JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY SECURITY AND AUDIT

2ND YEAR 1ST SEMESTER 2024/ 2025 ACADEMIC YEAR

COURSE CODE: ICM 1205

COURSE TITLE: ADVANCED CYBERCRIME INVESTIGATIONS

EXAM VENUE: KISUMU CAMPUS

DATE: **STREAM**: **MASTER OF SCIENCE IN IT SECURITY AND AUDIT**

TIME: 3 HOURS **EXAM SESSION**:

INSTRUCTIONS:

1. **Answer QUESTION ONE and any other TWO (2) questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

Question One – Compulsory (30marks)

a) Define the following terms

   i) Phishing

   ii) Identify theft

   iii) Data breach (6marks)

b) What is honeypot and what is it's significance in cybercrime investigations. (3marks)

c) Security is about more than simply protection. It allows companies the freedom to operate without fear. And while sophisticated security systems and due diligence will help protect against cybercrime, there is one key weapon that will keep defenses as strong as possible: Collaboration. Explain (6marks)

d. Case study

This is the case of a 15-year-old student at a secondary school somewhere in the a rural village in Siaya. They were a well-respected student who was doing fine at school. The student was getting help from one of their teachers one day and watched over the teacher's shoulder as the teacher typed in their username and password to log on to the computer. The student remembered the username and password. A little while later the student was on their own, sat down at a computer. They logged in using the teacher's username and password. They had a look around the teacher's account. The student found an email which contained the KCPE results for all of the students who had just left, well before KCPE result day had come. The student published some KCPE results for students they did not know on Twitter. They asked if anyone wanted to see more results. Fortunately, someone told the school staff what was going on. The student was identified and the Tweets taken down before many people saw them. The account compromise was locked down with the teacher's password changed. The Police were called and the student investigated for a criminal offence. The school expressed a desire not to ruin their student's future with a criminal record. Nobody whose KCPE results had been published wished to have the student prosecuted.

The student was given a form of restorative justice – 'Conditional Caution'. This is a low-level criminal record. They had to apologise to their Victims and write an essay on the Computer Misuse Act.

Think about the case

a. Discuss this Cybercrime

b. In your opinion who is/are the victim(s)?

c. Identify and explain some of the harms this crime led to.

(15marks)

Question Two (20marks)

a. In 2022, Kenya reported about 700 million online cybercrimes, systems vulnerabilities constituted 65% of this, being the highest form of cybercrime in the country. With examples discuss some of the issues contained in systems vulnerabilities. (6marks)

b. Distinguish between the penalties accorded by the Kenyan laws of the following cybercrimes, as illustrated in the Computer Misuse Cybercrime Act (CMCA) 2018.

   i) Unauthorized access

   ii) Unauthorized interference

(6marks)

c. The Kenya National Crime Research Centre (KNCRC) conducted a research in 2023 on Information Communication technology crimes and offense in Kenya, in one of their findings they identified ICT experts as one of the highest-ranking perpetrators of ICT crimes and offences in Kenya. What do you think are the main motivators to this fact? (8marks)

Question Three (20marks)

a. You have been assigned to lead an investigation team on a drug dealing case, and a search warrant has been provided. While viewing computer files, you come across images of child pornography. Instead of waiting for a new warrant, you kept searching and collecting the data. When you presented the report for adjudication, all the evidence regarding the pictures was excluded.

   i) Discuss which rules of digital evidence that you might have violated

(10 marks)

b. Digital forensics always face numerous challenges while conducting investigation. Discuss any FIVE challenges and the future research areas of cybercrime investigations. (10marks)

Question Four (20marks)

a. There are several investigation models available, with the aid of a diagram, discuss the 6-step Casey model of digital forensics investigation. (10marks)

b. An incident happened last year where Dr. Lucas Tina, a KEMRI researcher, was suspected of mailing anthrax-contaminated letters causing ten deaths and injury to dozens of more people. It is said that Dr. Tina used disposable e-mail accounts with false names during the time of the anthrax attacks. Although Dr. Tina eventually died early last month in a road accident before being charged, he was the primary suspect in these anthrax attacks. Before he died, a case was in court after the bereaved families sought legal redress with a view of claiming compensations. Consider yourself having been engaged as an expert to assist in this case. Explain in details how you would conduct your investigation and effectively assist the jury in solving this case. (10marks)

Question Five (20marks)

c. Digital forensics tools are hardware and software tools that can be used to aid in the recovery and presentation of digital evidence. Law enforcement can use digital forensics tools to collect and preserve digital evidence and support or refute hypotheses before courts. Name and describe any FIVE software tools used in digital forensics. (10marks)

d. Ms. Julia has been receiving harassing phone calls from a spoofed telephone number and reported the case to the police. As part of the investigators tasked to pursue this case, you searched the Internet for spoofing services and discovered the service that was used to spoof these calls. This was based on the Ms. Julia's phone number existing in the spoofing services logs. A search warrant to the spoofing service provided billing records and call logs related to the Julia's phone number. Information provided included the suspect's billing information, date of the account being created, address, and a log of every call made. In this case, there were a total of 88 calls made. Provide a detailed report on how you conducted this investigation and admissible evidence retrieved to be used in court of law to prosecute this case. (10 Marks)