Course Syllabus

Digital Intelligence®

Digitalintelligence.com

Forensics of Internet Related Evidence (FIRE)

INTERMEDIATE LEVEL

Course Objectives

This 2 day class is designed to familiarize the student with the many artifacts left behind on Windows based media and mobile devices from the most popular internet browsers and Email applications.

Prerequisites

This intermediate course is designed for an experienced digital forensic or eDiscovery practitioner with a solid understanding of Microsoft Windows system functionality.

To gain the maximum benefit from this course you should meet or exceed the following requirements:

- Read and understand the English language
- Have attended basic digital forensic training
- Have at least 6 months experience conducting digital forensic examinations
- Be familiar with the Microsoft Windows environment and data recovery concepts

Course Outline

The course will follow adult learning principles through training aids such as presentations, diagrams, and practical instructor led examples. Each topic covered will be presented in either one or two 50 minutes sessions followed by review questions. Students will be given the opportunity throughout the course to ask questions and discuss topics in more detail. Ample time will be allotted for hands on exercises to reinforce learning.

Introduction and Tools Used During the Course

- Introduction by the course instructor and students
- An overview of commercially available products, such as NetAnalysis, Internet Evidence Finder/Axiom, Belkasoft, EnCase and Forensic ToolKit, and tools that are free and in the public domain.

World Wide Web

- Clear/Deep/Dark Web
- Browser introduction
- TOR browser

Internet Connectivity and Topology

- TCP/IP basics
- DNS
- DNCP
- Transport protocols

Internet Explorer and Edge

- Explanation of internet cookies
- Explanation of internet history and downloads
- Explanation of temporary internet files
- Explanation of tabbed browsing
- Explanation of favorites or bookmarks
- Identifying the location of the artifacts left behind while browsing
- Describe the recoverable artifacts with InPrivate browsing

Mozilla Firefox

- Identify the location of artifacts left behind while browsing with Firefox
    - ◊ Cookies
    - ◊ History
    - ◊ Cache or temporary internet files
- Form data and password recovery and the master password implications
- Describe the private browsing feature of Firefox

Google Chrome and Edge Chromium

- Identify the location of the artifacts left behind while browsing with Google Chrome
    - ◊ Cookies
    - ◊ History
    - ◊ Cache or temporary internet files
    - ◊ Downloads
- Explanation of internet history and downloads
- Functions of the Chrome omnibox
- Aero Peek option with Chrome
- Incognito mode

Windows Live Mail

- Identify the locations of the locally saved mail
- Recovery of deleted mail
- Explain the recovery of Windows live mail from the temporary internet files

Microsoft Outlook

- Explanation of the PST file
- Explanation of the OST file
- Describe deleted mail recovery with an email archive