investigating officer is able to track the last known location of Bertie's phone to Atticus' offices. Atticus seems ready for them, explaining that Bertie had left the devices with Atticus for safekeeping. Both devices are turned off and Atticus claims that he does not know how to gain access to them (he does not know any passcodes or passwords).

a) Using a diagram to support your answer, briefly describe the process you would take to ensure that the cellphone is secured for transport to the laboratory. (4)

b) Explain the difference between a class and an individual characteristic in terms of evidentiary value. Use attributes of the iPhone to provide an example of each. (4)

c) The investigating officer notices a box with the label ***GrayKey*** on Atticus' desk. What is it meant to do? (2)

[10]

Question 5

Upon inspection, the investigating officer notices that there is a single hard mechanical hard drive in Bertie's laptop.

Using a diagram, illustrate what the structure of the disk should look like if it contains a single partition that contains a FAT formatted volume. (10)

[10]

Question 6

As part of the preservation process, the officer decides to make a forensic copy of the hard drive that is on the laptop.

Provide a detailed guide to assist the officer in carrying this out. Include tools and alternatives *(e.g. working with mechanical hard drives as opposed to SSDs for your target drive)*, highlighting any potential advantages or disadvantages of doing so. Explain your steps, motivating the rationale behind that step. Your guide should include preparation and reporting. (15)

[15]

Question 7

With the forensic copy made, the investigating officer mounts the image and begins their investigation. Judging from the jump lists, it would appear that certain files have been deleted. These files cannot be found in the Recycle Bin either.

a) What are jump lists? What value is there in analysing them? (3)

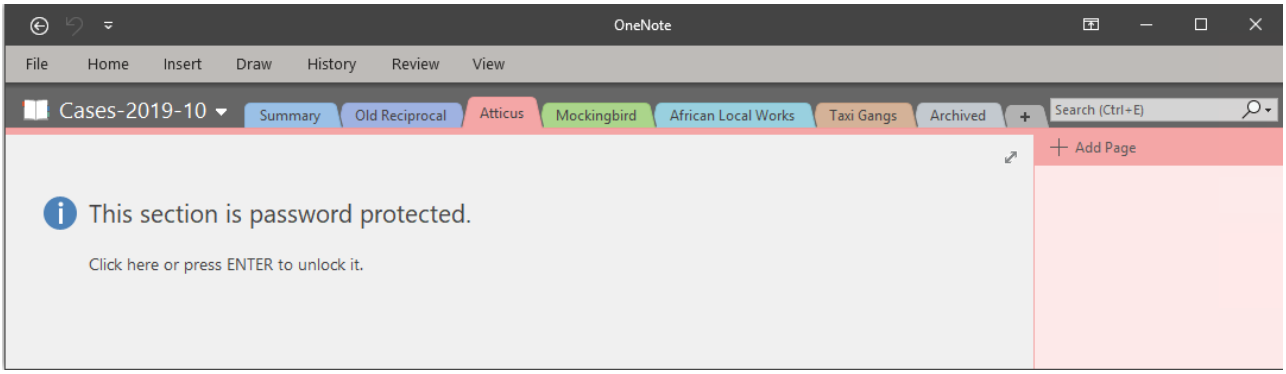
b) Which file system is likely in place? Explain how it may be possible to recover deleted files through this file system. (7)

c) Another approach is to use file carving to attempt to recover the deleted files. Explain this concept. (5)

[15]

Question 8

Through the techniques mentioned in Question 7, the police are able to recover several files on Bertie's laptop. Of particular interest to the investigators is the Microsoft OneNote file entitled `Cases-2019-10.one`. *While several tabs are viewable, one tab labelled "Atticus" is password protected.*



Describe two appropriate strategies that could be employed to gain access to this section's content. Your discussion should relate to how practical it is to implement the two strategies. (10)

[10]

Question 9

With the Atticus section of the `Cases-2019-10.one` *file unlocked, investigators confirm that Bertie had indeed been investigating his brother. According to the notes, Atticus was allegedly using the Tomorrow Foundation servers to spread xenophobia, suggesting that South Africans resort to more radical means to drive out the foreign nationals.*

The investigating officers are now concerned that this latest development potentially goes outside their original case of investigating their colleague's death.

With the report coming back that Bertie's iPhone has also had content deleted off it around the same time as those files on his laptop, the investigating officers are now of the opinion that there is evidence of a deliberate attempt to defeat the ends of justice and thus, Atticus Warbucks must be investigated further.

a) In terms of the ECT Act, would Atticus be guilty of commiting a crime? What about the Cybercrimes Bill *(as presented in October 2018)*? Motivate your answers. (6)

b) The investigating officers plan to apply for a court order requesting for permission to surveil Atticus. What must the investigating officers do? Your answer must take into consideration the Johannesburg High Court ruling made on 16 September 2019. (4)

[10]

The End

＼(＾∀＾)／(＾∀＾)／