Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2021/2022

COURSE NAME	:	DIGITAL FORENSICS AND CYBER LAW
COURSE CODE	:	CII 11103
PROGRAMME CODE	:	CII
EXAMINATION DATE	:	JANUARY / FEBRUARY 2022
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL QUESTIONS** 2. THIS FINAL EXAMINATION IS AN **ONLINE** ASSESSMENT AND CONDUCTED VIA **OPEN BOOK**

THIS QUESTION PAPER CONSIST OF **FOUR (4)** PAGES

Q1 **(a)** Why some digital forensic tools are made open source?

(3 marks)

(b) How do companies get profit from their open source digital forensic tools?

(2 marks)

(c) Why RAM Forensics is also important in digital forensics?

(5 marks)

(d) Demonstrate a way to detect a PDF file with its file extension changed to JPG?

(10 marks)

(e) Compare between hiding message in JPEG image and slack space. Give **TWO (2)** facts.

(5 marks)

(f) Compare obtaining evidence from email and from master boot record (MBR).

(5 marks)

(g) Compare between the functionalities of National Institute of Standards and Technology (NIST) and American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) in digital forensics.

(5 marks)

(h) Compare between header/footer and Bi-Gap Carving (BGC).

(10 marks)

(i) Explain the File Extension Mismatch option in Autopsy.

(5 marks)

(j) Demonstrate how to detect malware using registry.

(5 marks)

Q2 You are required to explain, how digital forensics is used to solve the following case studies.

(a) On 25th, December 2020, an officer from Human Resource department, posted selfies from a golf-course taken from his cell phone to his public Instagram account. However, one month after that, the officer is accused of absence from his duty for that particular day.

(5 marks)

(b) Mrs X was wearing her fitness tracker when found dead in her home in Jan 2021. Her husband, Mr Z claimed that, upon entering his house, he was tortured by an intruder. He told police that the intruder then shot and killed her wife when she returned home from Tesco supermarket nearby. Nevertheless, Mr Z was found guilty of murdering his wife.

(5 marks)

(c) Mr Y worked as an engineer for Proton's autonomous car division and has been given a network userid. He had been with the company 2 years when he announced that he would be resigning and returning to Singapore to take care of his elderly mother. He told his manager that he would be working for an electric car manufacturer in Singapore. The conversation left the manager suspicious. Company security started an investigation. Finally, he was then found guilty of stealing trade secret.

(5 marks)

(d) Mr A worked as a GCB driver. On May 2021, he accidentally knocked down a wall of a building on a new construction site. He was found guilty due to negligence.

(5 marks)

Q3 Digital evidence is admissible if it establishes a fact of matter asserted in the case, it remained unaltered during the digital forensics process, and the results of the examination are valid and reliable.

Suggest **FOUR (4)** ways on how to support admissibility of digital evidence in a hard disk.

(10 marks)

Q4 Staff A in an IT Department, uses his friend's PC to gain unauthorized access to his company firewall. He changes the setting in the firewall to block all users from accessing their company's email server.

Justify related cyberlaw act to be used and what would be the offenses done according to the section in the Act. Discuss the penalty, if he is convicted.

(15 marks)

-END OF QUESTIONS-