Digital Forensics Module
Part 2

Jaap van Ginkel
Silvio Oertli

July 2016
Hands-On (Acquisition)
Tools used in the Hands-on Workshop

- We will use open source tools for this part
  - DEFT 8.2 (Forensic Linux distribution)
  - Guymager (Graphical Acquisition Tool)
• Booting Computer with DEFT-CD or USB Stick
  – Depending on the Computer, you need to change Bootingdevice (F2/F6/F9/…)

DEFT Linux 8 live
DEFT Linux 8 live text mode
Install DEFT Linux 8
Check disc for defects
Test memory
Boot from first hard disk

F1 Help   F2 Language   F3 Keymap   F4 Modes   F5 Accessibility   F6 Other Options
• When you see the Desktop, insert the evidence USB-Stick on the computer
• Doubleclick the Guymager-Icon on the left
Rightclick on the USB-Stick-Entry and Choose Acquire image
• Fill in your Case data
• State turns green after finishing. Your done!
Theory in Practice
You’re part of the local branch of a global CERT-Team in your country. The main office advice you to seize and analyze all local devices which could contain evidence about data leakage on Project XXX.
• What to expect on-site...

Image Source: http://images.hayneedle.com/mgen/master:BHI305.jpg

Spot the hidden USB-key...

Image Source: http://nixuxu.ru/load/344430.jpg
Toolbox

- Paper and Pencils (yes, even nowadays...)
- Camera
- Tools
  - Screwdrivers (Torx, Crosshead, Flathead, etc.)
  - Tweezers
  - Antistatic wrist strap
  - etc.

Image Source: http://www.nachi.org/images10/wrap.jpg
We have to ensure that the target media is empty before we use the device for storing evidence:

- We can re-use storage media if we wipe their content before using it.
- There might even be data on virgin storage media directly coming from the manufacturer.
- Ensure that there is no data from old cases left. This might ruin your day.
  - Especially important if no container formats are used (we discuss this in a moment).
  - The commands can be found in the references.

Be careful to specify the right storage media when wiping drives…

Do not execute the commands in the references during the hands-on exercises!
• Verify your Tools
  – Tools should do what they have to
  – Document the tests

• Use high quality equipment (e.g. Enterprise disks)
Reducing altering

- Separate Persons from equipment
- Prevent altering evidence by accident or on purpose
- Pay attention on user credential
- Cloud storage
Locating Evidence

- Private even more
  - TV’s, Playstation, more
The ON vs. OFF Debate

- Depends on the circumstances whether to leave a computer running or to turn it off

- Turning a computer off means loosing all volatile evidence
  - RAM
  - Might be a problem with encrypted file systems where the password is not known

- Keeping a computer running means altering evidence
  - Memory content changes constantly
  - Disk is used and file fragments might be overwritten
Evidence Handling

• Definition from [12]:
  – **Chain of custody** (CoC) refers to the chronological documentation or **paper trail**, showing the seizure, custody, control, transfer, analysis, and disposition of **evidence**, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward **acquittal** or to overturning a guilty verdict upon **appeal**. The idea behind recording the **chain of custody** is to establish that the alleged evidence is in fact related to the alleged crime, rather than having, for example, been **planted fraudulently** to make someone appear guilty.

• Goal: Prove that the evidence came from or was produced by the suspect and not inserted or altered by the forensics analyst.

• Document who had access (physical and electronic) to the evidence at every given moment.

• Prepare for the worst during an investigation!
  – Quick-and-dirty approach → Other party might sue the investigator afterwards or court rejects the evidence
Evidence Handling

• Forensic Logbook
## Order of Volatility

- Taken from [13]: Guidelines for Evidence Collection and Archiving

<table>
<thead>
<tr>
<th>Volatility</th>
<th>Archival media</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>Physical configuration, network topology</td>
</tr>
<tr>
<td></td>
<td>Remote logging and monitoring data that is relevant to the system in question</td>
</tr>
<tr>
<td>volatile</td>
<td>Disk</td>
</tr>
<tr>
<td></td>
<td>Temporary file systems</td>
</tr>
<tr>
<td></td>
<td>Routing table, arp cache, process table, kernel statistics, memory</td>
</tr>
<tr>
<td></td>
<td>Registers, Cache</td>
</tr>
</tbody>
</table>
Write Blockers

- Altering evidence must be avoided either
  - with software
    - Mounting read-only
  - with hardware
    - Some hard disks (e.g. SCSI drives) have jumpers
    - Forensic write blockers

- The suggested way to go is hardware write blockers
  - Depends on circumstances

Image Source: https://www2.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges/t35es-r2.aspx
• Raw Copy
  – 1:1 copy using dd from a physical drive to identical physical drive
  – Forensically sound
  – Not very convenient to work with
  – Can only be used for single devices such as hard drives, memory sticks, etc.
  – Not possible to store on servers using this method
  – Deprecated for most situations
• Container Format
  – 1:1 copy from a physical drive into a (forensic) container file
  – Forensically sound
  – Libraries and tools available to work conveniently with containers
  – Container files can be stored everywhere including Servers
  – This approach is used most often nowadays
• Disk Imaging

• Imaging over a Network
• Physical
  – RAID → disk configuration
  – Good environment 80GB/hour
  – Get all included deleted files

• Logical
  – Fast
• RAID 0 (stripe)

• RAID 1 (mirror)
  – 1:1 copy on both disks
• RAID 5
  – Speed and Redundancy

• Just a bunch of disks (JBOD)
• `shasum -a 256 test.txt`
  – 2f50fe79a03391be5b8001606b030f26a5e8fe1dfdb137f7e28d74d2accfc3e9

• `shasum -a 256 test.txt`
  – 6f9ea996741487099e783bba8654f2e09c194e8e0eb37f33cd0549c360e493b2
• Master Boot Record (MBR)
  – Up to 4 primary Partitions
  – Up to 2 TB per Disk

• Globally Unique Identifier Partitiontable (GPT)
  – Up to 128 Partitions
  – $2^{64}$ Blocks $\rightarrow$ 9.4 Zetabyte
ewfmount uses FUSE (Filesystem in Userspace) to mount your evidence

- sudo mkdir /mnt/evidence
- ewfmount /home/evidence/20160901_df01/USB_20160901_df01_001.E01 /mnt/evidence
Mounting an image

- Check partition table
  - `mmls /mnt/evidence/ewf1`
Mounting an image

- Mount Windows partition (NTFS)
  - `mkdir windows_mount`
  - `mount -o ro,loop,show_sys_files,streams_interface=windows,offset=65536 -t ntfs /mnt/evidence/ewf1 /mnt/windows_mount`
• A lot of different Filesystems (ntfs, FAT, HFS+, ext2, ZFS)

• But all like Books (table of contents → pages)
• A lot of different Filesystems (ntfs, FAT, HFS+, ext2, ZFS)

• But all like Books (table of contents → pages)

• Deleting Files just deletes or marks Entry in “Table of content”
  – File still exists on the Harddrive
Evidence on File systems

• Finding Documents by name
  – `find . -name "*.doc"`

• Finding Documents with specific content
  – `grep -r "many secrets"`

Analysis
Evidence on File systems

- Finding Document of specific format in unallocated space
  - Carving (Scalpel)

- Filesystems magic numbers
  - Officefiles (bin): 0xD0CF11
  - Officefiles (zip): 0x504B04  PK..
  - JPG: 0xFFD8FF  ÿØÿ
  - GIF: 0x474946383761  GIF87a
  - PDF: 0x25504446  %PDF
  - EXE: 0x4D5A  MZ
Artifacts of programs can be on different places in different formats

- $USER/AppData/*
  - Example AppData/Roaming/Mozilla/Firefox/Profiles/m3k5a7px.default/formhistory.sqlite
  - Open with sqlitebrowser
• Artifacts of programs can be on different places in different formats
  – $USER/AppData/*
    • Example AppData/Roaming/VeraCrypt/History.xml
    • Open with vi
• Artifacts of programs can be on different places in different formats
  – $USER/AppData/*
    • Example AppData/Roaming/VeraCrypt/Configuration.xml
    • Open with vi
    • Look for LastSelectedDrive

![Example Configuration.xml content with LastSelectedDrive highlighted]
• If you are investigating an event in the past, you want to know what happened when in order to create a timeline of events
• End result for the report
• timescanner
  – Perlscript uses log2timeline to scan recursive directory and write csv file
  – timescanner –d /mnt/windows_mount/ -w 
    /home/evidence/20160901_df01/timeline.csv
  – Open it with LibreOffice Spreadsheet
Registry is a system wide Database in Windows divided in Hive-Files

- Windows/System32/config/SAM
- Windows/System32/config/SECURITY
- Windows/System32/config/SYSTEM
- Windows/System32/config/SOFTWARE
- <$USER>/NTUSER.DAT
Registry is a system wide Database in Windows divided in Hive-Files

- Thomas Ehrhart/NTUSER.DAT
- `reglookup "/mnt/windows_mount/Users/Thomas Ehrhart/NTUSER.DAT" | grep "U:"`
There are known files by from the Systems which you don't like to investigate.

- Elimination through Hashlist
- NSRL Downloads (http://www.nsrl.nist.gov)
• Report your findings in a document
• An other Digital Forensic Expert should follow your Document and
  – Come to the same findings
  – Can proof your findings
• Report Facts, not guesses