**LEMUEL OKECHUKWU**

**VEPH/20B/CY082**

**TASK 36B**

**THE FORENSIC INVESTIGATION PROCESS**

**TASK 36B :**

* Discuss the processes of evidence collection and preservation in digital forensics, highlighting best practices to maintain forensic integrity, and enumerate commonly used digital forensic tools and software.

[](https://recfaces.com/articles/digital-forensics)

As the internet, technology, and [digital forensics](https://eclipseforensics.com/digital-forensics/) expand, it is more important than ever for the concerned professionals to deploy the best practices to preserve digital evidence. Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to [cybercrime](https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/cybercrime-types-prevention-digital-forensics/). The term digital forensics was first used as a synonym for computer forensics. Since then, it has expanded to cover the investigation of any devices that can store digital data. Although the first computer crime was reported in 1978, followed by the Florida computers act, it wasn’t until the 1990s that it became a recognized term. It was only in the early 21st century that national policies on digital forensics emerged.

How Well Do You Know Digital Forensics?

**Steps of Digital Forensics**

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

**1. Identification:** First, find the evidence, noting where it is stored.

**2. Preservation:** Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.

**3. Analysis:** Next, reconstruct fragments of data and draw conclusions based on the evidence found.

**4. Documentation:** Following that, create a record of all the data to recreate the crime scene.

**5. Presentation:** summarize and draw a conclusion.

Looking back at the history of digital forensics, law enforcement during that age had a minimal understanding of the application of digital forensic techniques. However, during the 1970s and 1980s, the forensics team were mostly representatives of federal law enforcement agencies with a computer background. The first area of concern for law enforcement was data storage, as most documentation happened digitally. Undeniably, seizing, retaining, and analyzing the documentation was a long task for the authorities. In this situation, the FBI launched the Magnet Media program in 1984, which was the first official digital forensics program.



In the 1990s, digital investigations were carried out via live analysis and using the device in question to examine digital media was commonplace. In time, the increasing use of devices packed with huge amounts of information made live analysis inefficient. Eventually, digital forensic tools were created to observe data on a device without damaging it. Presently, digital forensic tools can be classified as digital forensic open source tools, digital forensics hardware tools, and many others.

**What Are Digital Forensics Tools?**

**The Sleuth Kit**: (earlier known as TSK) is a collection of Unix- and Windows-based utilities that extract data from computer systems. It is an open-source software that analyzes disk images created by “dd” and recovers data from them. With this software, professionals can gather data during incident response or from live systems. Professionals can integrate TSK with more extensive forensics tools.

**FTK Imager**: is an acquisition and imaging tool responsible for data preview that allows the user to assess the device in question quickly. The tool can also create forensic images (copies) of the device without damaging the original evidence.

**Xplico**: is a network forensic analysis tool (NFAT) that helps reconstruct the data acquired using other packet sniffing tools like Wireshark. It is free and open-source software that uses Port Independent Protocol Identification (PIPI) to recognize network protocols. The tool is built on four key components: Decoder Manager, IP Decoder, Data Manipulators, and Visualization System.

In digital evidence collection today, live forensics has become a necessity. Among many forensic professionals both in law enforcement and private practice it has long been recognized that the tradition of first pulling the plug on a PC under examination is an outdated and overly conservative approach that can destroy valuable evidence