3 June 2016

Act 4.3 Introductory course on Digital Forensics (Basic training)
15-17 June 2016

Act 4.3 Live Data Forensics Training (Advanced training)
20-22 June 2016

PHILLJA Training Center, Tagaytay, Philippines

Outline

Background

As the use of and reliance on information technology becomes ever more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and in sophistication. Against these threats and rising number, police officers tasked with fighting cybercrime should have both technical expertise necessary to secure electronic evidence and seek active partnerships with other institutions that can provide advanced knowledge and skills. This includes the focus on live data forensics, which is often an essential process for extracting evidence in the context of real-time monitoring of traffic data, as required by Article 20 of the Budapest Convention.

At the same time, live data forensics skills and capabilities are a step above the basic knowledge and skills required for digital forensics on computer system and data, in particular stored data. Often, the focus on different forensics capabilities and skills is determined by the specialization of investigative units that investigate specific forms of cybercrime, or deal with specific types of electronic evidence (e.g. mobile forensics); however, the basic set of skills in terms of environments, equipment and procedures is similar across various forensic units and experts.

In this light, it is important that the law enforcement is in hold of the wide range of forensic skills and capabilities that assist in investigation and prosecution of cybercrime in the most efficient, timely and legally sound manner.

Objective

The aim of this activity is to support the law enforcement agencies of the Philippines that are specialized in dealing with cybercrime and electronic evidence, to get familiarized with both basic (stored data and computer systems forensics) and advanced (live data forensics) digital forensics skills and capabilities necessary for criminal intelligence and proper handling of electronic evidence in cybercrime cases.

Participants

Police investigators, forensics experts, criminal intelligence experts, members of CSIRT/CERT teams, PNP, NBI or other criminal justice experts and supporting personnel dealing with digital forensics

Programme (draft)

The training will be divided into two distinct parts.

A group of 35 participants will undertake a 3-day introductory course in digital forensics management and procedures that is neutral enough to include most common types of devices and electronic evidence.

Following on-the-spot assessment of the introductory course, selected group of participants (up to 35 persons) will undergo the advanced forensics course on live data forensics.

Trainers: Mr Fernando MENDES (Portugal) and Mr Alexandru STOIAN (Romania)

Basic Course

Wednesday, 15 June 2016	
09h00	Session 1 : Introduction to Computer Forensics & Computer Forensics ISO Standards
11h00	Session 2 : Bits and Bytes - Partitionning
13h00	Lunch break
14h30	Session 3 : File systems – a forensic approach – part I
16h00	Session 4 : File systems – a forensic approach – part 2
17h30	End of day 1
Thursday, 16 June 2016	
09h00	Session 5 : Keyword low level searchers
11h00	Session 6 : File metadata and carving on file type signature
13h00	Lunch break
14h30	Session 7 : Forensic imaging
16h00	Session 8 : Live Data Forensics
17h30	End of day 2
Friday, 17 June 2016	
09h00	Session 9 : Windows Forensics - overview
11h00	Session 10 : Windows Forensics – Registry
13h00	Lunch break
14h30	Session 11 : Computer Forensics – Ram Up
16h00	Session 12 : closing session, discussion and feedback
17h30	End of day 3

Advanced Course

Monday, 20 June 2016	
09h00	Session 1 : Forensics principles – and limitations of post mortem forensics
11h00	Session 2 : Live Data forensics - introduction
13h00	Lunch break
14h30	Session 3 : Live Data forensics – methodology and tools
16h00	Session 4 : Live Data forensics – practical exercise
17h30	End of day 1
Tuesday, 21 June 2016	
09h00	Session 5 : Live Data forensics – memory analysis
11h00	Session 6 : Live Data forensics – memory analysis – part II
13h00	Lunch break
14h30	Session 7 - Case study
16h00	Session 8 – Case study
17h30	End of day 2

Wednesday, 22 June 2016	
09h00	Session 9 : Case study
11h00	Session 10 : Case study
13h00	Lunch break
14h30	Session 11 : Live Data Forensics – Ramp Up
16h00	Session 12 : closing session and feedback
17h30	End of day 3

Hardware/software requirements

The requirements listed below are a basic reference and more specific requirements will be set after the selection of expert trainers:

1. PC hardware requirements: CPU: dual core, 2 GHz, with support for virtualization (VT-x or AMD-V) RAM: at least 4 GB, 6 GB recommended HDD: 80 GB of free space WiFi card

2. All PC's must have installed the last version of VirtualBox: https://www.virtualbox.org/wiki/Downloads

3. Internet connectivity WiFi connectivity for all participants (should be well dimensioned to sustain more than 50 connections)

Location

The training will take place at PHILJA Training Center, in Tagaytay City, Manila, Philippines.

Contact

At the Council of Europe:

Manuel PEREIRA
Project manager
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 32
Email: manuel.pereira@coe.int

Polixenia CALAGI
Project Officer
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 7807
Email: polixenia.calagi@coe.int

In Philippines

Jed Sherwin G. UY
Agent-in-Charge
Office of Cybercrime
Department of Justice
Manila, Philippines
jsguy@doj.gov.ph

Angela Marie M. DE GRACIA
State Counsel
Department of Justice
Republic of the Philippines
amdegracia@doj.gov.ph