7/1/2019

09.30 - 11.30am

Basement 1, Kevin Street

DUBLIN INSTITUTE OF TECHNOLOGY

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

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

DT282/4 BSc. (Honours) Degree in Computer Science (International)

WINTER EXAMINATIONS 2018/2019

IT FORENSICS [CMPU4028]]

DR. MARTIN MC HUGH
DR. DEIRDRE LILLIS
MS. PAULINE MARTI N – DT211C
DR. MARTIN CRANE – DT228/DT282

MONDAY 7TH JANUARY 9.30 A.M. – 11.30 A.M.

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)** Describe in your own words the concept of particularity, and identify the two forms that it takes.

(13 marks)

(b) Discuss how a computer system compares to a sealed container in the eyes of the court when executing a warrant. Under what conditions can you search and/or seize such a container?

(12 marks)

(c) Describe the hearsay rule in your own terms, and explain how it relates to the concept of an expert witness.

(8 marks)

2. **(a)** What is the plain view doctrine, and why does it have such a significant impact on digital forensics? What are three approaches to ascertaining whether the doctrine applies to a specific case?

(16 marks)

(b) Explain Locard's principle, and describe how it is relevant to a digital investigation.

(9 marks)

(c) What makes the transportation of evidence such a critical factor in an investigation. Explain how the opposition might latch onto an error in the transportation cycle to disqualify evidence.

(8 marks)

3. **(a)** What are two network tools of value to the investigator that are freely available on any machine with network access?

(9 marks)

(b) A lot of emphasis was placed on the necessity of using a write-protection device when capturing images of media. What does a write-protection device do, and why is its function so important?

(9 marks)

(c) Why is it important what order you follow in collecting evidentiary material? Discuss the order of volatility and why this is critical.

(15 marks)

4. **(a)** How can server log files be used to corroborate evidence found on a suspect's computer? Provide an example to support your answer

(9 marks)

(b) What are four categories of anti-forensic behaviour? Explain each category.

(12 marks)

(c) What are the three forms of service offered by cloud computing? Briefly describe each one in terms of form and function.

(12 marks)