Amir Alsbih and Christian Schindelhauer

Distributed Storage and Computer Forensic

Distributed Storage Networks and Computer Forensics Winter 2011/12
Recap
A set of tools

- Volatility Framework
- Win32dd
- memdump
- pd: Process Dumper is able to make a dump of a running process
- pdgmail: gather gmail artifacts
- pdfbook: gather facebook artifacts
- Skypeex: gather skype chat artifacts
Network connections

```
# netstat -anp
- a: all sockets
- n: do not resolve host names
- p display PID/Programm name for sockets
```
List processes

- `# ps -aux`
- `-a`: all
- `-u`: use effective user ID
- `-x`: processes without tty
List open files

- `# lsof -n`
- `-n: no host names`
Other things

- Current date/time:
  # date

- Partition map
  # fdisk -l

- Mount points
  # mount

- System uptime
  # uptime

- OS type
  # uname -a

Sample output of mount
On Windows WFT

- WINDOWS FORENSIC TOOLCHEST (WFT):
  - Memory Image
  - Network Information
  - Process Information
  - Filesystem and Registry
  - Files with hashes
  - System Information
  - ...

Source: foolmoon.net
DD

# dd if=INPUT of=OUTPUT [options]
- bs=value: set block size to value
- count=value: copy only value blocks
- skip=value: skip value blocks in input
- conv=noerror,sync: skip unreadable sections

On Windows also:
- --cryptsum HASHTYPE [md5,sha, sha1, sha256]
- --log file
- --cryptout file
- --verify
# dc3dd if=INPUT of=OUTPUT [options]

- bs=value: set block size to value
- count=value: copy only value sectors
- skip=value: skip value blocks in input
- seek=value: skip value blocks in output
- conv=noerror,sync: skip unreadable sections
- progress=on: Display a progress meter
- Hash=ALG: computes hash of the input [md5,sha1,sha256,sha512]
- hashlog=FILE
- log=file
Host Protected Area (HPA)

- Discs can have an HPA.
- A user cannot read or write to this area.
- Typically used for a preloaded OS for install and recovery purposes.
HPA detection/removal

- **The Sleuth Kit:**
  - Detection:
    
    ```
    # disk_stat DEVICE
    ```
  - Removal:
    
    ```
    # disk_sreset DEVICE
    ```

- **Windows DD:**

  ```
  Dd if=INPUT of=OUTPUT --ata_hpa
  ```

Distributed Storage Networks and Computer Forensics Winter 2011/12  Amir Alsbih
It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts. —Sherlock Holmes
Timelines

- Timelines shows file accesses and modifications around an interesting time.
  - Files that were accessed, deleted, and modified
  - Tools that were executed
- Rootkits will have limited benefit, since the file system will log the activities.
- Works on all file systems.
- The timeline only shows the last access time.

Distributed Storage Networks and Computer Forensics Winter 2011/12  Amir Alsbih
Timeline MAC

- Ext2/3 and NTFS uses C for the change of metadata.
  - (File changes, security permissions change, owner change)
- FAT and NTFS uses B for the file creation („Birth“).
Timeline Content

- **Date:** All entries are grouped
- **Size:** Size of the file
- **Type:** The Timestamps that has been modified
- **Mode:** The file permissions
- **UID and GID:** Owner
- **Meta:** The metadata address
- **File Name:** The corresponding filename
Timelines shows file accesses and modifications around an interesting time.

1. Parse the filesystem for gathering the timestamps of the metadata (BODY file).
   - Allocated files
   - Deleted file names
   - Unallocated inodes
2. Parse the BODY file into human-readable format.
Bodyfile and Timeline

- **Bodyfile of Logfiles:**
  
  ```
  # log2timeline -o mactime -z TIMEZONE -r -w BODY.file LOGFILE-DIR/IMAGE.DD
  ```

- **Bodyfile of File-System:**
  
  ```
  # fls -r -m /mountpoint image.dd >> BODY.file
  ```

- **Bodyfile of the Registry:**
  
  ```
  # regtime.pl -m <HIVENAME> -r /path-to/registry_hive >> BODY.file
  ```
  
  (SYSTEM, SAM, SECURITY, SOFTWARE, and all NTUSER.dat)

- **Creation of the Timeline:**
  
  ```
  # mactime -d -b bodyfile > timeline.csv
  ```

Distributed Storage Networks and Computer Forensics Winter 2011/12 Amir Alsbih