FORC Pathway Courses

Partner countries are going to implement the FORC courses as a Pathway. The rationale behind this decision is to allow those who are interested in digital forensics to enroll in the courses, despite their registration status (i.e. students and none-students). This way we can easily target and accept people interested in learning digital forensics form the locale community or from neighboring countries without the need to go through the typical bureaucratic procedures associated with establishing new undergraduate courses that might prevent an interested person from attending the courses due to their age, education background, etc. For example, someone from a Law/business/medical background will be able to attend the courses. Moreover, the FORC topics will be offered as special (elective) topics for the undergraduate students in the Computer Science major as well as the upcoming major in Data Science.

The 8 courses were condensed into 4 courses in professional certification layout. The details for each course are listed below.

I. Foundation of Digital Forensics

- **Duration**: 40 Training Hours.
- **Level**: Beginner.
- **Topics**:
  1. Fundamentals of digital forensics investigation
  2. Digital forensics process and procedures
  3. Evidence gathering techniques.
  4. Documenting and reporting investigation results
  5. Introduction to law and the legal system
  6. Overview of criminology and digital crime
  7. Legal aspects of digital forensics
  8. Expert witness in a court of law
  9. Standards, framework and best practices for incident response and digital forensics
  10. Ethical and Social issues in digital forensics

II. Digital Forensics Tools and Techniques

- **Duration**: 40 Training Hours.
- **Level**: Intermediate.
- **Topics**:
  1. Introduction to Digital Forensics Investigation
  2. Digital Forensics Evidence Acquisition
  3. Digital Forensics Techniques
  4. Internet investigation
  5. Introduction to Database Forensics
  6. Windows Artifacts

7. Linux Artifacts
8. Macintosh Artifacts
9. Memory Analysis

III. Networks Forensics

- **Duration**: 40 Training Hours.
- **Level**: Intermediate.
- **Topics**:
  1. Introduction to Network Forensics
  2. Technical Fundamentals and Incident Response
  3. Network Forensics Tools
  4. Network Evidence
  5. Network Protocols
  6. Traffic Analysis
  7. Log Data Collection, Aggregation and Analysis
  8. Firewall and Network Device Forensics
  9. Email Investigations
  10. Network Intrusion Detection/Prevention Systems
  11. Investigating Encrypted Traffic
  12. Covert Channels, C&C, and Malware Traffic Investigations
  13. New Trends: IoT, Social Media, and Cloud Forensics
  14. Reporting and Evidence Presentation

IV. Mobile Forensics

- **Duration**: 40 Training Hours.
- **Level**: Advanced.
- **Topics**:
  1. Fundamentals of Mobile Devices and Cellular Network
     1.1. Cellular Network
     1.2. Mobile Device Hardware
     1.3. Smart Cards
     1.4. Standards, Societies and Body of Knowledge
  2. Mobile Forensics Process, Methods and Techniques
     2.1. Mobile Forensics Process
     2.2. Acquisition Methods
     2.3. Emerging Techniques in Mobile Forensics
  3. Mobile Forensic Tools
     3.1. Cellebrite
     3.2. Oxygen Forensics
     3.3. MSAB
     3.4. Magnet Forensics
     3.5. Open-Source Mobile Forensic Tools
  4. Mobile Device Forensics
     4.1. Android, BlackBerry, iOS and Windows Mobile Forensics

4.2. Artefacts Extraction
4.3. Data and File Carving
4.4. Deleted Files Recovery
4.5. Bypassing Security Controls

5. U/SIM Cards Forensics
   5.1. U/SIM Card Artefacts Extraction
   5.2. U/SIM Card Cloning
   5.3. U/SIM Card Forensic Tools
   5.4. Bypassing U/SIM Card Security Controls
   5.5. APDU Commands