1. COMPULSORY QUESTION: Answer the following questions about the fundamentals of forensic computing.

a) Name and briefly describe the four key areas of forensic computing, according to McKemmish. (8)

b) Give two examples of where a forensic analyst would look for digital evidence (2)

c) Name and briefly describe the 4 rules of forensic analysis (8)

d) Describe "volatile evidence", giving two examples. (2)

2. Answer the following questions about digital and electronic evidence

a) Name and briefly describe the first step in the forensic examination of a computer hard drive (2)

b) Describe the reason behind performing this first step. (1)

c) Describe why cryptographic hashes, also known as message digests, such as MD5, are used in the management of digital and electronic evidence (2)

c) Describe the difference between "delete" and "delete and empty trash", and how the operating system handles files that are "deleted" or "deleted and trash emptied", and why it is still possible to recover files or parts of such files. (3)

d) Describe how digital photographs can give evidence of the make of camera used to capture the photograph, and why this information can make the forensic analyst's job easier. (2)

3. Answer the following questions about honeypots.

a) Honeypots can be classified into two major types. Name and describe these two types and explain what sort of uses are most appropriate for each type. (6)

b) Describe the risks involved in the use of honeypots. (2)

c) What are the possible legal implications of the use of honeypots? (2)

4. Answer the following questions about the challenges facing forensic analysts.

a) Name three significant challenges becoming increasingly problematic for forensic analysts, and describe why these challenges make the forensic analyst's job harder (6)

b) Describe how strong encryption favours privacy at the cost of security and evidence gathering. (2)

c) Describe the purpose of the DBAN application, and how it achieves its aims. (2)