JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

2ND YEAR 1ST SEMESTER 2021/2022 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT 5215

COURSE TITLE: ADVANCED CYBERCRIME INVESTIGATIONS

EXAM VENUE: **STREAM: Msc**

DATE: DECEMBER 2022 **EXAM SESSION:**

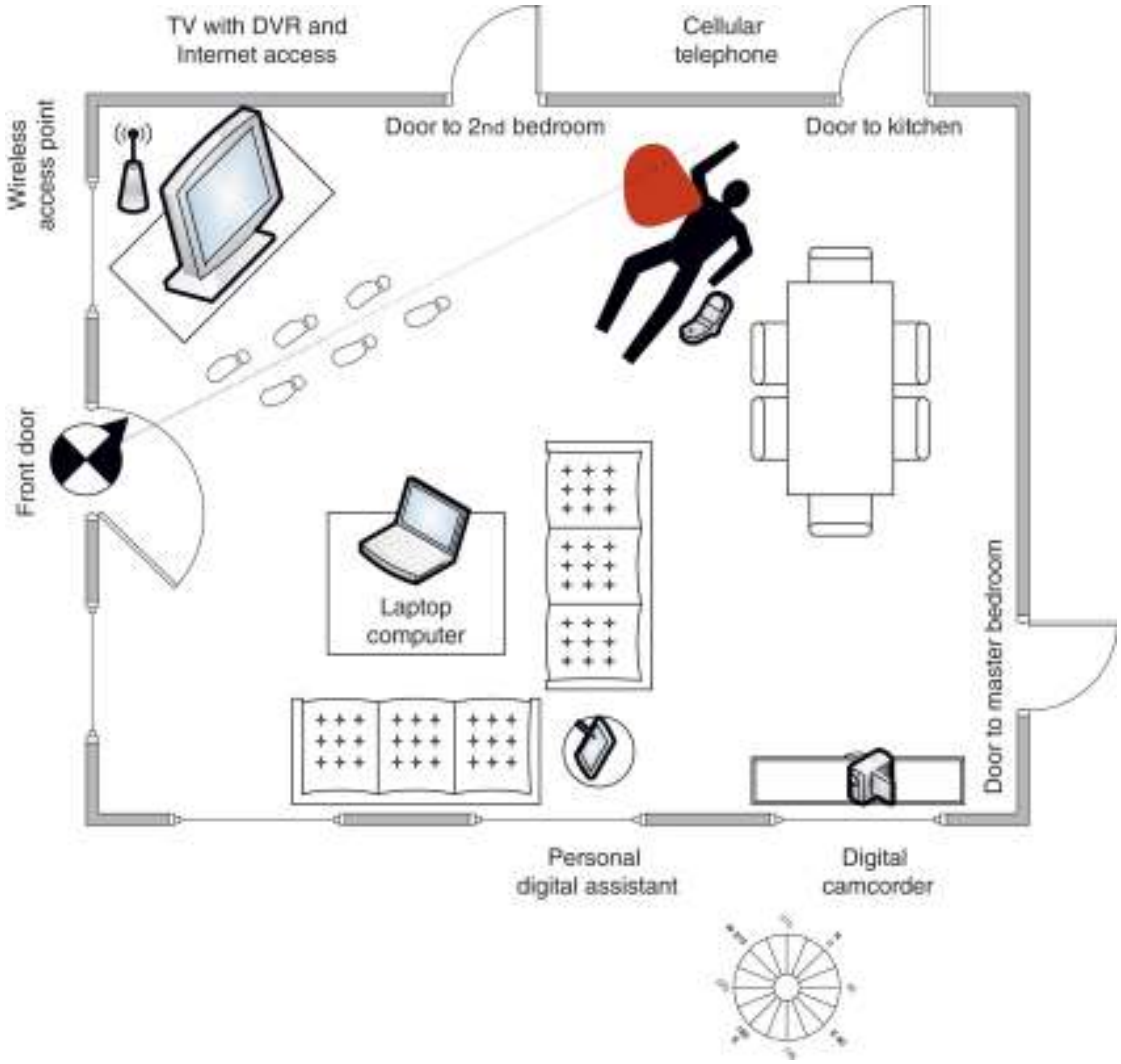
TIME: 3.00 HOURS

INSTRUCTIONS:

1. **Answer ANY three 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 **[20 MARKS]**

Below is a murder crime scene. Use the diagram to help in answering the questions that follow.



i) Identify any four sources of digital evidence and the respective digital evidence retrieved from the identified sources. [8 Marks]

ii) Describe the methods, tools and techniques that can used in processing the crime scene above. [8 Marks]

iii) Appy the Locard's Principle while processing the crime scene above. [4 Marks]

QUESTION TWO **[20 MARKS]**

Explain the significance of the following to cybercrime investigation in Kenya.

a) The Computer Misuse and Cybercrime Act, 2018 [4 Marks]
b) Kenya Information and Communication Act [4 Marks]
c) Data Protection Act [4 Marks]
d) The National Payment Systems Act,2011 [4 Marks]
e) Critical Infrastructure Protection Act,2019 [4 Marks]

QUESTION THREE **[20 MARKS]**

a) An incident happened last year where Dr. Lubanga Moeba, 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. Moeba used disposable e-mail accounts with false names during the time of the anthrax attacks. Although Dr. Moeba 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. [10 Marks]

b) During a search warrant executed at a Milimani residence in Kisumu, two iPhones were seized along with other items. You participated as an investigator where an analysis of the iPhones recovered sexually explicit chat messages with minors. Coupled with child pornography discovered on the seized computers, you continued with the investigation and obtained even more evidence of these crimes, including postings on Facebook and Instagram that were pertinent to the case. Write a detailed report that you shall present as an expert witness in the High Court in Kisumu, Kenya. Remember the admissibility or inadmissibility of the digital evidence shall define the life of the case.
[10 Marks]

QUESTION FOUR **[20 MARKS]**

a) The DCI has received an anonymous letter with information that Mr. Mwalagho is involved in child molestation. All details in the anonymous letter were confirmed except for the child molestation allegations. To prove or disprove the allegations, you have been incorporated in the investigation team to help unravel this mystery. One of the strategies included by the DCI is to initiate an undercover online conversation with Mwalagho, assuming the role of an underage boy. Subsequent chats and instant messages culminated in the probable cause in Mwalagho's intention to meet the undercover officer to perform a sexual act. He was subsequently arrested. Describe the whole investigation process capturing the methods, tools and techniques used in the whole process. Include also the chain-of-custody handling in this case. [10 Marks]

b) Ms. Amito 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. Amito'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 Amito'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]

QUESTION FIVE **[20 MARKS]**

a) Mr. Aboko infected computers with a malware that allowed him to gain control of the computers of more than 200 computers, affecting about 700 people. He also installed keylogging software on the victims' computers, stealing their credit critical personal information, which he used to his advantage. Mr. Aboko also covertly recorded videos of the victims, in compromising and intimate acts. He demanded that the victims create and send sexually explicit videos to him or he would release the videos he made online. As one of the investigators in this case, you were able to obtain his e-mail from the victims and a search warrant of the email address identified additional victims of him through the e-mails produced. While conducting further investigation, you discovered even domain names associated with the e-mail address that was registered in his name. The break in the case was that he was apparently not aware that his e-mail address was associated with

several of his registered domain names that used his real name. Produce a detailed account on how, together with your team, were able to conduct this investigation.
[10 Marks]

b) Discuss the current challenges and future research areas for cybercrime investigation. [10 Marks]

- END –