VAStar Cyber Security

Digital Forensics

Goals

- Learn what digital forensics is
- Learn about different types of cyber crime
- Learn how digital evidence is gathered & analyzed
- Learn about disk imaging

What is Digital Forensics?

Digital forensics is the identification, recovery, and analysis of digital materials, usually related to computer crime. Digital forensics is helps prove innocence or guilt in criminal court cases by proving how digital files were created, when they were transferred or modified, and recovering them if they were deleted.

Digital forensics can also be used by private companies for internal investigations or to trace hackers who have broken into a system.

Cyber Crime

Digital forensics is most commonly used to help fight cyber crime. Cyber crime is any crime that takes place via a computer or network. This includes crimes like fraud, identity theft, extortion, cyber terrorism, and piracy.

Sovereign nations also engage in large-scale cyber crime, known as cyber warfare. Using computer systems as vectors of attack, these nations target mechanical control systems, power grids, financial institutions, telecommunication hubs, transportation facilities, and water infrastructure.

Digital Evidence

Digital evidence is any evidence to a crime stored or transmitted in digital form that may be used at trial. Digital evidence in the US is bound by the Federal Rules of Evidence and needs to be found 'admissible'. Additionally, the Federal Rules of Civil Procedure enacted strict rules for digital evidence to ensure that it is preserved and disclosed properly.

Due to this, digital evidence is strictly captured in 3 stages: Evidence Acquisition, Evidence Extraction, & Evidence Analysis.

Phase 1: Evidence Acquisition

The evidence acquisition phase ensures the data integrity of the digital evidence. The basic steps for evidence acquisition are:

- Document the hardware and software configuration
- Verify the working operation of the device
- Disassemble the device to gain physical access to digital storage devices
- Document the storage devices (condition, make, model, jumper settings)
- Disconnect storage devices
- Power system down
- Enable write protection on storage devices, if possible.

Disk Images & File Backups

Evidence acquisition usually includes turning off the device and creating a full backup of the data in the form of a 'disk image'. A disk image is a digital file that contains the entire contents of a digital storage medium such as a hard drive, solid state disk, usb drive, or optical disc.

Saving disk images preserves all of the data from being deleted or altered, and protects against any countermeasures on the device.

System preservation continues through the entire forensic process. Even after individual files have been recovered or recreated from the disk, backups are made of each of the files as well.

Phase 2: Evidence Extraction

Evidence is extracted from storage media in two possible ways, physical or logical.

Physical extraction physically recovers data from the storage media with no regard to it's file system. This method pulls all of the zeros and ones from the device and will recover the most information. This allows you to recover files that may not be visible to the operating system or file system. It also allows you to determine if all of the storage space is accounted for, and that there are no hidden partitions. This is the most time consuming method.

Logical extraction recovers data from storage media based on the file system through the operating system. This method recovers files and file metadata (name, type, timestamps, size, location). This also includes deleted, password-protected, encrypted, and compressed files. Unfortunately, however, this method misses files that are not seen by the operating system itself.

Phase 3: Evidence Analysis

Evidence analysis creates a story using the extracted evidence. The analysis is typically used to back up or refute the criminal events depicted at trial. Different types of analysis will yield different information.

Timeframe analysis: determines when events on a computer occurred, such as when a file was last modified or when a specific website was visited

Data hiding analysis: determines the contents of hidden or deleted files that may indicate knowledge or intent of a crime

Application and file analysis: determines file content, configuration settings, emails, internet history, and other application or file-specific data

Ownership analysis: determines who created, modified, or accessed a file. This is used heavily in conjunction with the other types of analysis to create a cohesive story.

The Future of Digital Forensics

Computers were largely ignored by law enforcement in the US until 2007, when a gunman killed and wounded multiple people at the Virginia Tech campus. Once law enforcement investigated his computer, they were able to create an entire psychological profile and understand the gunman's motive behind the tragic event.

Since then, digital forensics is becoming increasingly prevalent in criminal cases. The US digital forensics industry is expected to grow to $1.7 Billion by 2019, indicating a large public and private sector interest in the field.