Programme Code: TU856, TU857, TU858
DT228, DT211C, DT282
Module Code: CMPU 4028

TECHNOLOGICAL UNIVERSITY DUBLIN

Grangegorman

TU857-BSc. (Honours) Degree in Computer Science (Infrastructure)

TU856-BSc. (Honours) Degree in Computer Science

TU858-BSc. (Honours) Degree in Computer Science (International)

Year 4

SEMESTER 1
EXAMINATIONS 2023/24

Forensics

Internal Examiner(s):
Jonathan McCarthy
Dr. Paul Doyle

External Examiner(s):
Sanita Tifentale – TU856, TU858
Dr. Charles Markham – TU857

Exam Duration: 2 hours

Instructions to Candidates

Answer all questions.

Question (1) is worth **40** marks.
Questions (2) and (3) are worth **30** marks each

Question 1

1. a) Explain in detail how Locard's principle is relevant to a digital forensic investigation. Use a digital example to complement your answer.

(8 marks)

1. b) *"An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction and restoring IT services".* Explain the main structure and role of a Computer Incident Response Team (CIRT). How does this differ from the role of a digital forensics professional?

(12 marks)

1. c) Paragraph (e) of the General Scheme of Garda Síochána (Powers) Bill implements the recommendations of the Law Reform Commission that a person executing a search warrant should have certain powers in relation to the persons present at the place. It also includes the power to require a person to give passwords, and to produce material in a visible and legible form. Explain this statement and describe why this legislation was needed. How is this beneficial to an investigation?

(10 marks)

1. d) Reverse Image Lookup is an OSINT technique to discover related information about a given image. Explain in detail how to perform a Reverse Image Lookup and give an example of how this could be used in a digital forensics investigation.

(10 marks)

Question 2

2. a) A hardware write blocker is an important component when creating a forensically sound image. Detail the process of creating a forensically sound image using a hardware write blocker. How can you validate the image is an exact copy of the disk drive?

(8 marks)

2. b) *"First responders need to understand the order of volatility, to ensure they protect any potential evidence".* Explain this statement describing what the order is from most volatile to least volatile when collecting evidence?

(12 marks)

2. c) What is a RAM capture and describe what sources of information can this offer to an investigation?

(10 marks)

Question 3

3. a) The Master File Table is a rich source of information when dealing with a NTFS file system. Explain in detail the basic overview of a MFT record. What is the difference between a resident and a non-resident file?

(10 marks)

3. b) What are the main digital forensic challenges in working in a cloud computing environment?

(10 marks)

3. c) "*Steganography is the art and science of communication in such a way that it cannot detect the presence of a message".* Explain in detail how Steganography can be used as an anti-forensics technique and what approaches can be taken by an investigator to recognise files to which a steganographic technique has been applied?

(10 marks)