

Part 4
Digital Forensics Module

Silvio Oertli
Peter Haag
Adrian Leuenberger



Agenda - Part 4

- Further Topics
 - Running a suspect image
 - Printed evidence
 - Tools
 - Limitations
 - Upcoming Topics in Forensics
 - Certification

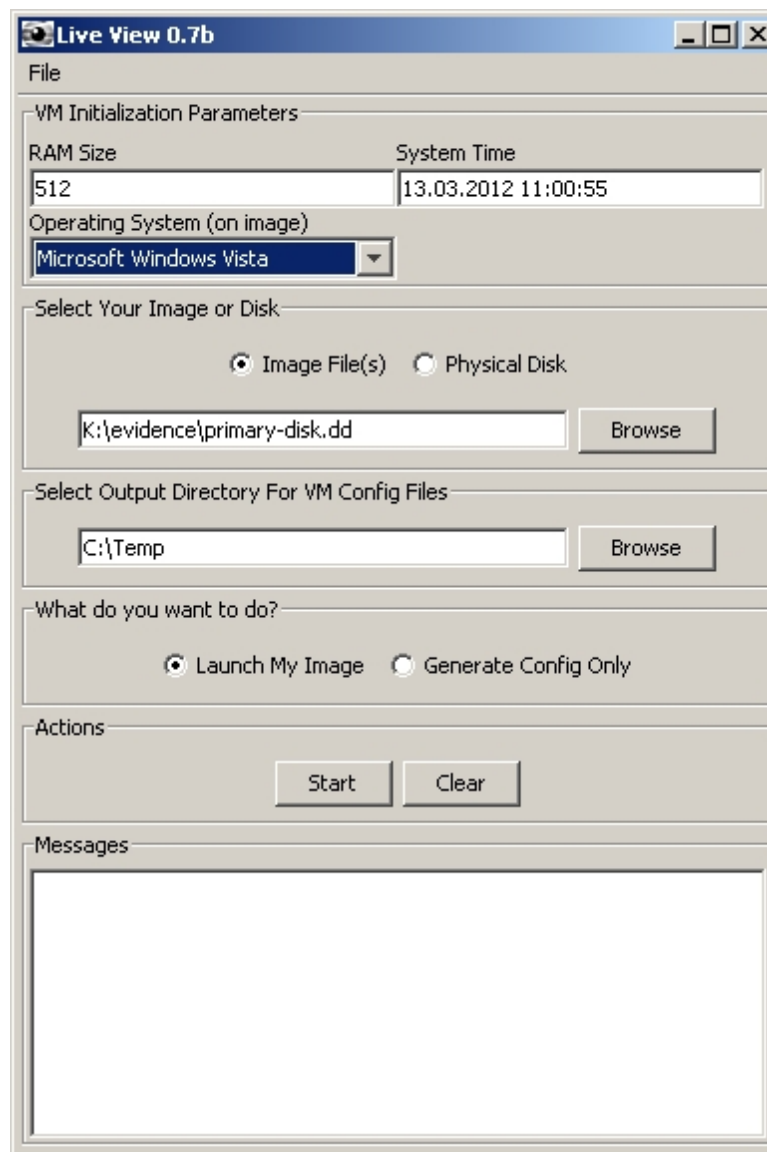


Forensics – The Field

- 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

Running an Image

- 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>
 - 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

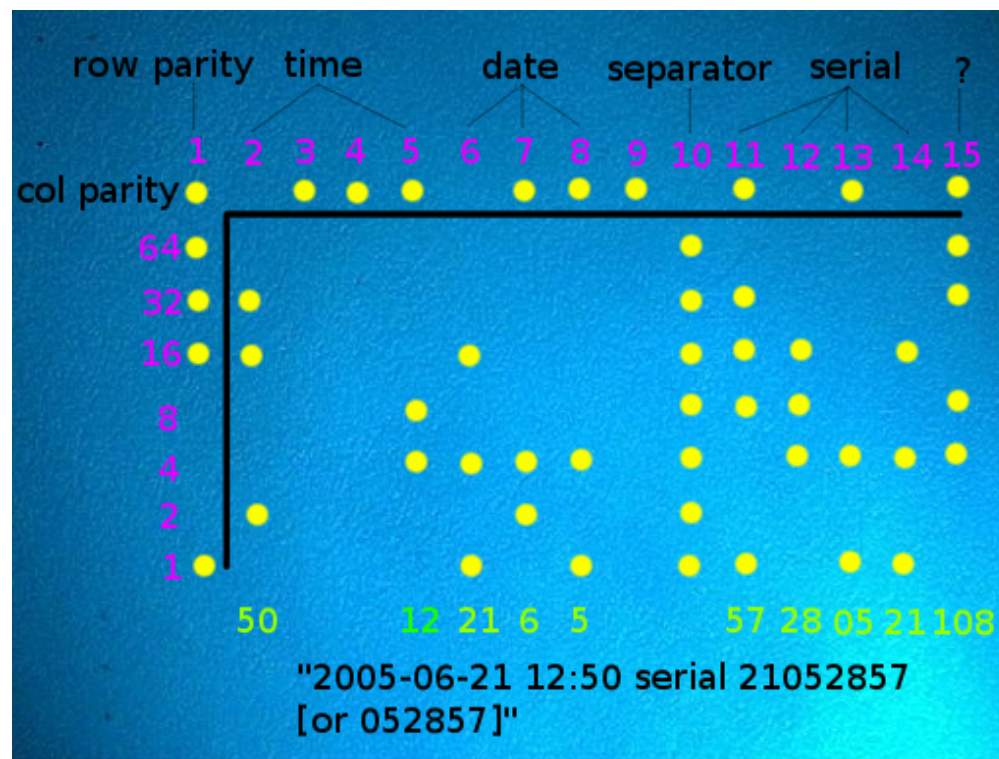
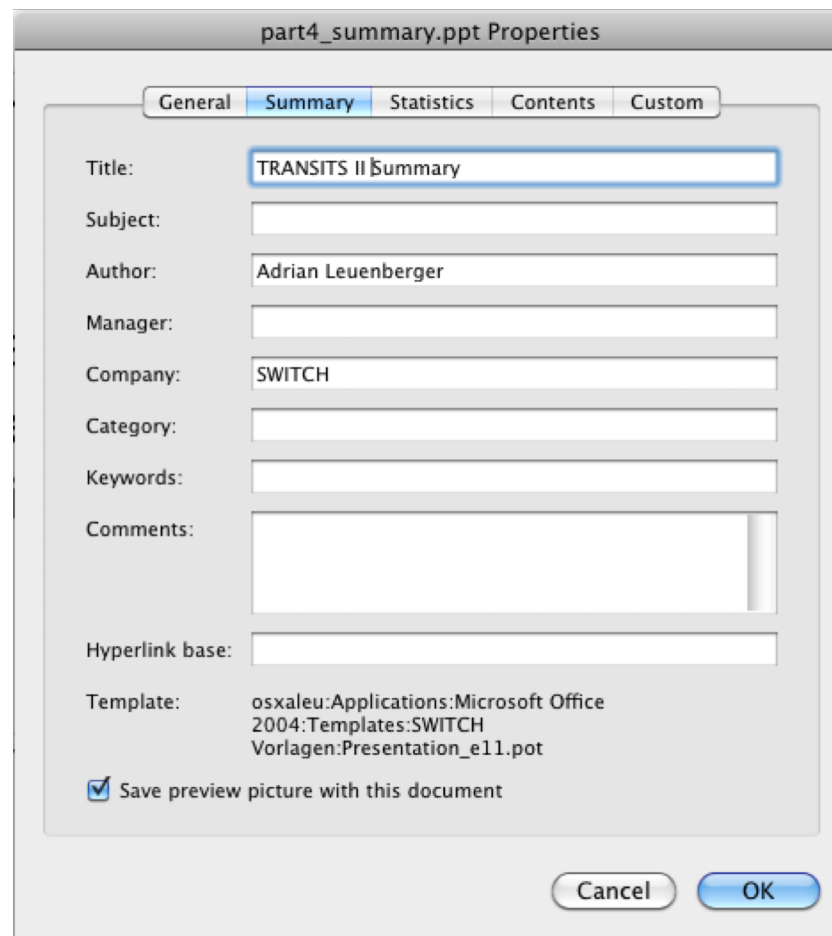


Image source: <https://w2.eff.org/Privacy/printers/docucolor/>

Document Metadata

- 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



part4_summary.ppt Properties

General Summary Statistics Contents Custom

Title: TRANSITS II Summary

Subject:

Author: Adrian Leuenberger

Manager:

Company: SWITCH

Category:

Keywords:

Comments:

Hyperlink base:

Template: osxaleu:Applications:Microsoft Office
2004:Templates:SWITCH
Vorlagen:Presentation_e11.pot

Save preview picture with this document

Cancel OK

Document Metadata - Images



exiftool Jungfraujoeh.jpg

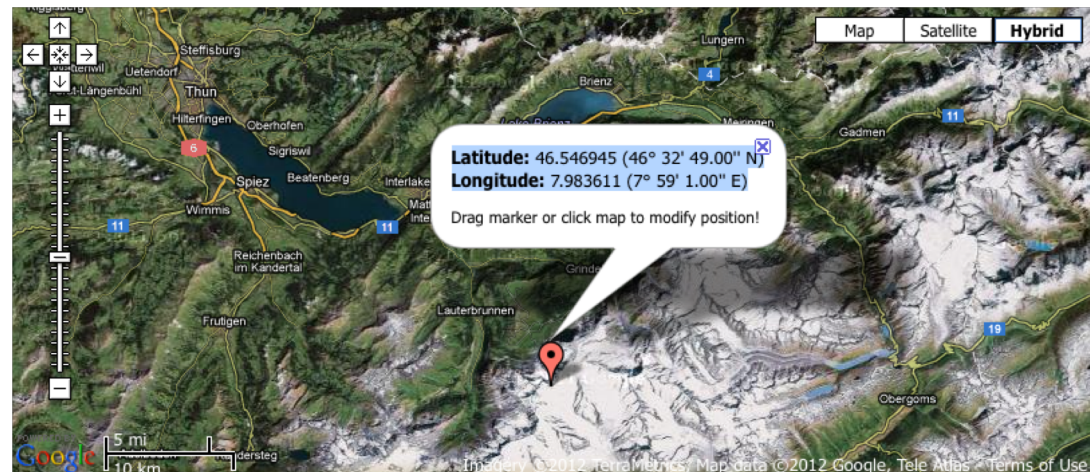
File Name : Jungfraujoeh.jpg

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



E-mail Forensics. Simplified.



Tooling opensource



Autopsy® based on
The Sleuth Kit®





Tooling mobile forensics





Tooling mobile forensics (Cellebrite)

The screenshot displays the Cellebrite software interface for an iPhone extraction. The left sidebar shows a project tree with categories like Device Info, Images, Memory Ranges, File Systems, Archive, Analyzed Data, Application Usage (26), Bluetooth Devices (1), Calendar (27), Call Log (92), Chats (4), Contacts (419), Emails (446), Installed Applications (67), Locations (385), MMS Messages (12), Notes (1), SMS Messages (2338), User Accounts (9), User Dictionary (906), Web Bookmarks (158), Web History (15), Wireless Networks (31), Bookmarks (0), Data files, Images (11732), Videos (37), Audio (1845), Text (244), Tags, and Reports.

The main window shows the 'Extraction Summary' for the project 'iPhone_4_(GSM)_4.3.4-4.3.5_File_System_Extraction_14-08-11_06.03.52'. It includes a 'Generate Report' button and a 'Device Information' section with a small image of the iPhone and the following details:

- Device Name: iPhone_4_(GSM)_4.3.4-4.3.5_File_System_Extraction_14-08-11_06.03.52
- Device Type: Apple iPhone (Physical)
- Connection Type: Cable No. 110
- Extraction end date/time: 14/08/2011 6:11:06 PM
- Extraction start date/time: 14/08/2011 6:03:54 PM

The 'Image Hash Information' section contains a warning: 'Hash data is available for this project. Click to verify.' with 'Show Details' and 'Verify' buttons.

The 'Device Info' section provides technical specifications:

ECID	000002EBE	CPID	85 0
IMEI	01253400	Serial number	870507
Board	n90ap	iBoot (firmware) version	iBoot-1072.61
Capacity	30GB	Passcode	
Owner Name	Bob Elder's iPhone		

The 'Device Content' section is divided into 'Phone Data' and 'Data Files'. 'Phone Data' includes:

- Application Usage: 26 (0)
- Bluetooth Devices: 1 (0)
- Calendar: 27 (0)
- Call Log: 92 (3)
- Chats: 4 (0)
- Contacts: 419 (31)
- Emails: 446 (0)
- Installed Applications: 67 (0)
- Locations: 385 (0)
- MMS Messages: 12 (0)
- Notes: 1 (0)
- SMS Messages: 2338 (41)
- User Accounts: 9 (0)
- User Dictionary: 906 (0)
- Web Bookmarks: 158 (0)
- Web History: 15 (0)
- Wireless Networks: 31 (0)

'Data Files' includes:

- Images: 11732 (0)
- Videos: 37 (0)
- Audio: 1845 (0)
- Text: 244 (0)



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>
```

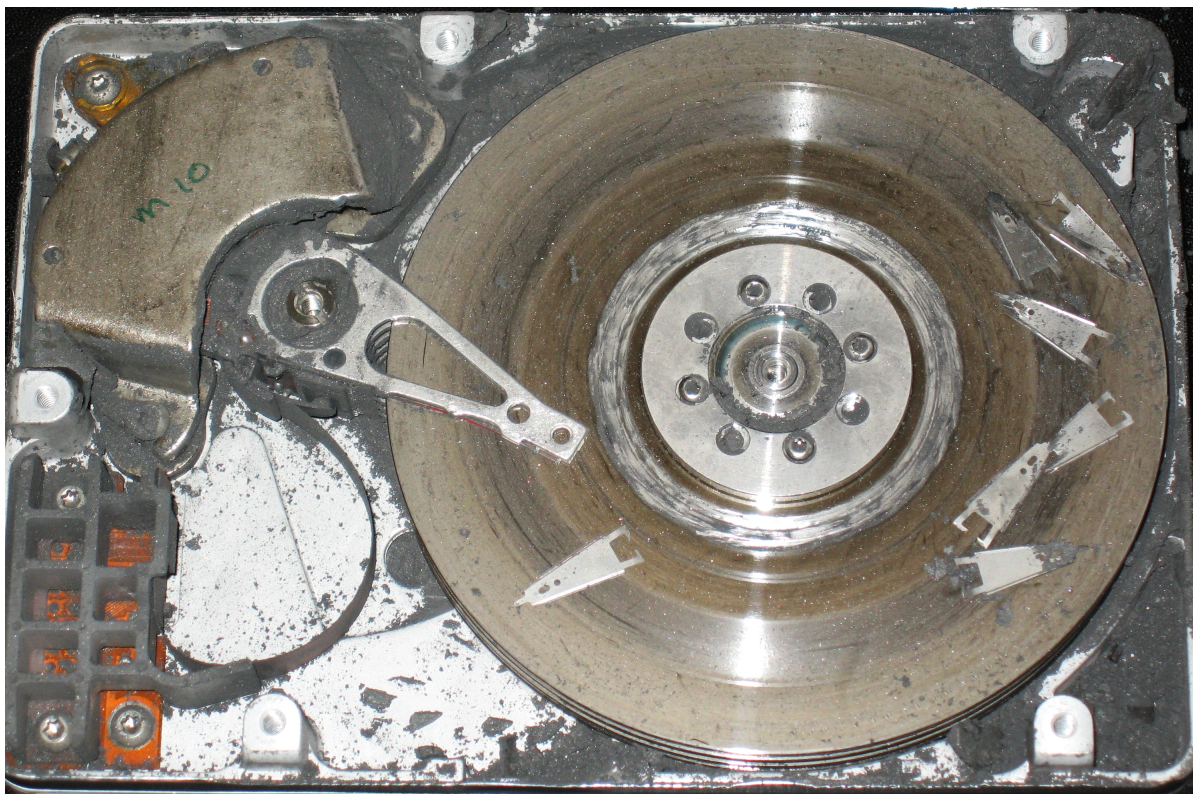


Mobile forensics (Android)

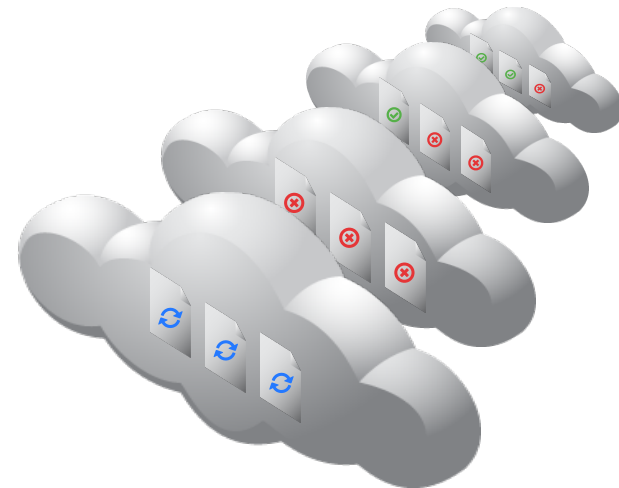
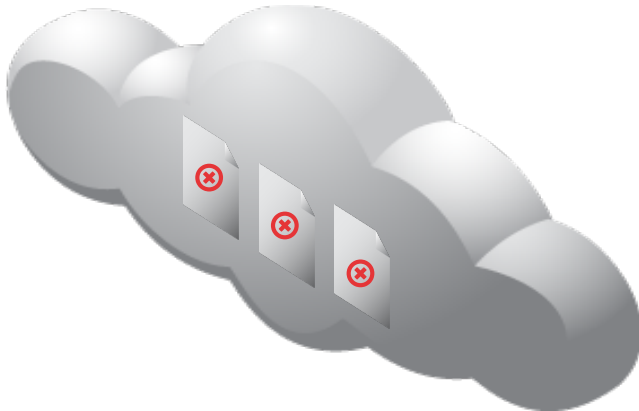
- Data Storage of devices
 - Internal data of all apps is saved in /data/data/<apppkg>
- Methods of datastorage
 - Sharedpreferences
 - Internalstorage
 - Externalstorage
 - SQLitedatabase
 - Network
- Logs
 - /data/data/<apppkg>/files/log.txt

Limitations

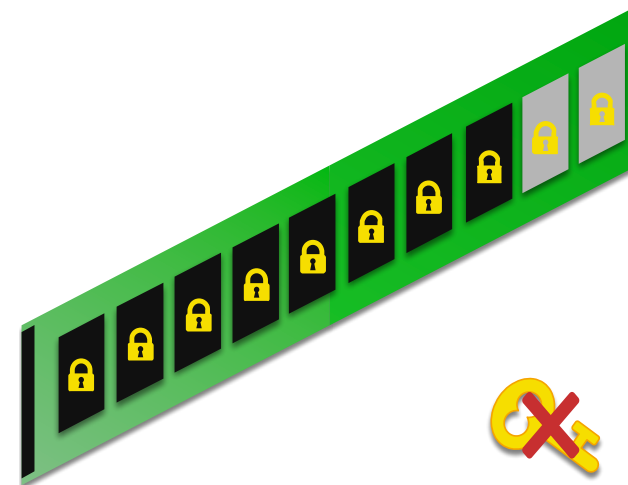
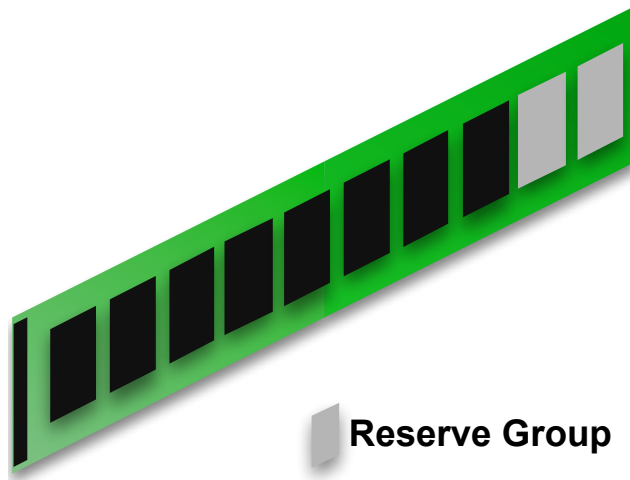
- There might be circumstances that prevent you from getting evidence that are beyond your control
- Wiped disks / Defect disks
- Encryption where you do not have the password



- Cloud 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

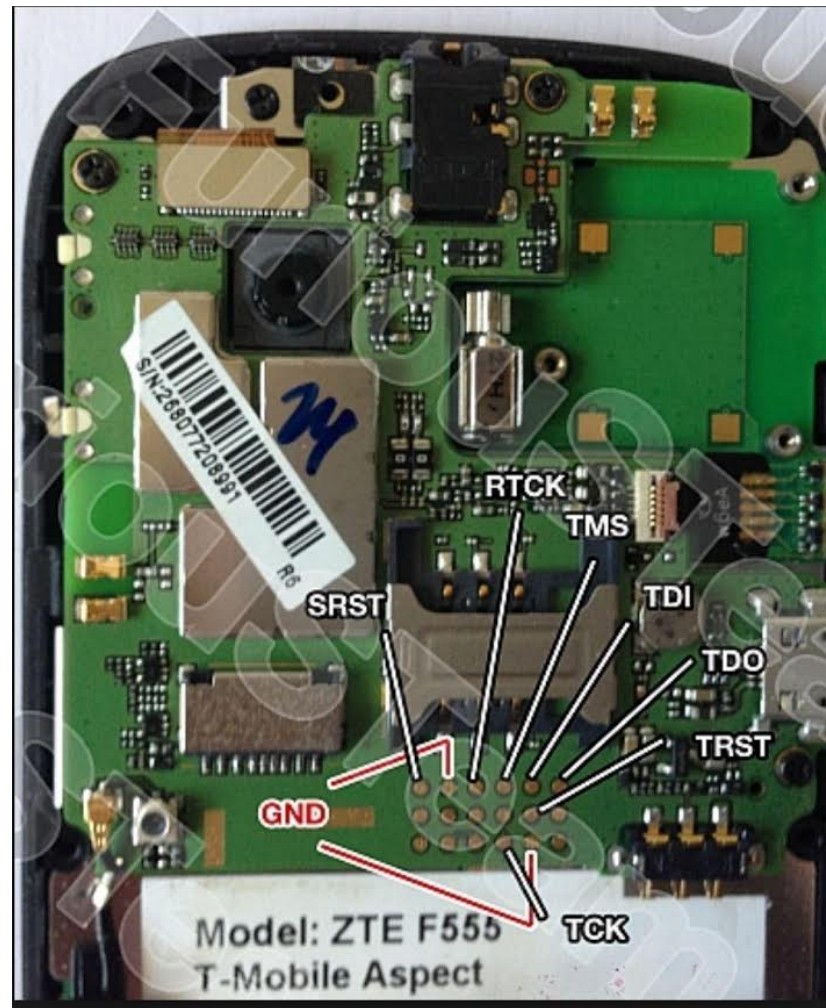




Upcoming Topics

- 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
 - <http://old.honeynet.org/challenge/index.html>
- Wiki / Blog
 - <http://www.forensicswiki.org>
- Books: Hacker's Challenges 1-3

