

Internet - Forensic investigation

Aim

The aim of this module is to enable delegates develop the necessary skills and knowledge to investigate and recover admissible evidence from computers which have been used to exchange information across the Internet.

Audience

This course is suitable for the first responder, Fraud investigator, Paralegal, Barrister, Solicitor and constitutes a good foundation for the computer Forensic investigator advanced course.



Syllabus

Introduction

- History of the internet
- Architecture and topology of the internet
- The role of the ISP
- Benefits of the internet
- Current developments – from Web1 to Web2

How information is transferred on the internet

- Basic introduction to computer networking
- The OSI networking model with emphasis on
- The Network layer
- The transport layer
- The session layer
- The application layer

The problem with the internet

- Legal issues
- Hackers
- Viruses, Malware, Trojans, backdoors

Hacking methodology

- The hacking community
- Why hack
- How hacking is effected
- Some control measures

Internet platforms

- Domain structures
- Web sites – Purpose, scope and types
- Services provided on the internet
- Online Commerce
- Collaboration Portals – share point

- Emails, FTP sites
- Research - Google
- Blogging
- Forums

Common Applications used on the internet

- Internet explorer, Google
- Web sites
- Emails
- FTP
- Peer- to-Peer
- wiki's

Where is internet evidence located?

- Web cache
- Temporary files
- Internet history file
- Cookies
- Windows Registry
- Firewalls
- Routers
- IDS

Investigating internet use and abuse (Part 1)

- The legal frame work
- Do's and Don'ts
- Automated vs. Manual
- Tools for automated investigation
- Practical class – examining internet history file (index. dat)

Investigating internet use and abuse (Part 2)

- Hacking tools
- Spoofing
- Phishing
- Trojan
- Malware
- Cookies
- Rootkit

Practical

- examination of internet history files
- examination of email header
- interpreting a who is trace
- Using Dig from the command line

Preparing the investigative report

- Documentation
- Reporting requirements
- Essentials of the report
- Testifying in court

Intended Learning Outcomes

On successful completion of this module the student will be able to:

Knowledge

- Demonstrate an understanding of the law as it affects internet transactions
- Demonstrate an understanding of internet technologies and the associated cast of characters.
- Demonstrate an understanding of the scope of activities that take place on the internet – Social, Business, public and private
- Identify the core areas containing evidence or information about Internet transactions on a Computer Hard disk and apply this knowledge to recovery of relevant data.
- Interpret and decode relevant system files connected with the use of the internet
- Demonstrate an understanding of the file download process
- Demonstrate knowledge and understanding of the procedures which have taken place electronically in the transmission and reception of E-mail and attachments
- Demonstrate knowledge and understanding of the procedures which have taken place electronically in the posting, circulation and downloading of Usenet Newsgroup items.
- Demonstrate knowledge and understanding of the effects of Malware, viruses and backdoors.

Skills

- Identify and assess the data structures of a number of leading Internet related applications and consequently adopt the correct data recovery strategy.
- Quickly create a template for the examination of a computer that has been used to access the Internet by identifying relevant areas for examination.
- Preparing acceptable reports for use in trial or arbitration
- Participate as a technical witness in court.