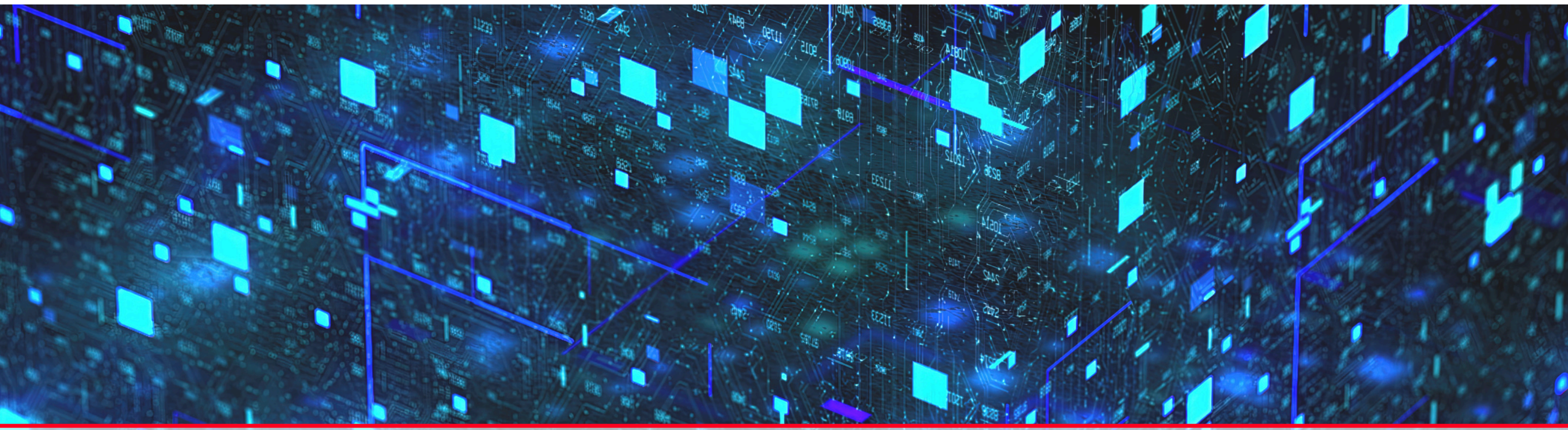
CYBEREYE™
The Science of Security
BY
US-COUNCIL



CYBEREYE
Digital Forensic Expert

CYBEREYE Digital Forensic Expert course is designed to provide comprehensive training in digital/computer forensics, covering various aspects and techniques essential for investigating digital crimes and incidents.

Key Topics:

- Live computer Forensics
- Dead computer Forensics
- Disk Imaging
- Disk Image Analysis

Module 1: Introduction to Digital Forensics

- What is Digital Forensics
- Different fields of Digital Forensics
  - Computer Hard Drive/ SSD/ NVMe imaging
  - Disk Image Analysis
  - Live Computer Analysis
  - RAM Dump Analysis
  - MAC Forensics
  - Video Forensics/ DVR Forensics
  - Mobile Forensics
  - Cloud Forensics
- Forensic Investigation Phases
- Chain of Custody

Module 2: Computer Hard Drive/ SSD/ NVMe imaging

- Hard Drive
  - What is a Hard Drive
  - Different types of Hard Drive & their connector types
    - IDE
    - SATA
    - SCSI
  - How data is stored on a Hard Drive
    - Tracks
    - Sectors
    - Clusters
- SSD/ NVMe
  - What is a SSD/ NVMe
  - How is a SSD/ NVMe different from Hard Drive
  - Different typed of SSD drives
    - SATA SSD
    - M.2 SSD (MSATA)
  - SSD/ NVMe connector types
- Write-Blocker
  - What is a write-blocker
  - Different types of write-blockers
  - Hardware write-blocker
  - Software write-blocker
- Creating a Disk Image
  - Creation of Disk Image using a hardware write-blocker
  - Creation of Disk Image using a software write-blocker
  - Forensic Disk Image types
    - RAW/ DD
    - E01
    - AFF
  - Verifying Disk Image creation logs along with Cryptographic Hash values.

Module 3: Analysing Disk Image

- Manual analysis of evidence
  - Mounting the Disk Image
  - Launching a Virtual Machine using the Disk Image
- Application based analysis of evidence

Module 4: Live Computer Analysis

- What is Live Computer Analysis
- When is Live Computer Analysis required
- Live Computer Analysis procedure
- RAM Dump Analysis
  - What is RAM Dump
  - How is RAM Dump useful in Forensic Investigation
  - Conditions in which RAM Dump is necessary
  - How to collect RAM Dump
  - Analysing RAM Dump