Chapter 15 - Lab Activity 1 - Expert Testimony in Digital Investigations

Alex Arnold

Identify five (5) digital forensic procedures, techniques, technical definitions, or tools discussed by the witness, that have been covered in this class.

1) Data / device imaging

**What is it?**

the process of bit-by-bit copying of the contents of any media such as Hard Disk, USB drive or a partition of the OS which does not leave any areas of the disk untouched.

**How is it used?**

It is used to copy the information stored on a device to create a duplicate of the data that is then used by the examiner to analyze it for information related to a crime or investigation.

**Why is it important?**

This is important as creating a duplicate of the information on a device allows the investigator to search the device and do an investigation without the risk of damaging or altering the information on a suspect device.

2) Allocated and unallocated Space

**What is it?**

This is space on a drive that is either in use by the system and currently tracked as containing information or space that my contain data but has been marked as free space but the system that can be overwritten as needed.

**How is it used?**

As the investigator in the video said in his analogy it is like a box of paper with a table of contents. The enable tells the system where files are stored and as information is “deleted ” by the user is removed from the table but those locations may still contain data.

**Why is it important?**

Allocated space is important as this is where files are stored in the system. The unallocated space can potentially be more important to a forensic investigator as a suspect may try to delete files to hide evidence. That hidden evidence may still exist within the unallocated space and be able to be recovered by a forensic investigator.

3) File headers

**What is it?**

This is information that is stored at the start of a file that contains information about the type of file so that an OS or software know what to do with the file.

**How is it used?**

This data is used by the system and software to know what to do with the file / how the file needs to be handled to be read correctly.

**Why is it important?**

**This is important because these headers can be used to identify files that have been deleted, modified with false file types, or the software needed is not readily available. This would then allow investigators to discover what kind of file they are looking at and what kind of software is needed to view the file. As for deleted files It can allow investigators to search for particular file types and extract the files without being able to access the drive in other ways or find similar files of interest.**

4) Key Word Search

**What is it?**

Key Word Search is using a string to search files / data for information that matches that string of information.

**How is it used?**

This is used to search suspect data for information that the investigator needs to find in the suspect data. Examples of this can be addresses, names, emails, simple words and so on.

**Why is it important?**

This is important as this can save a great deal of time and effort over having to manually comb data by hand for this information. If this was not used it could hamper or the search or information in a timely fashion or have information that could be important be entirely missed by the investigation.

5) Encase

**What is it?**

EnCase is the shared technology within a suite of digital investigations products by Guidance Software (acquired by OpenText in 2017[2]). The software comes in several products designed for forensic, cyber security, security analytics, and e-discovery use. EnCase is traditionally used in forensics to recover evidence from seized hard drives. It allows the investigator to conduct in-depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

**How is it used?**

This software is used by digital forensic specialists to review and analyze data related to criminal investigations and digital crimes.

**Why is it important?**

This is important as it allows Forensic investigators to analyze data recovered from suspect devices in a timely and efficient manner. This also has the ability to do things like keyword searches, analysis of deleted / unallocated files, report generation and other such practices that are used to collect information relevant to an investigation. Without this software and others like it investigators would be hard pressed to do a thorough and timely search of suspect information for evidence.