ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Amir Alsbih and Christian Schindelhauer

Distributed Storage and

Computer Forensic

2 Recap

A set of tools

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

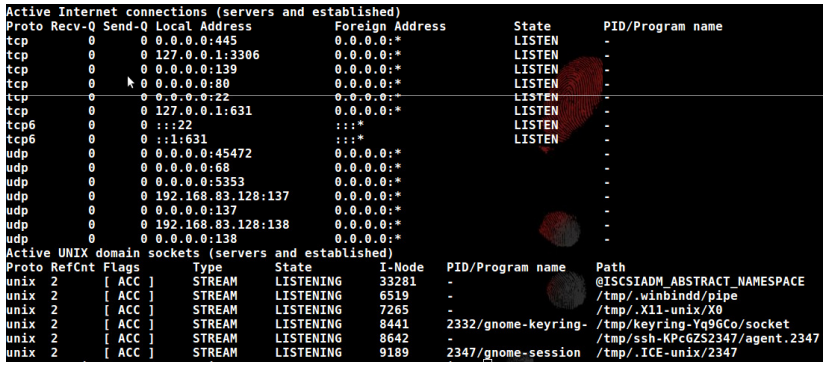
- Volatility Framework
- Win32dd
- memdump
- pd: Process Dumper is able to make a dump of a running process
- pdgmail: gather gmail artifacts
- pdfbook: gather facebook artifacts
- Skypeex: gather skype chat artifacts

Network connections

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

 # netstat –anp

- -a: all sockets
- -n: do not resolve host names
- -p display PID/Programm name for sockets



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:45472           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 192.168.83.128:137      0.0.0.0:*                           -
udp        0      0 0.0.0.0:137             0.0.0.0:*                           -
udp        0      0 192.168.83.128:138      0.0.0.0:*                           -
udp        0      0 0.0.0.0:138             0.0.0.0:*                           -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     33281    -                    @ISCSIADM_ABSTRACT_NAMESPACE
unix  2      [ ACC ]     STREAM     LISTENING     6519     -                    /tmp/.winbindd/pipe
unix  2      [ ACC ]     STREAM     LISTENING     7265     -                    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     8441     2332/gnome-keyring-  /tmp/keyring-Yq9GCo/socket
unix  2      [ ACC ]     STREAM     LISTENING     8642     -                    /tmp/ssh-KPcGZS2347/agent.2347
unix  2      [ ACC ]     STREAM     LISTENING     9189     2347/gnome-session   /tmp/.ICE-unix/2347
```

List processes

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- # *ps –aux*
- -a: all
- -u: use effective user ID
- -x: processes without tty

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2620  1492 ?        Ss   20:03   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   20:03   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   20:03   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   20:03   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   20:03   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   20:03   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   20:03   0:00 [cpuset]
root         8  0.0  0.0      0     0 ?        S<   20:03   0:00 [khelper]
root         9  0.0  0.0      0     0 ?        S<   20:03   0:00 [netns]
root        10  0.0  0.0      0     0 ?        S<   20:03   0:00 [async/mgr]
root        11  0.0  0.0      0     0 ?        S<   20:03   0:00 [kintegrityd/0]
root        12  0.0  0.0      0     0 ?        S<   20:03   0:00 [kblockd/0]
root        13  0.0  0.0      0     0 ?        S<   20:03   0:00 [kacpid]
root        14  0.0  0.0      0     0 ?        S<   20:03   0:00 [kacpi_notify]
root        15  0.0  0.0      0     0 ?        S<   20:03   0:00 [kacpi_hotplug]
root        16  0.1  0.0      0     0 ?        S<   20:03   0:11 [ata/0]
root        17  0.0  0.0      0     0 ?        S<   20:03   0:00 [ata_aux]
root        18  0.0  0.0      0     0 ?        S<   20:03   0:00 [ksuspend_usbd]
root        19  0.0  0.0      0     0 ?        S<   20:03   0:00 [khubd]
root        20  0.0  0.0      0     0 ?        S<   20:03   0:00 [kseriod]
root        21  0.0  0.0      0     0 ?        S<   20:03   0:00 [kmmcd]
root        22  0.0  0.0      0     0 ?        S<   20:03   0:00 [bluetooth]
root        23  0.0  0.0      0     0 ?        S    20:03   0:00 [khungtaskd]
root        24  0.0  0.0      0     0 ?        S    20:03   0:00 [pdflush]
root        25  0.0  0.0      0     0 ?        S    20:03   0:00 [pdflush]
root        26  0.0  0.0      0     0 ?        S<   20:03   0:00 [kswapd0]
root        27  0.0  0.0      0     0 ?        S<   20:03   0:00 [aio/0]
root        28  0.0  0.0      0     0 ?        S<   20:03   0:00 [ecryptfs-kthrea]
root        29  0.0  0.0      0     0 ?        S<   20:03   0:00 [crypto/0]
```

List open files

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- # lsof –n
- -n: no host names

```
COMMAND     PID          USER   FD      TYPE     DEVICE SIZE/OFF       NODE NAME
init          1          root  cwd   unknown                             /proc/1/cwd (readlink: Permission denied)
init          1          root  rtd   unknown                             /proc/1/root (readlink: Permission denied)
init          1          root  txt   unknown                             /proc/1/exe (readlink: Permission denied)
init          1          root NOFD                                       /proc/1/fd (opendir: Permission denied)
kthreadd      2          root  cwd   unknown                             /proc/2/cwd (readlink: Permission denied)
kthreadd      2          root  rtd   unknown                             /proc/2/root (readlink: Permission denied)
kthreadd      2          root  txt   unknown                             /proc/2/exe (readlink: Permission denied)
kthreadd      2          root NOFD                                       /proc/2/fd (opendir: Permission denied)
migration     3          root  cwd   unknown                             /proc/3/cwd (readlink: Permission denied)
```

Other things

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- Current date/time:
  # date
- Partition map
  # fdisk -l
- Mount points
  # mount
- System uptime
  # uptime
- OS type
  # uname -a

```
/dev/sda3 on / type ext3 (rw,errors=remount-ro)
proc on /proc type proc (rw)
none on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type tmpfs (rw,mode=0755)
none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /dev/shm type tmpfs (rw,nosuid,nodev)
none on /var/run type tmpfs (rw,nosuid,mode=0755)
none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)
none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/dev/sdb1 on /cases type ext3 (rw)
/dev/sda1 on /boot type ext3 (rw)
```

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

 # 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)

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- 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

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- The Sleuth Kit:
  - Detection:

    # disk_stat DEVICE
  - Removal:

    # disk_sreset DEVICE
- Windows DD:

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

Timelines

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 interessting time.
  - Files that where accessed, deleted and modified
  - Tools that where executed
- Rootkits will have limited benifit, since the file system will log the activities.
- Works on all file systems.
- The timeline only shows the last access time.

Timeline MAC

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- 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

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- Date: All entries are grouped
- Size: Size of the file
- Type: The Timestamps that has been modified
- Mode: The file permisions
- UID and GID: Owner
- Meta: The metadata adress
- File Name: The coressponding filename

Timelines

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- Timelines shows file accesses and modifications around an interessting 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

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- 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