



IOCE 2000 Conference – 13-15 December 2000 – Rosny sous Bois, France

Internet Investigation Training.

Rosny sous Bois, France 13th –15th December 2000

1. Identification of core level skills.

Basic knowledge

Investigative techniques.

Computer/digital devices.

Equipment/systems/software\ infrastructure.

Universe of Available Data

Rules of Behaviour for 1st responders.

Don't touch

Call for help

Wait for or defer to Computer Forensic specialist.

Law: Know the specific legal system and relevant legislation – what is permissible and what is not.

Accumulated evidence to date on the particular case.

2. Training.

Appropriate and increasingly specialized courses in:

1. Recovery
2. Copying
3. Preservation
4. Chain of custody

Know and explain the limits of what is available on the computer and networks. (manage case team expectations)

Skills

Add as per workshop1

Abilities

Experience provides the ability:

To recognise what is relevant data

To Search for evidence.

To preserve evidence.

Notes/notes/notes

Documenting procedures

Testifying:

Mock Court/role playing experimental courses.

Rehearsals and preparation.

Presentation of credentials.

Description of evidential procedures for capture, preservation, processing and handling.

2. Collecting Evidence

Knowledge

Operating Systems ie Windows, Unix, Novell.

Computer hardware

Network infrastructure

Types of storage media

Packaging and transport evidence

Chain of custody (evidence)

Types of imaging enquiry software

File systems and logical/physical -slack space etc

System time and file time stamps

Hidden files/flags/rename/steganography

Encryption/compressed files

Packet switch networks

Internet services: web, www, chat, file transfer protocol (FTP),

Internet relay chat (irc), newsgroups

Internet Protocols (TCP, IP)

Dynamic /static ip –protocols

Limitations of location –offsite (offshore) data

**Time Critical /Perishable data i.e. log files, email on servers –
chains of traffic data**

E-commerce, digital signatures,

File sharing concepts i.e. napster, Freenet, data havens.

Skills

To use recovery software

How to handle computer hardware

To use backup software

Logical copies

Abilities

Obtain information from other sources of information

Interviewing violators or system administrators

Negotiation skills

Relate what you did on scene

Accurate inventory

3. Analysis and Results

Knowledge

All of previous (in depth)

Tools

Limitations

Capabilities

Origin

Skills

Experience: Applying knowledge

Organisational skills

Specialization: research, Unix, Macs

Abilities

Present findings in proper format

Know when do I stop? Determine the limits of examination

Know your limitations, and when to transfer to subject matter expert

4. Court/ Prosecutors

Knowledge

Basic computer knowledge

training together with the police (working along side investigators

Prosecutors should communicate (feedback- discuss) with analyst/investigator

Understanding of laws relating to computer crime

Laws may be absent or cannot keep up with technology

Know that examination may be time consuming

Chain of information

Tell police what he wants to know

5. Managers.

1. Recognition of time / effort taken to do case or cases.
 - a. Cases which are voluminous or large in scope require considerable resources
2. Domestic share of trans-national cases dependent upon recovery of domestic share of available evidence.
 - a. Evidence may reside in a domestic market and countries which fail to capture evidence will not pursue the case or the criminals\ fines\ jail terms
3. Continuous investment in equipment, training and resources.
 - a. Technical proficiency and equipment have an 18 month life cycle and require updating—failing to do so will render resources ineffective and forensic expert will fall behind in investigations of criminal activity.

Closing Remarks

The participants believed that industry-provided training for emerging technologies and new software products prior to their release, would enhance their ability to do their jobs.