FOR300 Basic Digital Media Forensics

Course Overview

FOR300 - Basic Digital Media Forensics provides an introduction to media collection, imaging and analysis. Students will discuss file systems, partition structures and data storage to better understand how and where data is stored on multiple types of digital media, as well as the best methods to access it.

The course is an optimal starting point for individuals looking to expand their forensic knowledge and outlines a number of ways to achieve forensic goals while ensuring all processes are completed in a forensically-sound manner. Chain of custody and evidence handling is addressed, as well as what to do and what not to do when dealing with 'live' evidence.

Objectives

- Provide a solid understanding of what is considered valuable digital media used as forensic evidence for an investigation, including how data is stored, retrieved and analyzed

Target Audience

- Professionals looking to broaden their cyber skills or begin developing a strong skill set within the forensic community

Estimated Course Length: 24 hours

Day 1

During the first lesson, students will learn about setting up a Forensic workspace. In addition, students will learn about preparing target media to ensure a forensically sound process prior to imaging.

Topics List

- Preparation of target media/wiping using dc3dd
- Forensic imaging using FTK Imager
- Identification and discussion of various digital media that has been and could be useful in a forensic investigation

Day 2

A lesson consisting of Incident response and acquisition. Students will also learn about forensic tools, windows file systems, and partition structures.

Topics List

- Forensic imaging of different media using FTK Imager
- Forensic analysis of a raw image using autopsy
- Exifdata analysis

Day 3

Students will become more familiar with Forensics for Windows, and learn the value of metadata, and exifdata in forensic analysis.

Topics List

- Forensic analysis of a raw image using autopsy
- Exifdata analysis
- Viewing of data in a hex editor

Day 4

Students will learn the proper techniques for Forensic reporting and documentation.

Topics List

- Lab will begin by conducting analysis on another dd image
- Answering a line of questions that pertains to that provided image
- Conduct imaging and analysis of a smaller image
- Draft a comprehensive forensic report

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

Students will conduct a forensically-sound acquisition and analysis of assigned media. After which, they will be required to write a comprehensive forensic report.

About CyberStronger

Comtech provides cybersecurity solutions and services tailored to training and workforce development. The CyberStronger product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech CyberStronger offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

Comtech
cyberstronger.com | comtechtel.com
275 West Street, Annapolis, MD 21401