Part 4
Digital Forensics Module

Silvio Oertli
Peter Haag
Adrian Leuenberger

October 2017
• Further Topics
  – Running a suspect image
  – Printed evidence
  – Tools
  – Limitations
  – Upcoming Topics in Forensics
  – Certification
Forensics – The Field

• Forensics is a broad field
  – Covers nearly all aspects of information technology

• But still a relatively young science
  – Not yet court-tested in every jurisdiction
  – Few cases and experience in law enforcement agencies
• It might be convenient if one has the same experience as the suspect in front of the computer
  – Running an image is possible with LiveView, which allows converting a *.dd image into a VMWare virtual machine (http://liveview.sourceforge.net/)
  – Potential problem: You need to have the login credentials or hack your way into the operating system
Printed Evidence

- Colour laser printers print valuable evidence onto every page
  - [https://www.eff.org/issues/printers](https://www.eff.org/issues/printers)
  - Serial number of the printer
  - Date and time of the printout
  - Encoding not publicly documented. Some have been reverse engineered
  - Might help in case of counterfeit fraud or (printed) data theft

Image source: [https://w2.eff.org/Privacy/printers/docucolor/](https://w2.eff.org/Privacy/printers/docucolor/)
• **Office Documents**
  – Title
  – Author, Creation Date and Time
  – Company name
  – Computer name
  – Document Revisions
  – Comments
  – Etc.

• **PDF Documents**
  – Title
  – Author, Creation Date and Time

• **Images**
  – EXIF data
# exiftool Jungfraujoch.jpg

File Name                  : Jungfraujoch.jpg
File Modification Date/Time: 2012:03:13 14:02:44+01:00
File Type                  : JPEG
GPS Position               : 46 deg 32' 49.00" N, 7 deg 59' 1.00" E
Image Size                 : 7500x2450
Tooling commercial
Tooling commercial specialized
Tooling opensource

Autopsy® based on The Sleuth Kit®
Tooling mobile forensics (Cellebrite)
Mobile forensics (Android)

- Installing the Android APK
  - Because we need the Android Debug Bridge (ADB)

- Enable USB Debugging
  - Setting -> Developer options -> Enable USB Debugging
  - Setting -> Info -> Hit many times Buildnumber until it shows “You are developer” -> go back -> Developer options -> Enable USB Debugging

- ADB Shell with Memorycard
  
  ```
  dd if=/dev/block/mmcblk0 of=/sdcard/blk0.img bs=4096 conv=noerror
  ```

- Connect the device and use the ADB to perform Backup
  
  ```
  adb devices
  adb backup -apk -shared -all -f <filename incl. path>
  ```
Mobile forensics (Android)

- **Data Storage of devices**
  - Internal data of all apps is saved in `/data/data/<apppkg>`

- **Methods of data storage**
  - `SharedPreferences`
  - `Internal storage`
  - `External storage`
  - `SQLite database`
  - `Network`

- **Logs**
  - `/data/data/<apppkg>/files/log.txt`
Limitations

• There might be circumstances that prevent you from getting evidence that are beyond your control

• Wiped disks / Defect disks

• Encryption where you do not have the password
Cloud forensics

- Cloud provider supports
  - Versioning
  - Recycle Bin
    - Restoring possible up to 90 days
  - Not always possible to delete instantly
• Operating System cannot see the whole disk
  – Reserved groups
  – Encryption on controller level may be used
Upcoming Topics

• Anti-forensics
  – Prevent evidence from being stored on the computer
  – Place wrong data or obfuscate data
  – Use of encryption

• TV’s / Surveillance Cams/ SMART Home
  – Interfaces ?
  – Proprietary Filesystems

• JTAG / CHIP off
  – Using Joint Test Action Group Pins on Mainboard to directly access Chipdata
  – Solder out the chip
  – Get an image of the data on the chip
JTAG
Certification / Courses

• What can be certified / accredited
  – Persons
    • Vendor certification for specific software (eg. EnCE, ACE)
    • GIAC Certified Forensic Examiner (GCFE) -> SANS.org
    • Certified Forensic Computer Examiner (CFCE) -> Iacis.com
    • EC-Council: CHFI
    • University degrees: MSc Forensics at several universities worldwide
  – Labs
Interesting Resources

- DFRWS (Digital Forensics Research Conference)
  - www.dfrws.org
- Digital Investigations Magazine (Springer)
  - http://www.elsevier.com/locate/diin
- Forensic Challenges
  - http://computer-forensics.sans.org/challenges/
- Project Honeynet Forensic Challenges
- Wiki / Blog
  - http://www.forensicswiki.org
- Books: Hacker’s Challenges 1-3

Image sources: www.amazon.com