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)

DT8900/1 International Pre Masters for MSc in Computing

WINTER EXAMINATIONS 2017/2018

IT FORENSICS [CMPU4028]]

DR. MARTIN MC HUGH
DR. DEIRDRE LILLIS
MR. ALAN FAHEY – DT211
DR. MARTIN CRANE – DT228/DT282

THURSDAY 18TH JANUARY 2.00 P.M. – 4.00 P.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) A man was brought to trial after employees at a computer repair shop discovered child pornography on his computer. He tried to get the evidence disqualified as the result of an illegal search, but the judge denied his motion. What was the reasoning behind the denial?

(12 marks)

(c) A warrant has been issued to search the premises of a suspected narcotics trafficker. Those tasked with executing the warrant have been authorized to delay notifying the subject of the warrant for seven days. What type of warrant is this and what is the role of these type of warrants?

(8 marks)

2. (a) Identify and explain the four different types of information that can be claimed as "privileged".

(16 marks)

(b) What are the three primary factors that determine whether evidence collected during an investigation will be admissible in court?

Briefly discuss each of these factors.

(9 marks)

(c) You have a printed version of a document along with the digital file that was used to create that document. List two things that the digital document has that the paper document doesn't. What are two pieces of evidence that might be obtained from the paper document that you wouldn't get from the digital file?

(8 marks)

3. **(a)** What is a "footprint" in memory, and what significance does it have to your work?

(9 marks)

(b) Explain in your own words how the file system in use on a computer system can be significant to an investigator when looking for evidence. What makes the search approach different between file systems? What makes a search more or less difficult with any given file system?

(9 marks)

(c) What are three forms of metadata that can be useful to an investigator, and how are they of use?

(15 marks)

4. **(a)** List five types of temporary files that are of use in an investigation, and explain how they can be used.

(10 marks)

(b) Explain the headers that are used in a standard e-mail message and why they are relevant to an investigation. Why is it dangerous to use information you find without some form of collaborative evidence?

(12 marks)

(c) Explain the concept of knowledge of possession. Explain a technique an investigator can employ to demonstrate that a user knew that a particular file existed on her computer?

(11 marks)