Basic **FORENSICS Cheatsheet**

CERN Computer Security
Computer.Security@cern.ch
https://cern.ch/computersecurity

Evidence Collection

Preparation

- Snapshots and remote backup
- Deploy forensic instance and toolkit
- Disable log rotation of the central services such as DNS, firewall, …

Investigation Timeline

```
forensics$ script ~/evidences/investigation-host1.txt
host1$ export PS1='[\D{%FT%T%z}] \u@\h \w\$ '; unset HISTFILE
```

Memory Collection

Full memory

```
host1$ avml /tmp/mypath/memory.dmp
```

Processes

```
host1$ export PID=12345; kill -STOP $PID
host1$ cp /proc/$PID/exe $PID.exe
(Method A) host1$ gcore $PID
(Method B) host1$ gdb -p $PID # Type gcore, detach, exit
```

Disk Image

Local capture

```
host1$ dd if=/dev/sdX bs=4M | gzip -c > /tmp/mypath/image.dd.gz
```

Remote capture

```
host1$ dd if=/dev/sdX bs=4M | gzip -c | nc forensics [PORT]
forensics$ nc -v -l -p [PORT] > ~/evidences/image.dd.gz
```

Artifacts Collector

```
host1$ git clone https://github.com/tclahr/uac; cd uac
host1$ ./uac -p ir_triage /tmp/mypath
OR ./uac -a live_response/network,live_response/process /tmp/mypath/
```

Network Capture

```
host1$ tcpdump -G 60 -W 1 -w /tmp/mypath/host1.pcap -I [INTERFACE]
```

Data Forwarding

```
host1$ scp -r /tmp/mypath [USER]@forensics:~/evidences
host1$ tar -zv /tmp/mypath | nc forensics [PORT]
```

Evidence Analysis

Storage Analysis

Backdoors

```
$HOME/.ssh/authorized_keys
/etc/sudoers, /etc/sudoers.d/, /etc/passwd
```

Persisting malware

```
Service start-up scripts:
/etc/systemd/system,
/usr/lib/systemd/system
/etc/init*
```

```
Scheduled tasks:
/etc/cron*
/var/spool/cron/crontabs
/var/spool/cron/atjobs
```

History

```
/home/USER/.bash_history, /root/.bash_history
```

Network

```
forensics$ tshark -n -r host1.pcap -Tfields -e ip.src
-e tcp.srcport  -e ip.dst -e tcp.dstport | sort | uniq -c
forensics$ tshark -r host1.pcap -Y "udp.port == 53" -T fields
-e dns.qry.name -e ip.src -e ip.dst | sort | uniq -c
```

Libraries

```
/etc/ld.so.conf /etc/ld.so.conf.d
```

Other

```
Kernel Modules: lsmod, *.ko
Hidden files: /dev/shm
```

Metadata Timeline with The Sleuth Kit

```
forensics$ mmls image.dd
forensics$ fls -o 20992 -r -m / image.dd > fls_20992.txt
forensics$ for file in fls_*.txt; do mactime -b $file >
"${file/.txt/.timeline}"; done
```

Unallocated space

```
forensics$ blkls image.dd > ~/evidences/unallocated.blkls
```

Memory Analysis with Bulk Extractor

```
forensics$ bulk_extractor –o outputdir memory.dmp
```

Checklist

- [ ] Preparation
- [ ] Investigation Timeline
- [ ] Memory Collection
- [ ] Disk Image
- [ ] Artifacts Collector
- [ ] Network Capture
- [ ] Data Forwarding
- [ ] *Report Incident
- [ ] Access to remote investigators
- [ ] Evidence Analysis

Report Incident

- TLP and PAP
- Incident date and time
- Actions taken
- Type of observed activity
- Detailed narrative of the event
- Severity/impact of the incident
- Organization name and contact details
- Number and type of systems affected
- People informed
- Resources available for the incident
- Indicators of Compromise

Toolkit

- CERN Forensics: https://cern.ch/forensics
- The Sleuth Kit (TSK): https://sleuthkit.org/sleuthkit/
- Bulk Extractor: https://forensics.wiki/bulk_extractor/
- Volatility: https://github.com/volatilityfoundation/volatility
- Unix-like Artifacts Collector (UAC): https://github.com/tclahr/uac
- LiME: https://github.com/504ensicsLabs/LiME
- dcfldd: https://github.com/resurrecting-open-source-projects/dcfldd
- Acquire Volatile Memory for Linux (AVML): https://github.com/microsoft/avml
- tcpdump: https://www.tcpdump.org/
- tshark: https://www.wireshark.org/docs/man-pages/tshark.html

Considerations

- Live collection of data may tamper evidences such as access times, memory, disk, etc.
- /tmp/mypath is just a reference, it's recommended to use external mounted FS or forward data directly to a proxy and don't host evidences on the investigated host.
- Network capture should be done on the interface with internet access.