Programme Code: TU856, TU857, TU858
DT228, DT211C, DT282
Module Code: CMPU 4028
CRN: 26672, 29298, 31086

TECHNOLOGICAL UNIVERSITY DUBLIN

CITY CAMPUS - 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 2024/25

Forensics

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

External Examiner(s):
Dr. Colm O'Riordan
Dr. Jamal Abdul Nasir

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) *"In Cyber Forensics, carving is a helpful technique in finding hidden or deleted files from digital media"*. In your own words explain how the file carving technique works and use an example to complement your answer.

(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 structure and role of a Computer Incident Response Team (CIRT). What potential role could a digital forensics professional offer to a CIRT incident?

(12 marks)

1. c) *"Forensic experts have a duty to present the objective, unbiased truth as part of their investigation"*. Explain this statement and describe 3 examples of how a digital forensics professional will abide by this in their investigative process.

(12 marks)

1. d) On a Windows system a file located in unallocated space may have no entry on a NTFS file system. Distinguish the main differences between a file that is part of a NTFS file system and a file that was recovered with no MFT record.

(10 marks)

Question 2

2. a) The primary evidence in email investigations is the email header. Describe the main contents of an email header and explain how this is useful to a forensic investigation?

(8 marks)

2. b) *"Measuring the suitability of forensic tools is essential when choosing a tool to use in an investigation"*. Why is this import in an investigation and describe the four necessary traits to determine if the tool is suitable?

(10 marks)

2. c) *"The practice of RAM Capture is an important aspect of memory forensics that can be used during a digital forensic investigation of criminal activity"*. Explain this statement detailing the process an investigator will follow to perform a RAM capture and describe 3 examples of content that are often only found in memory?

(12 marks)

Question 3

3. a) *"The Criminal Justice (offences relating to information systems) Act 2017 was introduced to cater for a number of very specific criminal offences"*. Explain this statement detailing why the new Act was needed based on the evolution of technology and cybercrime activities.

(8 marks)

3. b) *"Packet analysis is a primary traceback technique in network forensics"*. How can a network protocol analyser be used to analyse packets to gain insights to a malware infection? Use an example to complement your answer.

(10 marks)

3. c) The National Institute of Standards and Technology (NIST) offers guidelines on four different states a mobile device can be in when you extract data. Name each state and offer a brief description of its meaning.

(12 marks)