SYLLABUS

DIGITAL FORENSICS PROFESSIONAL

The world's premier online Digital Forensics course

eLearnSecurity
Forging security professionals

eLearnSecurity has been chosen by students in over 140 countries in the world and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

COURSE DESCRIPTION & GOALS

The Digital Forensics Professional (DFP) course is an online, self-paced training course that provides you with the necessary knowledge and techniques to not only investigate intrusions and prepare intrusion reports but also to assist in cases of incident response or proactive threat hunting.

Regardless of which blue-team role you possess, having the ability to conduct digital forensics investigations will make you an all-around and valuable blue-team member. As an incident responder or threat hunter, you could still benefit from having digital forensics skills, as such skills will enable you to identify and gather digital evidence as well as retrieve and analyze data from both the wire and endpoints.

Digital Forensics Professional is an interactive, hands-on course that provides the learner with foundational materials and concepts, supplemental video demonstrations, as well as the opportunity to apply and test the acquired knowledge in our Hera labs environment. Through this method of instruction, you will learn:

- The fundamentals of digital forensics and how to perform a detailed digital investigation
- Different tips and techniques to aid your data acquisitions
- How to use various tools and techniques for different investigation cases
- How to analyze disks and file systems at a low level
- How to locate and analyze different Windows OS system artifacts
- How to analyze the user profile (NTUSER.DAT)
- How to investigate the usage of a thumb drive (portable devices: USBs)
- How to analyze and investigate different network attacks
- What logs are and how they will support your investigations
- Techniques and tools to generate a timeline to help you with your analysis
- Why documentation is important and how to prepare an investigation report and much more.

Upon completing this course, you will be:

- Capable of conducting a complete Digital Forensic Analysis and writing a final investigation report
- Able to locate artifacts, that can be used as compelling evidence
- Able to understand how disks operate and what different partitioning schemes are being used today
- Familiar with digging down to lower disk levels and analyzing both FAT and NTFS file systems

- Able to reconstruct the activities and events performed on a system being investigated
- Capable of analyzing different Windows system artifacts, the Windows Registry, and User Profiles.
- Able to analyze network traffic and system logs
- Familiar with creating different timelines to perform a timeline analysis

PRE-REQUISITES

The DFP training course covers foundational topics on Digital Forensics; however, a good working knowledge coupled with experience in information technology, with a focus on information security, prior to the class will be needed to aid you in your learning. You should have:

- A solid understanding of the fundamentals of modern Operating Systems
- Basic understanding of Networks, Network Protocols, and Programming Languages

WHO SHOULD TAKE THIS COURSE

This training course is primarily intended for Digital Forensics professionals, Incident Responders and Threat Hunters, that would like to gather and analyze digital evidence retrieved from both the wire and endpoints inside their environments.

As a seasoned red-team member, you could also benefit from this course, since knowing what digital evidence each attack leaves behind is crucial in updating your current techniques, tactics, and procedures.

By design, the Digital Forensics Professional (DFP) course is the definitive online and hands-on course if your goal is to become a digital investigator, as it will provide you not only with the fundamentals of Digital Forensics but with practical investigation skills as well.

The target audience for this course is:

- Security professionals, Digital investigators, and Digital Forensics examiners
- Incident Responders and Threat Hunters
- Digital Forensics Instructors and students
- Red team members who want to update their techniques, tactics, and procedures

COURSE ORGANIZATION

This training course is completely self-paced with interactive slides and video material that students can access online without any limitation. Students have lifetime access to the training material.

Students can study from home, the office or anywhere an internet connection is available. Some course versions allow a student to download course material and study offline.

While studying online, it is always possible to resume your studying from the last slide or video accessed.

The Digital Forensics Professional course is also integrated with Hera Lab, the most sophisticated virtual lab in IT Security. Hera Lab provides real-world IT Security scenarios on demand where a student can practice each topic seen in the course in a dedicated and isolated environment.

WILL I GET A CERTIFICATE?

The DFP course leads to the eCDFP certification.

The certification can be obtained by successfully completing the requirements of a practical exam hosted in our eLearnSecurity Hera Labs, followed by an online exam.

ORGANIZATION OF CONTENTS

The world of Digital Forensics is extensive, with many fields in forensic analysis. The student is provided with a suggested learning path to ensure both maximum success rate and minimum effort.

Section 1: Introduction & Acquisition

- Module 1: Introduction to Digital Forensics
- Module 2: Data Acquisition

Section 2: File & Disk Analysis

- Module 3: Data Representation and Files Examination
- Module 4: Disks
- Module 5: File Systems

Section 3: System & Network Forensics

- Module 6: Windows Forensics
- Module 7: Network Forensics

Section 4: Logs, Timelines & Reporting

- Module 8: Log Analysis and Correlation
- Module 9: Timeline Analysis
- Module 10: Reporting

SECTION 1: Introduction & Acquisition

In the first part of this section, you will learn about the fundamentals of digital forensics, digital evidence, and intrusion reconstruction. The challenges an investigator could face are also documented. The second part will cover what data acquisition is and the different methods available for data acquisition. Additionally, storage formats and the required toolset will also be documented in this part. Acquisition isn't complete without discussing data validation, so this section concludes with the techniques used to validate your acquired data.

1. Introduction to Digital Forensics
- 1.1. Introduction
  - 1.1.1. Out of Scope
- 1.2. Background
  - 1.2.1. Digital Forensics Uses
- 1.3. Fundamentals
  - 1.3.1. Digital Evidence
  - 1.3.2. Digital Forensics Tools
  - 1.3.3. Scientific Method
- 1.4. Digital Evidence
  - 1.4.1. Digital Evidence Life Cycle
    - 1.4.1.1. Acquisition
    - 1.4.1.2. Analysis
    - 1.4.1.3. Presentation
  - 1.4.2. Types & Sources of Digital Evidence
    - 1.4.2.1. Active Data
    - 1.4.2.2. Archive and Backup
    - 1.4.2.3. Hidden Data Types
    - 1.4.2.4. Volatility
    - 1.4.2.5. Devices
- 1.5. Analysis Steps
  - 1.5.1. Creating a Forensic Image
- 1.6. Investigation Scope
- 1.7. Crime Reconstruction
- 1.8. Challenges of Digital Evidence
- 1.9. Major Concepts

2. Data Acquisition
- 2.1. Introduction
  - 2.1.1. Order of Volatility
  - 2.1.2. Types of Data Acquisition

2.2. Storage Formats
2.3. Acquisition Methods
2.4. Live Data Acquisition
2.5. Tools
    2.5.1. Write Blockers
    2.5.2. Bootable Disks
    2.5.3. Non-Writable USB
    2.5.4. FTK Imager
    2.5.5. Live Forensic Tools
    2.5.6. Memory Forensic Tools
    2.5.7. Other Forensic Tools
2.6. Validating Evidence
2.7. Exploring Evidence
2.8. Miscellaneous

SECTION 2: File & Disk Analysis

In this section, you will learn how to interact with the lower-levels of files and disks. Specifically, you will understand the file's structure and learn how to identify various file types. File's metadata will also be demystified in this section. You will then get familiar with disk drives, their types, and schemes used today by our systems. Volumes and partition concepts are up next. You will learn what they are, how to identify them and the techniques you can use to analyze them. Finally, you will dive into the world of file systems. You will be shown how to analyze FAT and NTFS file system structures and how to apply file carving techniques to retrieve previously removed data. You will have the chance to try each tool and technique mentioned in hands-on and practical labs.

3. Data Representation and Files Examination
3.1. Introduction
3.2. Data Representation
    3.2.1. Bits, Bytes and More
    3.2.2. Kilobit vs. Kilobyte
    3.2.3. From Decimal to Binary
    3.2.4. Hexadecimal
    3.2.5. From Binary to Hex
    3.2.6. From Hex to Binary
    3.2.7. ASCII
    3.2.8. View Data in Practice
3.3. File Identification and Structure

SECTION 3: System & Network Forensics

In this section, you will start by analyzing artifacts at the OS level. Specifically, this section dives deeply into the Windows OS and its artifacts. The location of each artifact, the tools needed for their analysis and the knowledge to translate tool results into answers are all documented in this section. You will also dive into to the world of networks in this section. You will start by understanding what network traffic is, what are the main network protocols and how to acquire traffic. Finally, you will get familiar with the tools and techniques required to analyze not only network traffic but different network attack as well.

- 6.3. Windows Artifacts
  - 6.3.1. LNK Files
  - 6.3.2. ThumbCache
  - 6.3.3. Volume Shadow Copy
  - 6.3.4. JumpLists
  - 6.3.5. Libraries
  - 6.3.6. Windows Search History
  - 6.3.7. Windows Recycle Bin
- 6.4. System and Application Cache Files
  - 6.4.1. Prefetch Files
  - 6.4.2. Application Compatibility Cache
- 6.5. Windows Registry
  - 6.5.1. Registry Artifacts
  - 6.5.2. User Hives
- 6.6. ShellBags
- 6.7. USB Forensics
- 6.8. Browser Forensics
  - 6.8.1. Internet Explorer (IE)
- 6.9. Skype Forensics

7. Network Forensics

- 7.1. Introduction
- 7.2. TCP/IP Protocol Suite
- 7.3. Classes of Traffic
- 7.4. Network Devices
- 7.5. Network Protocols
  - 7.5.1. HTTP
  - 7.5.2. Cryptography and SSL/TLS
  - 7.5.3. SMTP
  - 7.5.4. DNS
  - 7.5.5. DHCP
  - 7.5.6. ICMP
  - 7.5.7. ARP
- 7.6. Network Forensics
  - 7.6.1. Protocol Analysis
  - 7.6.2. Flow Analysis
  - 7.6.3. File Carving & Data Extraction
  - 7.6.4. Statistical Flow Analysis
  - 7.6.5. Network Forensics
- 7.7. Email Forensics
- 7.8. OSCAR
- 7.9. Network Evidence Acquisition

7.9.1. Berkeley Packet Filter
7.10. More Web Forensics
7.11. Network Attacks

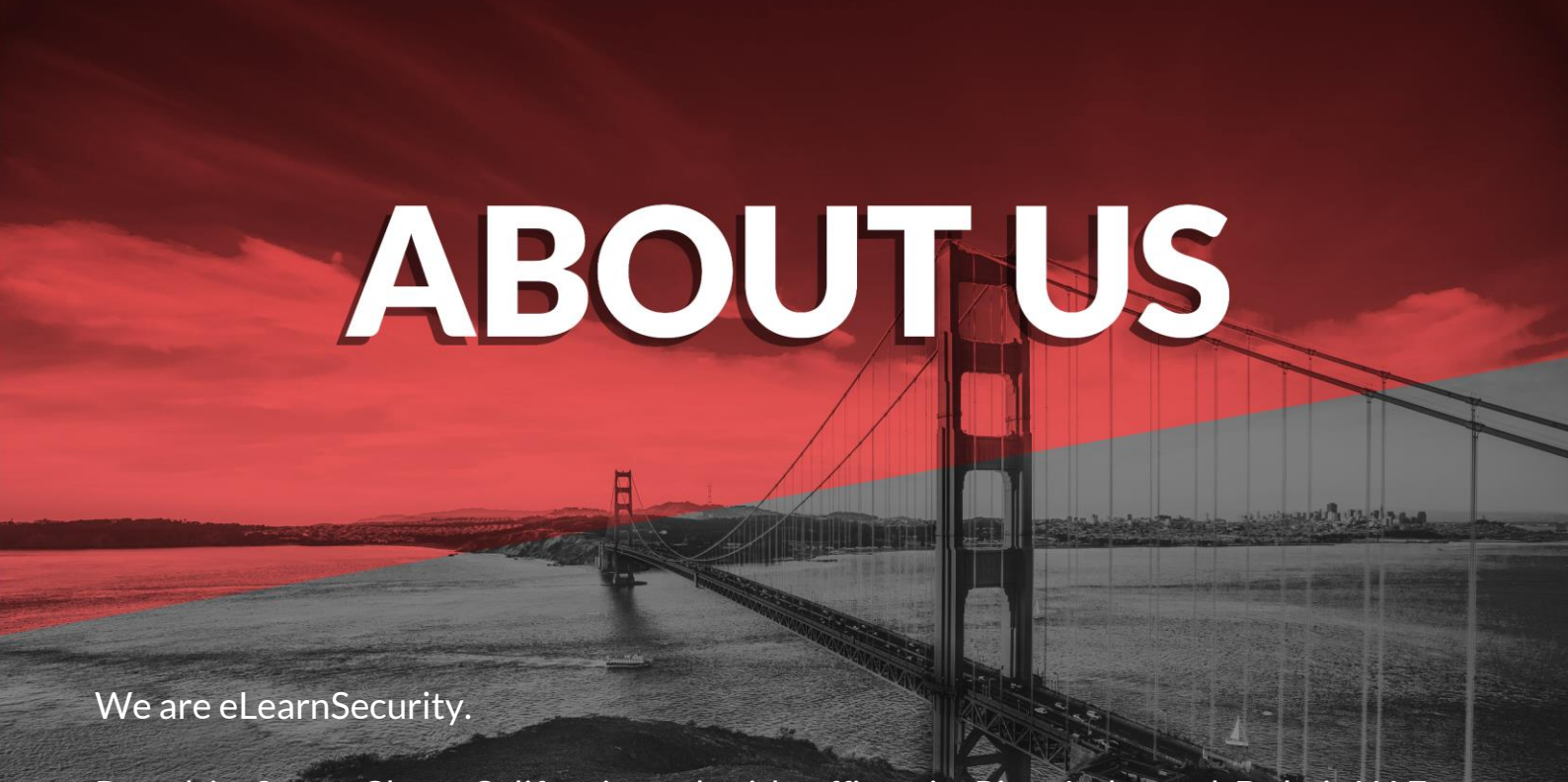
SECTION 4: Logs, Timelines & Reporting

In this section, you will first go through log analysis fundamentals. The various log files, how to extract them, how they can help you during an investigation and the various log analysis tools are all documented in this module. You will then move on to timeline analysis. Specifically, you will learn how to create a meaningful and actionable timeline, that can aid your investigation. This section concludes with the importance of documentation and reporting. Upon completing this section, you will know how to write an investigation report and the important sections that should be included in it.

8. Log Analysis and Correlation
8.1. Introduction
8.2. Logging Infrastructure
8.3. Using Linux Tools for Log Analysis
8.4. Web Logs
8.5. Windows Events
8.6. Syslog

9. Timeline Analysis
9.1. Introduction
9.2. Event Types
9.3. Approaches
9.4. Temporal Proximity
9.5. Timestamp Types
9.6. Timeline Fields
9.7. Creating Timelines

10. Reporting
10.1. Introduction
10.2. Tips on Reporting
10.3. How to Write a Report
10.4. Report Structure
10.5. What is a Good Report?
10.6. Report Samples



ABOUT US

We are eLearnSecurity.

Based in Santa Clara, California and with offices in Pisa, Italy, and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training. Best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, have changed the way students learn and practice new skills.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com

2040 Martin Ave.
Santa Clara, CA, USA

Via Gian Battista Queirolo
Pisa, Italy

Apricot Tower, Dubai Silicon Oasis
Dubai, UAE