FORENSIC EXPLORER

Advanced Forensics Software

GetData FORENSICS

Forensic Explorer (FEX) is software 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. Upon course completion participants will be awarded the Forensic Explorer Certified Examiner, FEXCE, professional qualification.

Level One

Forensic Explorer Overview and Introduction

- Installation and wworkstation configuration
- Case management
- Dongle activation and maintenance
- Advanced WiBu key and network configuration

Forensic Acquisition

- Write blocking v Write protection
- Network examinations and analysis
- GetData Forensic Imager

Creating a Digital Case

- Adding and removing evidence within FEX
- Assessment and preview of evidence
- Creating, converting previews and saving a case
- Creating and managing investigators profiles
- Understanding the evidence processor

Level Two

Forensic Explorer Interface

- Module data interpretation
- Customizing layouts
- Process logging and prioritization
- Date and time verification
- Digital forensics date and time analysis
- FAT, NTFS, HFS, HFS+, APFS, CDFS file systems
- Handling, Bitlocker and File vault encrypted containers
- Date and time information in the Windows registry

Case Investigation and Analysis

- Module structure and overviews
- Folder tree structure
- Categories filters
- Data Views
  - File list, Gallery, Disk, 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

Keyword and Index Searching

- Keyword Search – Management
  - Text, Hex, Regular Expressions (PCRE)
- dtSearch analysis and searching techniques

Bookmarking – Investigator's Notes and Observations

- Relationship between bookmarks and reports.
- Manual and automated bookmarking
- Modification of bookmarks

Level Three

Examining Shadow Copy

- Shadow copy identification
- Shadow copy file carving
- Shadow copy forensic analysis
- Recreating historic restore points

Live Boot / Mount Image Pro / Virtual Machine

- Live Boot virtualization of subject evidence
- Password bypass / recovery of user accounts
- Deployable Live Boot for VirtualBox

Hash Analysis

- Hash values and algorithms
- Creating and using hash sets

Signature Analysis and File Carving

- File signature analysis
- Signature/File header and footer identification
- Recovering Deleted Partitions

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

Level Four

Report Writing and Management

- Creating manual reports
- Creating and modifying templates
- Saving and exporting templates
- Exporting reports

FEX Viewer

- Review of case using dongle free viewer

Final Hands-on Practical

- Practical assessment covering all aspects of the previous four day's activities
- Award 'Forensic Explorer Certified Examiner (FEXCE)" certification upon successful completion