**DUBLIN INSTITUTE OF TECHNOLOGY**

# DT211C/4 BSc. (Honours) Degree in Computer Science (Infrastructure)

# DT228/4 BSc. (Honours) Degree in Computer Science

# DT228A/1 MSc. in Computing

# DT228B/1 MSc. in Computing

# DT228B/2 MSc. in Computing

# DT8900/1 International Pre-Masters for MSc in Computing

**WINTER EXAMINATIONS 2016/2017**

## IT FORENSICS [CMPU4028]]

DR. MARTIN MC HUGH
DR. DEIRDRE LILLIS
MR. ALAN FAHEY – DT211
MR. PAUL COLLINS – DT228
MR. CONOR SAYLES – DT228A, DT228B

MONDAY 9TH JANUARY 4.00 P.M. – 6.00 P.M.

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

1 **(a)** Explain the need for digital forensics in modern society and provide the unique characteristics of digital evidence.

(13 marks)

**(b)** Cloud computing has heralded a significant shift away from traditional computing. This shift has brought about advantages and disadvantages to modern computing. How has digital forensics been impacted by this shift to cloud computing?

(12 marks)

**(c)** The Chain of Custody is essential in ensuring the integrity and authenticity of evidence collected. Explain what the Chain of Custody is along with how the Chain of Custody is maintained and demonstrated.

(8 marks)

**2. (a)** The Daubert Standard is a key standard in terms of forensics evidence. Explain the purpose of the Daubert Standard and provide the factors which must be considered as part of the Daubert Standard.

(14 marks)

**(b)** When collecting digital evidence, there is a specific sequence which must be followed when collecting the various forms of evidence. Provide an ordered list of the evidence which must be collected.

(10 marks)

**(c)** Explain with the use of an example what Steganography is and provide examples of programs which employ Steganography.

(9 marks)

**3. (a)** Encryption is a key component for data security. What does encryption provide in terms of data security?

(8 marks)

**(b)** Provide an explanation of the following forms of network attack:

1. Smurf
2. Tear Drop
3. SYN Flood
4. Land
5. Fraggle
6. Packet Mistreating

(13 marks)

**(c)** Digital Forensics are typically performed using the command line interface when operating within Linux. Explain what each of the following Linux commands produce

1. History
2. Pstree
3. Pgrep
4. Top
5. File
6. Kill

(12 marks)

**4. (a)** Target disk mode is a very useful tool in digital forensics when gathering data from a Mac. Explain what target disk mode is and explain how it is useful in terms of digital forensics.

(10 marks)

**(b)** When testifying in court there are two distinct type of witnesses i.e. eye witness and expert witness. Compare and contrast these types of witnesses. What requirements must you meet in order to be considered as an expert witness?

(12 marks)

**(c)** In 1965 Gordon Moore identified that the number of transistors per square inch on integrated circuit boards had doubled every year since the integrated circuit board was invented. He also predicted that this trend could continue for the foreseeable future. This became known as Moore's Law. How does this affect the process of performing digital forensics and how must digital forensic analysis react?

(11 marks)