6. Acquisition

Digital Forensics and Cybercrime course

Prof. Zanero

Acquisition

- **<u>Forensic procedures have been developed with the USA in mind</u>**, but not all the world is the same!
  - Evidence in USA: “chain of custody”, and admissibility
  - In Italy, e.g., evidence is based on the evaluation performed by the judge - completely different!
- Applicable international law in CoE states:
  Convention of Budapest on cybercrime
  https://www.coe.int/en/web/cybercrime/the-budapest-convention
- Applicable international standards:
  - ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence
  - ISO/IEC 27035:2011, Information technology — Security techniques — Information security incident management
  - Guidelines for Evidence Collection and Archiving https://www.ietf.org/rfc/rfc3227.txt

Brittleness of digital evidence

- This is probably the single **most important concept** in these lessons
- ***Digital evidence is brittle***: if modified, there is no way to tell.
  - It is not, in other words, *tamper evident*
- I can theoretically create a perfect *fake*
  - I can (re)construct files, with timestamps that please me
  - Example: the *thesis alibi* (Garlasco case)
- I need procedures that ensure, insofar as possible, that digital evidence sources become *tamper evident*
- Needed to ensure:
  - Legal compliance
  - Ethical behaviour from all parties
  - Detection of errors in good faith
  - Detection of natural decay

The usage of hashes in digital forensics

- In order to seal digital evidence, **hashes** (and digital signatures) are routinely used
- If the hash of a digital object is recorded at a given step of acquisition, and then constantly checked in further steps, it can ensure on the <u>identity</u>, <u>authenticity</u> and <u>non-tampered state</u> of the evidence <u>**from that step on**</u>
- It is important to understand that:
  - <u>Hashes are not a dogma</u>: you cannot just say “there is no hash” and dismiss everything. Why is there no hash? Has any other measure been taken? Can we still reconstruct the chain of acquisition?
  - <u>Hashes are not magic</u>: computing a hash does not say anything about what happened before the hashing took place. So a proper *procedure* needs to be adopted
- To be useful, hashes must be either sealed in writing (e.g. on a signed report), or encrypted to form a digital signature

Typical hardware/software for acquisition

- Hardware:
  - Removable HD enclosures or connectors with different plugs
  - Write blocker (see in a few slides)
  - External disks
  - USB, firewire, SATA and e-SATA controllers, if possible
- Operating system:
  - Linux: extensive native file system support + ease of accessing drives and partitions without “touching” (mounting) them

Bitstream images

- We want to acquire, if possible, a bitstream image, a bit-by-bit clone of the original evidence media
- The reason will become evident when we discuss analysis, but basically if we only copy the allocated content we lose (potentially) information
- This may be different in special cases (e.g. RAID drives, encrypted or virtual drives…)
- Often called a “forensic clone” or “clone copy” or “image”
- Acquisition is also called “freezing” sometimes

Basic procedure of acquisition

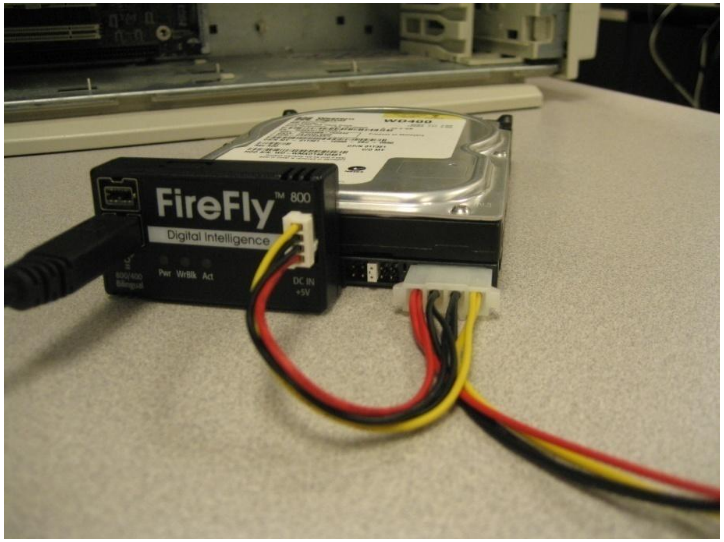
- <u>Basic acquisition of a powered-down system</u>
  - Disconnect the media from the original system (if possible, if not possible see ahead for usage of *forensic distributions*)
  - Connect the *source media* to analysis station, if possible with a *write blocker* (see next slide)
  - Compute the hash of the source, e.g.

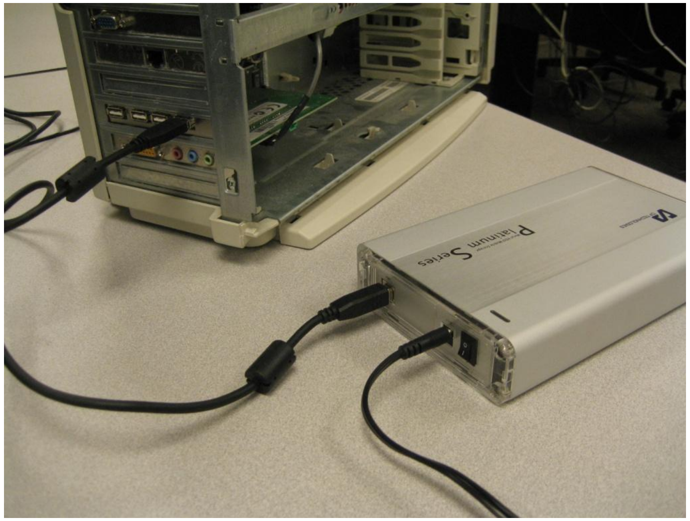
    ```
    #dd if=/dev/sda conv=noerror,sync | sha256sum
    ```
  - Copy the source, e.g.

    ```
    #dd if=/dev/sda of=/tmp/acquisition.img conv=noerror,sync
    ```
  - Compute the hashes of the source and the clone

    ```
    #dd if=/dev/sda conv=noerror,sync | sha256sum
    #sha256sum /tmp/acquisition.img
    ```
  - Compare the three hashes
- It could be good to compute also MD5 and SHA-1 hashes of the image at least, for redundancy and to be sure it can be compared

Write blocker





+ external USB drive

Challenges: time

- Typical hard drive capacity today: 1TB?
- Typical transfer speeds
  - SATA 2 can transfer over 300MB/s (SATA 3 doubles this), but traditional rotational drives reach approx 100MB/s at peak, and average at around 80MB/s. SSDs can max out the controller
  - USB transfers can be even slower: 20 to 100 MB/s
- This means that for a 1TB drive you can expect to wait several hours to complete a copy (or to run a hash)
- Some software (e.g., dcfldd) may automate part of the procedure (e.g. compute the source hash while copying, in parallel):

```
dcfldd if=/dev/sda hash=md5,sha256 md5log=md5.txt
sha256log=sha256.txt of= /tmp/acquisition.img
hashconv=after bs=512 conv=noerror,sync
```

Challenges: size

- Dealing with today's capacity in storage is complex, in particular for large-scale investigations
- Using external media (e.g. USB drives) slows down operations
- NAS (Network Attached Storage) or SAN (Storage Area Network) systems are common in forensic shops
- Sometimes, moving images across a network can be useful; simplest way to achieve is to setup on a host:
  ```
  #nc -lp 5678 > /tmp/acquisition.img
  ```
  And run on the acquisition side something like:
  ```
  #dd if=/dev/sda conv=noerror,sync | nc -p 5678
  <address>
  ```

Challenges: encryption

- There is an increasing use of encryption in regular laptops and PCs
- It is already a serious constraint in mobile devices as we will see
- Even if provided with key, performing acquisition in a repeatable way is challenging:

  https://re.public.polimi.it/retrieve/handle/11311/542763/559594/EuroSec08Zanero.pdf

Embedded forensic duplicators

Alternative operating procedures

Common variants

Alternate 1: booting from live distribution

- Sometimes we need to work directly on the machine:
  - Systems with weird HW and controllers or physical cases
  - RAID devices
  - Specific investigation constraints
- In this case we can live-boot the system under assessment using a Linux distribution targeted to forensic analysis
  - Ordinary live distros may mount, e.g., swap partitions
  - Once we boot, we can use the command lines we already saw to clone the drives from the "inside"
- Examples that work:
  - Tsurugi: https://tsurugi-linux.org/
  - BackBox: https://linux.backbox.org/

Alternate 2: Target powered on

- Can we turn it off? (hint: critical services?)
- Should we turn it off? (hint: live analysis of an intruder?)
- Network disconnect (to eject the intruder, if still connected)
- Work in volatility order
  - Dump of memory: if possible, and not costly; hardware tricks to perform the dump are available (firewire)
  - Save runtime information: network, process information, etc.
  - Finally, disk acquisition
- It could be possible to perform the acquisition without a shutdown; if impossible, pull the plug (do not perform the shutdown procedure, unless it is really necessary to ensure the reboot of the machine)
- Document all activities executed before sealing the evidence
  - Each command may alter the state

Some useful commands

- Network data
    - ifconfig -a ; netstat -anp ; route -n ; arp
- Process data
    - ps aux ; lsof *file*
- Users data
    - who; last; lastlog
- Memory acquisition
    - Mantech mdd, win32dd, Mandiant Memoryze
- Useful reading for memory analysis
    - http://computer-forensics.sans.org/blog/2008/11/19/memory-forensic-analysis-finding-hidden-processes/

Alternate 3: Live network analysis

- In some cases we will want to observe an attacker "live"
  - Honeypots, e.g.
  - An intruder can react if he feels observed
  - Reminder: tools installed on a compromised machine may be unreliable (e.g. rootkit)
- Key observation points:
  - Logs
  - Network traffic
- We will have a separate class on (live) network forensics

New challenges

- Cloud forensics (dedicated slide deck)
- Mobile devices (dedicated seminar)
- SSD peculiarities (dedicated slide deck)