

## FORENSIC TRACK

### FT310, Advanced Deployable Forensics Course (ADEF)

#### **Who Should Attend**

DoD and federal law enforcement personnel who will be deployed and required to analyze recovered digital media for mission relevant intelligence and investigative information.

#### **Prerequisites**

FT211 (DEF) or TT110 (INCH) and RT120 (CIRC)  
and FT210 (WFE-E) or FT215 (WFE-FTK) or Test Outs

#### **Duration**

5 Days

#### **Course Description**

Students learn advanced forensic techniques to quickly and accurately recover time-sensitive and mission relevant information from digital media when working in a hostile environment. Advanced techniques include advanced keyword searching, rebuilding RAID, imaging of cell phones, GPS devices and alternative portable devices. {Mobile}

#### **Objectives**

- Use a variety of software forensic tools to acquire images of digital media.
- Use Helix to recover data from various digital media types
- Extract data from cellular phones, global positioning systems (GPS), and media players.
- Image and Recover Redundant Array of Inexpensive Disks (RAID) using hardware and software tools.
- Preview and image a variety of alternative storage devices. techniques
- Use advanced features of the EnCase forensic software tool to quickly and tactically recover data.

#### **Topics Covered**

- Recovering deleted partitions
- Registry analysis
- Advanced keyword searching techniques
- Rebuilding RAIDS
- Advanced Helix techniques
- Logical acquisitions
- Use of cross-over cables
- Use of software write blockers
- USB imaging techniques
- Advanced cell phone, GPS, and alternative devices exploitation.

#### **Preparation**

To assist in your preparation for the Advanced Deployable Forensics (ADEF) course, we recommend the following:

##### **You should have:**

- A basic understanding of computer software and hardware, including Intel x86-based systems and associated peripheral hardware, operating systems, common software applications, and forensic tools.
- A basic understanding of the Helix Live CD.
- A working knowledge of the Linux command line interface.

## FORENSIC TRACK

### **You should review:**

- Linux Commands
- DCITA Live CD
- DCITA Helix USB View
- Automated Image and Restore (AIR)
- Adepto (graphic user interface front end)
- Physical Memory Acquisition
- Incident Response Tools
- RAIDs
  - Hardware
  - Software
- EnCase
- Virtual Machines
- Software Write Blockers
- Web Historian (Mandiant)

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (<https://www.dcita.edu>), the internet, at Books 24/7, in your organization's technical library or at the public library.

### **ADEF Grading Policy**

Student progress is monitored through instructor observation during lecture, discussion and practical exercises as well as Knowledge and Performance Tests. Minimum passing score on all DCITA tests is 70%.