Certified Forensic Investigation Specialist (CFIS)

<u>Course Outline</u>

1. Digital Forensic Investigations

- A review of the investigation process, best practice and equipment

2. Data Theft

- How can data be stolen, investigated and possibly mitigated?

3. Data Acquisition

- Images and Clones; Static, Booted and Live; Physical and selective
- Solid State devices
- Considerations and associated problems

4. Windows Domains

- Gathering information from Domain Controllers
- Capturing File Shares and inaccessible systems

5. RAID’s and Virtualisation

- Identifying and rebuilding RAID’s
- Capturing and examining virtualised systems

6. Volatile Data

- Memory capture and volatile data collection from ‘live’ systems
- Investigating memory using volatility

7. Data Collection – Other Sources

- Exchange servers and web-mail
- Facebook, Websites, Linux and Macs

8. File Systems Revisited

- Understanding FAT32, NTFS and ExFAT data structures from a forensic perspective

9. Data Deletion and Wiping

- Windows Recycle Bins
- Testing wiping software

10. Tracing System Activity

- Investigating the Windows Registry, User Accounts, Event Logs and USB connected devices

11. Tracing User Activity

- Identifying Program execution, Files opened and Folder navigation
- Windows Object ID’s and file tracking

12. Log File Analysis

- Web and FTP logs
- Examination using Cygwin

13. Databases

- SQLite and Chrome browser artefacts

14. Volume Shadow Copies and File History

- Approaches to extracting data from VSC’s
- Windows File History

15. NTFS Journals

- Understand the value of the NTFS journal in investigations