Fachgruppe Elektronik und EDV im BVS
Herbsttagung 2003 im Bundesministerium für Wirtschaft und Arbeit

Holger Morgenstern:

Open Source Computer Forensic Tools

Who is this guy?

- Ein Neuer aus dem Süden
- Region Bodensee-Oberschwaben
- Seit 2002 ö.b.u.v. Sachverständiger für „Systeme und Anwendungen der Informationsverarbeitung“
- Seit 1988 im „EDV-Geschäft“
  - Softwareentwicklung (C, C++, Java, VO, Clipper, DBMS, FP [Lisp, Miranda, Haskell…],…)
  - Hardwarevertieb und Support
  - Entwicklung internetbasierter Systeme (J2EE, Webservices, Usertracking / monitoring, eLearning, …)
  - Beratung
- Kontakt: http://www.gutachten.info/
  morgenstern@gutachten.info
  Tel. 07574-91401 / Fax 07574-91403

Computer Forensik – eine Definition

- *„Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.“* *(© 2003 DIBS USA Inc)*

- Vier Prinzipien der Computer Forensik:
  - Datenverluste minimieren
  - Alles aufzeichnen, nichts verändern
  - Analysen nur auf Kopien durchführen (*never touch original*)
  - Ergebnisse neutral, überprüf- und nachvollziehbar präsentieren

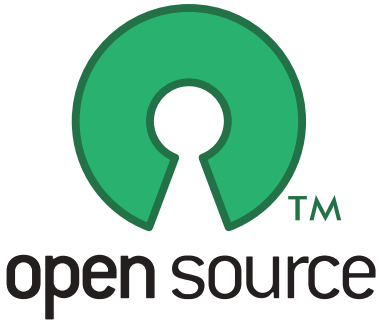
Der Computer Forensik Prozess

- Erstellen eines forensisch korrekten Abbilds der elektronisch gespeicherten Daten (*forensic sound imaging*)
- Authentifizierung des Abbilds
- Analyse der gespeicherten Daten
- Berichterstellung und Gutachten

Computer Forensik Tools

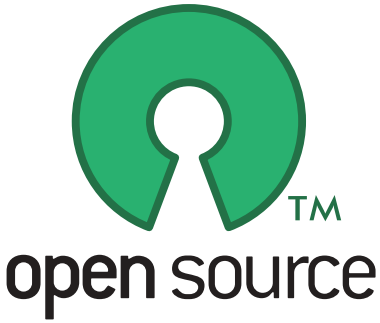
- Imaging Bereich
  - Forensische Hardwarelösungen
  - Softwaretools (Backup- / Deploymentbereich)
  - Forensische Imaging Software
- Analyse Bereich
  - Hex-Editor + Experte immer noch das Beste
  - Explodierende Speichergrößen / Datenmengen, erfordern effiziente Tools zur (Vor-) Analyse und Automatisierung von Abläufen

Was spricht für



- Ein paar K.O.-Fragen:
  - Macht Ihre Software Fehler?
  - Woher weiß ich, dass Ihre Software das tut, was sie sagt, das sie tut?
  - Können Sie persönlich validieren, was im Einzelnen mit den Daten gemacht wurde?

Was spricht für



- Überprüfung der Korrektheit durch Dritte (*peer-review*) wesentlich erleichtert
- Einblick in alle technischen Aspekte möglich (Lerneffekt)
- Erweiterungen und Spezialisierungen prinzipiell selbst durchführbar (*beat the tool!*)
- In der Regel wesentlich schnellere Beseitigung von Schwachstellen

Einige Vorteile von Linux als Forensische Plattform

- Alles, einschließlich Hardware, ist eine Datei
- Support für sehr viele Dateisysteme (40+)
- Dateien (➔Images) als *loopback device* mounten
- Sichere, minimal invasive Analyse eines *Live Systems* (keine Hard- oder Software *writeblocker* nötig)
- Umleitung von Standard output nach input (*command chaining*)
- Monitoring und Logging von Prozessen und Kommandos

Einige Vorteile von Linux als Forensische Plattform

- Möglichkeit den Sourcecode des Systems und der meisten Werkzeuge einzusehen
- Einfache Möglichkeit der Erstellung von schreibgeschützten, bootbaren Medien (Disketten, CDs, USB-Sticks) ➔ Leichte Herstellung einer vertrauenswürdigen Umgebung
- Ein „Out-of-the-box-Linux“ bringt schon sehr viele, für forensische Zwecke nutzbare Werkzeuge mit
- Der Preis ☺

Forensic sound imaging - Anforderungen

- Jedes bit der Quelle muss 1:1 (*raw)* und unabhängig vom logischen Dateisystem abgebildet werden
- Lesefehler müssen robust und nachvollziehbar behandelt werden
- Die Quelle darf keinesfalls verändert werden
- Prozess muss einer Überprüfung standhalten und reproduzierbar gleiche, durch Dritte verifizierbare Ergebnisse liefern
- In den USA müssen entsprechende Tools einen “legal test for reliability” bestehen. (➔http://www.cftt.nist.gov)
- In Deutschland ???

Forensic sound imaging - Anforderungen

- Gängige Tools aus dem Backup- und Deployment-bereich erfüllen diese Anforderungen nicht unbedingt
  - Norton Ghost markiert die Quelle u.U. als Ghost-Laufwerk
  - Drive Image interpretiert die logische Struktur und bricht bei Fehlern (z.B. bei defekter Partitionstabelle) ab
  - „SmartSector“ Funktionen dürfen keinesfalls benutzt werden
- Auch spezielle Forensik Komplettlösungen erfüllen die Anforderungen nicht komplett
  - EnCase: 3 Anomalien
  - SafeBack: 4 Anomalien
- Einzig dd (in der BSD Variante) erfüllt bisher alle Anforderungen
  - Linux kann im Moment nicht auf den letzten Sektor zugreifen, falls dieser ungerade ist

Forensic sound imaging: dd

- dd ist in den meisten Unix Distributionen enthalten
- Ursprünglich ein Tool zum Kopieren, Konvertieren und Formatieren von Textdateien
- Da in Unix alles eine Datei ist, kann dd als Nebeneffekt forensisch korrekte Abbilder von allen Medien, die das Betriebssystem erkennt, erstellen

Forensic sound imaging: dd

- Eigenschaften von dd
  - low-level-command
  - Kopiert bit für bit
  - Kennt die Struktur der Daten nicht
  - Kopiert
    - Dateien
    - Teile von Dateien
    - Partitionen
    - Logische und physikalische Platten, Disketten, Sticks, Bänder
    - Von Standard input nach output
- Dcfldd
  - Vom *DoD Computer Forensic Lab* erweitertes dd
  - Analoge Kommandozeilen Parameter
  - Integriertes MD5 Hashing auf Blockbasis

Forensic sound imaging: dd

- Typische Parameter:
  - if=device (input file oder device)
  - of=device (output file oder device)
  - bs=# (block size für eine I/O operation)
  - count=# (Anzahl zu kopierender Blöcke)
  - skip=# (Anzahl Blöcke, die am Anfang übersprungen werden
- dcfldd
  - hashlog=hashfile.txt
  - hashwindow=1024 (*hash every 1024 bytes*)

Forensic sound imaging: dd

- Einige typische Unix devices
  - /dev/fd0 (floppy)
  - /dev/st0 (tape)
  - /dev/hda erste IDE Festplatte
    - /dev/hda1 erste Partition dieser Platte
  - /dev/hdb zweite IDE Festplatte
  - /dev/sda erste SCSI Festplatte
    - /dev/sda1 erste Partition dieser Platte
  - /dev/sdb zweite SCSI Festplatte

Forensic sound imaging: dd

- Vorbereitung Zielmedium säubern (umstritten, aber sicher ist sicher ;-)
  - # dd if=/dev/zero of=/dev/sdb
- MD5 Fingerprint des Quellmediums erstellen
  - # md5sum /dev/hdb >hash.txt
- 1:1 Kopie erstellen
  - # dd if=/dev/hdb of=/dev/sdb
- Quelle auf Veränderungen prüfen
  - # md5sum /dev/hdb >>hash.txt
- MD5 Fingerprint der Kopie erstellen
  - # md5sum /dev/sdb >>hash.txt
- Falls keine Lesefehler vorgekommen sind, sollten die drei MD5 Hashwerte übereinstimmen und es wurde eine forensisch korrekte 1:1 Abbildung erstellt

Forensic sound imaging: dd

- Image einer Quelle erstellen
  - # dd if=/dev/hdb of=/mnt/sdb/case4711/image
- Image Datei wiederherstellen
  - # dd if=/mnt/sdb/case4711/image of=/dev/hdb
- Image Datei splitten
  - Parameter count und skip benutzen, oder mittels split Kommando
- Mit bs „spielen“ um Performance zu steigern
- Tipp für den Bereich Datenrettung
  - dd_rescue
    - Funktion analog zu dd, aber leicht geänderte Parameter
    - Angabe von Start- und Stopppositionen
    - Quelle kann rückwärts gelesen werden
    - Soft- und Hard-Blocksizes definierbar ➔ sehr gute Performance, Fallback auf Hard-Blocksize um möglichst viele Daten zu retten
    - Fehlerhafte Bereiche können von beiden Seiten bearbeitet werden

Forensic sound imaging: dd

- Netcat
  - „Einfaches“ Unix Werkzeug zum Lesen und schreiben von Daten über Netzwerk Verbindungen (TCP oder UDP)
  - Kann als Client und Server eingesetzt werden
  - Leitet Standard input / output über das Netzwerk weiter
- Netzwerk dd mit Netcat
  - Server: # nc –l –p 31337 | dd of=/dev/sdb
  - Client (Image der zweiten IDE Platte):
    # dd if=/dev/hdb | nc –w 3 {serverIP} 31337
  - Speicherinhalt einer laufenden Windowssession sichern:
    # dd if=\\.\PhysicalMemory conv=noerror | nc {serverIP} 31337
  - Windows Versionen von dd, nc und anderen Forensik Werkzeugen sind ebenfalls als Open Source erhältlich

Forensic sound imaging: ODESSA

- *Open Digital Evidence Search and Seizure Architecture*
- Teilprojekt ODD – Open Data Duplicator
  - Client/Server Modell.
  - Forensische Duplizierung über ein LAN
  - Kann gleichzeitig Zusatzfunktionen auf den duplizierten Daten ausführen
  - Enthält Module für
    - Berechnung von Checksummen und Hashes
    - Ausführen von string searches
    - Extrahierung von Dateien anhand ihrer Header
- Aktueller Status
  - Source Code erhältlich
  - Entwicklung

Forensische Datenanalyse

- Normale Unix Werkzeuge
  - grep, strings, hexedit, lde, script…
- Vielzahl spezieller Recovery und Forensic Packages
- Drei besonders interessante werden im Folgenden kurz vorgestellt:
  - Sleuth Kit
  - Autopsy
  - Foremost

Forensische Datenanalyse: The Sleuth Kit

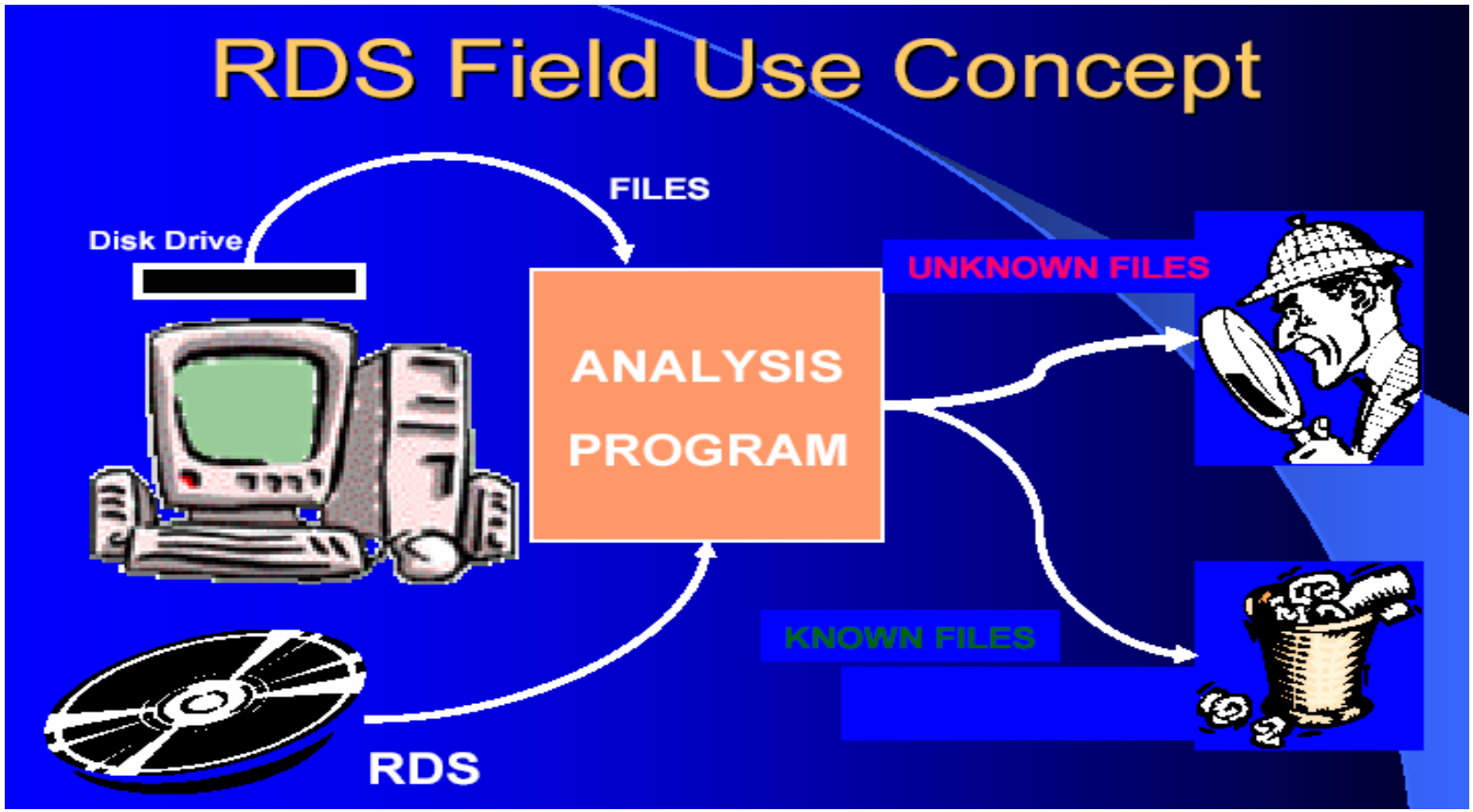
- Erweiterung von TCT (The Coroner's Toolkit and TCTUTILS)
- Sammlung von Unix Kommandozeilen Tools zur Forensischen Analyse von Dateisystem und Media Management
- Dateisystem Tools erlauben die Untersuchung von NTFS, FAT, FFS, EXT2FS, und EXT3FS
- Media Management Tools unterstützen DOS, BDS und MAC Partitionen sowie SUN Slices
- Können zur Analyse von mit dd erstellten Images genutzt werden
- Anzeige von detaillierten Dateisystemstrukturen
- Anzeige von allen NTFS Details und Inhalten (inkl. Alternate Data Streams)
- Erzeugung von Timelines der Aktivitäten im Dateisystem
- Ergebnisse können in Tabellenkalkulationen importiert werden (➔ Grafiken, Reports)
- Dateien können nach Typen organisiert ausgewertet werden

Forensische Datenanalyse: Autopsy

- Grafisches Interface zu den Sleuth Kit Tools (HTML basiert)
- Client/Server Modell
- Integriertes Case Management (Cases, Hosts, Images, Timezone, clock skew, Investigator)
- Detaillierte Datei und Inhaltsanalyse
- Keyword Suche (Vorherige Indexerstellung möglich)
- Metadaten Analyse
- Cluster Analyse
- Event Sequencer (Einarbeitung von zeitbasierten events aus IDS, Firewall, etc. Logs)
- Reports im ASCII Format ➔ Leichte Übernahme ins Gutachten
- Audit Logs inklusive Case Management Daten und exakten Sleuth Kit Kommandos
- Open Design, alle erzeugten Daten im raw Format ➔ leichter Einsatz von Zusatzwerkzeugen für spezielle Zwecke

Forensische Datenanalyse: Autopsy

- Zusammenarbeit mit den Hash Datenbanken der NSRL



➔z.B. Windows 2000 enthält 5933 bekannte Bilddateien ➔ ausschließen
➔erlaubt positive Identifikation von Hersteller, Produkt, Betriebssystem,…

Forensische Datenanalyse: Foremost

- Freies Forensik Tool für die Linux Plattform (völlig copyright-frei, da Arbeit der U.S. Regierung)
- Erlaubt die automatische Suche und Wiederherstellung von Dateien und Dateiteilen
- Unterstützt bit Images (dd) oder einen direkten Medienzugriff
- Basiert auf der Analyse von typischen Datei header und footer Paaren
- Suche frei konfigurierbar

Forensische Datenanalyse: Foremost

- Konfiguration erfolgt über die Angabe der für die Datei spezifischen Daten in einer frei editierbaren Konfigurationsdatei

```
# extension case size header footer
# GIF and JPG files (very common)
 gif y 155000 \x47\x49\x46\x38\x37\x61 \x00\x3b
 gif y 155000 \x47\x49\x46\x38\x39\x61 \x00\x00\x3b
 jpg y 200000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9
```

- Definitionen für Hunderte von Dateiformaten finden sich z.B. unter: http://www.wotsit.org
- Erzeugt eine Audit Log Datei mit allen relevanten Angaben zu Parametern, Image, Extrahierten Daten

Forensische Datenanalyse: Windows

- Einige Tools speziell für die Analyse von Windows Daten
- Galleta - A Internet Explorer Cookie Forensic Analysis Tool
- Pasco - An Internet Explorer Activity Forensic Analysis Tool
- Rifiuti - A Recycle Bin Forensic Analysis Tool

Open Source Computer Forensic
Where to start?

- Für viele Tools reicht ein normales Knoppix
- Enthält dd, dd_rescue
- Vorhandene Datenträger werden nicht automatisch gemountet
- Erhältlich unter http://www.knopper.net/

Open Source Computer Forensic
Where to start?

- Auch zum Einsatz spezieller Computer Forensik Tools kann (anfangs ;-) auf fertige CDs zurück gegriffen werden. Beispiele:
- Penguin Sleuth Kit Bootable CD
  http://www.linux-forensics.com/
- F.I.R.E
  http://fire.dmzs.com/
- Für alte Systeme können auch Boot-Disketten erstellt werden

- Fortlaufend aktualisierte Zusammen-stellung der Ressourcen und Tools demnächst unter:
  http://www.gutachten.info/forensik/