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 2022/23

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) Why is it important to have a device such as a Faraday bag available when transporting mobile phones as evidence?

(6 marks)

1. b) *"An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction and restoring IT services".* Explain the main aspects of a Computer Incident Response Team (CIRT) and what role a digital forensics professional plays in this process.

(12 marks)

1. c) What is EXIF metadata and what important pieces of information are commonly recorded for pictures?

(12 marks)

1. d) *"The Open Source Intelligence (OSINT) framework focuses on gathering information from free tools or resources".* Describe how a digital forensics investigator can use this in an investigation to source additional information for their investigation.

(10 marks)

Question 2

2. a) *"In Ireland the General Scheme of Garda Síochána Powers Bill gives Gardaí the powers to acquire the passwords and encryption keys of electronic devices belonging to anyone they are searching".* What issues would a digital investigator experience if they did not have the password for a mobile device?

(8 marks)

2. b) *"Data carving or file carving is a forensic method used for reassembling files in unallocated space".* Explain how data can exist in unallocated space and detail how an investigator can manually carve a file from unallocated space.

(12 marks)

2. c) *"The Autopsy digital forensics platform is the premier end-to-end open source digital forensics platform".* Explain in detail what Autopsy can offer in an investigation and describe what role ingest modules plays in this.

(10 marks)

Question 3

3. a) *“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? For the most volatile give an example of the type of evidence that may recovered.

(10 marks)

3. b) *“Memory forensics refers to the analysis of volatile data in a computer's memory dump”*. Discuss this statement and give 3 different examples of information that can be retrieved from a memory dump.

(10 marks)

3. c) *“Digital forensics is the practice of collecting, analyzing and reporting on digital data”*. Describe the basic operation of the steps associated with a digital forensic process model. What are the benefits of following a model?

(10 marks)