Week1.

# Concepts:

## Data hiding

Data hiding is the process of making data difficult to find while also keeping it accessible for future use. "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."

Some of the more common forms of data hiding include encryption, steganography and other various forms of hardware/software based data concealment. Each of the different data hiding methods makes digital forensic examinations difficult. When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.

**Types of data hiding.**

Encryption, Stegangraphy, Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system.

## Artifact wiping

The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques.

**Types of artifact wiping**

Disk cleaning utilities, File wiping utilities, Disk degaussing / destruction techniques.

## Trail obfuscation

The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process. Trail obfuscation covers a variety of techniques and tools that include "log cleaners, [spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing" \o "IP address spoofing), [misinformation](https://en.wikipedia.org/wiki/Misinformation" \o "Misinformation), backbone hopping, zombied accounts, trojan commands."

One of the more widely known trail obfuscation tools is Timestomp (part of the [Metasploit Framework](https://en.wikipedia.org/wiki/Metasploit_Framework" \o "Metasploit Framework)). Timestomp gives the user the ability to modify file [metadata](https://en.wikipedia.org/wiki/Metadata" \o "Metadata) pertaining to access, creation and modification times/dates. By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.[[citation needed](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed" \o "Wikipedia:Citation needed)]

Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework). In most file types the header of the file contains identifying information. A (.jpg) would have header information that identifies it as a ([.jpg](https://en.wikipedia.org/wiki/.jpg" \o ".jpg)), a ([.doc](https://en.wikipedia.org/wiki/.doc" \o ".doc)) would have information that identifies it as (.doc) and so on. Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header. If a forensic examination program or [operating system](https://en.wikipedia.org/wiki/Operating_system" \o "Operating system) were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it.

## Attacks against computer forensics (Attacks against digital forensic tools and processes).

In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information. Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations. These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.

During a typical forensic examination, the examiner would create an image of the computer's disks. This keeps the original computer (evidence) from being tainted by forensic tools. [Hashes](https://en.wikipedia.org/wiki/Cryptographic_hash_function" \o "Cryptographic hash function) are created by the forensic examination software to verify the [integrity](https://en.wikipedia.org/wiki/Data_integrity" \o "Data integrity) of the image. One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image. By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged.

# References:

<https://www.researchgate.net/publication/349312895> DOI: 10.5281/zenodo.4425257