Principles of Digital Evidence Collection

Objectives:

At the end of this episode, I will be able to:

Understand what digital evidence is, as well as the types and characteristics of digital evidence that an IH&R team member may need to work with.

Explain what the ACPO Principles of Digital Evidence, and the Scientific Working Group on Digital Evidence (SWGDE) Principles, Standards & Criteria are.

Identify what Incident Responders have to know about collecting physical evidence.

Define what the evidence Chain of Custody is, as well as what steps IH&R team members need to take to successfully package, transport, and store electronic evidence.

External Resources:

Principles of Digital Evidence Collection

What is Digital Evidence? -

Digital evidence is defined as “any information of probative value that is either stored or transmitted in a digital form”

Digital evidence may be present across computing devices, servers, routers, and so on. It is revealed during the forensics investigation while examining storage media, monitoring network traffic, or making duplicate copies of digital data.

What are the types of Digital Evidence? -

- Volatile - refers to the temporary information on a device that requires a constant power supply and is deleted if the power supply is interrupted.

- Non-Volatile - refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Nonvolatile data does not depend on power supply and remains intact even when the device is switched off.

What are the characteristics of Digital Evidence? -

The main characteristic of digital evidence is its relevance and weight (influence).

The term “relevance” refers to the connection between digital evidence and the fact(s) that is/are to be proved.

The term “weight" refers to how much the digital evidence changes the probability of the fact.

ALL EVIDENCE MUST BE:

- Admissible - related to the fact being proved
- Authentic - real and related to the incident in a proper way
- Complete - prove guilt or innocence
- Reliable - no doubt about the authenticity or veracity of the evidence
- Believable - clear and understandable

What are the different types of evidence that incident responders may have to deal with?

- Host based
- Network based
- Other

What are the ACPO Principles of Digital Evidence? -

▪ Principle 1 - No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

▪ Principle 2 - In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

▪ Principle 3 - An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

▪ Principle 4 - The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

What are the Scientific Working Group on Digital Evidence (SWGDE) Principles, Standards & Criteria? -

Principle 1: In order to ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system

Standards and Criteria 1.1: All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority

Standards and Criteria 1.2: Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness

Standards and Criteria 1.3: Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner

Standards and Criteria 1.4: The agency must maintain written copies of appropriate technical procedures

Standards and Criteria 1.5:The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure

Standards and Criteria 1.6: All activities relating to the seizure, storage, examination, or transfer of the digital evidence must be recorded in writing and be available for review and testimony

Standards and Criteria 1.7: Any action that has the potential to alter, damage, or destroy any aspect of the original evidence must be performed by qualified persons in a forensically sound manner

What does the Incident Responder have to know about collecting Physical Evidence? -

Physical evidence includes:

```
▪ Removable media
▪ Cables
▪ Publications
▪ All computer equipment, including peripherals
▪ Items taken from the trash
▪ Miscellaneous items
```

Tag all the objects identified as evidence, and mention all the required details on the tag, such as the time, date, incident responder’s name, and control number.

First responders must perform the following steps while collecting evidence from Powered On computers:

```
▪ If a computer is switched ON and the screen is viewable, photograph the
screen and document the running programs

▪ If a portable computer wakes up, record the time and date at which this
occurs, take a photograph of the screen, and provide a brief explanation of
all the programs running

▪ If a computer is ON and the monitor shows a screensaver, move the mouse
slowly without pressing any mouse buttons and then photograph and document
the programs

▪ After collection of all the volatile data, turn off the devices

▪ For portable computers, press down the power switch for 30 seconds to force
the power off, then remove the battery and unplug the power cord from the
power outlet

▪ If the computer is switched OFF, leave it in that state
```

First responders must perform the following steps while collecting evidence from Powered Off computers:

▪ If it is switched OFF, leave it OFF

If a monitor is switched OFF and the display is blank:

▪ Turn the monitor ON, move the mouse slightly, observe the changes from a blank screen to another screen, and note the changes

▪ Photograph the screen

If a monitor is switched ON and the display is blank:

▪ Move the mouse slightly

▪ If the screen does not change on moving the mouse slightly, do not press any keys

▪ Photograph the screen

First responders must perform the following steps while collecting evidence from network connected computers:

▪ Unplug the network cable(s) from the router and/or modem in order to prevent further attacks

▪ Photograph ALL devices connected to the victim's computer from several angles

▪ If any devices, such as a printer or scanner, are present near the computer, take photographs of those devices as well

▪ If the computer is turned OFF, leave it in that state, and if it is ON, photograph the screen and follow the steps for powered on computers

▪ Unplug all cords and devices connected to the computer and label them for identification

First responders must perform the following steps while collecting evidence about open files and startup files:

▪ Open any recently created documents from the startup or system32 folder in Windows and the rc.local file in Linux

▪ Document the date and time of the files

▪ Examine the open files for sensitive data such as passwords or images

▪ Search for unusual modified, accessed, or changed times on vital folders, and startup files

▪ Use the dir command for Windows or the ls command for Linux to locate the actual access times on those files and folders

What is Chain of Custody? -

The Chain of custody demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory.

The chain of custody covers the collection, handling, storage, testing, and disposition of evidence.

Chain of custody documentation should list all the people involved in the collection and preservation of evidence and their actions.

The Chain of custody document should contain complete information about the obtained evidence, such as:

```
▪ Case number
▪ Information about the individual releasing or forwarding the evidence item
to inquiry personnel
▪ Complete address and telephone number of the individuals who handled the
electronic evidence
▪ Location from where the evidence was obtained
▪ Date/time of evidence acquisition
▪ Item number/quantity/ description of items
```

What about the Evidence Bag Contents List? -

The panel on the front of evidence bags must, at the very least, contain the following details:

```
▪ Date and time of seizure
▪ Incident responder who seized the evidence
▪ Exhibit number
▪ Where the evidence was seized from
▪ Details of the contents of the evidence bag
▪ Submitting agency and its address
```

NOTE: Additional details required on the panel of the evidence bags include name of the officers who took photographs or prepared a scene sketch, sites where individual items were found, and names of the suspects, if any.

What about Packaging, Transporting, and Storing Electronic Evidence? -

First responders must package, store, and transport all the physical evidence for further analysis after collecting all the volatile information. They must perform the following:

- Label all the devices and their components and create a list
- Avoid turning computers upside down or putting them on their side during transport
- Keep the electronic evidence away from magnetic sources such as radio transmitters, speaker magnets, and heated seats
- Store the evidence away from extreme heat, cold, or moisture
- Avoid storing electronic evidence in vehicles for a long period of time
- Maintain proper chain of custody of the transported evidence
- Ensure that wireless devices do not connect to any networks by storing them in signal blocking containers