UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	**IT08X27** COMPUTER FORENSICS
CAMPUS	APK
EXAMINATION	JANUARY 2020 (SSA)

DATE	2020-01-TBD	**TIME**	TBD
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 3 (three) 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

It has been about two months since "Top Cop" Bertie Warbucks was killed in a freak accident at his family's Tomorrow Automobile assembly plant when a robot arm picked him up and threw him across the room.

Question 1

Because the robot arm is controlled by a desktop machine that can receive instructions remotely (over the Internet), as well as locally (e.g. typed in or uploaded via a USB on the desktop machine), investigators versed in working with digital evidence have been called in to provide their expertise.

Illustrate the case/incident resolution triangle, drawing on how it relates to the case provided above. Be sure to focus on the contribution of the digital investigator. (10)

[10]

Question 2

While investigators could not find any evidence that the robot arm had been provided with malicious instructions to do Bertie harm, their investigations did yield clues that Bertie had been investigating his brother, Advocate Atticus Warbucks, for using the family company's servers to spread xenophobic messages to incite violence.

As part of investigating Atticus further, part of the investigator's strategy is to surveil the advocate's communications.

How does current South African legislation shape how investigating officers monitor Atticus' communications? Refer to these laws, explaining what they restrict or permit. Your answer must bear in mind the circumstances of the current case. (10)

[10]

Question 3

Perusing through Atticus' communication logs, an investigating officer notices a message received on the day of Bertie's death – it comes from Bertie's fiancée, Liesl de Melker. The single message says: `"I panicked. He knows."`

In response, Atticus sends the following: `"Not here. Bridgefy."`

a) The exchange appears to be of interest to the investigation. What requirements must the investigating officers comply with to ensure that these data messages are admissible as evidence in a court of law? (7)

b) What is Bridgefy? For what potential reason might Atticus give this response? (3)

[10]

Question 4

Given Liesl's occupation as an IT professional and the wording of her message, the investigating officers decide to focus on Liesl's timeline to establish if she might have an alibi for when the robot arm incident took place.

While a private person, Liesl is also quite open to permitting technology to track her (she allows Google to track her location on her phone). It does look like this part of the investigation will go quickly, at least.

What are key pieces of information in alibis? Describe how alibi information can be falsified. What considerations should one make when investigating alibi information to ensure that they are a true reflection of what occured? (10)

[10]

Question 5

With a lack of evidence that would exculpate Liesl, the investigating officers decide that they would have to conduct an investigation into Liesl as a possible suspect in Bertie's death.

For each of the steps typically found in a investigative process model, name and discuss the step. Your discussion must include how the investigating officers would conduct this investigation. (20)

[20]

Question 6

One of the evidence items that have been acquired is an image of the hard drive on Liesl's desktop machine. In the laboratory, the technician who checks a copy of the image begins the process by generating a hash. They stop when they realise that the MD5 hash that was recorded is as follows:

```
b7c8a72fb3b167891be9f3db9b5cd88a
```

However, the MD5 hash that was just generated returned:

```
b7c8a72fb3b167891be9f3db9b5cd8aa
```

a) What does the above revelation mean? (1)

b) Provide a table denoting the Certainty Scale as proposed by Casey. (7)

c) Using Casey's Certainty Scale, assign a certainty value to the evidence. Justify your answer. (4)

d) How else are cryptographic hashes used in digital forensics? (3)

[15]

Question 7

The investigating officer proceeds with the investigation, come across a file that is password protected.

Discuss the various strategies you may employ to overcome encryption and password protection. (15)

[15]

Question 6

Having unlocked the file, the investigating officer discovers that it is information pertaining to the development of the software that is used to run robot arms like the one that killed Bertie. When taken in for questioning, Liesl admits that she had lost her temper and ordered the robot arm to attack Bertie, who had been ignoring her for his work.

a) With reference to the case above, discuss the different types of motives that exist and identify the one that fits Liesl. (8)

b) How is motive different from M.O.? (2)

[10]

The End

＼(＾∀＾)メ(＾∀＾)ノ