**Cyber Security for Cambodian LEO/Successive Police Instructors**

**25.01.2022 to 01.02.2022**

|  |  |  |
| --- | --- | --- |
| 1 | Area of Study | Cyber Security |
| 2 | Course type | E-ITEC |
| 3 | Course Name  | Cyber Security for Cambodian LEO/Successive Police Instructors |
| 4 | Start Date | 25.1.2022 |
| 5 | End Date | 1.2.2022 |
| 6 | Duration | 3-days |
| 7 | Aim & Objective of the course | Objectives:The purpose of this course is to provide understanding of the subject ‘* Cyber Security Fundamentals
* Modern Days Cyber Crimes
* Cyber Attacks and Network Threats
* Foot printing, Scanning, N/w Enumeration, Social Engineering
* Web Applications Security and Vulnerabilities
* Cryptography
* Advanced Cyber Security Issues
* Cyber Hygiene and Wellbeing practices
* System Security

Learning Outcomes:On completion of this course, participants should have gained a good understanding of the concepts of Cyber Security and how to secure the systems and network.  |
| 8 | Target Group | **Police Officers** |

COURSE ON DIGITAL FORENSICS FOR LEA/ SUCCESSOR POLICE INSTRUCTORS OF

 POLICE ACADEMY OF COMBODIA

03.02.22 TO 10.02.22

|  |  |  |
| --- | --- | --- |
| Sl.No | **CONTENT** |  |
| **DAY 1 (03.02.22)** |  |
| 1. | **Understanding of Digital Forensics & Evidences*** Digital forensics – Definition, classification
* Digital Evidence – Definition, characteristics, types, source of digital evidence, etc.
* Classification of Digital evidence – user created, user protected and system created.
* Difference between volatile and non-volatile memory
* Rules of Evidence – best evidence rule, hearsay evidence, etc.
* Traditional forensic evidence Vs. Digital Evidence
* Digital Forensics Vs. Traditional Forensics – Locard’s Exchange Principle, Daubert’s Rule, Repeatability and Reproducibility
* Understand pre-requisite for search & seizure and first responder kits

 Basic Dos and Donts during search |  |
| 2. | **SOP on Scene of Crime Management*** Pre search preparation and required forensic toolkit,
* Procedure of digital evidence collection and preservation,
* Chain of custody, Seizure Memos

 Preparing of legal documents, letters, etc |  |
| 3. | Uses of Write BlockerHashing Algorithms & Techniques**Practical Hands On**Write Blocker & Hashing Digital Evidence |  |
| **DAY 2 (08.02.22)** |  |
| 4. | **Overview of File Systems*** File System FAT, exFAT, NTFS, EXT, HFS+, APFS

**Introduction to Storage Devices & Disk Forensics**Hard disk, Pen drive, CD-DVD, Memory cards, Understanding Disk Geoetry, etc. |  |
| 5. | **Disk Forensic Imaging/Cloning Procedure*** Imaging of data using DD, FTK Imager, EnCase Imager, etc.
* Concepts of sterile media and imaging
* The significance of imaging of the drive
* Procedure for forensically cleaning of the

media* How to forensically clean the media
* Imaging procedure of the dirive/media
* Steps for the above and its documentation
* How to image the media – practical demonstration
* How to acquire the volatile data

Demonstration of such tools for acquiring memory**[Practical Hands On]**Imaging and Cloning of Digital Device/Evidence |  |
| 6. | **Introduction to Digital Forensic Tools and Analysis of Hard Disk Drive Image*** File mounting – Physical, logical
* Metadata analysis
* File Carving
* File Signature Mismatch analysis
* Keyword Framing, Searching and Indexing of Artifacts

Recovery of deleted data (within the slack, partition and unused memory) |  |
| **DAY 3 (10.02.22)** | memory |
| 7. | **Introduction to Digital Forensic Tools and Analysis of Hard Disk Drive Image** (Contd…..)* File mounting – Physical, logical
* Metadata analysis
* File Carving
* File Signature Mismatch analysis
* Keyword Framing, Searching and Indexing of Artifacts

Recovery of deleted data (within the slack, partition and unused memory) |  |
| 8. | **[Practical Hands on]****Analysis of Hard Disk Drive Image using various Tools using :*** **FTK**
 |  |
| 9. | **[Practical Hands on]****Analysis of Hard Disk Drive Image using various Tools using :*** **Autopsy**
 |  |