06.01.20

09.30 - 11.30am

CMPU 4028 Forensics

Basement 3, Kevin Street

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

TECHNOLOGICAL UNIVERSITY DUBLIN

KEVIN STREET CAMPUS

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

BSc. (Honours) Degree in Computer Science

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

Year 4

SEMESTER 1 EXAMINATIONS 2019/20

Forensics

Dr. Martin Mc Hugh
Dr. Deirdre Lillis
Ms. Pauline Martin – DT211C
Dr. Martin Crane – DT228/DT282

Two Hours

Instructions to Candidates.

ANSWER THREE QUESTIONS OUT OF FOUR.
ALL QUESTIONS CARRY EQUAL MARKS.

1 BONUS MARK WILL BE AWARDED TO EACH STUDENT.

Question 1

A. The Privacy Act of 1974 allows that no recordkeeping system should be in place whose very existence is kept secret from the public. Discuss some of the requirements set forth by the act that opens government records to the public. Would this act have a significant impact on the digital investigator? If so, how?

(13 marks)

B. Explain the concept of knowledge of possession. Identify two techniques an investigator can employ to demonstrate that a user knew that a particular file existed on her computer?

(12 marks)

C. Why is it necessary to ascertain a particular time frame in which an incident occurred as part of the initial response procedure?

(8 marks)

Question 2

A. Since information extracted from router or switch interfaces do not provide specific evidence of a particular crime in most cases, what use is the information collected from those devices?

(9 marks)

B. Describe the concept of alternate data streams. How can they be used to hide information? How do you detect them?

(12 marks)

C. Differentiate between near-line data and inaccessible data. Where does offline storage fit into the equation?

(12 marks)

Question 3

A. Explain two circumstances that would constitute "spoliation" in the eyes of the court, should evidentiary material conveniently disappear. Give an example of a mitigating circumstance that might convince the court to overlook the destruction of critical evidence.

(12 marks)

B. How would you describe the triage process used by a first response digital investigation team? What type of issues are considered, and what are the priorities?

(9 marks)

C. What are the four standards against which a tool is measured in regards to suitability for forensic use? How much impact does the failure of one measurement have on the usability of the tool?

(12 marks)

Question 4

A. In spite of their expense, there are a few significant advantages to using one of the commercially available suites as a standard in your investigative process. What are these advantages?

(9 marks)

B. Explain what certification programs Guidance Software offers. Which one is targeted for the entry-level examiner, and which is more advanced?

(12 marks)

C. Identify services that even a full-service organization may occasionally have to outsource. What risks does your organization assume when outsourcing services to another organization?

(12 marks)