Schedule and Components

- Basic Digital Forensics takes place over five 8-hour days.
- This training is for participants working in information security related roles who already have advanced system administration skills. Due the many practical tasks, technical prerequisites for this training include a PC for each student with the appropriate tools installed, including Live Response Tools (Sysinternals), Forensics Live CDs (Helix, DEFT) and Forensics Disk Imaging (FTK, dd, HDD). All are free tools we actively used in the workplace.
- It is impossible to study digital forensics (DF) without understanding its main principles.

Tools change with time, but basics and methods of work remain consistent.
Participants will receive not just a set of tools and instructions, but knowledge of fundamental principles and functionality. All practical tasks are based on real cases wherever possible without breaching customer confidentiality.

Day 1

Overview

Because a successful digital forensics process depends on successful incident response, the steps involved in efficient incident response will be covered along with some tools widely used in incident response for the acquisition of evidence from the system memory or hard drive on a live or shot down target system to what is called forensically sound image and techniques for mount and reading the acquired image on Windows and Linux operating systems.

Due to the constantly improving techniques, live analysis or response is a highly recommended practice in situations, where analysis of the target machine/s needs to be conducted immediately at the scene. On Day 1 we will demonstrate some live response techniques using different set of tools.

We will also provide students with essential knowledge about the digital forensics field, including definition, process and procedures. Building a workspace for digital forensics is no easy task when you consider the risk of data loss, hardware failure or even infection caused by the evidence under investigation. This section will deliver some guidelines about configuring the digital forensics workstation and will also explore the benefits of virtualization techniques in creating a multiplatform environment for running different tools.

Major differences in HDD and SSD or Solid State Drive operations makes it very difficult to follow the same procedures or use same tools for acquisition or analysis. In this module we will demonstrate why SSD are different and which challenges are present during the analysis of SSDs.

Day 2

Overview

The registry is one of the most important evidence-gathering components of the Windows operating system and a 'mandatory for analysis' element of the digital forensics process. Using the registry, the investigator will be able to retrieve important information about the operating system such as time zone, network address, browsed websites, security policy and startup executables. User activities such as login and opened files can also be extracted from the registry hives.
Malware executables usually acquire a registry location to guarantee survival during system reboot or user logoff, and this can provide the investigator with clues about malicious activity in the machine under investigation.

In this module, we examine the structure of the Windows registry and the location and contents of different registry hives in the file system. Students will learn how to navigate through the registry hives either online in a live system or offline by extracting the hives files from a backup of the forensic image.

Day 3

Overview

The Windows operating system uses different file structures and formats tostore data about its operations. As with the Windows registry, some files are ofparticular interest to the investigator. Information extracted from these files canprovide an added value to the investigation process, so understanding thesefiles structures is critical. In this module, the investigators will be able to locateand parse Event log files, .lnk files, Windows tasks, prefetch files and recycle bin contents. The module also covers the extraction of evidential information from compound files such as images with exif data, thumbnail files and Microsoft office files.

Day 4

Overview

During the normal web browsing, important information stored in the file system, the location and structure of data differing between browsers. In this section, the investigator will learn how to find and analyze the browsing history, internet cache files, bookmarks, cookies, etc. Leading browsers Chrome, Firefox and IE will be covered in this Module.

Email is a standard method of communication nowadays for official and nonofficial purposes. Email files can store considerable evidential information. Different implementations of the email service, by private mail server or web mail, and the existence of different clients such as Outlook and Lotus. The investigator needs to understand the behavior and workings of the email client in the user machine and to have the skills necessary to investigate these files in order to extract related data. In this module, we will discuss the remnants after usage web based e-mail services and Outlook and Lotus mail clients.

Day 5

Overview

On the final day, students undertake a number of exercises, covering different elements of the training and involving different types of files. Students must apply forensic analysis to these files in order to answer questions correctly. At the end of the day, the correct answers will be discussed with the students to obtain the maximum benefit from the exercise.

Skills gained

- Under our guidance students will learn how to collect digital evidence and deal with it properly
- During this training students will reconstruct an incident, use time stamps and find traces of intrusion on investigated components of the Windows OS
- The OS itself isn't the only source of knowledge. Students will also learn how find and analyze browser and email history and how to use this software to collect evidence

Veranstaltungsort:	**twelve** meetings | conferences | events Eingang Südfoyer, EG & OG Hertha-Firnberg-Straße 8 1100 Wien
Preis pro Person:	EUR 2.900,00 exkl. MWSt.