



FORENSIC EXPLORER CERTIFIED EXAMINER – 4 DAY PROFESSIONAL TRAINING COURSE

Forensic Explorer (FEX) is a specialized software tool engineered for the preservation, analysis and presentation of electronic evidence. Primary users of this software are law enforcement, government, military and corporate investigation agencies. This four-day certified training course has been developed to educate all levels of digital forensic investigators on how to best utilize FEX. Participants will perform practical hands on assessment and theory test throughout the training. At the conclusion and successful completion of the course, participants will be awarded the Forensic Explorer Certified Examiner, (FEXCE).

Day One

- **Forensic Explorer Overview and Introduction**
- **Key program features**
 - Installation
 - Forensic analysis work station – system settings and configuration
 - Case management
 - Dongle activation and update management
 - Advanced Wibu key and network configuration
 - Maintenance FEX License and Wibu key
- **Creating a Digital Case**
 - Adding and removing evidence within FEX
 - Assessing and previewing evidence
 - Creating, converting previews and saving a case
 - Creating and managing investigators profiles
 - Understanding the evidence processor
- **Forensic Explorer Interface**
 - Module data interpretation
 - Customizing layouts
 - Process logging and prioritizing
 - Date and time verification
 - Digital forensics date and time analysis
 - FAT, HFS, CDFS file system date and time
 - NTFS, HFS+ file system date and time
 - Date and time information in the Windows registry

Day Two

- **Case Investigation and Analysis**
 - Module structure and overviews
 - Folder tree structure
 - Categories filters
 - Data Views
 - File list
 - Gallery
 - Disk views
 - Category graph
 - File Views
 - Hex and text
 - Bookmark
 - Byte plot and character distribution
 - Display – (Native interpretation)
 - File system record
 - Metadata
 - File extent
 - Property viewer (Email Module)
- **Data Management**
 - Filters
 - Data and file view internal searching

Day Two (Continued)

- **Bookmarking – Investigator's Notes and Observations**
 - Relationship between bookmarks and reports
 - Manual and automated bookmarking
 - Modification of bookmarks
- **Keyword and Index Searching**
 - Keyword Search – Management
 - Text
 - Hexadecimal
 - Regular Expressions (PCRE)
 - dtSearch analysis and searching techniques

Day Three

- **Hash Analysis**
 - Hash values
 - Hash algorithms
 - Hash sets creation and analysis
- **Signature Analysis and File Carving**
 - File signature analysis
 - Signature/File header and footer identification
 - File algorithm analysis
- **Email Module**
 - Microsoft Outlook .PST email analysis
 - Identifying and analysis of email attachments
- **Registry Module**
 - Automated registry analysis
 - Deleted registry keys
- **Introduction to FEX Scripting Functionality**
 - Script functionality behind the FEX Interface
 - Using automated scripts

Day Four

- **Examining Shadow Copy**
 - Shadow copy identification and file carving
 - Shadow copy forensic analysis
- **Live Boot / Mount Image Pro / Virtual Machine**
 - Running Live Boot to show a virtual environment of subject evidence
 - Password bypass/recovery of user accounts
 - Recreating historic restore points
 - Deployable Live Boot for VirtualBox
- **Report Writing and Management**
 - Creating manual reports
 - Building report templates
 - Modifying existing report templates
 - Saving and exporting templates
 - Exporting reports
- **Class Review Final Examination and Closure**
 - Award of Forensic Explorer Certified Examiner Certificates - FEXCE