— Sample — 0011

THE OPEN UNIVERSITY OF SRI LANKA
B.SC. HONOURS (IT) DEGREE PROGRAMME – 2024/2025
FINAL EXAMINATION
COU6307 – DIGITAL FORENSICS
DURATION: TWO HOURS ONLY (02 HOURS)

Date: 15.11.2025 Time: 09.30 a.m. – 11.30 a.m.

Answer FOUR Questions ONLY.

Q1.

a) Name two (02) types of digital evidence or artifacts that can typically be recovered when investigating a desktop computer. [04 Marks]

b) List down the four (04) principles in the Association for Chief Police Officers (ACPO) guidelines for digital investigations. [08 Marks]

c) Consider a hard disk which is formatted to have 5 partitions containing individual file systems. Describe the appropriate organization of partition tables in MBR and EBR for this hard disk to keep track of the 5 partitions. You may use a diagram if you need. [07 Marks]

d) Using a suitable diagram, briefly illustrate how the sectors of a particular file in a FAT file system are kept in record. Your diagram should illustrate the relevant directory entry and the FAT table entries that belong to the file. [06 Marks]

Q2.

a) Briefly explain what is meant by volume slack in the context of file system forensics. [05 Marks]

b) Explain one (1) similarity and one (1) difference between resident and non-resident attributes in an NTFS $MFT (Master File Table) entry. [05 Marks]

c) In the NTFS file system, the Master File Table (MFT) is itself stored as a file. Explain why the first entry in the $MFT represents a file also named as "$MFT". [04 Marks]

d) Using a suitable diagram, illustrate the structure and key components of a $MFT entry in the NTFS file system. [05 Marks]

e) Explain the purpose of the following Sleuthkit commands.

i. mmls
ii. fsstat
iii. fls [06 Marks]

Q3.

a) Name two (02) types of information that can be found in a SIM card. [04 Marks]

b) Briefly describe the problem named as camera ballistics in the context of mobile forensics investigations. [05 Marks]

c) What is a digital evidence map used in the context of network forensics investigation? [05 Marks]

d) Using a suitable diagram, briefly explain how an email could be created by a third party pretending to be sent by another party. [05 Marks]

e) Briefly explain an appropriate method to acquire a live memory image of a computer running a Linux operating system. [06 Marks]

Q4.

a) Consider that a group of law-enforcement officers has found a smartphone lying on the floor of a crime scene. The device is already powered on. Imagine that you are the chief of the law-enforcement team at the crime scene and answer the following questions.

i. One officer in the team attempts to turn the device off. What would be your response? Briefly explain the rationale behind your response. [05 marks]

ii. One officer simply picks the device by hand, puts it into her pocket, and moves to the forensic lab. Briefly describe three (3) actions the officer should have done before moving the device to the forensic lab. [05 marks]

iii. The preliminary inspection at the forensic lab has revealed that the device data cannot be extracted through the USB port while keeping the device as it is due to security settings of the device. Propose two (2) alternative approaches that could be used to extract data from the device. For each method, explain its advantages and limitations. [06 marks]

b) Consider that you have successfully extracted an image of the volatile memory, i.e., RAM, of a computer. You are in need of finding the password used by the owner of the device to log into a particular website. Assuming that the device's RAM image still contains the previously entered passwords, briefly illustrate a procedure to identify correct password of the website. [05 Marks]

c) Discuss the forensic soundness and evidence integrity of a RAM image in contrast to a hard disk image taken from a computer. [04 Marks]

Q5.

a) Briefly discuss the difference and the usefulness of MAC and IP addresses from a network forensic investigator's point of view. [04 Marks]

b) Using a suitable example scenario, briefly explain how log files in a DHCP server would be useful in a network forensic investigation. [06 Marks]

c) Open Source Intelligence (OSINT) is a technique that can be used to gather forensically-useful information for an investigation. Briefly discuss a scenario where OSINT is the only available method to gather evidence in a digital forensic investigation. [05 Marks]

d) Answer the following two questions on mobile forensics and device storage. Mobile devices contain multiple storage components, such as internal flash memory and SD cards.

i. Briefly discuss an example investigative case where the required evidence can only be extract from the SD card of a mobile device. [05 marks]

ii. Briefly discuss an example investigative case where the required evidence can only be extract from the internal flash memory of a mobile device. [05 marks]

Q6.

a) How feasible is it to perform a manual analysis of a memory (RAM) image taken from a computer using a hex viewer? Briefly explain your answer. [05 Marks]

b) Briefly explain a scenario where a digital forensic investigation can only be progressed with an evidence found from a memory analysis, instead of a file system analysis. [05 Marks]

c) Briefly explain how software reverse engineering techniques can be useful in a forensic investigation. [05 Marks]

d) Ghidra and Volatility are two advanced tools that can be used for digital forensic investigators for purposes that are challenging to be achieved through manual techniques. For each tool, describe a scenario:

i. Where Ghidra is instrumental in malware analysis. [05 Marks]

ii. Where Volatality is instrumental in a memory analysis. [05 Marks]