Erste Hilfe in Digitaler Forensik

Dr. Dirk Wetter, (http://drwetter.de)

Hamburg

GUUG-Frühjahrsfachgespräch 2008, München 11.-14.3.2008

Agenda

I. Motivation

II. a. Was ist Forensik

b. Arbeitsweise in der Digitalen Forensik

III. Verdacht erkennen + erhärten

IV. Beweissicherung

Motivation

- Ersthelfer am „Unfallort“
  - keine Computerforensiker
  - meistens Admins wie „Du und ich“
- Einige „Hilfeleistungen“
  - falsch
  - nicht wiedergutzumachen

Grundlagenvortrag

- Methodik: Erkennen, Erhärten, Daten sichern
- Handwerkszeug Kommandozeile
- hier: Beschränkung auf
  - PC-Hardware unter Linux
  - OSS-Werkzeuge
- einfache Problemstellung, keine:
  - RAID-Rekonstruktion
  - DB-Forensik,
  - neuesten Rootkit-Technologien

Begriff Forensik

- Wikipedia:

  „*Unter dem Begriff Forensik werden die Arbeitsgebiete zusammengefasst, in denen systematisch kriminelle Handlungen identifiziert, analysiert oder rekonstruiert werden*.“

Begriff Forensik

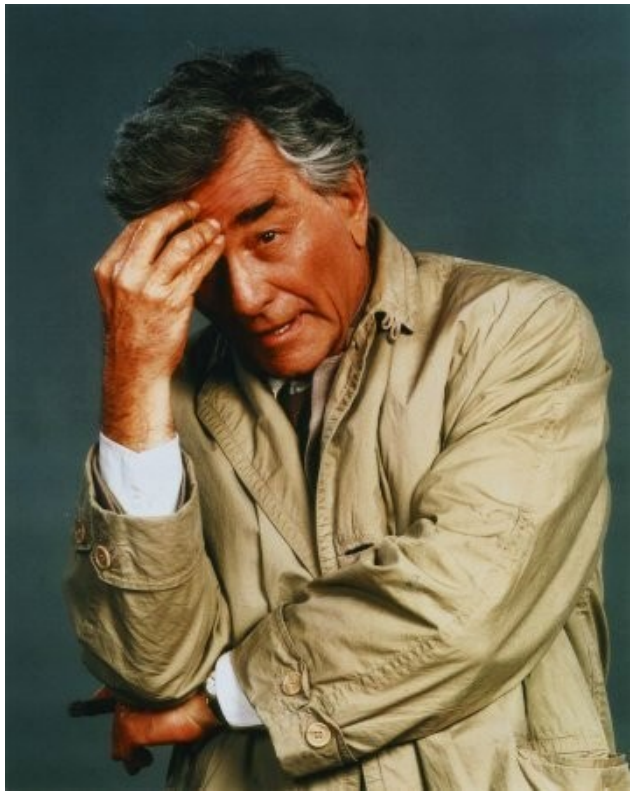
- Wikipedia:

  „*Unter dem Begriff Forensik werden die Arbeitsgebiete zusammengefasst, in denen systematisch kriminelle Handlungen identifiziert, analysiert oder rekonstruiert werden.*“

  - systematisch
  - kriminell
  - identifizieren
  - analysieren / rekonstruieren

Schlussfolgerung

- Es geht um *Digitale Beweise*
- kriminell:
  - gerichtliche Verwertbarkeit
- Zum Zeitpunkt der Entdeckung:
  - kein Wissen über Täter
    - intern / extern
    - Motivation
  - oder Schaden für die Firma



Methodik Hintergrund

- **Beweiskette** (Chain of Custody) für Gericht
  - Strafverfahren
  - Zivilansprüche
- Nachvollziehbarkeit für Nicht-Profis
- vier Augen beweisen mehr ... → Zeuge(n)
- Gerichtsfestigkeit:
  - Versetzen in die Rolle des Beschuldigten/Angeklagten

Umgang mit Beweisen

- sorgfältig!
- Digitale Beweise in der Live Response:
  1. Volatile Daten sichern
  2. Duplikation von Festplatte(n)
- sicheres Aufbewahren v. Original und Duplikat

Dokumentieren! (Wer, wann, was, wo, wie)

Dokumentieren!

Dokumentieren!

Dokumentieren!

Dokumentieren!

Dokumentieren!

Dokumentieren!

15:08:35

Dokumentation, technisch

- „5 x W“: Wer, Wann, Was, Wo, Wie

- Technische Hilfen, Papier!

cmdline	Papier
`date` (2x)	Ausdruck/Notiz mit Datum/Ort
`script`, `screen -L`	Unterschrift (2x)
`Prüfsummen`	Seitennummierung

„Incident Handling“

- Firma+Admin: Einen **Plan/Strategie** haben!
  - Firma
    - Sicherheit:
      - > keine ausschließlich techn. Angelegenheit
      - > Incident Handling erst recht nicht
    - Prozesse!
  - Admin
    - Erfahrung, Wissen, Voraussicht
    - technischer Ablaufplan

• Schadensausmaß Firma
• Risiko: Weiterbetreiben/ Runterfahren

15:08:35

Firma

- Notfallkonzept/Incident-Management-System
  - Organisat. Rahmenbedingungen
    - allgemein: Sicherheitskonzepte
    - Verantwortung
  - Prozesse
    - Meldung,
    - Handling (Entscheidung, wer was wie tut)

- BSI-Grundschutzkataloge
- (BSI 100-1: Aufbau eines ISMS)

BSI-Grundschutz, Bausteine

- B 1.3: Notfallvorsorge-Konzept
  - Planung/Konzeption
  - wie wichtig ist die betr. Komponente/sind die Daten?
  - CIA: normal, hoch, sehr hoch
- B 1.8: Behandlung von Sicherheitsvorfällen
  - Angemessen, Gefährdungslage
  - Schaden für die Firma (Betrieb, gespeicherte Informat.)
  - Lesenswerte schlechte Konstellationen:

    G 2.62, G.2.66, G 2.106

BSI-Grundschutz, Maßn.

- M 6: Maßnahmenkatalog Notfallvorsorge
  - Notfalldefinition, Verantwortlich im Notfall (M 6.2, M 6.7, M 6.59)
  - Notfallhandbuch (M 6.3)
  - M 6.58: Information an Leitungsebene
  - Meldewege (M 6.60), Eskalationswege, betroffene Stellen (M 6.65)
  - Nachbereitung von Vorfällen (M 6.63, M 6.66)

15:08:35

Kleine Lehre d. Versteckens

- erstes Rootkit: ~1990 für SunOS 4.1.1
- Rootkit manipuliert + versteckt:
  - Prozesse
  - Verzeichnisse, Dateien (Binär, Libs, Logs!)
  - Sockets
  - RAM
- Hintertür zur Fernsteuerung
- automatisiert: Exploit, Verstecken, Steuerung
- gezielt / Innentäter

Artenvielfalt Rootkits

- selten: reines User-Level-RK
  - zahlreiche Spuren
  - Hip: Ausnutzen löchriger PHP-Skripte
- häufiger: Kernel-RK
  - Kernel-Modul, `/dev/kmem` (Urvater SucKIT)
  - Umlenken syscalls –> Sichtbarkeit Netz, Dateien
  - Nur „imperfections“ live im Dateisystem zu finden

Artenvielfalt Rootkits

- weitere Klassifizierung: resident und nicht-resident
  - *memory-based* RK
    - „Zecke“ (Tobias Klein)
    - Shadow Walker

- Speicherbereiche sichern!

Anomalien

- Erkennung nicht trivial
  - IDS/Integritätschecker (Host, Netz)
  - Log-Meldungen
    - Art, Tageszeiten, fehlende
    - Proxy (Nachladen Exploit); Mail-Server: Spam
  - Netz
    - Verbindungen: Peers, Anzahl
    - Volumen, Art: Netflow, Firewall, NIDS ...
  - Status (PROMISC, fehlerh./fehlende Dateien)
  - „komische“ Dateien/Verz. Prozesse, Sockets

15:08:35

Beispiele

- **». « ».. « »...«**
- **/dev/ida /dev/.hdd , /dev/sdr0, /dev/caca**
- **/dev/proc/fuckit/**
- **/lib/security/.config/**
- **/usr/info/.t0rn/, /usr/src/.puta/,**
- **/usr/bin/ssh2d**
- Prozess **[kswap0]** mit owner www-data
- Ports 31337, 6666, 6667, (und alle erdenklich anderen)
- **core (file core!)**

Netz: minimal invasiv

- Mirror Port
- „Hubbing out“
- MITM: `ettercap` , C&A
- `nmap` (Backdoor)

- Problem:
  - Tageszeit des Netzwerkverkehrs
  - Verschlüsselung (immer häufiger)

Am System: invasiv

- zwei der Ziele bei späterer P.-M.-Analyse
  - Auffinden gelöschter Dateien
  - Timeline-Analyse:
    - Rekonstruktion: **wann was** passiert ist
    - atime, mtime, ctime, ggf. del time

- d.h. jeder Zugriff ab nun (Erhärtung/Sicherung) zerstört u.U. Beweise bei der P.M.!

Am System: Vorsicht...

- ... ist die Mutter des Forensikers
  - ~~`find / | xargs strings h8ckm3 >/sbin/datei.log`~~
  - `mount -o remount,noatime <dir> (ggf. ro)`
- Vertraue dem System nicht!
  - Binaries
  - Libs
  - Kernel

→ Externe Tools!

- statisch gelinkt:

```
pwned:/mnt/Static-Binaries/linux_x86 0# ./ldd uptime
        not a dynamic executable
pwned:/mnt/Static-Binaries/linux_x86 1# ./file uptime
uptime: [...], statically linked, stripped
```

- woher?
  - CD/DVD (manipuliersicher)
  - USB-Stick (-Platte)
  - falls vorhanden und eingehängt (ro!):
    - NFS, Samba, AFS, iSCSI
  - Server: ggf. rüberkopiertes Verzeichnis (Manipulation)

Womit?

- Helix:
  - www.e-fense.com/helix (GPL)
    - The Sleuth Kit (TSK)
    - The Coroners Tool Kit (TCT, tctutils)
    - u.a.
  - Drei Zwecke:
    - Beweis erhärten
    - Volatile+nicht volatile Daten sichern (Live Response)
    - Post-Mortem-Analyse
  - keine Solaris-Bins mehr (Windows: ja)
  - (`procget`), `pcat`, `pd`
  - selbst erweitern!

Am Anfang war ...

- schön aus Sicht der Digitalen Forensik: offene Konsole
- Vorbereitung
  - ggf. `mount <Tools> /mnt`
  - `PATH=/mnt/Static-Binaries/linux_x86; HISTFILE=/dev/null`
  - `env` inspizieren! (ggf.: `unset LD_LIBRARY_PATH LD_PRELOAD`)
- Netz / Status
  - `lsof (-i) -Pn / netstat -atupn`
  - `last -aix / who -a / ps -efwly`
  - `ifconfig | grep PROMISC`

15:08:35

Nützlich

- Dateien
  - fehlt `MARK` im Syslog (läuft Dämon?), `dmesg` inspizieren
  - `ls -la ~/.*history*` (Länge Null? Link `/dev/null`? Anschauen!)
  - `~/.viminfo`
  - `ls -aulrtF` / `ls -alrtF`
  - `rkhunter` et al. (`noatime`!)
  - `/bin/rpm -Va`, `debsums -s` für Debian-Dialekte (`noatime`!),
    - beides lokale DB: *Nur Anhaltspunkte!*

Prozess Firma

- ok. Jetzt weiß ich: Rechner ist kompromittiert.
- Und nun?

- Incident-Managementplan
  - Info an Leitungsebene
  - Anweisungen abwarten
  - forensische Datensicherung a.k.a. Live Response

Technisch: Daten sichern

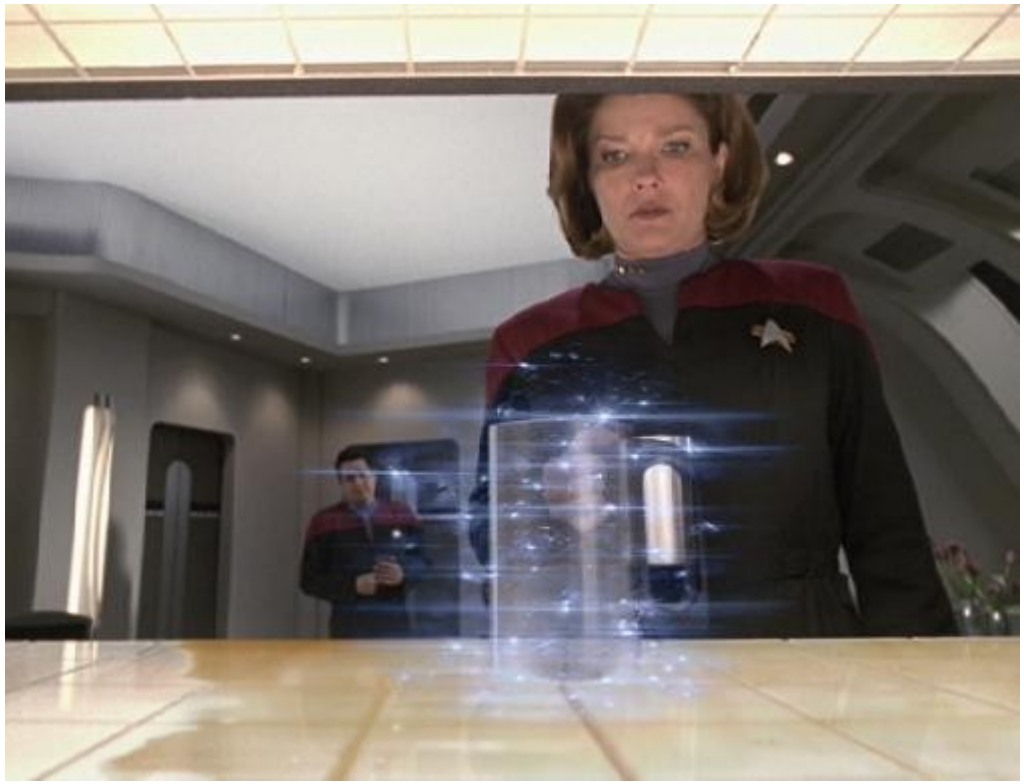
1.) Volatile Daten

2.) Rechner außer Betrieb

3.) Forensisches Duplikat

- „Dead Acquisition“

- 3 vor 2:
  - „Live Acquisition“
  - nur wg. Plattenformat
  - Skepsis wegen Kernel



Wie?

- Anzahl Kommandos i.d. Reihenfolge der T½
  - Ausgaben:
    - Stempel korrektes Datum (Tag+Uhrzeit)
    - „Hinreichende“ Prüfsummen:
      - (`md5sum,md5deep`), `sha1/sha1deep`,
      - am besten: `sha256deep`

- **Skript**
  - Helix-CD
  - ähnliches bzw. eigener Werkzeugkasten

15:08:35

GUUG-Frühjahrsfachgespräch 2008 in München, 11-14.3.2008, © Dr. Dirk Wetter

Skript

- Vorsicht Helix: `linux-ir.sh`
  - sichert überflüssigerweise nicht-flüchtige Daten
  - MD5-Summen ohne `noatime`
  - vergisst einiges

- besser, nicht ganz perfekt
  - iX 7/2007: http://computer-forensik.org/tools/ix/
  - oder: http://software.drwetter.de/ir/

15:08:35

Skript: Was alles?

- RAM
- Anderes Volatiles, Neustart=Verlust
  - Info + Status
  - Verschlüsselte Dateisysteme (!) → manuell!
  - (ggf. Swap, `/tmp`) → manuell!

Skript: Was alles?

- **`date`** (Uhrzeit/Datum korrekt?)
- `PATH=/mnt/Static-Binaries/linux_x86:/usr/bin:/bin:/sbin:/usr/sbin`
- `HISTFILE=/dev/null`
- `env, unset LD_LIBRARY_PATH LD_PRELOAD`

- Platte: `df -kT`, `mount -l`, `pv/vg/lvdisplay`, `mmls`
- Prozesse: `ps -eflwy`, `lsof -Pn`, `top -cbn1`
- Netz: `ifconfig -a`, `arp -a/-n`, `netstat -atunp`, `lsof -i -Pn`, `iptables-save`
- Status: `uptime`, `dmesg`, `sysctl -A`

15:08:35

Skript: Was alles?

- `/proc/kcore`, `/dev/(k)mem` : `memdump` (TCT)
- `/proc`:
  - `modules`, `cmdline`, `version`, `kallsyms`, `swaps`, `mount`, `devices`, `uptime`, `diskstats`, `misc`, ...
  - jeden einzelnen Prozess: `/proc/[0-9]*/*` (`pd`, `pcat`)
- geht immer & spart Platz: `gzip -c`
- ggf.: Krypto-Dateisysteme, `/tmp`, swap sichern
- Prüfsumme(n) und Datum nicht vergessen!
- Ausdruck, Unterschrift

Wohin Ausgabe?

- Netz | (externe) Platte
  - Platte:
    - USB/Firewire (ext. Platte, -Stick: Platz Hauptspeicher)
      - > Einfach
      - > Zugänglichkeit
  - Netz
- Vorsicht: /dev/stderr! (Skriptaufruf)

15:08:35

GUUG-Frühjahrsfachgespräch 2008 in München, 11-14.3.2008, © Dr. Dirk Wetter

Wohin, Netz

- `fws:/forensik/case1 0#` **`netcat -lp 42 >datei.txt`**
- `pwned:~ 0#` **`cat /proc/version | netcat fws 42`**

- Nachteil:
  - `netcat`: unverschlüsselt/-authentifiziert
  - besser:
    - `cryptcat` (`-k` *`passphrase`*) (Twofish)
    - `socat`: sehr mächtig, X509-Key-Auth sinnvoll* (–> OpenSSL)
    - [`sbd`, `aes-netcat`, `ncat` (Proxy, AES, ...)]

* prinzipiell auch mit `openssl s_client -connect` *`host:port`* plus server

Generelles

- Runterfahren:
  - Fasst Hunderte von Dateien an (`atime`)
  - Modifiziert nicht wenige (`*.pid`, `*log`, ..)
  - Unvorhersagbar: Reallozierung Platz gelöschter Dateien
- Ausschalten:
  - Dateisysteme unsauber (erschwert stellenw. Analyse)
  - Durch **Netzstecker**, nicht „Power“-Knopf!
  - ggf: SysRq-[S,S,U,O] (ggf `sysctl -w kernel.sysrq=1`)
  - serielle Konsole: SysRq-[T,Q,P] : sichern

Was?

- Die ganze Platte! („mindestens“, s.u.)
- Profis: Write Blocker
- Nicht partitionsweise!
  - Lücken, (absichtlich) unbenutzte Bereiche
- Besser `mmls` als `*fdisk`
  - Übersichtlichkeit
  - Lücken
- Demo!

Was?


```
fws:~ 0# mmls /dev/sda
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
[...]
21:  -----   0196780186   0196780247   0000000062   Unallocated
22:  07:00   0196780248   0213552044   0016771797   Linux LVol.Manager (0x8e)
23:  -----   0213552045   0234441647   0020889603   Unallocated
```

Demo: Zylinderlücke (21)

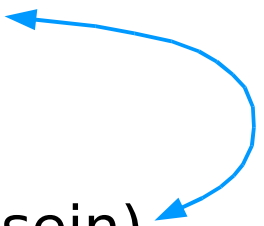

```
pwned:bin 0#
pwned:bin 0# dd if=/dev/sda skip=0196780186 count=62 | xxd -c 32 | cut -d' ' -f1,10-100 | head
-20
62+0 Datensätze ein
62+0 Datensätze aus
31744 Bytes (32 kB) kopiert, 0,000355064 s, 89,4 MB/s
0000000: 2320 2020 2023 2020 2023 2323 2320 200a   ####   #    #  #    #   ####  .
0000020: 2320 2020 2023 2020 2320 2020 2023 200a  #    #  #    #  #    #  #    # .
0000040: 2320 2020 2023 2020 2320 2020 2020 200a  #       #    #  #    #  #      .
0000060: 2320 2020 2023 2020 2320 2023 2323 200a  #  ###  #    #  #    #  #  ### .
0000080: 2320 2020 2023 2020 2320 2020 2023 200a  #    #  #    #  #    #  #    # .
00000a0: 2023 2323 2320 2020 2023 2323 2320 200a   ####    ####    ####    ####  .
00000c0: 2020 2020 2020 2020 2020 2020 2020 200a                                 .
00000e0: 2020 2020 2020 2020 2020 2020 2020 200a                                 .
0000100: 2020 2020 2020 2020 2020 2020 2020 200a                                 .
0000120: 2320 2020 2020 2020 2323 2323 2323 230a  ######  #     # #       #######.
0000140: 2320 2020 2020 2020 2020 2020 2023 200a  #     # #     # #             # .
0000160: 2320 2020 2020 2020 2020 2020 2320 200a  #     # #     # #           #  .
0000180: 2320 2020 2020 2020 2020 2023 2020 200a  ######  #     # #         #    .
00001a0: 2320 2020 2020 2020 2020 2320 2020 200a  #   #   #     # #       #      .
00001c0: 2320 2020 2020 2020 2023 2020 2020 200a  #    #  #     # #         #     .
00001e0: 2323 2323 2323 2320 2323 2323 2323 230a  #     #  #####  ####### #######.
0000200: 0000 0000 0000 0000 0000 0000 0000 0000  ................................
0000220: 0000 0000 0000 0000 0000 0000 0000 0000  ................................
0000240: 0000 0000 0000 0000 0000 0000 0000 0000  ................................
0000260: 0000 0000 0000 0000 0000 0000 0000 0000  ................................
pwned:bin 0#
pwned:bin 0#
pwned:bin 0#
pwned:bin 0#
```

15:08:35

Demo: „Ex-Partition“ (23)

Kopie der ganzen Platte

- Frisches Dateisystem auf Sicherungsplatte
- Einhängen (hier `/mnt`)
- **`D=/mnt/mmls_hdX_`date +%F,%T``**
- **`mmls /dev/hdX >$D; $sum $D > $D.$sum`** Liste Partitionen
- **`$sum /dev/hdX >/mnt/hdX.$sum`** Prüfsumme Platte
- **`$dd if=/dev/hdX >/mnt/hdX.img`** Duplizieren Platte
- **`$sum /mnt/hdX.img`** (sollte gleich sein) Prüfs. Duplikat



- `$sum`: (`md5sum`), `sha1`/`sha1deep`, `sha256deep`
- ggf. durch `gzip`-Pipe

dd=Disk Dump

- Standard-Blockgröße 512 Bytes ist zu(?) langsam, aber sicher
  - „Standard-`dd`“ (fileutils): `conv=noerror`
  - `sdd` (Schily): „verbessertes dd“, schneller
  - `dd_rescue`: besser bei Lesefehler und Spulen (Kurt Garloff @ Suse)
  - `GNU ddrescue`
  - `rdd` (NFI): toleranter Lesefehler, Netzübertragung+Split
  - `dcfldd (dccidd)`
    - `-hash=md5|sha1|sha256..sha512` (`-hashlog`), `-status`
    - Sinnvoll: `{hashlog,errorlog}=`*`Dateiname`*
  - `dc3dd`: Neu, Patch zu GNU `dd`, Features ähnlich `dcfldd`

Mein Favorit: dcfldd

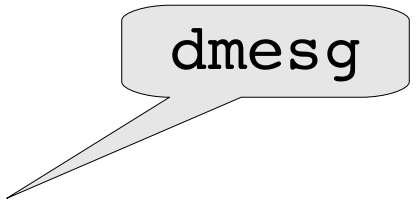

```
host:~|0% dcfldd if=/dev/urandom of=/dev/null count=768 \
  hash=sha256
256 blocks (8Mb) written.
512 blocks (16Mb) written.
768 blocks (24Mb) written.Total (sha256): 70554677ac031d-
  d45da2b9de6ba3fe8661c8d75af8aa61d65b479f6143284f55

768+0 records in
768+0 records out
host:~|0%
```

15:08:36

Reicht dd?

- Nein, Hidden Data Areas:
  - ATA HPA




```
ata6.00: Host Protected Area detected:
         current size: 976772168 sectors
         native size: 976773168 sectors
ata6.00: ATA-8: ST3500320AS, SD15, max UDMA/133
```

    - `disk_stat` (TSK), `hdparm -N`
    - hpafs (fuse), fiesta, hpatools
    - Thinkpad default: #40-Serie, X61, ... („Predesktop Area“)
  - weitere:
    - ATA DCO
    - marked bad blocks: hdparm 8.1! :-)

Weiteres

- Nun:
  1. Original-Beweis sicherstellen
  2. Post-Mortem-Analyse,

     Kopie von der Kopie (Arbeits-Disk, Case-Disk)

- Zeitgleich/danach:
  - Rechner neu aufsetzen
  - Neue Passwörter
  - Konsequenzen aus P.M. schließen! (BSI GsKat. M 6.66)
    - Stimmen Prozesse, Sicherheitsleitlinien, Technik, Maßnahmen?

Danke für die Aufmerksamkeit! Fragen?

Dirk Wetter
mail@drwetter.de

Sicherheitsanalysen, Digitale Forensik

GUUG-Frühjahrsfachgespräch 2008, München 11.-14.3.2008