



# Forensic Software

CYBER INCIDENT RESPONSE

# Forensic Software

- Commercial and Open-Source for:
  - Imaging
  - Analysis
  - Hashing and validation
  - Process and memory dumps
  - Password cracking
  - Log viewer

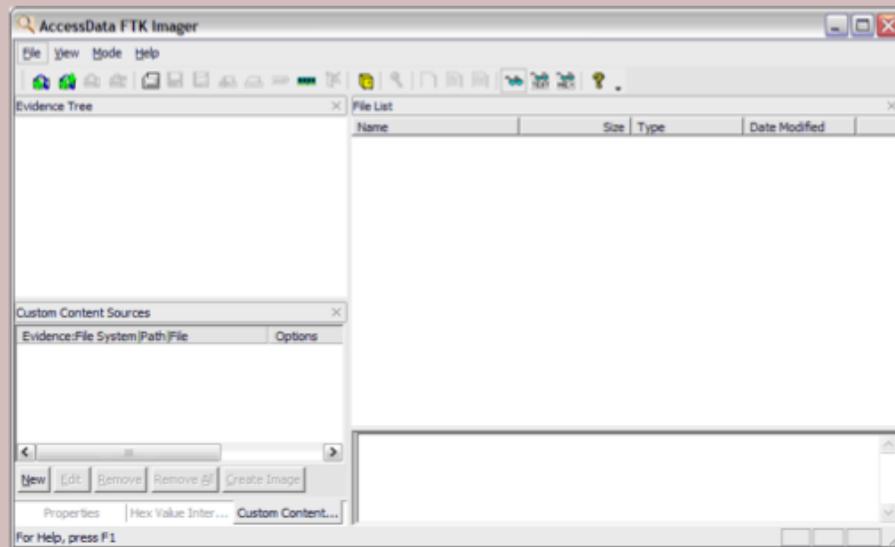
```
Terminal - wikipedia@linux: -
File Edit View Terminal Go Help
wikipedia@linux:~$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w|-d] [-t <type>] [-s <blocks>] [-k <size>]
  [-b <size>] [-c <file>] [-o <dir>] [-i <file>]

-V - display copyright information and exit
-t - specify file type. (-t jpeg.pdf ...)
-d - turn on indirect block detection (for UNIX file-systems)
-i - specify input file (default is stdin)
-a - Write all headers, perform no error detection (corrupted files)
-w - Only write the audit file, do not write any detected files to the disk
-o - set output directory (defaults to output)
-c - set configuration file to use (defaults to foremost.conf)
-q - enables quick mode. Search are performed on 512 byte boundaries.
-Q - enables quiet mode. Suppress output messages.
-v - verbose mode. Logs all messages to screen
wikipedia@linux:~$
```



# Imaging Media and Drives

- Bit by bit copy of a drive, including the slack space and unallocated space
- FTK Imager
- EnCase Imager
- dd



# Analysis Software

- Creates timeline of system changes
- Validates file against known good copy
- File system analysis for hidden files, changes, access, and metadata
- Windows Registry analysis
- Log file parsing and analysis
  
- Examples:
  - Commercial:  
FTK and EnCase
  - Open-source:  
SIFT, CAINE, and Autopsy



## Hashing and Validation

- Creates a unique file integrity check of a disk image after creation
- Used as part of chain of custody
- EnCase uses built-in hashing with its .EO1 format
- Should use both MD5 & SHA1/SHA256



## Process and Memory Dumps

- State of the Operating System and data in-resident memory at time of collection
- Difficult to collect without changing the contents contained
- Useful to capture decryption keys for full disk encryption
- Hibernation files and crash dumps can also contain some of this data



# Process and Memory Dumps

- Tools

- fmem and LiME (Linux)
- DumpIt (Windows)
- Volatility Framework (Windows, Linux, OS X)
- EnCase
- FTK

- Memory dumps on system can be found at  
`%SystemRoot%\MEMORY.DMP`

- Dumps analyzed with Microsoft's WinDbg



## Password Cracking/Recovery

- Encrypted and password protected files required cracking or guessing password
- Hacking tools like John The Ripper and Cain and Able can be used
- DOC, XLS, PPT, and ZIP files have other specialized password cracking tools:
  - Advanced Office Password Breaker
  - ElcomSoft's Distributed Password Recovery
  - Zip2John
  - ...numerous others...



# Log Viewers

- Used to analyze log files from collected system images
- Can create timelines and visualize the data

