Data Acquisition

Objectives:

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

Understand what the process of forensic data acquisition is that an IH&R team member may need to work with.

Explain what the two categories of data acquisition are.

Identify what Incident Responders have to know about Duplicating the Data (Imaging).

Define what IH&R team members need to know about Verifying Image Integrity.

External Resources:

Data Acquisition

What is Data Acquisition? -

Forensic data acquisition is a process of imaging or collecting information from various media in accordance with certain standards for analyzing its forensic value.

It is one of the most critical steps of digital forensics as improper acquisition may alter data in evidence media, and render it inadmissible in a court of law.

Incident responders should be able to verify the accuracy of acquired data, and the complete process should be auditable and acceptable to the court.

The two categories of data acquisition are:

```
▪ Live/Volatile Data Acquisition - Volatile data is fragile and lost when the
```

system loses power or the user switches it off. Such data reside in registries, cache, and RAM. Since RAM and other volatile data are dynamic, a collection of this information should occur in real time.

```
▪ Static Data Acquisition - Incident responders can recover data from hard
```

drives as well as from slack space, swap files, and unallocated drive space. Other sources of nonvolatile data include DVD-ROMs, USB thumb drives, and smartphones.

What about Duplicating the Data (Imaging)? -

Data duplication is an important step in securing the original evidence.

Investigating the original evidence can cause damage to the identity of the evidence that would make it no longer useful to the case.

Data duplication includes bit-by-bit copying of the original data using a software or hardware tool.

The points to remember while duplicating the data:

```
▪ Make a duplicate of the collected data so as to preserve the original
▪ The data should be duplicated bit by bit to represent the same original data
▪ Use industry standard or licensed hardware or software tools to duplicate
```

the data
▪ Once a copy of the original data is made and verified, you can use the copy for further processing

What about Verifying Image Integrity? -

Hash values are equivalent to data fingerprints, as a result, two files should not contain the same hash values.

The hash algorithms used in forensics are MD5 and SHA.

Perform the following steps to verify image integrity:

```
▪ Calculate the hash value of the original data and the forensic image
```

generated
▪ If there is a match it means that the forensic image is an exact replica of the original data