



Elements for the testing of Internet Investigators

1. General considerations – preparing the scenario – results expected

There will be different tests necessary for different allegations, for example evidence that is relevant to an allegation of illegal content may be vastly different from that sought in a hacking allegation. It will be appropriate to test the knowledge of individuals by creating a scenario-based test. There are a number of different sources from which evidence may be available and these should be included in the testing process. Some of these are as follows:

Victims system – must be able to identify and understand:

System

Audit

Connection

In the Corporate/Network Environment there may be the following logs:

Firewall

Network Intrusion Detection

Sniffer

The tested person must also be able to demonstrate an ability to communicate with technical persons and to be able to interpret what they say to enhance their investigation.

ISP Systems – must be able to identify and understand:

(1) Network Access Systems (NAS)

- access logs specific to authentication and authorization servers such as TACACS+ or RADIUS (Remote Authentication Dial In User Service) used to control access to IP routers or network access servers

- date and time of connection of client to server
- userid
- assigned IP address
- NAS IP address
- number of bytes transmitted and received
- Caller Line Identification (CLI)

(2) Email servers

- SMTP (Simple Mail Transfer Protocol) log

- date and time of connection of client to server
- ip address of sending computer
- Message ID (msgid)
- sender (login@domain);
- receiver (login@domain)

- POP (Post Office Protocol) log or IMAP (Internet Message Access Protocol) log

- date and time of connection of client to server
- IP address of client connected to server
- userid
- in some cases identifying information of email retrieved

(3) File upload and download servers

- FTP (File Transfer Protocol) log

- date and time of connection of client to server

- IP source address
- userid
- path and filename of data object uploaded or downloaded

(4) Web servers

- HTTP (HyperText Transfer Protocol) log
 - date and time of connection of client to server
 - IP source address
 - operation (i.e., GET command)
 - path of the operation (to retrieve html page or image file)
 - "last visited page"

(5) Usenet

- NNTP (Network News Transfer Protocol) log
 - date and time of connection of client to server
 - protocol process ID (nnrpd[NNN...N])
 - hostname (DNS name of assigned dynamic IP address)
 - basic client activity (no content)
 - posted message ID

(6) Internet Relay Chat

- IRC log
 - date and time of connection of client to server
 - duration of session
 - nickname used during IRC connection
 - hostname and/or IP address

The ability of the individual to recognise that ISP data is volatile and may only be held for short periods of time is of paramount importance and should be tested. The difference in retention periods for different types of data should also be tested.

Suspects - must be able to identify and understand:

The following outline should be used to test an officers ability to identify the common findings of a forensic examination as they relate to specific crime categories. This outline will also help define the scope of the examination to be performed.

Auction Fraud (Online)

- Account data regarding online auction sites.
- Accounting/bookkeeping software and associated data files.
- Address books.
- Calendar.
- Chat logs.
- Customer information/credit card data.
- Databases.
- E-mail/notes/letters.
- Financial asset records.
- Images files.
- Internet activity logs.
- Internet browser history/cache files.
- Online financial institution access software.
- Personal financial records.
- Phone call records.
- Records/documents of "testimonials."

Child Exploitation/Abuse

- Chat room logs.
- Date and time stamps.
- Digital camera software.
- Games.
- Graphic editing and viewing software.
- Internet activity logs.
- Images.
- Letters/notes/e-mail.
- Movie files.
- User-created directory and file names that classify images.

Computer Intrusion

- Address books.
- Configuration files.
- E-mail.
- Executable programs.
- Internet activity logs.
- IP address and user name.
- IRC chat logs.
- Source code.
- Text files (user names and passwords).
- Existence of sniffer logs
- Existence of hacking tools
- History of hacking activity
- Log Analysis – different OS
- Collection of Network Logs – Firewall, Router, Network Intrusion Detection
- Recovering Deleted information
- Locating Hidden Directories
- Knowledge of Hash Functions
- Online pursuit and associated integrity and authentication of the product

Death Investigation

- Address book.
- Diaries.
- Images.
- Internet activity logs.
- Legal documents and wills.
- Letters/notes/e-mail.
- Medical records.
- Personal financial records.
- Phone call records.

Domestic Violence

- Address book.
- Diaries.
- Letters/notes/e-mail.
- Medical records.
- Personal financial records.
- Phone call records.

Economic Fraud (including Online Fraud, Counterfeiting)

- Address books.
- Calendar.
- Check, currency, and money order images.
- Customer information/credit card data.
- Databases.

- E-mail.
- False financial transaction forms.
- False identification.
- Financial/asset records.
- Images of signatures.
- Internet activity logs.
- Online financial institution access software.
- Credit card skimmers.

E-Mail Threats/Harassment/Stalking

- Address book.
- Diaries.
- Images.
- Internet activity logs.
- Legal documents.
- Letters/notes/e-mail.
- Personal financial records.
- Phone call records.
- Victim background research.

Extortion

- Date and time stamp.
- E-mail.
- History log.
- Internet activity logs.
- Temporary Internet files.
- User names.

Gambling

- Address books.
- Calendar.
- Customer database and player records.
- Customer information/credit card data.
- Electronic money.
- E-mail.
- Financial/asset records.
- Image players.
- Internet activity logs.
- Online financial institution access software.
- Sport betting statistics.

Identity Theft

- Hardware and software tools.
 - Backdrops.
 - Credit card generators.
 - Credit card reader/writer.
 - Digital cameras.
 - Scanners.
- Identification templates.
 - Birth certificates.
 - Check cashing cards.
 - Digital photo images for photo identification.
 - Driver's license.
 - Electronic signatures.
 - Fictitious vehicle registrations.

- Proof of auto insurance documents.
- Scanned signatures.
- Social security cards.

- Internet activity related to ID theft.
- E-mails and newsgroup postings.
- Erased documents.
- Online orders.
- Online trading information.
- System files and file slack.
- World Wide Web activity at forgery sites.

- Negotiable instruments.
- Business checks.
- Cashiers checks.
- Counterfeit money.
- Credit card numbers.
- Fictitious court documents.
- Fictitious gift certificates.
- Fictitious loan documents.
- Fictitious sales receipts.
- Money orders.
- Personal checks
- Stock transfer documents.
- Travelers checks.
- Vehicle transfer documentation.

Narcotics

- Address books.
- Calendar.
- Databases.
- Drug recipes.
- E-mail.
- False identification.
- Financial/asset records.
- Internet activity logs.
- Prescription form images.

Prostitution

- Address books.
- Biographies.
- Calendar.
- Customer records/databases.
- E-mail.
- False identification.
- Financial/asset records.
- Internet activity logs.
- Medical records.
- Online World Wide Web page advertising.

Software Piracy

- Chat logs.
- Image files of software certificates.
- Internet activity logs.
- Letters/notes/e-mail.
- Serial numbers.
- Software cracking information and utilities.

- User-created directory and file names that classify copyrighted software.

At a physical scene, look for duplication and packaging material.

Telecommunications Fraud

- Cloning software.
- Customer database.
- Electronic Serial Number (ESN)/Mobile Identification Number (MIN) pair records.
- Financial records.
- How to Phreak manuals.
- Internet activity.
- Letters/notes/e-mail.
- Phone numbers.

The following information, when available, should be documented to assist in the forensic examination:

- Case summary.
- Type of crime.
- Passwords.
- Keyword lists.
- Internet protocol address(es).
- Nicknames.
- Point of contact.
- Supporting documents.

2. General Items for inclusion in competence testing

Interview Skills

The tested person must be able to demonstrate an ability to both interview witnesses and suspects within the scenario.

Presentation Skills

The tested person must be able to present the findings of their investigation to both managers, prosecutors and the court in a manner in which they are understood.

Legal Issues

Legal requirements for accessing evidence vary from country to country and between sources of evidence. For example there may be different requirements for accessing communications data and content and even further requirements for accessing evidence held by a suspect. It is necessary to test the knowledge of individuals of the laws that are relevant in their countries as part of the testing process.