W228/414C

DUBLIN INSTITUTE OF TECHNOLOGY

DT228 BSc. (Honours) Degree in Computing

Year 4

WINTER EXAMINATIONS 2015/16

IT FORENSICS [CMPU4028]

DR. MARTIN MC HUGH
DR. DEIRDRE LILLIS
MR. PAUL COLLINS

THURSDAY 7TH JANUARY 4.00PM – 6.00PM

DURATION: 2 HOURS

ANSWER **THREE** QUESTIONS OUT OF **FOUR**.

ALL QUESTIONS CARRY EQUAL MARKS. One (1) complimentary mark will be given.

1 (a) Why can choosing the method used to shut down a suspect computer be a difficult decision to make?

(15 marks)

(b) Why are timelines of computer usage and file accesses important when processing computer evidence?

(8 marks)

(c) How does an expert witness differ from a regular witness? Will the CV of forensic investigator validate him/her as an expert witness?

(10 marks)

2. (a) Discuss the advantages and disadvantages of performing live forensics analysis.

(8 marks)

(b) You are called regarding a possible computer intrusion into a defence contractor's network. After performing an initial interview with the reporting person by phone, you feel confident that an incident has occurred and that you should continue your investigation. Explain the steps you would take next gather additional information to launch an investigation?

(12 marks)

(c) Explain the difference between logon events and account logon events and identify items of particular investigative interest when examining logon and account logon.

(13 marks)

3 (a) Today security executives perform the difficult task of balancing the art and science of security. While the art relates to aspects of diplomacy, persuasion, and the understanding different mind-sets, the science deals with establishing measures, forensics and intrusion detection. Given that security is indeed an art and a science, discuss the role of computer forensics in the overall security of the enterprise.

(20 marks)

(b) Computer Forensics investigation can be conducted by either internal or external experts, discuss the pros and cons of using internal and external experts.

(6 marks)

(c) When a warrant is issued to search the computer systems of a particular entity, it generally specifies what forms of hardware are to be searched and the location of that hardware. Why is that impossible if the target of the warrant employs cloud computing? How can this problem be overcome?

(7 marks)

4. (a) The HKEY_USERS hive of the registry can offer several clues as to what has gone on with a computer. How do the most recently used (MRUs) of the registry aid in an investigation? What do software keys potentially tell you?

(12 marks)

(b) Discuss the four steps involved in the computer forensics process and comment on when a search should be conducted on-site and off-site.

(12 marks)

(c) An administrator at a victim company, who is also a potential suspect in your investigation, attempts to stonewall your request for the logs from all of the domain controllers by stating that the logs are all identical on all domain controllers since they are replicated between them. Discuss if this statement is correct.

(9 marks)