



International Organization of Computer Evidence

IOCE Training Workshop

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

1. Identification and Preservation of Digital Evidence at the Scene

Knowledge

Investigative techniques

Computer/digital devices

Equipment/systems/software/infrastructure

Universe of Available Data

Rules of Behaviour for first Responders

Don't touch

Call for help

Wait for or defer to computer forensic specialist

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

Accumulated evidence to date on the particular case

Training

Recovery

Copying

Preservation

Chain of custody

Limits of what is available on the computer



Skills

Be able to recognise electronic equipment; Computers, Laptops, Cell Phones, PDA's (Electronic Organisers), Fax machines & Digital Storage devices

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 evidentiary procedures for digital capture
preservation, processing and handling**



2. Collecting Digital Evidence

Knowledge

Operating Systems

Computer hardware

Network infrastructure

Types of storage media

Packaging and transport evidence

Chain of custody (evidence)

Types of imaging software

Skills

To use imaging 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

Operating systems (i.e. windows,NT, Novell, Unix)

File systems and logical/physical -slack space etc

System time and file time stamps

Hidden files/flags/rename/steganography

Encryption/compressed files, packet switched networks

**Internet services: web, www, chat, file transfer protocol (FTP),
Internet relay chat (irc), newsgroups**

Internet Protocols (TCP, IP)

Dynamic /static ip – addressing

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. napstar

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



Closing Remarks

The workshop participants enumerated the following concerns:

The availability of relevant training is curbed by budgetary constraints and a lack of knowledge by upper management. Training for managers is essential for the successful outcome for developing training skill sets as outlined above.

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.

Moderators

Carrie Whitcomb whitcomb@mail.ucf.edu

Laurie Norton laurie.norton@nhtcu.org