Introduction to Digital Forensics

Content of workshop

- Digital forensics?
- File?
- Memory forensics?
- Network analysis?
- Mindset & tricks

Digital forensics

Digital forensics can be summarized as the investigations to a virtual crime.

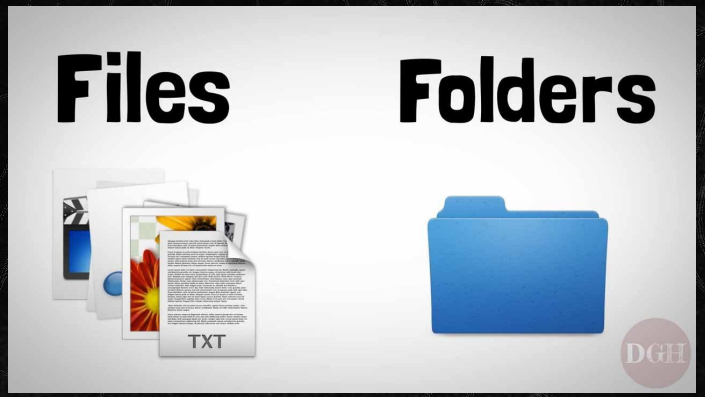
In simpler words it is the art of gathering computer related evidence of a hack.

Digital forensics & Incident response

- Origin of the hack
- Lost/Stolen data
- Hacker identity
- Fixes

Back to basics, what is a file ? really ?

Files



Files are just a bunch of bytes!

File	determine file type
xxd	make a hexdump or do the reverse.
hexedit / https://hexed.it	view and edit files in hexadecimal or in ASCII
binwalk	searching binary images for embedded files and executable code

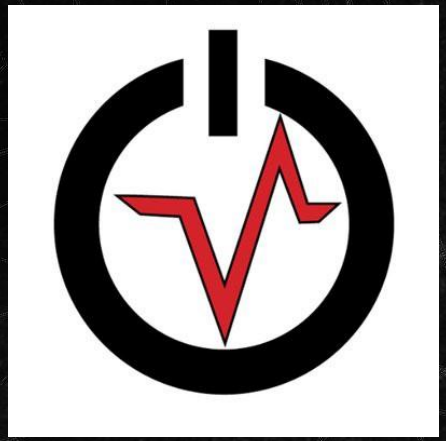
Memory forensics

Persistent Memory

Sleuth kit

mmls	Display the partition layout of a volume system (partition tables)
fls	fls - List file and directory names in a disk image.
icat	Output the contents of a file based on its inode number.
mount	mount a filesystem

Volatile Memory



Volatility framework

installation

Mindset & tricks in DFIR

- Be curious
- Google around
- Don’t be afraid of tools
- Don’t neglect any piece of data

Time for questions!