CDFS

CBIT Digital Forensics Services

M365 & Google Vault eDiscovery and Digital Forensics Training

(4-day instructor-led course)

Course Summary

This course has been tailored to address the unique needs of Digital Forensic and eDiscovery teams. Developed under the guidance of seasoned industry professionals, this curriculum offers comprehensive insights into harnessing the power of M365 and Google Data Analysis for eDiscovery and Digital Forensic purposes.

Learn how to extract data from Microsoft and Google Services and hone your skills to serve both legal and investigative objectives with finesse. Our instructors will guide you through the intricacies of these platforms, ensuring you navigate them with confidence.

M365 (including Email, MS Teams, OneDrive and SharePoint)

- Security and licensing identification.
- Setting up a Case
- Putting Custodians on Legal Hold
- Utilizing Legal Hold Notification Feature.
- Running Searches.
- Creating Review Set for the gathered content.
- Doing Review work (culling, tagging of content).
- Export of Content.

Google

- Security and licensing\versioning identification.
- Running searches.
- How to consider documents 'linked attachments' on a G Drive.
- Export results.

COURSE OUTCOMES

- Digital Forensic Triage
- Digital Forensic Acquisition
- Reviewing Digital Evidence
- Communicate and work efficiently with Digital Forensic and Cyber Teams
- Mobile Device Technology Overview

TARGET AUDIENCE

- eDiscovery & Forensics Team

THEORY AND PRACTICAL

- Multiple practical exercises are provided to enforce key concepts learned.

DAY 1 (M365)

MODULE 1: SECURITY AND LICENSING IDENTIFICATION

- Overview of Microsoft 365 Security and Compliance Centre
- Licensing options for eDiscovery and Digital Forensics
- Security considerations for eDiscovery and Digital Forensics
- Data Protection and Retention policies

MODULE 2: SETTING UP A CASE

- Creating a new case
- Assigning case permissions
- Adding and managing custodians
- Creating a search query
- **Types of data available:**
  Including, but not limited to, MS Teams, OneDrive and SharePoint
- Estimating search results
- Previewing search results

MODULE 3: PUTTING CUSTODIANS ON LEGAL HOLD

- Understanding legal hold
- Creating and managing legal hold
- Creating and managing legal hold notifications
- Releasing legal hold

MODULE 4: RUNNING SEARCHES

- Understanding search functionality
- Creating and running search queries
- Refining search queries
- Saving search queries

MODULE 5: REVIEWING AND ANALYSING CONTENT

- Creating review sets
- Adding content to review sets
- Managing review sets
- Reviewing content in review sets
- Applying tags and labels to content
- Using analytics to review content

DAY 2 (M365)

MODULE 6: EXPORTING CONTENT

- Creating export jobs
- Configuring export settings
- Previewing export results
- Downloading exported content

MODULE 7: MANAGING PROCESSING ERRORS

- Identifying processing errors
- Resolving processing errors
- Managing remediation of items and content

MODULE 8: ADVANCED TOPICS

- Machine learning and predictive coding
- Custom search queries using KQL and query builder
- Advanced analytics for eDiscovery and Digital Forensics

MODULE 9: PRACTICAL LABS (THROUGHOUT DAY 1 & 2)

- Case creation and management
- Search queries and refinement
- Custodian management and legal hold
- Review set creation and management
- Content review and tagging
- Export job creation and management

DAY 3 (GOOGLE)

MODULE 10: GOOGLE FORENSIC ARTEFACTS

- **Configuration:**
  Service, Application, Access Settings and Configurations
- **Logs**
  Track Administrative Actions and Access across Google Cloud resources
- **Reports**
  Statistical information presented in pre-built graphs and tables
- **Alerts**
  Provides Google pre-configured and custom alerting
- Practical (instructor led) with in-depth parsing of the above Google Forensic artefacts from a DFIR perspective

MODULE 11: ACQUISITION

- Google Takeouts
- **Gmail and Email Clients**
  Including, but not limited to, linked and attached files
- Backups including Android Backup
- **Commercial and open source software**
  Testing, review and discussion
- **Student Practical**
  3-5 acquisitions using different approaches and comparing results

DAY 4 (GOOGLE)

MODULE 12: ANALYSIS

- Forensic Analysis of Emails
- Forensic Analysis of Gmail Mailbox artefacts
- Student Practical
- Analysis of email headers and “My Activity”

MODULE 13: EXAMINATION & REPORTING

- Examination based on case scenario and preparation of a report
- **Report structure includes:**
  Scope
  Triage, Acquisition and Authentication
  Examination and Analysis
  Reporting and Presentation

PRICE

$6,000
per person ex GST