FOR600

ADVANCED DIGITAL MEDIA FORENSICS

FOR600 - Advanced Digital Media Forensics provides an in-depth look at forensic acquisition and analysis of multiple types of media. The course outlines a number of ways to achieve forensic goals while ensuring all processes are completed in a forensically-sound manner, and covers advanced automated tools, as well as manual tools and methodologies.

Advanced Digital Media Forensics focuses on a variety of Windows Internet, Chat, and Social Media artifacts. Additional topic discussions include data obfuscation and obtaining and analyzing intentionally hidden, overwritten, or deleted data. Students will also consider deploying discussed forensic methodologies in both a proactive and reactive manner.

TARGET AUDIENCE

Professionals looking to expand their digital forensic knowledge and obtain a better understanding of tips, tricks, and methodologies for data locations and recovery. This class is for the examiner/investigator that may face a multitude of examination requirements

OBJECTIVE

Provide an advanced analytical perspective on data considered to have forensic value

CYBRScore™

DAY 1

During the first lesson, students will learn about incident response and memory analysis.

Topics List

- Memory Analysis
- Live Memory Capture
- Typical Windows Functionality
- Windows Event Logs

DAY 2

Students will learn about advanced automated tools, advanced filtering, creating and using custom filters, manual, data carving, fuzzy hashing and rolling hashes.

Topics List

- Manual Data Carving
- Setting Custom/Advanced Filters
- SSdeep

DAY 3

Students will learn advanced Windows forensics, data hiding and obfuscation (how to detect, protect, and create), application artifacts and cryptography.

Topics List

- Alternate Data Streams
- Creating and Detection
- Deleted Partition Recovery
- Volume Shadow Copy/Restore Point Analysis
- Password Cracking

DAY 4

Students will learn about forensic reporting and documentation. Student will review all the course modules and labs and work through a practical lab. The practical will encompass a multitude of methodologies learned throughout the course in order to apply all techniques simultaneously.

DAY 5

Review all submitted forensic reports at the end of Day 4 and discuss items of concern within both the processes and the reporting.

Capstone Exercise

Conduct forensically sound memory acquisition and answer a line of questions. Furthermore, complete the rest of the investigation using all of the discussed and practiced skills throughout the class. The student must successfully complete the investigation and answer any corresponding questions while effectively reporting on the appropriate steps taken to achieve said goal.

FOR600

ADVANCED DIGITAL MEDIA FORENSICS

CYBRScore™