

## FORENSIC TRACK

### FT211, Deployable Forensics Course (DEF)

#### **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**

Basic understanding of computer software/hardware (including Intel x86-based systems), Operating Systems, common software applications and forensic tools.

#### **Duration**

10 Days

#### **Course Description**

Students learn to quickly and accurately recover time-sensitive and mission relevant information from digital media when working in a hostile environment. Students also learn to identify hardware and digital media, use data search and recovery techniques, configure and use common forensic software tools, and image digital media. {Mobile}

#### **Objectives**

- Identify the equipment and materials necessary to meet mission-specific needs
- Identify various digital media types.
- Properly seize and transport digital media
- Properly configure and operate commonly used forensic software
- Preview and image a variety of digital media using forensically sound techniques
- Search digital media and media images using various search techniques to identify items of mission or investigative interest

#### **Topics Covered**

*Computer Hardware - Students are introduced to computer hardware and digital media that may be encountered in the field.*

- Identify computer hardware and operating systems
- Assemble and use hardware that would be used in the field to process digital evidence

*Evidence Handling - Learn about the legal implications and proper handling of digital media that may be involved in future legal proceedings.*

- Evidence collection techniques
- Chain of custody and on-scene documentation
- Evidence packaging and management

*Initial Response - Learn how to safely preview evidence and acquire forensically sound images.*

- Image digital media with commonly available imaging tools
- Maintain and document the evidential integrity of collected digital media

*Forensic Analysis - Learn how to analyze digital media to recover mission-relevant information.*

- File identification and keyword searching
- Analyzing e-mail and newsgroups
- Alternate device analysis

## FORENSIC TRACK

*Mission Preparation - Learn how to prepare for mission.*

- Identify deployable hardware and software
- Planning a computer-related seizure

### **Preparation**

To assist you in being better prepared for the class, we recommend the following:

- Students need 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.

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.

### **DEF 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%.