CYBERCRIME AND ELECTRONIC EVIDENCE WORKSHOP

25th - 29th July 2022 Park Inn By Radisson Nairobi Westlands| Kenya

Delivered Face to Face

INTRODUCTION

The increasing widespread adoption of computers in society has led to unprecedented computer-related crimes. By abusing technology, cybercriminals can ruin businesses and even lives. Many organizations around the world are fighting to stop cybercriminals and help to make systems more secure. One of the best prevention methods is education. Those in charge of investigating these crimes need training on the rules that govern investigation, presentation and admissibility of electronic evidence in court as well as legal issues around electronic evidence.

COURSE OUTLINE

As nearly every case now has an element of electronic evidence it has become important to have a proper understanding of how this type of evidence can be used. This seminar covers many aspects of cybercrime, both theoretical concepts, as well as practical knowledge including nature of electronic evidence, how and where it can be acquired and the processes required in ensuring integrity and authenticity of the electronic evidence. The basic concepts of digital forensics and how to analyze and report on electronic evidence is covered. Each Module is as self-contained as possible, while fitting into an overarching theme.

MODULE 1: CYBERCRIME AND COMPUTER RELATED OFFENSES

The increasing widespread adoption of computers in society has led to numerous computer related crimes. Some of these crimes are 'pre-computer' that existed before the advent of computers such as embezzlement, fraud or threats while others are completely 'modern technology' crimes that began with the evolution of computers such as hacking, viruses, phishing, denial of service and many more. Technological advancement has shown that many objects now have computing devices embedded in them and are capable of storing, processing and transferring data. This means that criminals can exploit these devices to create new opportunities for crime. This module discusses cybercrimes or computer related crimes as well as available legal tools and resources to investigate and prosecute cybercrimes. The following topics will be covered:

- Definition of cybercrime
- Classification of cybercrimes
- Cybercrime as a Service (CaaS)
- Deep and Dark Web
- How Dark Web fuels cybercrime
- International efforts to curb cybercrime
- Challenges in investigating cybercrimes
- Cyber warfare

MODULE 2: INTRODUCTION TO ELECTRONIC EVIDENCE

When cybercrime activity is committed, it is often important to investigate the crime. However, the evidence which is always electronic in nature is volatile, intangible and more often located in places not visible to naked eyes. Accessing such evidence also has implications for human rights as well as the rule of law. This module will discuss the methods to identify and handle electronic evidence in such ways that will ensure its integrity and authenticity for later admissibility in the court of law. It also provides an overview of the kinds of issues that often arise when dealing with electronic evidence and offers advice on how to deal with them. Topics covered include:

- What is electronic evidence?
- Nature of electronic evidence
- Admissibility of electronic evidence
- Principles of electronic evidence
- Sources of electronic evidence

MODULE 3: INTRODUCTION TO DIGITAL FORENSICS

The process of investigating, gathering and analyzing evidence after cybercrime incidences is known as digital forensics. Generally, digital forensics is defined as "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data". Thus digital forensics refers to post incident response measures. This module discusses the process of conducting digital forensics and presenting the evidence in the court of law. Topics covered:

- What is digital forensics?
- Steps in digital forensics investigations
- Identification, Preservation, Collection, Examination and Presentation
- Securing and evaluating crime scene
- Evidence management
- Chain of Custody
- Reporting and Documentation

MODULE 4: CHALLENGES AND LEGAL FRAMEWORK

Digital forensics integrates the fields of computer science and law to investigate crime. For digital evidence to be legally admissible in court, investigators must follow proper technical and legal procedures when recovering and analyzing data from digital devices. Unfortunately, laws written before the era of computer forensics are often outdated and cannot adequately assess the techniques used in a computer system search. The inability of the law to keep pace with technological advancements may ultimately limit the use of electronic evidence in court. This module discusses the legal landscape relating to cybercrime and highlights the need for harmonized legislation. Topics covered include:

- Substantive, procedural, and preventive cybercrime laws
- Admissibility Challenges
- Evidence Authentication
- Expert Witness in Court
- Case Laws

MODULE 5: CYBERCRIME INVESTIGATION

Investigating cybercrime involves a multitude of stakeholders including law enforcement agencies, organizations, businesses, and individuals. The nature and extent of their involvement depends on the type of cybercrime committed. Stakeholder involvement is also determined by the geographic location of stakeholders and countries' cybercrime laws. This module critically examines the processes involved in reporting cybercrime and the stakeholders responsible for investigation cybercrime. Special attention is paid to the obstacles encountered during cybercrime investigations. Topics covered include:

- Discuss and assess cybercrime reporting practices
- Identify and discuss the stakeholders involved in cybercrime investigations
- Explain and critically evaluate the resources leveraged during a cybercrime investigation and the obstacles encountered by investigators
- International Cooperation against Cybercrime
- Describe and appraise the role of knowledge management in cybercrime investigations

WHO SHOULD ATTEND

- Practicing lawyers
- In-house Counsel
- Compliance Officers
- Cybercrime prosecutors
- Forensic Investigators
- Financial Officers
- Judges and Magistrates
- Tax Investigators
- Risk Managers
- Auditors
- IT Security Officers
- Security Managers
- Fraud investigators

DELIVERY METHOD

- 5 days of instructor-led classroom training
- Fee : USD 1500 VAT Inclusive per Delegate

- **Contacts: ldinga@managecom.co.ke**
  groseline@managecom.co.ke

- **Date: 25th - 29th July 2022**

Managecom
Systems Limited
Enabling Knowledge Economy

Systems is a leading Cyber Security and Cyber Forensics consulting services provider in Africa. We deliver state of the art information security and digital forensics products and services to individuals, corporations and law enforcement across Africa.

Visit us at **https://www.managecom.co.ke**

INSTRUCTOR

Lawrence is a seasoned consultant with wealth of experience and expertise in cybersecurity, digital forensics and cybercrime investigations and cyber capacity building. Lawrence is also a digital forensic expert witness in court and has testified in many cases of cybersecurity and digital forensics. He holds Master of Science degree in Forensic Computing and Security from the University of Derby, England, LLM in ICT Law from the Open University of Tanzania and Diploma in Law from the Kenya School of Law as well as Certified Information Systems Security Professional (CISSP) certification.

Currently, Lawrence is an approved consultant for the following organizations:

- The Cybercrime Programme Office (C-PROC) at the Council of Europe (CoE) on Law Enforcement and Judicial Training in Cybercrime and Electronic Evidence.
- The European Union Agency for Law Enforcement Training (CEPOL) on Cybercrime – Attacks against information systems and Law Enforcement Technologies - Forensics and Other Specific Areas.
- Council of Europe (CoE) - International consultant in capacity building of legal professionals and conducting research, assessments and drafting analytical studies and reports for the project on Supporting the Effective Implementation of Turkish Constitutional Court Judgments in the Field of Fundamental Rights.

Lawrence has conducted cyber capacity building to the Communications Authority of Kenya (CAK), East Africa Law Society (EALS), the Kenya School of Law (KSL), the Law Society of Kenya (LSK), Kenya Magistrates and Judges Association, African Advanced Level Telecommunications Institute (AFRALTI), Kenya Revenue Authority (KRA), the National Cyber Command Centre (NC3), National Telecommunications Commission of Sierra Leone, Rwanda Revenue Authority, South Sudan National Communications Authority, the Uganda Judiciary among others. Lawrence is a presenter and many times a panelist at national and international level in cybersecurity and cybercrime issues.

CLIENTS' TESTIMONIES

"I write to express our utmost gratitude and appreciation for the digital forensics training you conducted for members of the Nairobi Branch. The feedback we received rated the training at excellent and most members were of the view that you demonstrated a good mastery of the subject. We hope that when we call again on you in the near future to conduct another training (as we certainly will), you will honor our call."

Chair, LSK Nairobi Branch

"At East Africa Law Society, we have found a great partner in Lawrence Dinga. Lawrence has assisted us to retool our members drawn from 6 countries in the area of electronic evidence, digital forensics, and effective handling of these tools in courtroom situations. The feedback from the sessions he has had with our members is overwhelmingly speaking of his merit and competence; he breaks down concepts so easily and is at ease with law and technology."

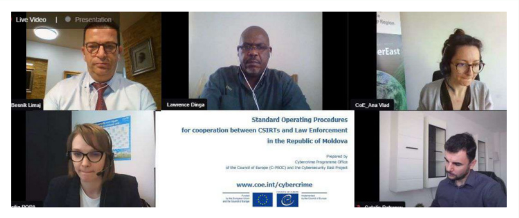
CEO, East Africa Law Society

"This is a worthy and timely course that I would for sure recommend for all judicial law enforcement and officers who need to cope with the new realities of the cyber world where almost any legal dispute now involves some form of digital evidence. On top of the excellent, well- structured, and informative course, Lawrence was a reservoir of well-mixed technical and legal knowledge with a passion for his work"

President, Kenya Magistrates and Judges Association

The Network Layer
• The network layer is concerned with logical addressing and routing. The network layer is the home of the Internet Protocol (IP), which makes a best effort at delivery of datagrams from their source to their destination.

Training members of Kenya Revenue Autrhority on Digital Forensics


Live Video
Presentation
Besnik Limaj
Lawrence Dinga
CoE_Ana Vlad
Standard Operating Procedures
for cooperation between CSIRTs and Law Enforcement
in the Republic of Moldova
www.coe.int/cybercrime

Training law enforcement and CSIRT of the Republic of Moldova (Europe)

Training law enforcement and prosecutors of the Repulic of Armenia (Europe) electronic data preservation

Members of South Sudan National Communications Authority training on cybersecurity

Managecom Systems Limited
Enabling Knowledge Economy

CYBERCRIME AND ELECTRONIC EVIDENCE

25th – 29th July 2022, Park Inn By Radisson Nairobi Westlands, Kenya
Fee: USD 1500 VAT Inclusive per Delegate

Thank you for your interest in the course. To register, please provide the following information

DELEGATE(S) INFORMATION

1. Dr. /Mr. /Mrs. /Miss: .... *Email:* ....
Department: .... *Mobile:* ....
Position:

2. Dr. /Mr. /Mrs. /Miss: .... *Email:* ....
Department: .... *Mobile:* ....
Position:

3. Dr. /Mr. /Mrs. /Miss: .... *Email:* ....
Department: .... *Mobile:* ....
Position:

4. Dr. /Mr. /Mrs. /Miss: .... *Email:* ....
Department: .... *Mobile:* ....
Position:

REGISTER ME / US FOR THE COURSE BELOW

□ 5 Day Course - USD 1 500 VAT Inclusive

AUTHORIZATION – THIS BOOKING IS INVALID WITHOUT A SIGNATURE

Signatory must be authorized to sign on behalf of contracting organization

Name: ....
Organisation: ....
Physical Address: .... *Code:* ....
Telephone: ....
Signature:

PAYMENT DETAILS

Account No.: 0102012975101
Account Name: Managecom Systems Ltd
Bank: Standard Chartered Bank
Branch: Kenyatta Avenue
Swift Code: SCBLKENXAXXX
NAIROBI