IMF 2013 - 7th International Conference on IT Security Incident Management & IT Forensics

"Anti-Forensics: The Next Step in Digital Forensics Tool Testing"

Felix Freiling, Christian Moch, Martin Wundram

Image source: mpavlov / Clipdealer

Agenda

I. What is Anti-Forensics?

II. Examples for Anti-Forensics

III. Catagorization of actions in Anti-Forensics

IV. Anti-Anti-Forensics: What can we do?

V. Lessons learned

VI. Questions?

Greetings

About the authors

- Martin Wundram, TronicGuard GmbH, Cologne:
  - Focus on IT-Security and IT-Forensics, e.g. web security, penetration testing, ISO/IEC 27001, e-discovery
  - Entitled by the chamber of commerce of Cologne as an officially approved and sworn in expert witness for systems and applications in information processing *(Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung)*
- Felix Freiling, Friedrich-Alexander-University, Erlangen
- Christian Moch, Friedrich-Alexander-University, Erlangen

Greetings

About the topic/paper

- How about combining IT security and IT forensics? How about stress testing and attacking IT forensics tools?
- Are they as robust and reliable as We assume?
- First talk 2011 at 28C3 in Berlin (Chaos Communication Congress by Chaos Computer Club)
- Previous work by others (two examples):
  - *"Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem"*, Ryan Harris, 2006
  - *„Counter Forensics"*, Noemi Kuncik und Andy Harbison, Digital Forensics Magazine, 2010
    - Data Destruction, File Deletion, Re-Formatting, Defragmentation

What is Anti-Forensics?

Storytelling

What is Anti-Forensics?

Storytelling – Conclusion

- Not new at all: IT forensics can be a complex task, while dealing with large or huge amounts of data one can easily overlook important facts
- Also not new: anti forensics is possible with simple or even very simple methods.
- Anti anti forensic in this case wasn't that simple, but doable with standard forensics tools (intensive search for deleted data, +abnormalities in filenames and timestemps). You could have overlooked important details easily.
- A secure deletion of data could possibly prevent an elucidation of this case.

What is Anti-Forensic?

Storytelling

Image source: treenabeena - Fotolia.com

What is Anti-Forensics?

Storytelling – Conclusion

- IT forensics software helps us
  - to be more efficient (how to examine e.g. 4 TB of data?)
  - to be more effective (how to understand and interpret the database structure in that shiny new instant messenger?)
- Involved parties tend to rely on the tools outcome
  - **Forensics software has a leading portion at the extraction and evaluation of findings from certain issues**
- But IT forensics software is just that: software which can produce wrong results
- At court *upraising of general doubts on the results/correctnes of your tool can be impossible to defute*. Although your software in that case probably has produced correct and complete results

What is Anti-Forensics?

Definition

“[...]any attempts to compromise the availability or usefulness of evidence to the forensics process.[...]” (based on definition by Ryan Harris)

- There are three essential classes of methods:
  - **Data prevention and concealment**
  - **Elimination of data** (possibly unnoticeable)
  - and **active attacks** (often causing noticeable irregularities).

- In this talk: focus on attacks on forensics tools

What is Anti-Forensics?

Points of attack in IT forensics processes

- **Simplified process view:**
  - **Identification → Seizure → Analysis → Presentation**

- Possible target resources:
  - Evidence
  - Tools
  - experts in IT forensics

What is Anti-Forensics?

Points of attack in IT-forensics processes

- Some examplary questions from the examiners point of view:
  - Is every action documented and comprehensible?
  - Is the enemy partially more experienced then the expert in IT forensics?
  - Is there anything unsuspicious that wasn't further reviewed?
  - Was a pressure of time cause of a prevention to work thoroughly? Were there any distractions?
  - Was the evaluation system connected to the internet or to an internal network?

What is Anti-Forensics?

When and why to make use of Anti-Forensics

- From an **attackers point of view**: when there is an assumption, that relevant systems could be investigated in the future:
  - Cracker obliterates traces of intrusion
  - Downloader conceals traces of downloads
  - Registry cleaner and disk wiper to clear traces of e.g. the creation of a fake invoice
  - Person encrypts personal data
  - → *Thats well known*
  - **New**: direct attacks against forensic tools!
    - **„Poison“ your system and let the „virus“ sleep until a forensic examiner inspects your system/data and gets infected**

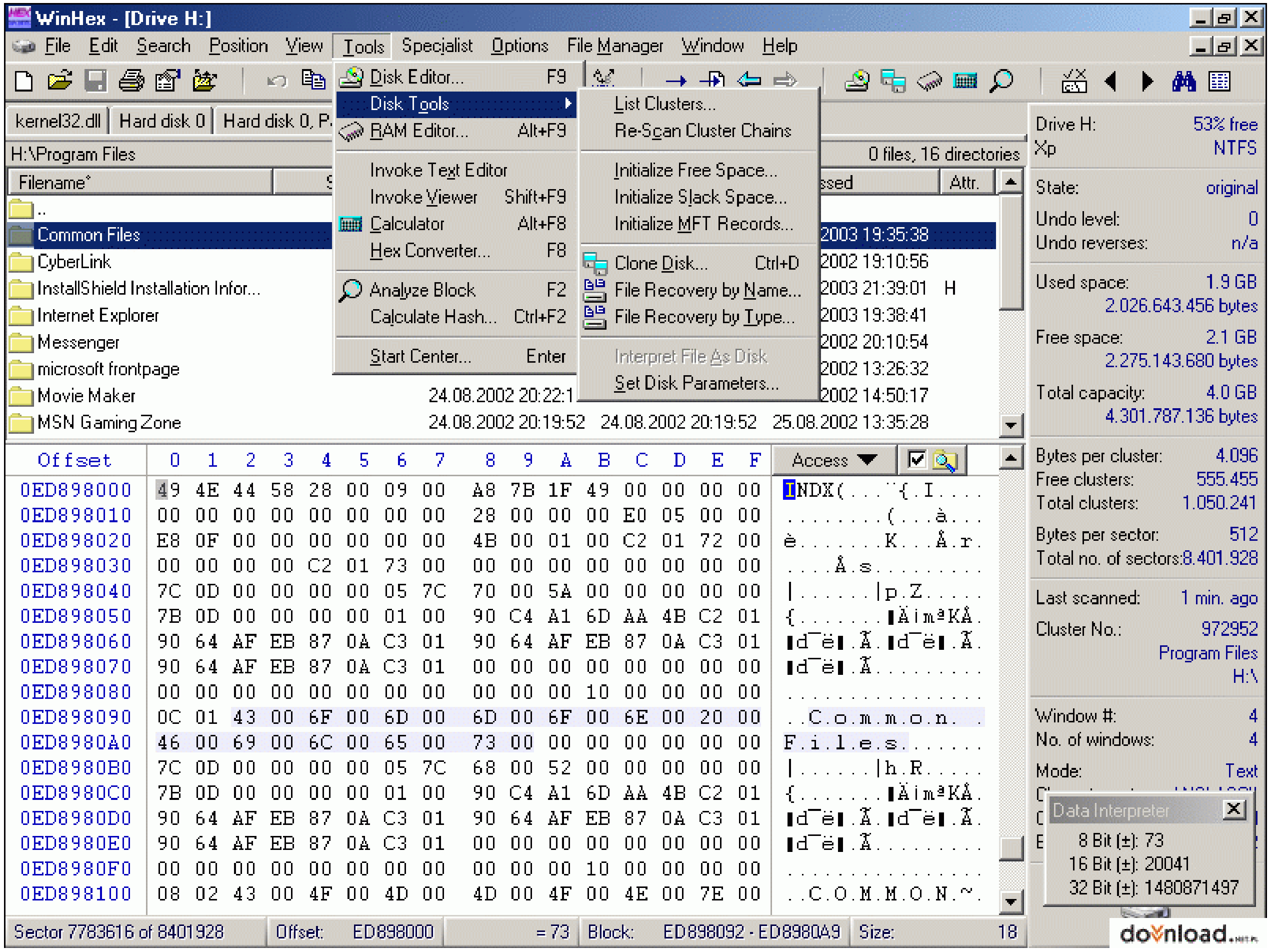
Examples for Anti-Forensics

Critical XSS vulnerability in X-Ways Forensics

- Widespread in Germany and other countrys
- All in all good and valuable software
- A now fixed, but serious problem:
    - XSS classic, after Artur Janc „**Resident XSS**“
    - HTML/Javascript Code can be inserted into a suspects registry, then resides there „silently“ waiting for its victim
    - X-Ways tranfers this code into its own HTML reports
    - Results:
        - Hiding of evidence
        - Adding fake evidence
        - Attack the examiners host computer and other systems

Examples for Anti-Forensics

Critical XSS vulnerability in X-Ways Forensics



```
H:\Program Files                                  0 files, 16 directories
..
Common Files                                                          2003 19:35:38
CyberLink                                                             2002 19:10:56
InstallShield Installation Infor...                                   2003 21:39:01  H
Internet Explorer                                                     2003 19:38:41
Messenger                                                             2002 20:10:54
microsoft frontpage                                                   2002 13:26:32
Movie Maker                 24.08.2002 20:22:1                        2002 14:50:17
MSN Gaming Zone             24.08.2002 20:19:52  24.08.2002 20:19:52  25.08.2002 13:35:28
```

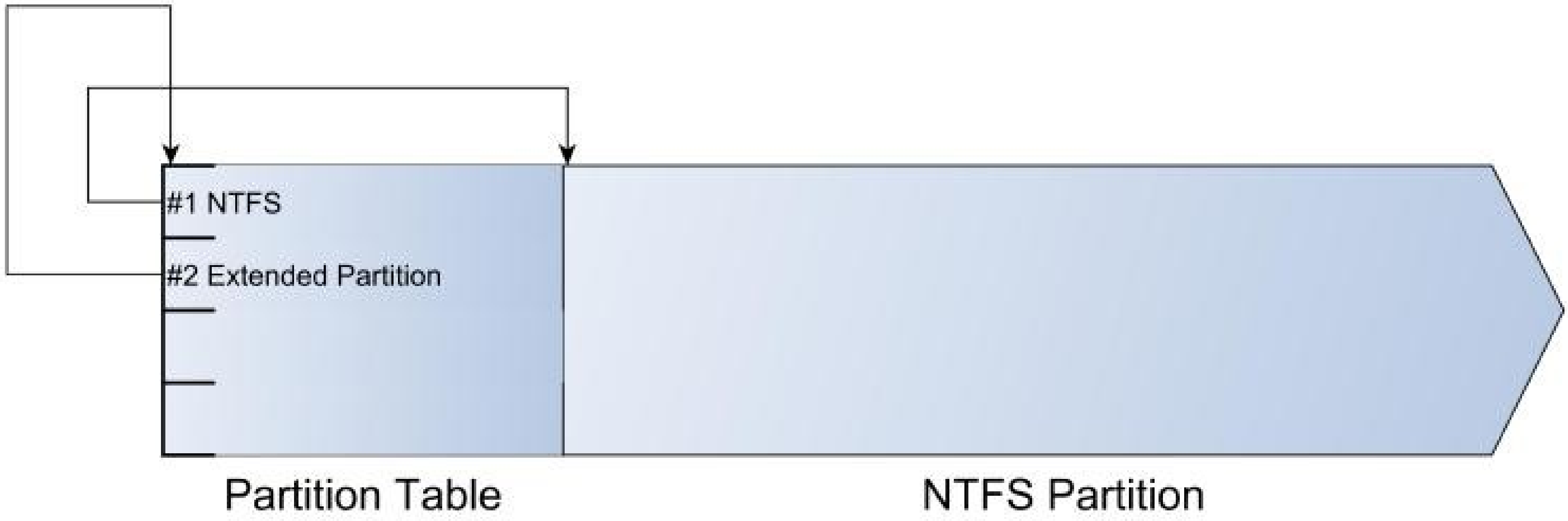
```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0ED898000  49 4E 44 58 28 00 09 00  A8 7B 1F 49 00 00 00 00   INDX(...¨{.I....
0ED898010  00 00 00 00 00 00 00 00  28 00 00 00 E0 05 00 00   ........(...à...
0ED898020  E8 0F 00 00 00 00 00 00  4B 00 01 00 C2 01 72 00   è.......K...Â.r.
0ED898030  00 00 00 00 C2 01 73 00  00 00 00 00 00 00 00 00   ....Â.s.........
0ED898040  7C 0D 00 00 00 00 05 7C  70 00 5A 00 00 00 00 00   |......|p.Z.....
0ED898050  7B 0D 00 00 00 00 01 00  90 C4 A1 6D AA 4B C2 01   {.......▌Äím ªKÂ.
0ED898060  90 64 AF EB 87 0A C3 01  90 64 AF EB 87 0A C3 01   ▌d¯ë▌.Ã.▌d¯ë▌.Ã.
0ED898070  90 64 AF EB 87 0A C3 01  00 00 00 00 00 00 00 00   ▌d¯ë▌.Ã.........
0ED898080  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00   ................
0ED898090  0C 01 43 00 6F 00 6D 00  6D 00 6F 00 6E 00 20 00   ..C.o.m.m.o.n. .
0ED8980A0  46 00 69 00 6C 00 65 00  73 00 00 00 00 00 00 00   F.i.l.e.s.......
0ED8980B0  7C 0D 00 00 00 00 05 7C  68 00 52 00 00 00 00 00   |......|h.R.....
0ED8980C0  7B 0D 00 00 00 00 01 00  90 C4 A1 6D AA 4B C2 01   {.......▌Äím ªKÂ.
0ED8980D0  90 64 AF EB 87 0A C3 01  90 64 AF EB 87 0A C3 01   ▌d¯ë▌.Ã.▌d¯ë▌.Ã.
0ED8980E0  90 64 AF EB 87 0A C3 01  00 00 00 00 00 00 00 00   ▌d¯ë▌.Ã.........
0ED8980F0  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00   ................
0ED898100  08 02 43 00 4F 00 4D 00  4D 00 4F 00 4E 00 7E 00   ..C.O.M.M.O.N.~.
Sector 7783616 of 8401928   Offset:   ED898000   = 73   Block:   ED898092 - ED8980A9   Size:   18
```

```
Drive H:                 53% free
Xp                           NTFS
State:                   original
Undo level:                     0
Undo reverses:                n/a
Used space:                1.9 GB
            2.026.643.456 bytes
Free space:                2.1 GB
            2.275.143.680 bytes
Total capacity:            4.0 GB
            4.301.787.136 bytes
Bytes per cluster:          4.096
Free clusters:            555.455
Total clusters:         1.050.241
Bytes per sector:             512
Total no. of sectors:8.401.928
Last scanned:          1 min. ago
Cluster No.:               972952
                    Program Files
                              H:\
Window #:                       4
No. of windows:                 4
Mode:                        Text

Data Interpreter
 8 Bit (±): 73
16 Bit (±): 20041
32 Bit (±): 1480871497
```

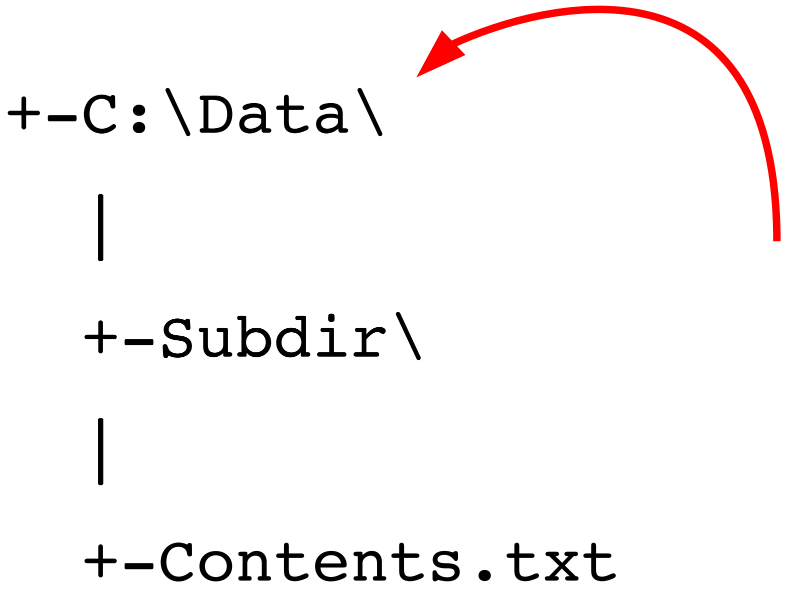
Examples for Anti-Forensics

Partition loops



Examples for Anti-Forensics

Directory loops

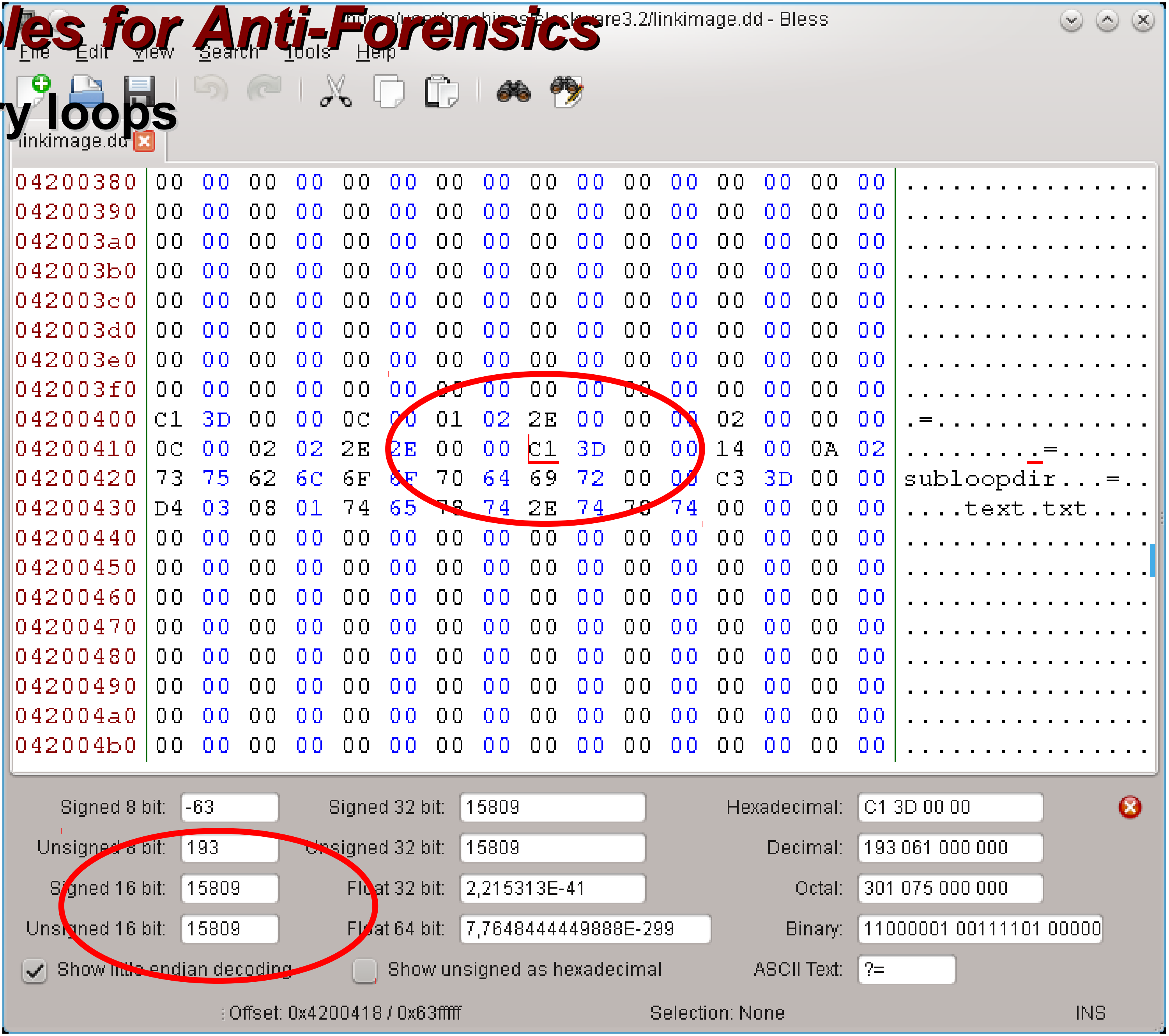


```
+-C:\Data\
  |
  +-Subdir\
  |
  +-Contents.txt
```

```
+-C:\Daten\
  |
  +-Subdir\
  | |
  | +-Subdir\
  | | |
  | | +-Subdir\
  | | +-Contents.txt
  | |
  | +-Contents.txt
  |
  +-Contents.txt
```

Examples for Anti-Forensics

Directory loops


...re3.2/linkimage.dd - Bless
File Edit View Search Tools Help
linkimage.dd

```
04200380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042003a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042003b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042003c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042003d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042003e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042003f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200400 C1 3D 00 00 0C 00 01 02 2E 00 00 00 02 00 00 00 .=..............
04200410 0C 00 02 02 2E 2E 00 00 C1 3D 00 00 14 00 0A 02 .........=......
04200420 73 75 62 6C 6F 6F 70 64 69 72 00 00 C3 3D 00 00 subloopdir...=..
04200430 D4 03 08 01 74 65 78 74 2E 74 78 74 00 00 00 00 ....text.txt....
04200440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
04200490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042004a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
042004b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Signed 8 bit: -63
Unsigned 8 bit: 193
Signed 16 bit: 15809
Unsigned 16 bit: 15809
Signed 32 bit: 15809
Unsigned 32 bit: 15809
Float 32 bit: 2,215313E-41
Float 64 bit: 7,7648444449888E-299
Hexadecimal: C1 3D 00 00
Decimal: 193 061 000 000
Octal: 301 075 000 000
Binary: 11000001 00111101 00000
ASCII Text: ?=
☑ Show little endian decoding
☐ Show unsigned as hexadecimal

Offset: 0x4200418 / 0x63fffff Selection: None INS

Examples for Anti-Forensics

"Self anti forensics"

- **Product A**: ~30% of the Firefox history (SQLite-DB!) were not observed/examined
- **Product B**: „Error 42 in Component XY at analysing the MFT. Press OK to continue" → a lot of data was not presented, including an Outlook .PST with exculpatory evidence!
- **Product C** (Live Forensics Tool): reproducable crash while saving DNS cache, no further analysis possible → tool was completely unusable in that specific case

Anti-Anti-Forensics: What can we do?

Lockdown every user of Anti-Forensics and every knowledge about it!

Image source: YuriArcurs / Clipdealer

Anti-Anti-Forensics: What can we do?

Building awareness

- Experts in IT forensics have to deal with anti-forensics, because:
    - Criminals already do it
    - IT forensics and IT security coming closer
    - **Live forensics becoming more important, growing number of cases with „only one try“**
    - Every scenario ist hypothetical until it comes true
    - **Forensic software could create false results even without external influences**
    - It is always good to be prepared!

Anti-Anti-Forensics: What can we do ?

Time, ressources and better software

- **More reliable and precise software**
  - Development of **more robust** tools
  - Make irregularities clearly visible, more debug information
  - **Check routines**, which check and warn for known anti-forensics issues and other abnormalities
  - Heuristics, which can defuse certain attacks
- *Forensics software should not just be checked for the capability of finding evidence, but also for the reliability and robustness of the software itself!*

Anti-Anti-Forensics: What can we do?

From an academic perspective

- **Acquire more knowledge about raw data and artefacts**
- Less focus on specific tools and their handling
- Don't encourage or promote magic-button „nintendo forensics“

Lessons learned, future work?

- IT forensics in relation to IT security rather „uncemented“
- Old stuff (XSS) coming back and shining again
- The demands on correct methods and correct results are very high
- Little problems can cause fatal results (exculpatory file overseen?)
- Probably lots of weaknesses in forensics software have not been found yet...
- Experts in IT forensics and software developers have to work more carefully and with more awareness

Lessons learned, future work?

- Forensic Tool Testing (Computer Forensics Tool Testing – NIST)
- Further research: evaluate more tools in a more thoroughly manner with broader and deeper simulated attacks
- Develop a clear taxonomy and a systematic catalogue of testing scenarios and methods
- Training station for simulated cases of live forensics
    - A specially prepared Linux system (hidden anti-forensics kernel module)
    - Several traps which will perform typical and new techniques in anti-forensics
    - Our aim: gain a better insight from an examiners perspective and build up routine

Questions? / Contact

Questions? Hints? :-)

- Thank you!
- Contact:
  - Martin Wundram
  - wundram@tronicguard.com, wundram@digitrace.de
  - Phone: +49 (179) 213 82 67
  - Www.tronicguard.com Www.digitrace.de
  - Cologne/Düsseldorf

TG TRONICGUARD

DigiTrace
Kompetenz in IT-Forensik