Forensic Analysis of Cell Phones and SIM Cards

Technical Service Center of Information and Communication Services

- Logical and physical analysis of cell phones and SIM cards
- Cases:
  - Theft, Murder, Rape, etc.
  - And **Terrorism**

Logical Analysis in a Nutshell

- Commercial Products:
  - Oxygen, .XRY, MobileEdit, etc.
- AT Commands, OBEX Commands
- Manufacturer Software Products
- Hardware: IRDA, USB Cable

Physical Analysis in a Nutshell

- UFS_HWK, UST PRO II, Flash and Backup, etc.
- Removing memory chips
- Reverse engineering, Scripts
- Commercial products such as CPA, XACT

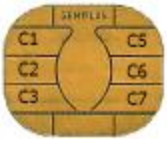
But...

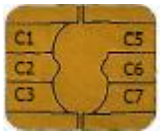
Analysing the SIM Card

- Card Reader
- SIM Reading Software

Analysing the SIM Card (cont.)

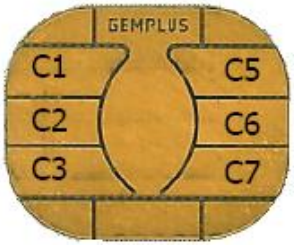
- Looking at the actual SIM Chip
- Different Architectures

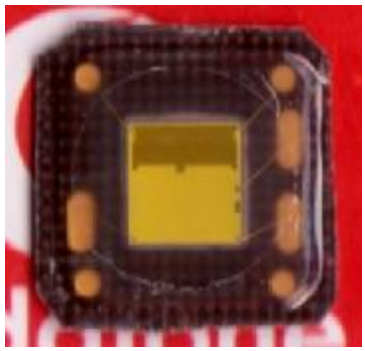




Analysing the SIM Card (cont.)

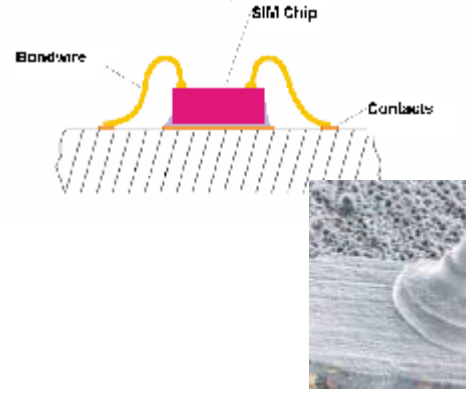
- Cutting the plastic form the other side of the chip
- What do we have?



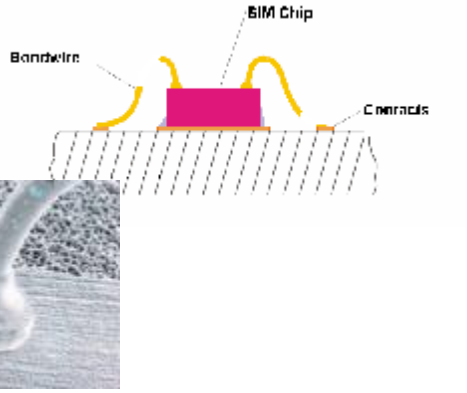


Analysing the SIM Card (cont.)

Bond wires intact

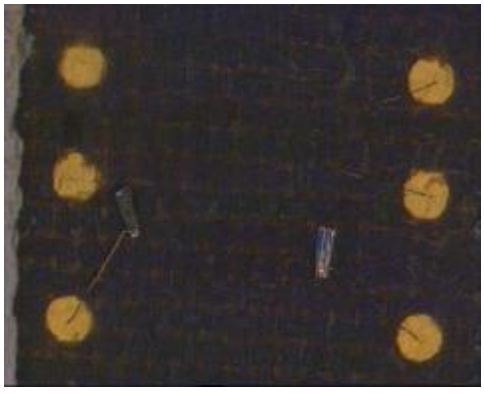


Bond wires detached

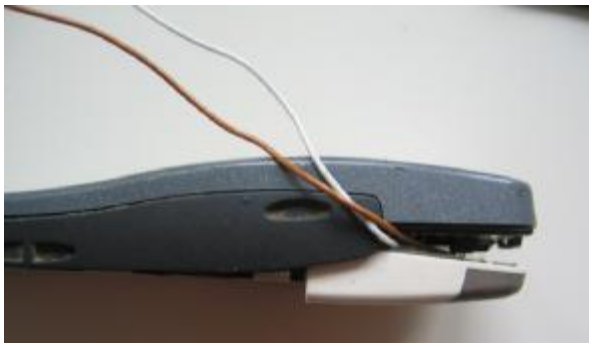


Analysing the SIM Card (cont.)

Result: No Data



Analysing the Cell Phone – Case 1



Analysing the Cell Phone – Case 1

Analysing the Cell Phone – Case 1

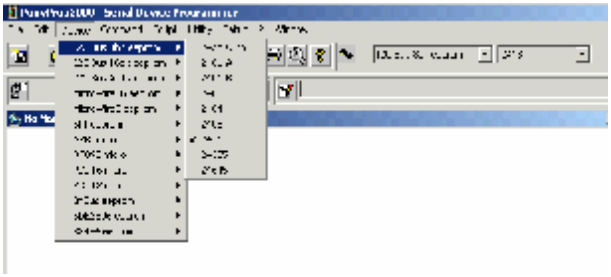
- Identifying the memory chip
- ATMEL 2416
- EEPROM

Analysing the Cell Phone – Case 1

- Removing the memory chip
- Mounting it onto a board, for dumping the EEPROM data

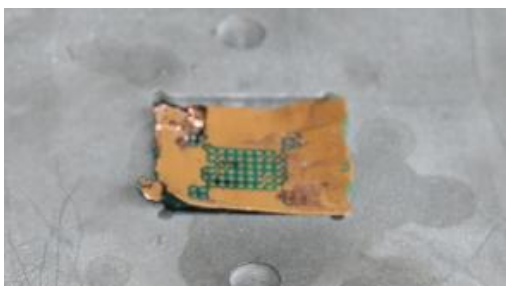
Analysing the Cell Phone – Case 1

- Read process, using a common EEPROM Reader



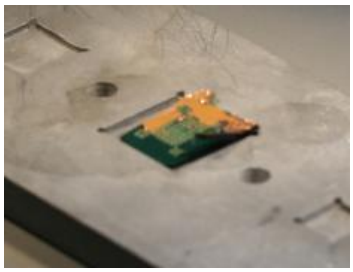
Analysing the Cell Phone – Case 2

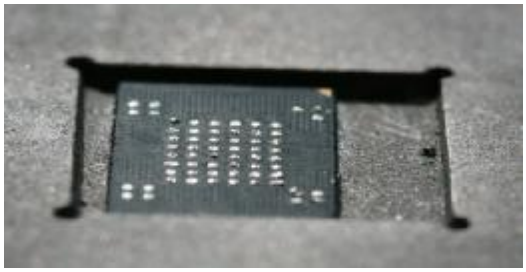
- The phone triggered the explosion and only fragments are left.



Analysing the Cell Phone – Case 2

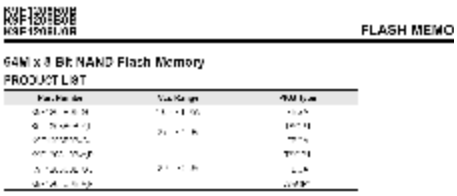
- Identifying the chip
- Cleaning the chip with a soldering iron





Analysing the Cell Phone – Case 2

- Datasheet_ Chip: Samsung K9F120 NAND (64MB)



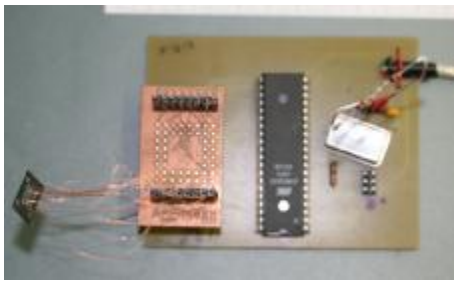
FLASH MEMO

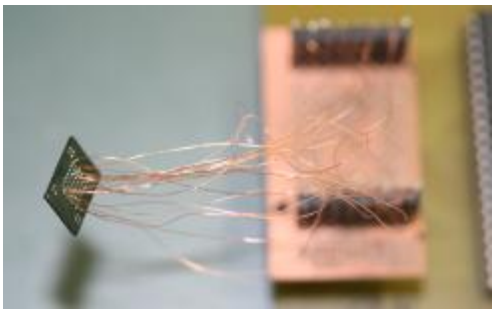
64M x 8 Bit NAND Flash Memory

PRODUCT LIST

Analysing the Cell Phone – Case 2

Ø Connecting the chip to a socket-board





and the Professionals...

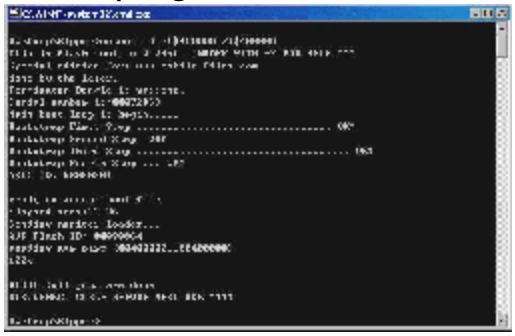
Workstation

Chip & 1 cent

ReadingDevice

Flash_Dumping

- Bit per bit dumping of the entire memory chip



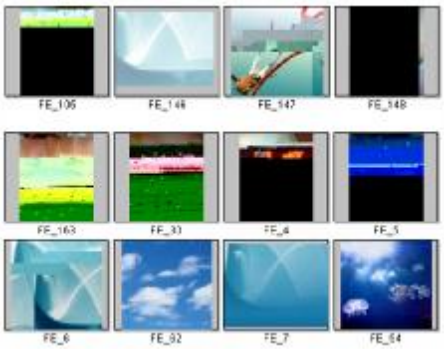
Interpreting the data
Example: Picture

- Search file for known headers:
  - JPG: **FF D8 FF E#**; GIF: **47 49 46 38 39**
  - AVI: **52 49 46 46**; 3GP: **18 66 74 79 70 33**

Interpreting the data
Example: Picture

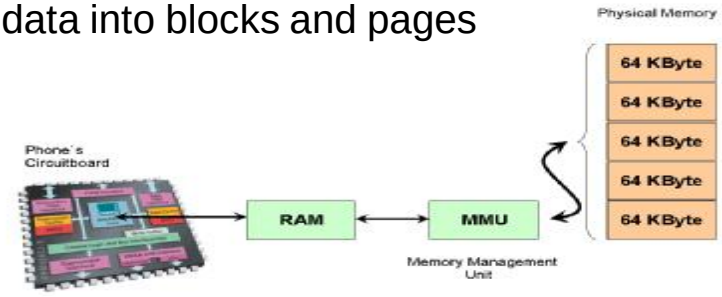
- Results not satisfactory
- Reason:

  Storage management of phone and chip



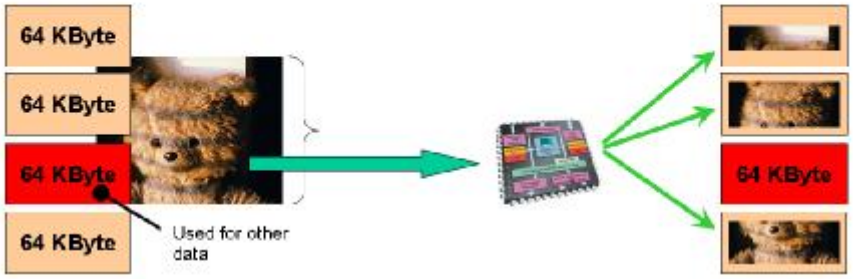
Storage Management

- The Storage management results in a storage of data into blocks and pages



Storage Management

- If data is larger than 64 Kbytes- the data is fragmented



Data_Reconstruction

- Reverse Engeneering of proprietory Cell Phone Operating Systems
  - Filesytem of Phone
  - User Data (Phonebook, Call Logs with date and time, Pictures, MMS, SMS, Kalender, etc)
  - IMSI/ICC-ID Log

Data_Reconstruction

Ø Example Log:

1	✗	SIMKartennummer (ICCID)	894900030812010086??
2	✗	SIMKartennummer (IMSI)	9001010123456789
3	✓	Last Area Information (LOCI)	0000000000FF
4	✓	SIMKartennummer (ICCID)	89490200000487872157
5	✓	SIMKartennummer (IMSI)	9262018600134366

Thank you for your attention!

Questions?!

Contact information:
Katja Koennecke
Bundeskriminalamt / Federal Criminal Police Germany
+49 (0)2225 89 23 106
KatjaVerena.Koennecke@bka.bund.de