

IT-Forensik

Live Forensik

von

Michel Erbach

Tobias Banaszak

Fachhochschule Aachen

11.12.2009



Live Forensik

Inhalt

- ***Was ist Live Forensik?***
- Vorgehensweise
 - Beispiel
- Ausblick

Live Forensik

Live Forensik

- Definition „*flüchtige*“ Daten
- Definition Live Forensik
- Ausprägung
- Probleme
- Nutzen

Live Forensik

flüchtige Daten

„Nicht persistente Daten eines Daten verarbeitenden Systems, werden flüchtige Daten genannt. Diese sind in ihrer Lebensdauer extrem beschränkt, was im Regelfall durch einen häufigen Schreibzyklus auf dieselbe Speicherstelle oder Verlust durch Unterbinden der Stromversorgung beschrieben wird.“

Live Forensik

flüchtige Daten

- CPU Register
- CPU Cache
- CMOS
- RAM
- Festplattenpuffer
- Netzkartenpuffer
- Prozesslisten

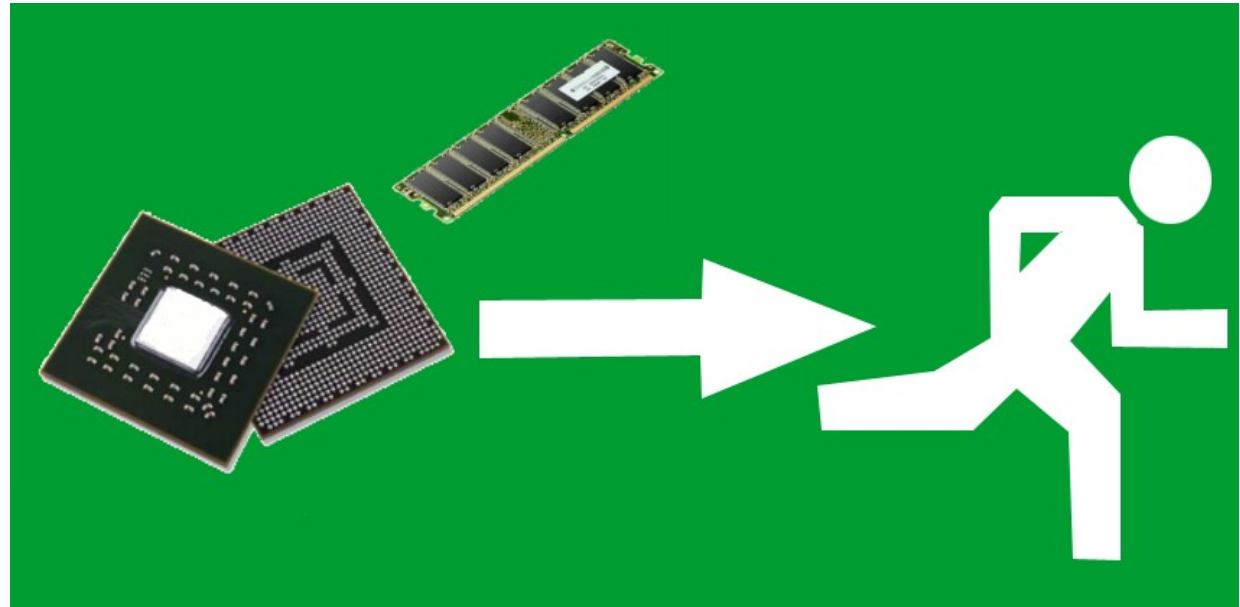
Live Forensik

Live Forensik

„Live Forensik hat als Ziel, die flüchtigen Daten eines Daten verarbeitenden Systems in einer nachvollziehbaren und wieder-verwendbaren Momentaufnahme für die eigentliche forensische Analyse und Interpretation zu sichern.“

Live Forensik

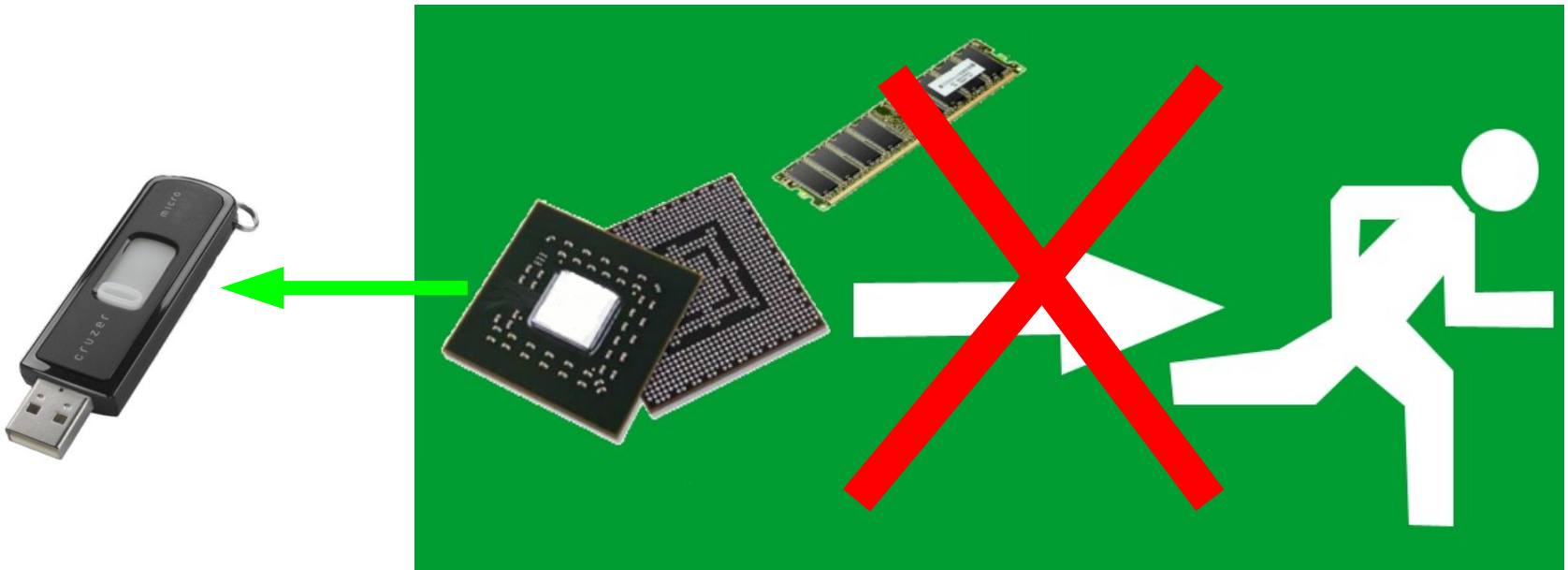
Live Forensik



So finden wir es vor...

Live Forensik

Live Forensik



So wollen wir es...

Live Forensik

Probleme

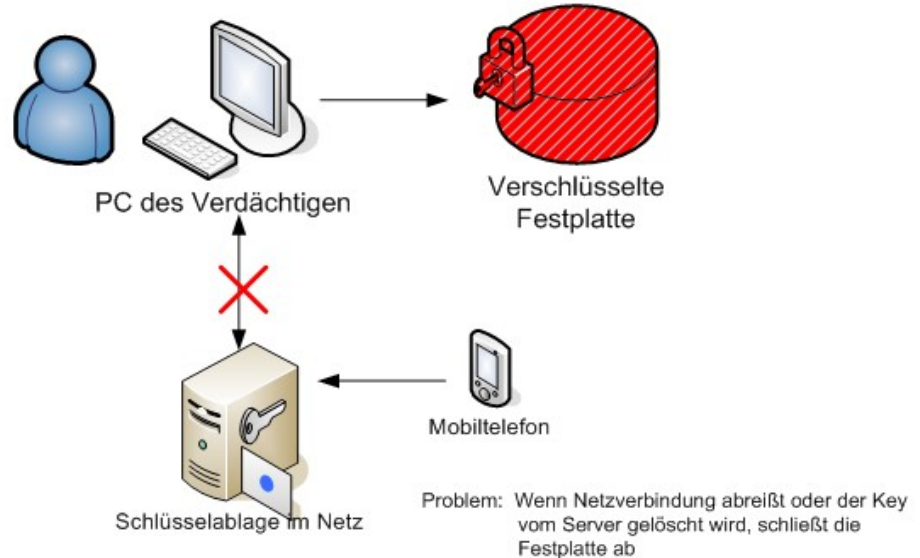
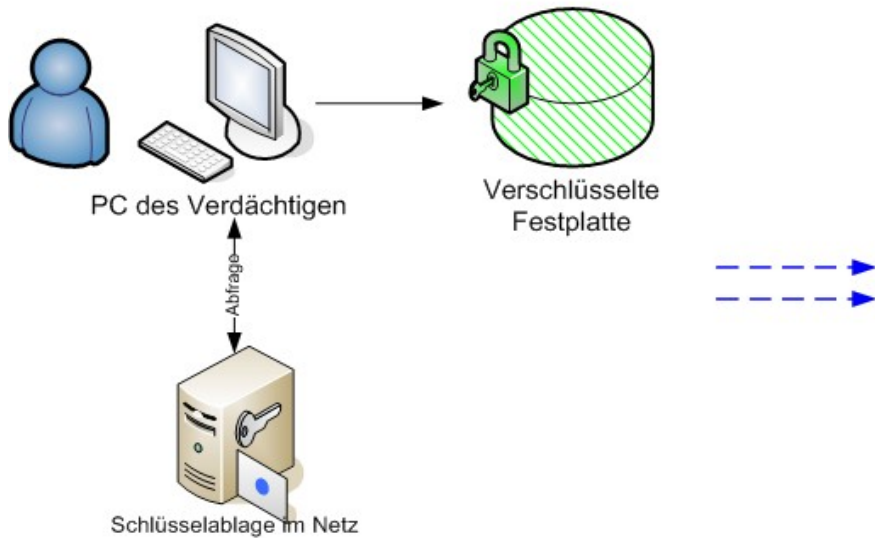
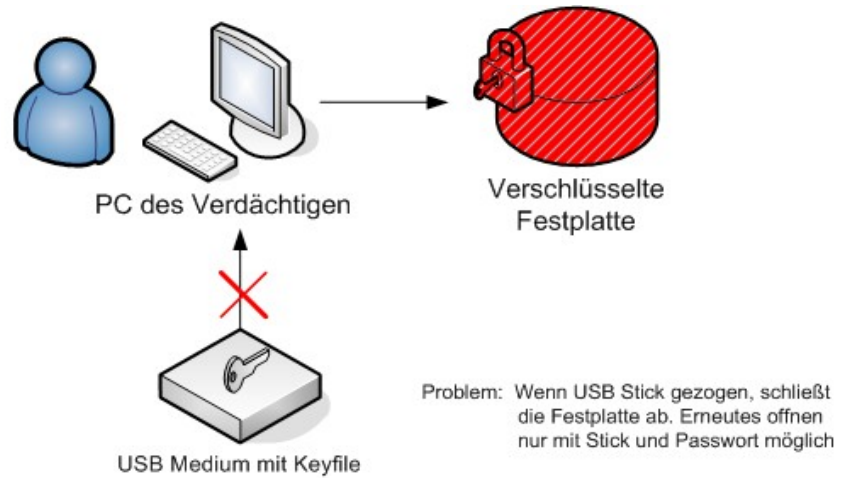
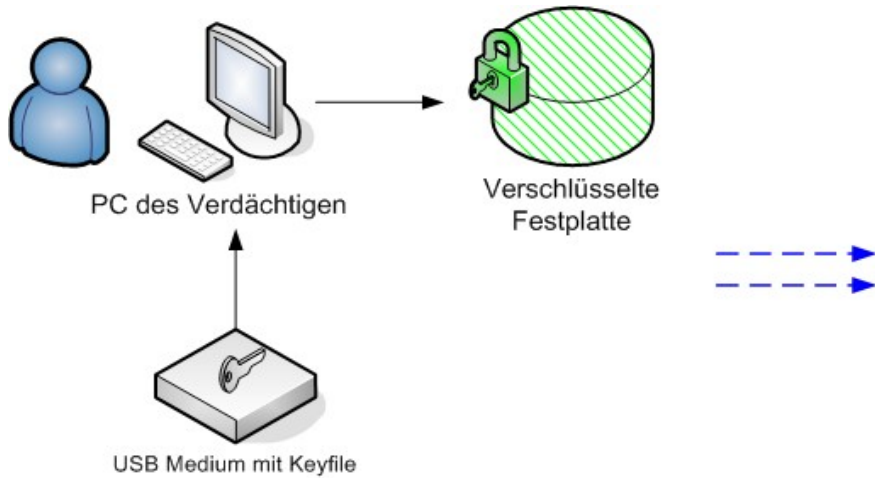
- Flüchtige Daten sind schwer zu fangen
- Manipulation bei Sicherungsvorgang
- Ungewollte Manipulation durch OS
- Ungewollte Manipulation durch Apps
- Manipulation durch Dritte
- Stromausfall kann alles beenden

Live Forensik

Nutzen

- Informationen sammeln, die die forensische Analyse unterstützen
- Informationen stehen ab dem Zeitpunkt der Gewinnung zur Verfügung
- Schmauchspuren der „Smoking gun“

Live Forensik



Live Forensik

Nutzen, z.B.

- Passworte oder Schlüssel im RAM
- Verbindungsdaten zu Servern
- Aktive Prozesslisten
- Besonderheiten in Log-Dateien
- Hinweise auf verborgene Inhalte
- Häufig benutzte / offene Dateien

Live Forensik

Inhalt

- *Was ist Live Forensik?*
- ***Vorgehensweise***
 - Beispiel
- Ausblick

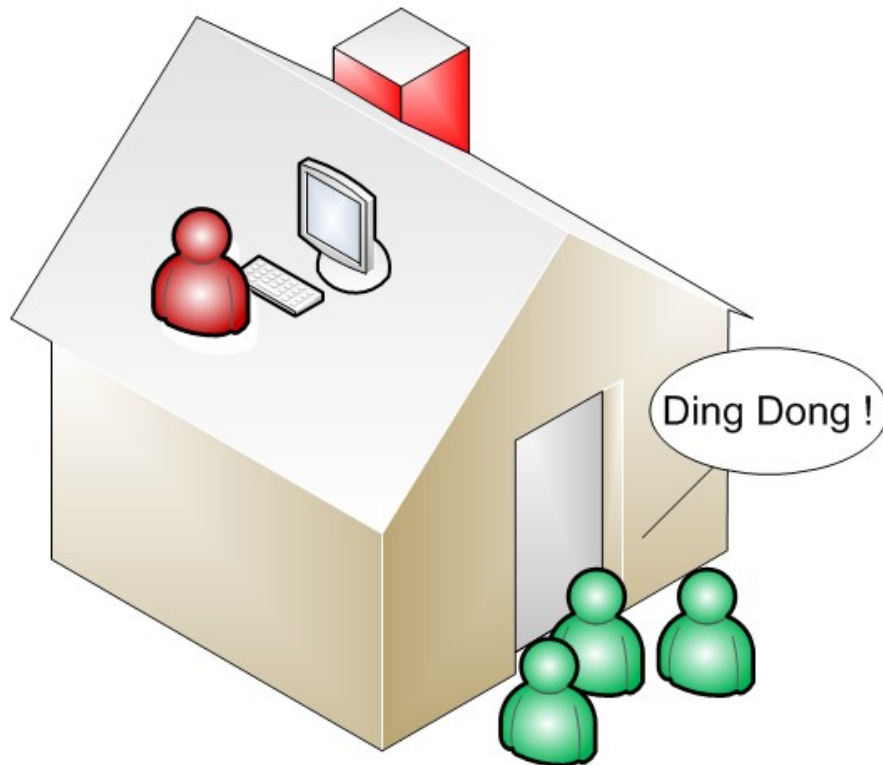
Live Forensik

Fokus

- Einzelrechner
- Heimumgebung
- Keine Virtualisierung
- Ggf. Festplattenverschlüsselung

Live Forensik

Fokus



Um 6:00 Uhr

„Polizei, guten Morgen.

Wir haben einen
Durchsuchungsbefehl.

Wir haben unseren
Computertypen mitgebracht.“

Live Forensik

Durchführung

- Was ist das Ziel der Ermittlung?
 - Antworten:
 - Wer?
 - Wann?
 - Warum?
 - Wo?
 - Was?
 - Wie?
 - Womit?

Live Forensik

Durchführung

- Wissenschaftliche Methoden und Analyse

Prozess der Beweisfindung

- Identifizierung
- Sicherstellung
- Analyse
- Präsentation

Live Forensik

Durchführung

„Spielregeln“

- Glaubwürdigkeit
- Reproduzierbarkeit
- Integrität
- Kausalität
- Akzeptanz der Methoden
- Dokumentation

Live Forensik

Durchführung

„Spielregeln“

- Glaubwürdigkeit
- Reproduzierbarkeit
- Integrität
- Kausalität
- Akzeptanz der Methoden
- **Dokumentation**

Live Forensik

Durchführung

Prozess der Beweisfindung

- Identifizierung
- Sicherstellung
- Analyse
- Präsentation

Live Forensik

Durchführung

Identifizierung

- Sachlage klären
- „Schlachtplan“ bereitlegen
 - Gefahren?
 - Was ist zu sichern?

Live Forensik

Durchführung

„Schlachtplan“

- „sterile“ Datenträger
- Kamera
- Dokumentationsbögen (Beweiskette)
- Verpackungsmaterial
- Instruktionen an Mitarbeiter
- Was muss mitgenommen werden?

Live Forensik

Durchführung

Sicherstellung

- „Schlachtplan“ durchführen
 - Fotos
 - flüchtigen Speicher sichern
 - Datenträger sicherstellen
 - Beweiskette

Live Forensik

Durchführung

Analyse

- Was sagen mir die gesicherten Daten?
- Versuchen die *W*-Fragen zu beantworten
- Viel Fachwissen nötig
- Objektive Folgerungen

Live Forensik

Durchführung

Präsentation

- Bericht verfassen
- Dritte müssen Folgerungen verstehen
- Fakten vs. Vermutungen

Live Forensik

Bericht

1. Aufgabenstellung

Die [redacted] GmbH erhielt per Kurier am 03. Dezember im Ermittlungsverfahren gegen [redacted] der Staatsanwaltschaft wegen des Verdachts des Verbreitens und Besitzes kinderpornografischer Schriften folgende Gegenstände zur Auswertung:

- 1 PC ‚NoName‘.

Aufgabe war es gem. Auftragschreiben der Staatsanwaltschaft vom 26. Oktober die Festplatten des beigegeführten Rechners auf das Vorhandensein kinderpornografischer Bild- oder Filmdateien zu untersuchen.

Außerdem war festzustellen, ob und ggf. wann und an wen der Beschuldigte derartige Dateien weitergegeben hat und wann bzw. von wem er ggf. derartige Dateien erhalten hat.

Nach kinderpornografischen Texten sollte nicht gesucht werden.

Ferner war die Untersuchung auf den aktiven Bereich der Festplatte zu beschränken.

Live Forensik

Bericht

1. Aufgabenstellung

Die GmbH erhielt per Kurier am 03. Dezember im Ermittlungsverfahren gegen der Staatsanwaltschaft wegen des Verdachts des Verbreitens und Besitzes kinderpornografischer Schriften folgende Gegenstände zur Auswertung:

- 1 PC ‚NoName‘.

Aufgabe war es gem. Auftragschreiben der Staatsanwaltschaft vom 26. Oktober die Festplatten des beigegeführten Rechners auf das Vorhandensein kinderpornografischer Bild- oder Filmdateien zu untersuchen.

Außerdem war festzustellen, ob und ggf. wann und an wen der Beschuldigte derartige Dateien weitergegeben hat und wann bzw. von wem er ggf. derartige Dateien erhalten hat.

Nach kinderpornografischen Texten sollte nicht gesucht werden.

Ferner war die Untersuchung auf den aktiven Bereich der Festplatte zu beschränken.

Live Forensik

3. Ergebniszusammenfassung

Es wurde festgestellt,

- dass in Orphan-Files 3 Bilddarstellungen vorhanden sind, die vermutlich als Kinderpornografie einzustufen sind,
- dass durch Nutzung der MSN-Group am 13 Bilddateien verschafft wurden die vermutlich als Kinderpornografie einzustufen sind,
- dass am [redacted] durch die MSN-Group und [redacted] sowie von der Webseite [redacted] insgesamt 73 Bilddarstellungen verschafft wurden, die vermutlich als Kinderpornografie einzustufen sind,
- dass am [redacted] von der MSN-Group [redacted] sowie der Webseite [redacted] insgesamt 1.108 Bilddateien verschafft wurden, die vermutlich als Kinderpornografie einzustufen sind,
- dass am [redacted] von der MSN-Group [redacted] insgesamt 35 Bilddateien verschafft wurden, die vermutlich als Kinderpornografie einzustufen sind,
- dass am [redacted] aus der MSN-Group [redacted] 12 Filmdateien verschafft wurden, die vermutlich als Kinderpornografie einzustufen sind,
- dass durch Nutzung der Yahoo-Groups [redacted] sowie [redacted] insgesamt 5 eMail-Nachrichten empfangen wurden, die Darstellungen zum Inhalt haben, die vermutlich als Kinderpornografie einzustufen sind,
- dass auf dem untersuchten Rechner Programme zur Zerstörung von Spuren (Internetspurenvernichter) installiert sind,
- dass durch Nutzung des Clients der Tauschbörse [redacted] 69 pornografische Filmdateien zum Download bereitstanden.

Erstellt am: 8.12.

Seite: 2 von 5

Live Forensik

4. Besitz

4.1 Vermutlich Kinderpornografie

Bei Durchsicht des übergebenen PC des Beschuldigten wurde festgestellt, dass in so genannten Orphan-Files insgesamt 3 Bilddarstellungen vorhanden sind, die **vermutlich** als Kinderpornografie einzustufen sind. Einen entsprechenden Ausdruck finden Sie in **Anlage 1**.

Bei **Orphan-Files** handelt es sich um Dateien, die aus einem gelöschten Verzeichnis stammen. D.h., der ursächliche Speicherpfad ist nicht mehr bestimmbar, da das Verzeichnis in dem diese Dateien vorhanden waren, gelöscht wurde. Die Dateien selbst sind jedoch noch vorhanden.

5. Verschaffung

Bei Durchsicht des übergebenen PC des Beschuldigten fiel auf, dass im Internet-Cache zahlreiche Bild- und Filmdarstellungen vorhanden sind, die vermutlich als Kinderpornografie einzustufen sind. Eine Rückverfolgung, woher diese Bild- und Filmdarstellungen stammen, führte zu der Erkenntnis, dass diese durch Nutzung von MSN-Groups, Webseiten sowie von Yahoo-Groups verschafft wurden.

5.1 Vermutlich Kinderpornografie - Bilder - MSN-Group

Bei Überprüfung der im Internet-Cache vorhandenen Bilddarstellungen wurde festgestellt, dass diese aus der MSN-Group stammen. Sie finden einen Ausdruck der insgesamt 13 Bilddarstellungen, die vermutlich als Kinderpornografie einzustufen sind, in **Anlage 2** sowie zudem einen Ausdruck aus der Index.dat-Datei, welcher belegt, dass diese Bilddarstellungen der MSN-Group entstammen. In diesem Zusammenhang ist ferner festzuhalten, dass die Spalte „hits“ Auskunft darüber gibt, wie oft diese Webseite

Live Forensik

Durchführung

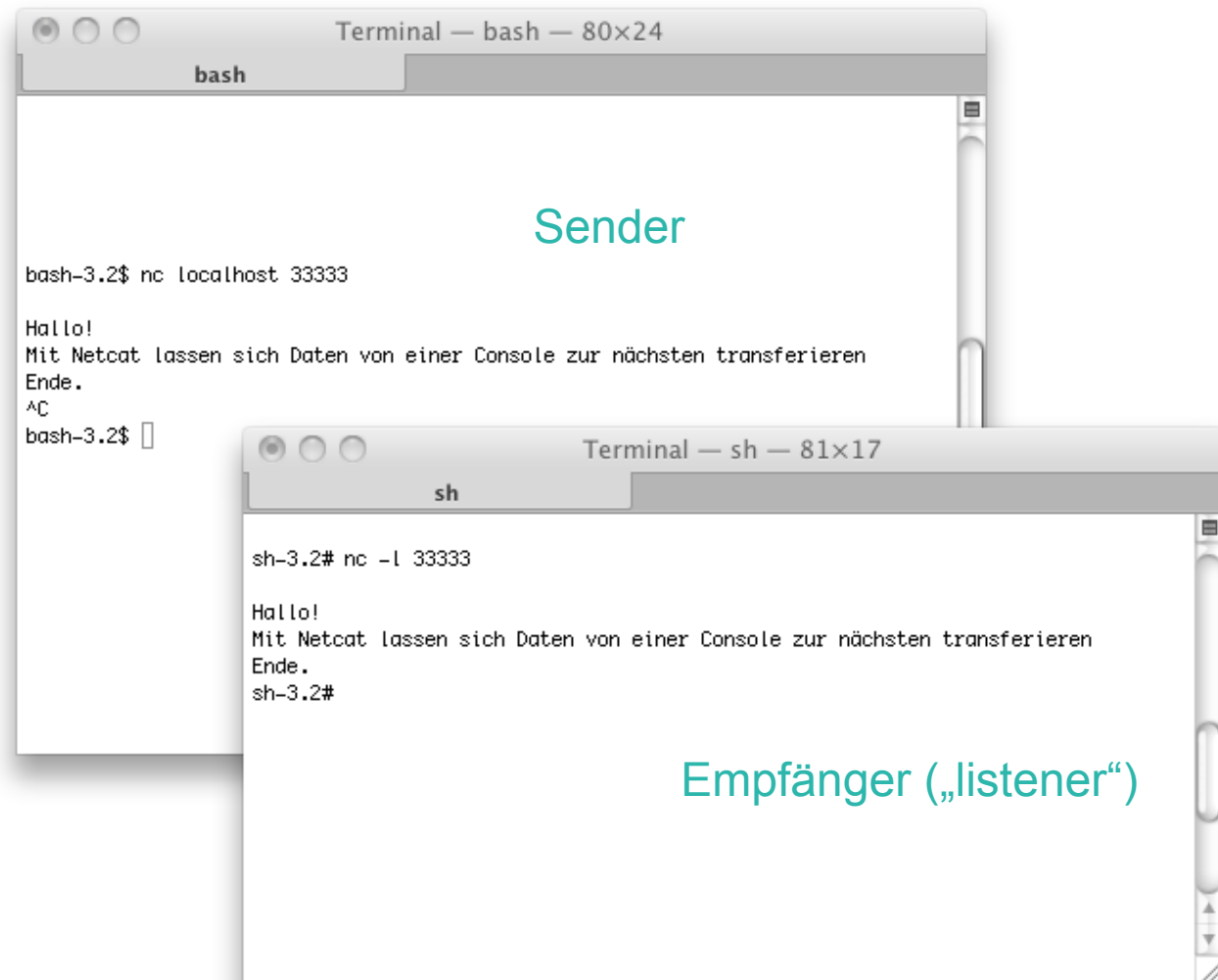
Sicherstellung am Beispiel

- Schutz des Systems
- Dokumentation der Umgebung
- Uhrzeit (des Systems)
- Cache
- Speicher
- Netzwerkverbindungen
- Laufende Prozesse
- Logs
- Speichermedien

Durchführung

- netcat

Live Forensik



Durchführung **Live Forensik**

- dd
 - Erstellt Images von Festplatten
 - # `dd conv=noerror bs=512kb ↵`
`if=/dev/disk0 ↵`
`of=/Volumes/forensik/ddtimg.dd`
 - 1:1 Kopie: incl. Lesefehler
 - Über Netcat
 - # `dd if=/dev/disk0 | nc ip port`

Durchführung Live Forensik

- dd
 - Kann auch unter Windows ganze Platten:
 - `if=\\.\PhysicalDrive0:`
 - Oder RAM:
 - `if=\\.\PhysicalMemory`

Durchführung

Live Forensik

- Analyse von Festplattenimages
in eigenem Vortrag

Durchführung Live Forensik

- PTfinder
 - Musteranalyse vom RAM-Image
 - Liefert RAM für jeden Prozess
- pmodump
 - Extrahiert ausführbare Daten aus RAM
- Starke Verbesserung der RAM-Analyse-Tools in den letzten Jahren

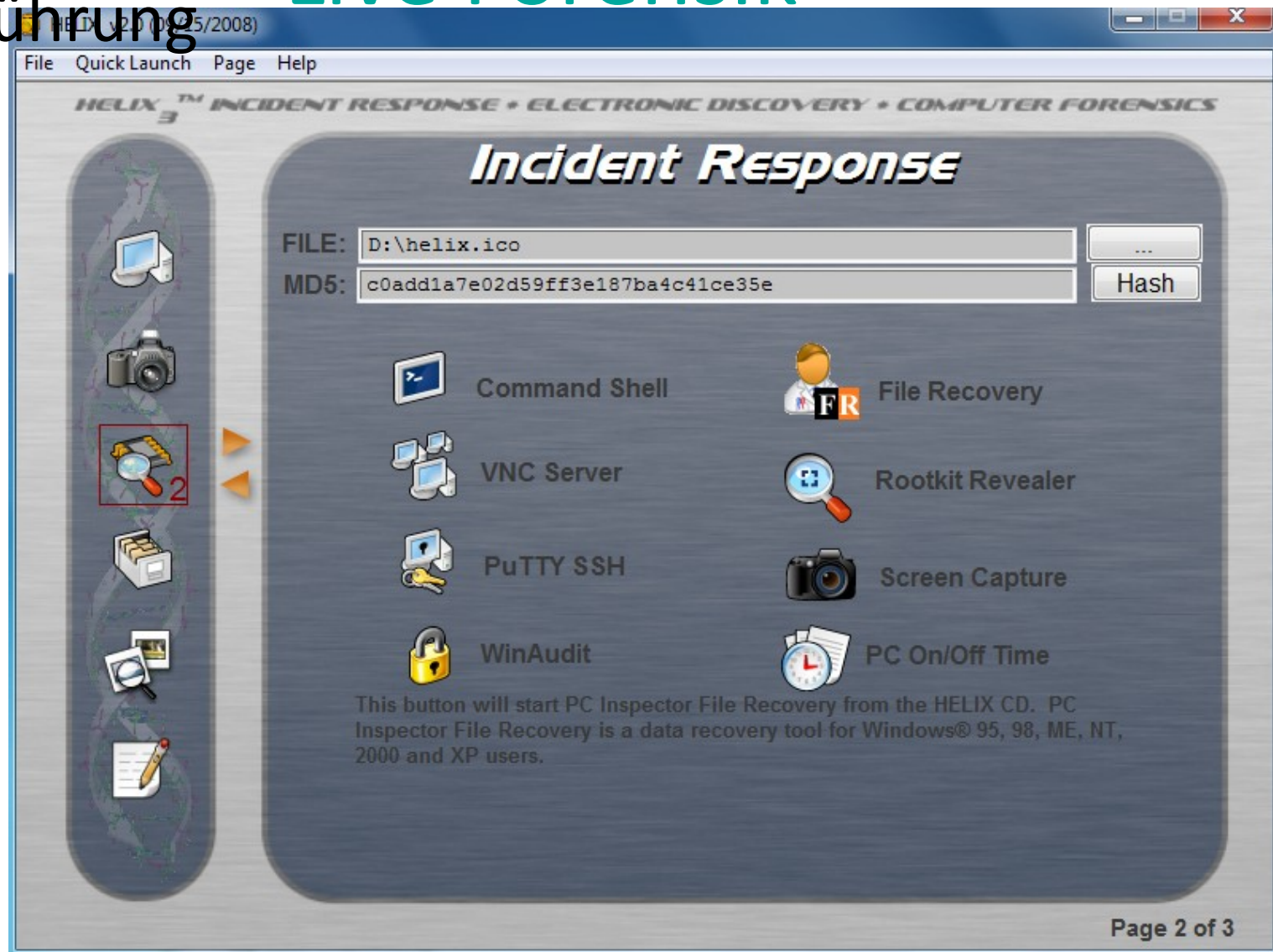
Durchführung **Live Forensik**

- Tools für alles
 - Browser-History
 - IM-/Mail-Passwörter
 - Netzwerkverkehr
 - Papierkorb
 - On/Off-Time
 - USB-Nutzung

Durchführung Live Forensik



Durchführung Live Forensik

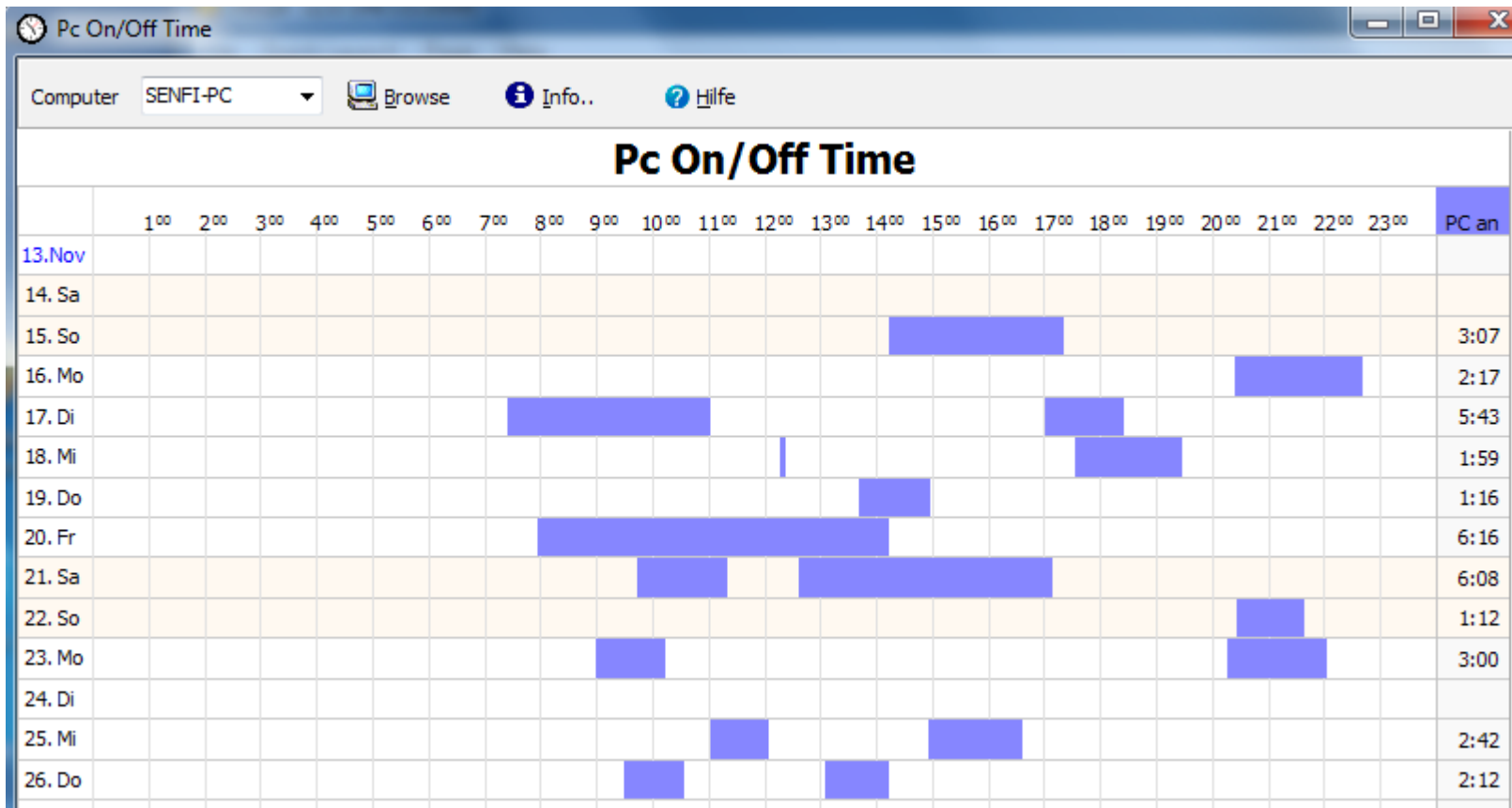


Live Forensik

Durchführung



Durchführung Live Forensik




Durchführung

Live Forensik

IEHistoryView: C:\Users\senfi\AppData\Local\Microsoft\Windows\History

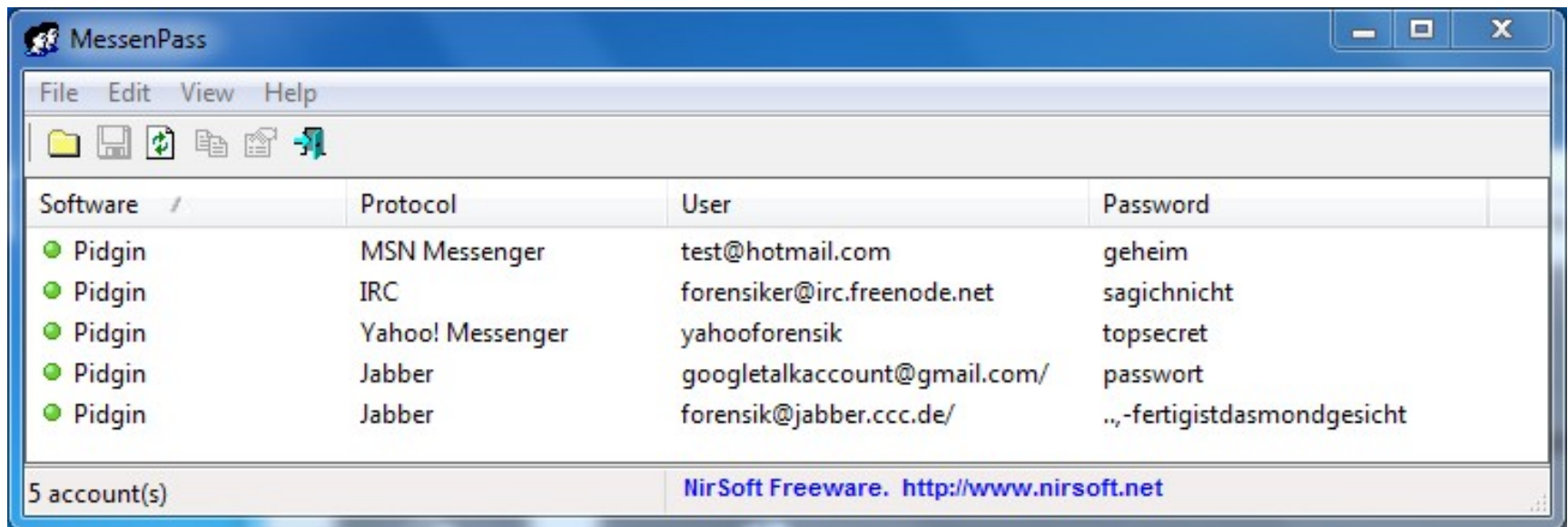
File Edit View Help



URL	Title	Hits	Modified Date	Expiration Date
<input type="checkbox"/> http://www.it-forensik.fh-aachen.de/index.php?option=com_...	Anmeldung	1	03.12.2009 10:51:54	29.12.2009 10:51:56
<input type="checkbox"/> http://www.it-forensik.fh-aachen.de/favicon.ico		3	03.12.2009 10:51:48	29.12.2009 10:51:50
<input type="checkbox"/> http://www.it-forensik.fh-aachen.de/index.php?option=com_...	Forensik Seminar 2009	1	03.12.2009 10:51:48	29.12.2009 10:51:50
<input type="checkbox"/> http://www.it-forensik.fh-aachen.de	IT-Forensik FH Aachen	1	03.12.2009 10:51:46	29.12.2009 10:51:48
<input type="checkbox"/> http://www.google.de/search?hl=de&q=it-forensik+fh+aach...	it-forensik fh aachen - Google-Suche	5	03.12.2009 10:51:20	29.12.2009 10:51:22
<input type="checkbox"/> http://www.google.de/search?hl=de&source=hp&q=forensik...	forensik fh aachen - Google-Suche	5	03.12.2009 10:51:06	29.12.2009 10:51:08
<input type="checkbox"/> http://www.google.de	Google	5	03.12.2009 10:50:57	29.12.2009 10:50:58

7 item(s)

Durchführung Live Forensik



Durchführung Live Forensik

- Weitere Software-Suiten
 - Helix <http://www.e-fense.com/>
 - grml <http://grml.org/>
 - ForensiX (c't)
<http://computer-forensik.org/tools/ix/>
 - Caine <http://www.caine-live.net/>
 - EnCase <http://www.guidancesoftware.com/>
 - X-Ways <http://www.x-ways.net/>
 - Cofee

Live Forensik

Inhalt

- *Was ist Live Forensik?*
- *Vorgehensweise*
 - *Beispiel*
- ***Ausblick***
- **Praxisteil**

Live Forensik

Ausblick

Online-Durchsuchungen
am Beispiel von MegaPanzer & Poison Ivy

Live Forensik

Online-Durchsuchungen



- megapanzer.com
- Schadsoftware: Trojaner / Rootkit
- Zielsysteme: Windows
- Entwickelt von Schweizer Unternehmen
- Nach Rechtsstreit mit Entwickler nun unter GPL

Live Forensik

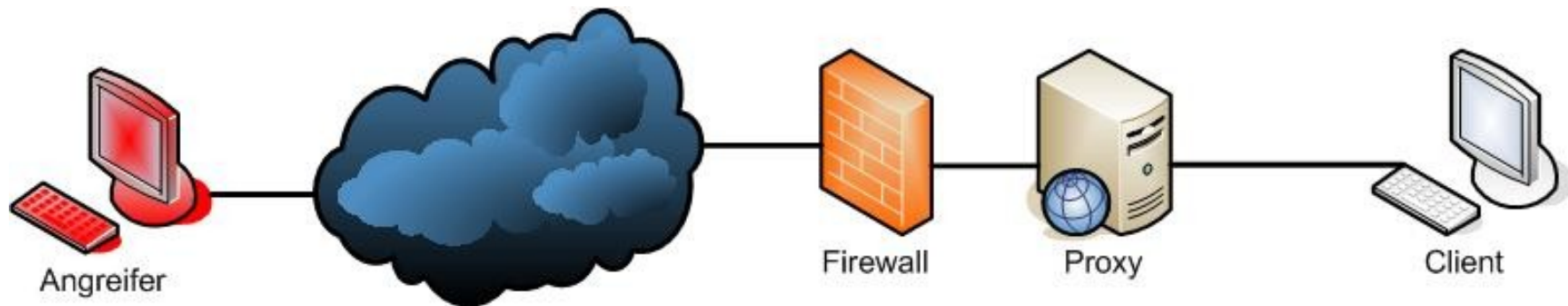
Online-Durchsuchungen



- Versteckter Schadcode
- Verbindet sich zurück zum Angreifer umgeht so NAT und Proxy
- Ermöglicht Remote-Shell
- Als „Bundestrojaner“-Variante gehandelt
- Überlebenselixier: keine AV Signatur

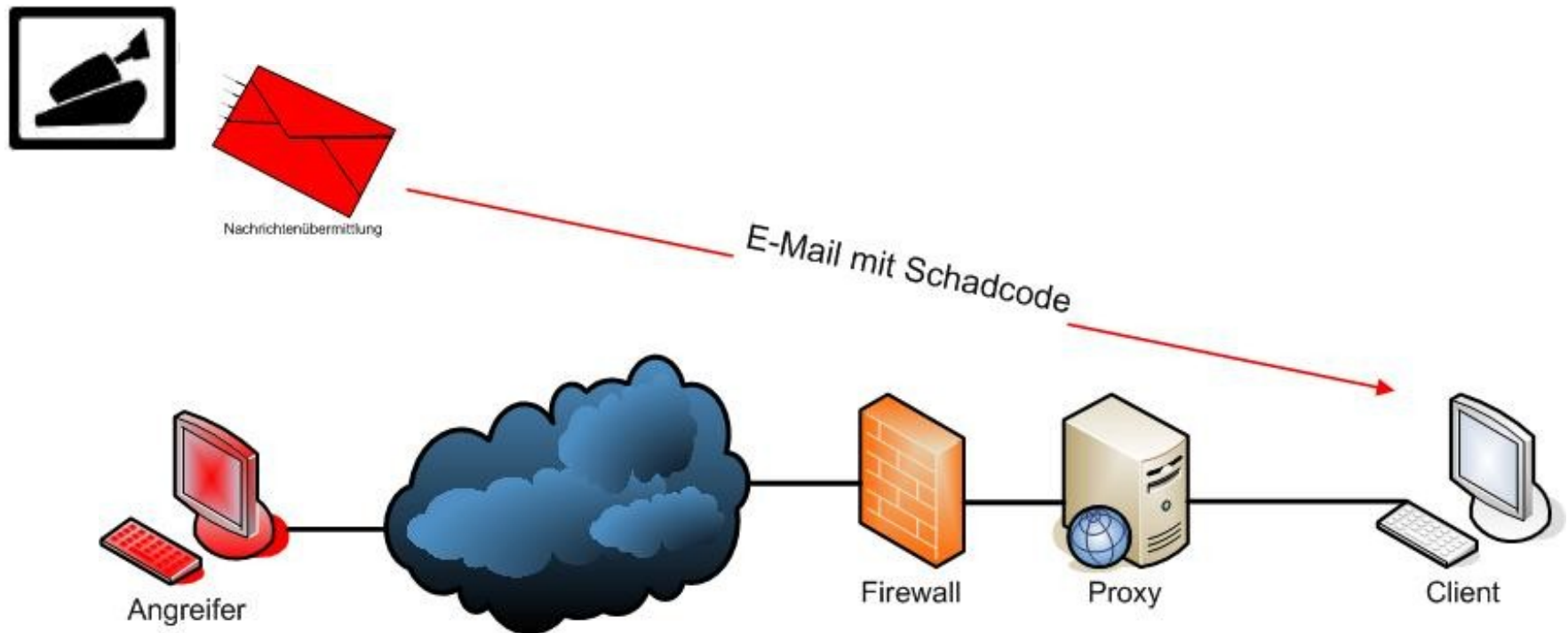
Live Forensik

Online-Durchsuchungen



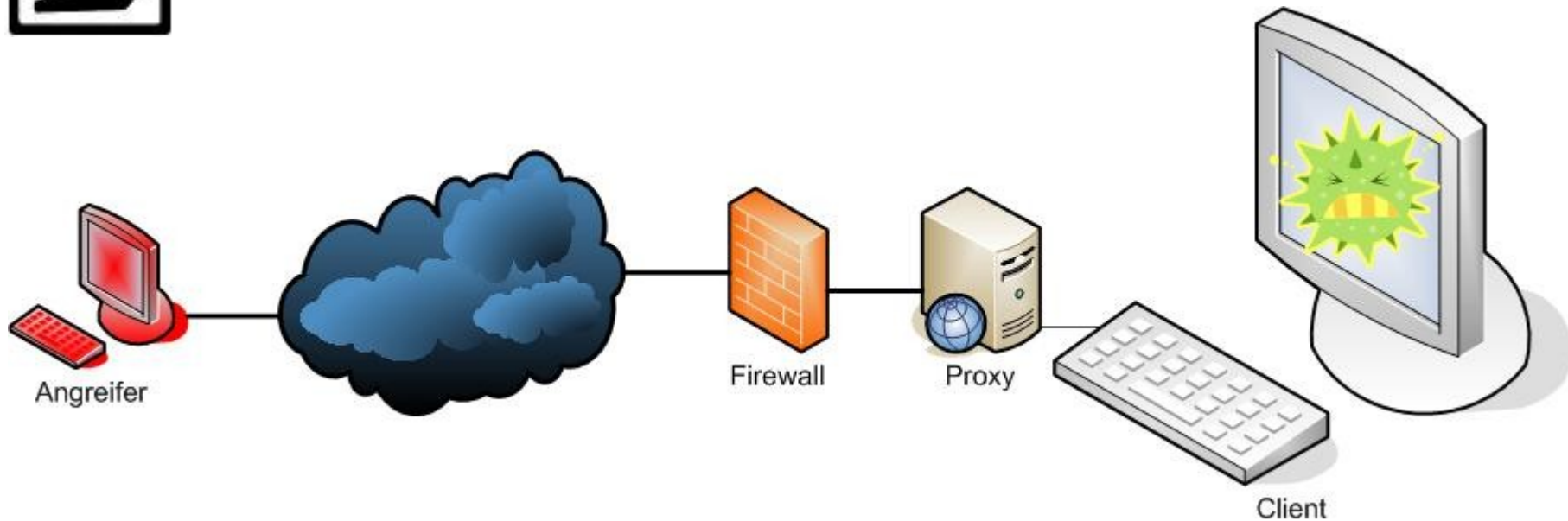
Live Forensik

Online-Durchsuchungen



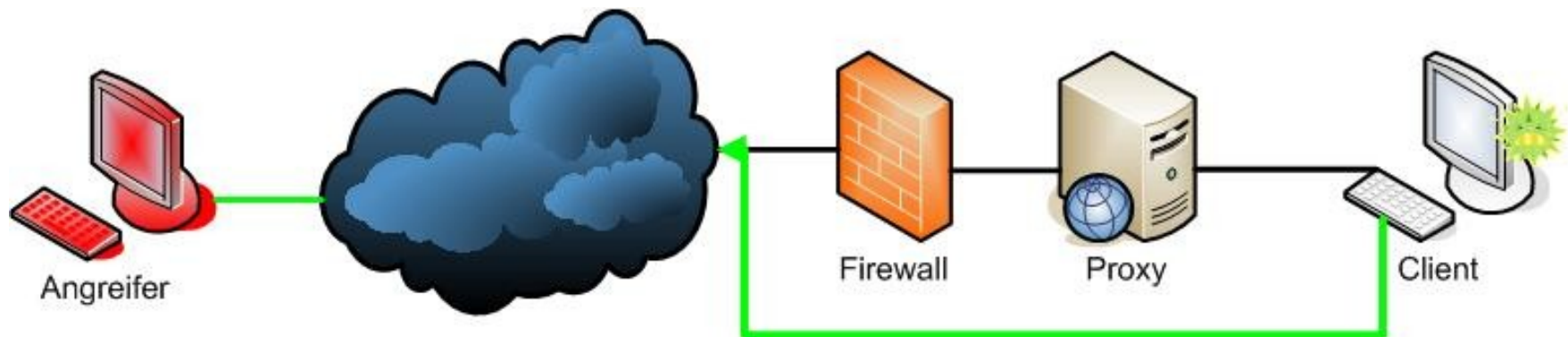
Live Forensik

Online-Durchsuchungen



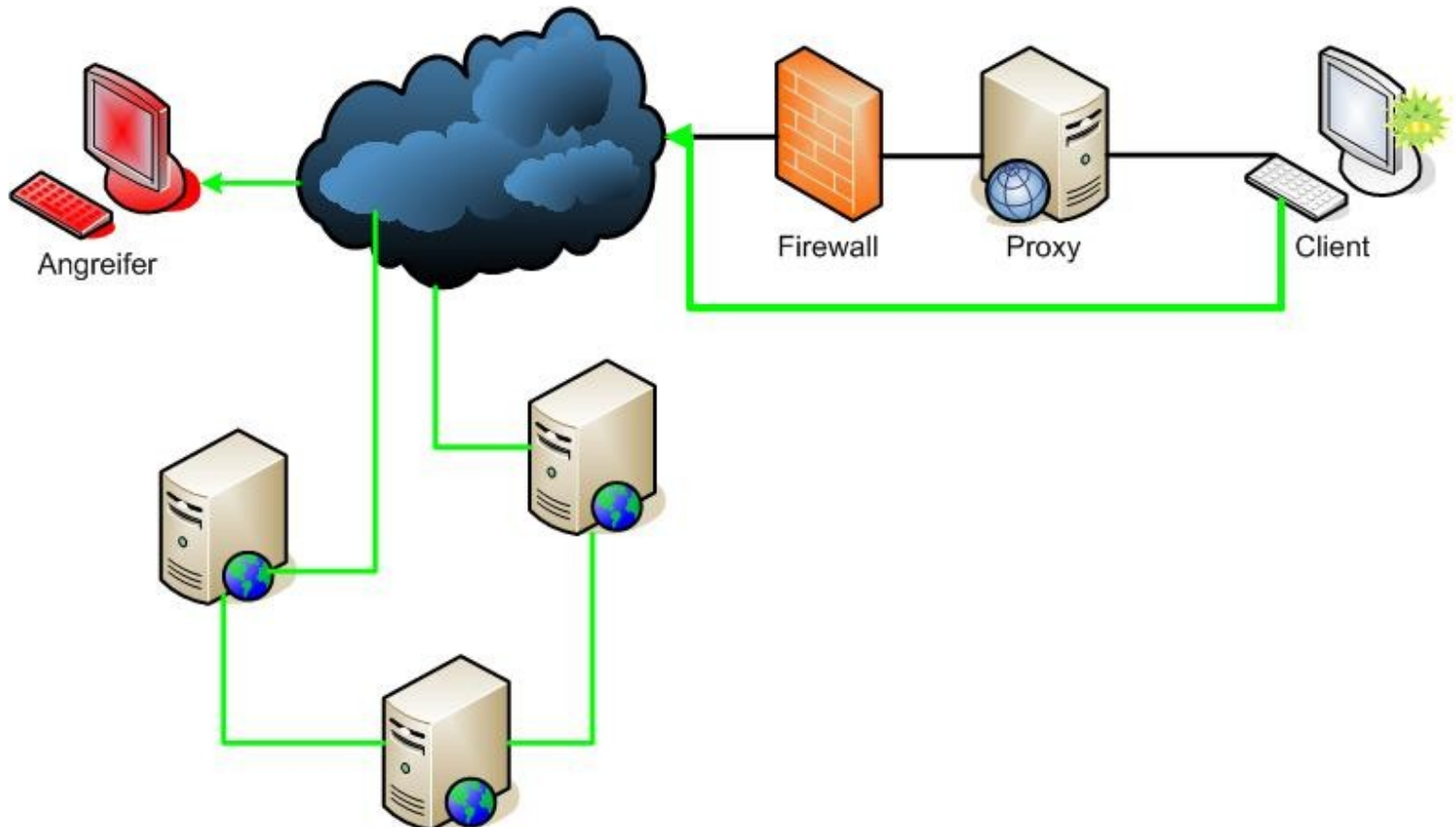
Live Forensik

Online-Durchsuchungen



Live Forensik

Online-Durchsuchungen



Live Forensik



victim_carrumba (v0.1)@192.168.100.50:2627

Resource name	Resource type	Username	Password
http://webmail.....ch/src/login.php	AutoComplete Passwords
http://webmail.....ch/src/login_retry.php	AutoComplete Passwords
http://www.facebook.com	Mozilla Firefox
http://www.megapanzer.com	Mozilla Firefox
http://www.....ws	Mozilla Firefox
http://www.....ch	Mozilla Firefox
https://webmail.....ch/de/src/login.php	AutoComplete Passwords
https://webmail.....ch/src/login.php	AutoComplete Passwords
https://webmail.....ch/src/login_retry.php	AutoComplete Passwords
https://www.google.com	Mozilla Firefox
mail.....ch	OutlookExpress

Connected to victim_carrumba (v0.1)@192.168.100.50:2627

Live Forensik



Megapanzer 0.1

File Tools Help

Target ID	Target IP	User name	Computer name	Operating system	Processor	RAM	Last command
victim_carrumba (v0.1)	192.168.100.50:...	run	CHRISTAN	Windows XP	Intel(R) Core(TM)2 Duo C...	1.030 gb	

victim_carrumba (v0.1)@192.168.100.50:3322

- Target system data
 - Downloaded files
 - Display captures
 - Keylogging data
 - Microphone captures
 - Webcam captures
 - System state data
- Tools
 - Delete Mega Panzer
 - Account data
 - Installed software
 - Browser history
 - Browser favorites
 - Listening sockets
 - Open connections
 - Transfer file
 - DNS manipulation
 - Remote shell
 - Manager
 - List processes
 - Win32 processes
 - List services
 - Registry browser
 - Filesystem browser
 - Surveillance
 - Keyboard captures
 - Screen capture
 - Microphone capture
 - Webcam capture
 - SSL Man in the Middle
 - Inject certificate
 - List certificates

21.10.2008 14:13	<DIR>	Outlook Express
06.12.2007 16:07	<DIR>	Pidgin
08.03.2009 13:50	<DIR>	Poseidon
20.10.2007 11:27	<DIR>	QuickTime
04.09.2007 17:15	<DIR>	Real
29.11.2007 21:18	<DIR>	RealVNC
10.01.2008 19:32	<DIR>	Skype
09.08.2007 22:35	<DIR>	Swisscom Mobile
10.08.2007 00:14	<DIR>	ThinkPad
09.08.2007 23:58	<DIR>	ThinkVantage
04.07.2007 18:58	<DIR>	ThinkVantage Fingerprint Software
14.07.2008 00:27	<DIR>	TortoiseSVN
03.01.2008 17:47	<DIR>	Vidalia Bundle
07.07.2007 18:09	<DIR>	Videolan
27.11.2008 18:41	<DIR>	Vuze
27.10.2008 16:20	<DIR>	WebScarab
30.07.2008 08:31	<DIR>	Windows Live
10.08.2007 00:10	<DIR>	Windows Live Toolbar
07.10.2007 16:59	<DIR>	Windows Media Connect 2
21.10.2008 14:13	<DIR>	Windows Media Player
21.10.2008 14:13	<DIR>	Windows NT
07.03.2007 09:06	<DIR>	WinID
04.01.2008 15:35	<DIR>	WinPcap
09.08.2007 19:29	<DIR>	WinRAR
11.12.2007 13:30	<DIR>	WinSCP
04.01.2008 15:35	<DIR>	Wireshark
05.07.2007 02:29	<DIR>	xerox
	0 Datei(en)	0 Bytes
	85 Verzeichnis(se), 95'919'370'240 Bytes frei	

dir|

Remote shell environment

```
Working directory      : c:\programme\
User ID                : run
Last command           : dir
```

Megapanzer 0.1 Listening on port 80

Megapanzer 0.1 - Log console

```
Sun Mar 08 22:08:08 GMT+0100 2009 : Received command output
Sun Mar 08 22:08:16 GMT+0100 2009 : REQUEST "114!c:\dir pro
Sun Mar 08 22:08:16 GMT+0100 2009 : Received command output
Sun Mar 08 22:08:49 GMT+0100 2009 : REQUEST "114!c:\cd pro
Sun Mar 08 22:08:49 GMT+0100 2009 : Received command output
Sun Mar 08 22:08:50 GMT+0100 2009 : REQUEST "114!c:\progran
Sun Mar 08 22:08:50 GMT+0100 2009 : Received command output
```


Live Forensik


Online-Durchsuchungen



- Plugin-Architektur
- Abhören von Skype
- File und Informationstransfer
- Webcam und Bildschirm Inhalte
- Mikrofon


Live Forensik

Online-Durchsuchungen

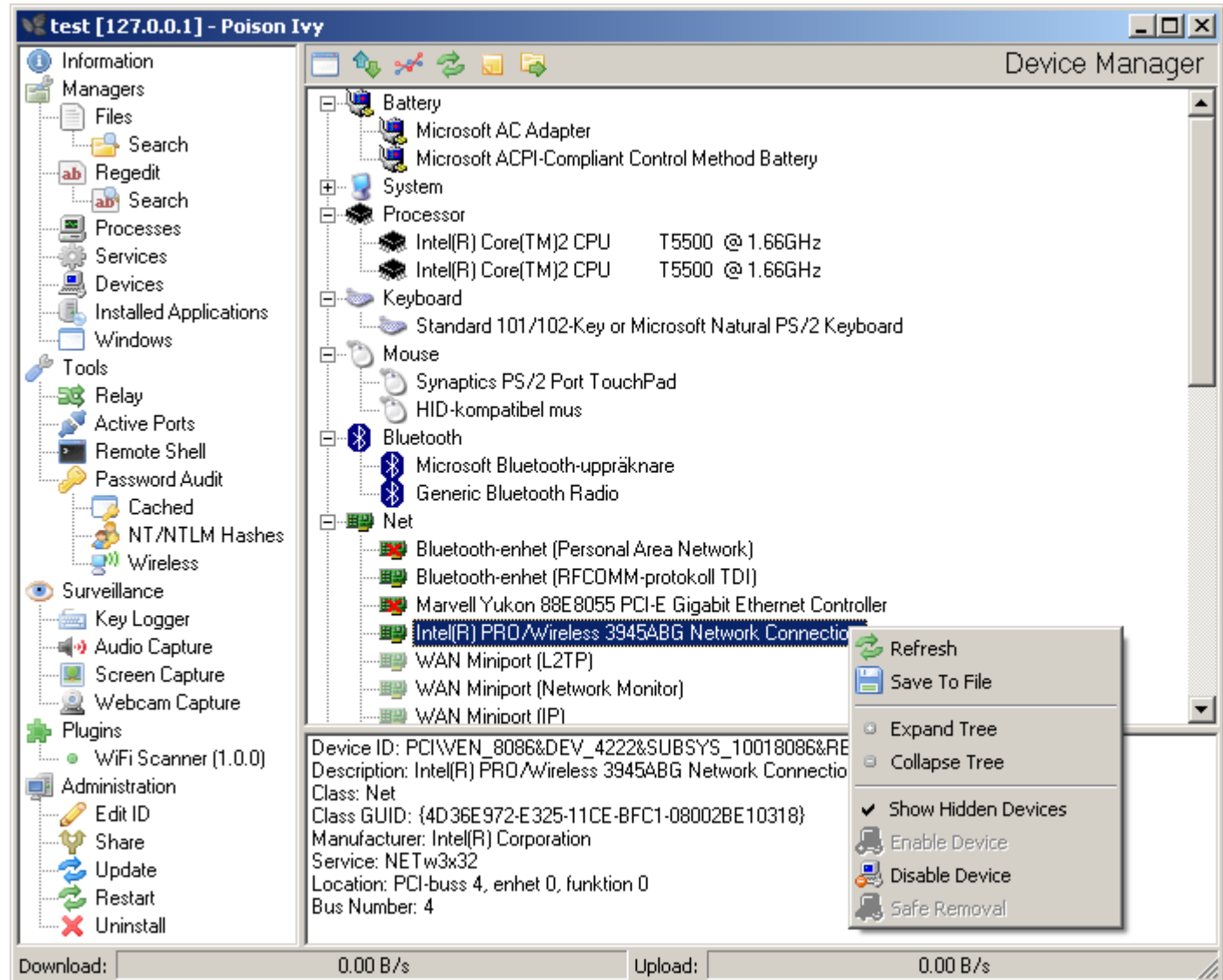
- 
- posionivy-rat.com
 - Schadsoftware: Trojaner / Rootkit
 - Zielsysteme: Windows
 - „Remote Administration Software“
 - Seit 2008 nicht aktiv weiterentwickelt

Live Forensik

Online-Durchsuchungen

- 
- A vertical, slightly curved branch with several small, bright green leaves, positioned on the left side of the slide.
- DNS/Port-Editor
 - Dateimanager, -suche, -transfer
 - Regedit
 - Prozessmanager, Servicemanager, offene Ports
 - Remote-Shell, NT/NTLM Hashes, Screen-Capture
 - Relay, Socket Traffic, Audiomitschnitt
 - Share server, Installierte Programme, Windows-Manager
 - SSL MITM, WIFI-Scanner, ...

Live Forensik

test [127.0.0.1] - Poison Ivy

Information
Managers
Files
 Search
 Regedit
 Search
Processes
Services
Devices
Installed Applications
Windows
Tools
 Relay
 Active Ports
 Remote Shell
 Password Audit
 Cached
 NT/NTLM Hashes
 Wireless
Surveillance
 Key Logger
 Audio Capture
 Screen Capture
 Webcam Capture
Plugins
 WiFi Scanner (1.0.0)
Administration
 Edit ID
 Share
 Update
 Restart
 Uninstall

Device Manager

- Battery
 - Microsoft AC Adapter
 - Microsoft ACPI-Compliant Control Method Battery
- System
- Processor
 - Intel(R) Core(TM)2 CPU T5500 @ 1.66GHz
 - Intel(R) Core(TM)2 CPU T5500 @ 1.66GHz
- Keyboard
 - Standard 101/102-Key or Microsoft Natural PS/2 Keyboard
- Mouse
 - Synaptics PS/2 Port TouchPad
 - HID-kompatibel mus
- Bluetooth
 - Microsoft Bluetooth-uppräktnare
 - Generic Bluetooth Radio
- Net
 - Bluetooth-enhet (Personal Area Network)
 - Bluetooth-enhet (RFCDMM-protokoll TDI)
 - Marvell Yukon 88E8055 PCI-E Gigabit Ethernet Controller
 - Intel(R) PRO/Wireless 3945ABG Network Connection**
 - WAN Miniport (L2TP)
 - WAN Miniport (Network Monitor)
 - WAN Miniport (IP)

Device ID: PCI\VEN_8086&DEV_4222&SUBSYS_10018086&RE
Description: Intel(R) PRO/Wireless 3945ABG Network Connection
Class: Net
Class GUID: {4D36E972-E325-11CE-BFC1-08002BE10318}
Manufacturer: Intel(R) Corporation
Service: NETw3x32
Location: PCI-buss 4, enhet 0, funktion 0
Bus Number: 4

- Refresh
- Save To File
- Expand Tree
- Collapse Tree
- Show Hidden Devices
- Enable Device
- Disable Device
- Safe Removal

Download: 0.00 B/s Upload: 0.00 B/s

Live Forensik

Ausblick

Internetforensik

Am Beispiel Metasploit-Decloak

Live Forensik

Internetforensik

METASPLOIT

- decloak.net
- aus Metasploit Suite
- Ermittelt echte IP
- Auch bei Nutzung von Anonymisierern
- Java, JavaSkript, Flash, Embedded X

Live Forensik

Internetforensik

metasploit

HOME FRAMEWORK CONTRIBUTE RESEARCH BLOG



This test can take up to 30 seconds to complete.
(ID: [de2252bff819a10417edc51a9af76798](#))



[msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Community

- Issue Tracking
- Mailing Lists
- Metasploit U
- Rapid7 FAQ

Product Downloads

- Metasploit 3.3 Beta (WIN32)
- Metasploit 3.3 Beta (UNIX)
- Rapid7 NeXpose VM (trial)

Live Forensik

metasploit

HOME

FRAMEWORK

CONTRIBUTE

RESEARCH

BLOG

DECLCLOAKING REPORT (DE2252BFF819A10417EDC51A9AF76798)

Field	Data	Dependency
External Address	87.189.88.131	Browser
Internal Host	unknown	Java
Internal Address	unknown	Java
DNS Server (Java)	unknown	Java
DNS Server (HTTP)	unknown	Browser
DNS Server (FTP)	unknown	Browser
DNS Server (Word)	unknown	Office
DNS Server (iTunes)	unknown	iTunes
DNS Server (Quicktime)	unknown	Quicktime
External NAT (FTP)	unknown	Browser
External NAT (Java)	unknown	Java
External NAT (Flash)	87.189.88.131	Flash
External NAT (Word)	unknown	Office
External NAT (iTunes)	unknown	iTunes
External NAT (Quicktime)	unknown	Quicktime

Ausblick

Owned by an iPod

Am Beispiel FireWire und DMA

Live Forensik

Owned by an iPod



- FireWire alias i.Link oder IEEE 1394
- '86 von Apple entwickelt
- '95 Markteinführung
- Serielles Bussystem
- Eigentlich Nachfolger für SCSI



Live Forensik

Owned by an iPod



Live Forensik

Owned by an iPod



Bekannte Einsatzgebiete:

- Externe Multimedia- und Peripheriegeräte
- Externe Massenspeicher
- Medienanschluss in Fahrzeugen



Live Forensik

Owned by an iPod



Features (S3200, Auszug):

- 3,2 Gbit/s Übertragungsbandbreite
- LAN (IP over FireWire)
- Hot plug, volle Stromversorgung
- Direct Memory Access



Live Forensik

Owned by an iPod



Direct Memory Access

„Der Begriff Speicherdirektzugriff oder englisch Direct Memory Access (DMA) bezeichnet in der Computertechnik eine Zugriffsart, die über ein **Bussystem direkt auf den Speicher** zugreift.

Diese Technik erlaubt angeschlossenen Peripheriegeräten, wie Netzwerkkarte oder Soundkarte, ohne Umweg über die CPU direkt mit dem Arbeitsspeicher zu kommunizieren. Der Vorteil des Speicherdirektzugriffs ist die **schnellere Datenübertragung** bei gleichzeitiger Entlastung des Prozessors.“

Quelle: de.wikipedia.org

Live Forensik

Owned by an iPod

Ein Schelm, wer Böses dabei denkt ...

Live Forensik

Owned by an iPod

- Dr.jur. Maximilian Dornseif
- i4 der RWTH Aachen
- Vortrag auf Core05
- „FireWire -
all your memory are belong to us“
- Sicherung des RAM via OHCI in
FireWire

Live Forensik

Owned by an iPod

- Memory Dumps, ohne nötige Software
- Kein Sicherungsverlust/Verfälschung
- OS im Standardzustand sind abgreifbar
- Es gibt durchaus Abwehrmaßnahmen
- Interesse? → *Quellenverzeichnis*



Live Forensik

Inhalte

- *Was ist Live Forensik*
- *Beispiel der Anwendung*
- *Ausblick*
- ***Praxisteil***

Live Forensik

Praxisteil

- Windows Betriebssystem
- Arbeitsspeicher sichern
- Zuletzt verwendete Dateien
- Programmliste
- Log Files
- Alles sichern und dokumentieren

Live Forensik

Ende

Vielen Dank für Ihre Aufmerksamkeit

Live Forensik

Quellen

- Alexander Geschonneck: Computer Forensik. dpunkt Verlag, 2008
- M. Becher, M. Dornseif, C.N. Klein: „FireWire – all your memory are belong to us“
<http://cansecwest.com/core05/2005-firewire-cansecwest.pdf>
- F. Freiling, T. Holz: Vorlesung „Forensische Informatik“ im SS09 an der Uni Mannheim <http://pi1.informatik.uni-mannheim.de>
- M. Dornseif: „Angewandte It-Sicherheit“
<http://md.hudora.de/presentations/>

Live Forensik

Bildnachweis

- F1, Logo.
Daniel Hütten, Eigenerstellung
- F7, F8, Schaubild Datenflucht
<http://de.wikipedia.org/wiki/Notausgang>, Veränderte DIN Vorlage, public domain
- F12, Schaubild Plattenverschlüsselung
Michel Erbach, Eigenerstellung via Microsoft Visio
- F16, Schaubild Polizeibesuch
Michel Erbach, Eigenerstellung via Microsoft Visio
- F41-F50, Icon Megapanzer
megapanzer.com,
- F43-F47, Schaubild Funktionsweise Megapanzer
Michel Erbach, Eigenerstellung via Microsoft Visio
- F48-F49, Screenshot Megapanzer
megapanzer.com

Live Forensik

Bildnachweis

- F51-53, Icon Efeu
Microsoft Visio ClipArts
- F53, Screenshot PoisonEvy
<http://www.poisonivy-rat.com/index.php?link=sshot>,
- F56-F58, Icon Metasploit
decloak.net
- F57-F58, Screenshot decloak.net
Michel Erbach, Eigenerstellung
- F59-F63, Icons FireWire und Schnittstellen
Qurren, CC-BY, Wikimedia Commons, <http://de.wikipedia.org/wiki/Firewire>
- F65, Icons RWTH und CON05
<http://md.hudora.de/presentations/>
- F67, Icon iPod
Matthieu Riegler, CC-BY, Wikimedia Commons, <http://de.wikipedia.org/wiki/iPod>