

Forensics im IT Umfeld

(Verfahren, Möglichkeiten und Grenzen)

Prof. Konrad Marfurt
Carlos Rieder
Hochschule für Wirtschaft, Luzern

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -1

FACHHOCHSCHULE ZENTRALSCHWE
HSW
IWI → INSTITUT FÜR
WIRTSCHAFTSINFORMATIK LUZERN

Zielsetzungen

- Aufzeigen der Stärke der IT als Informationsquellen
- Wo bleiben Spuren
- Kennenlernen der Möglichkeiten und Grenzen

GEWUSST WO!!

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -2

FACHHOCHSCHULE ZENTRALSCHWE
HSW
IWI → INSTITUT FÜR
WIRTSCHAFTSINFORMATIK LUZERN

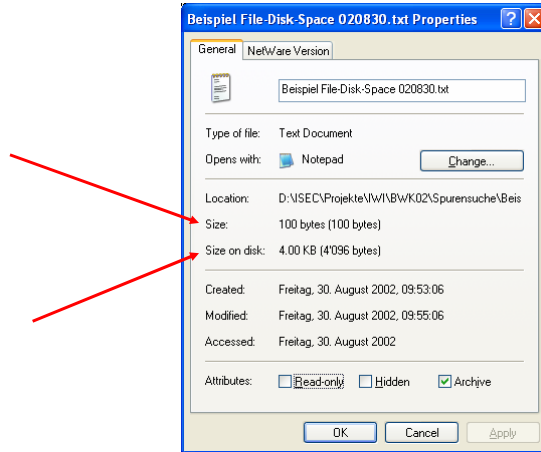
Übersicht

- Arten von Spuren
 - Betriebssysteme
 - Applikationen
 - Backup
 - Übertragungswege
- Spurensuche
 - Prinzipielles
 - 3 Phasen des Vorgehens

Betriebssystem

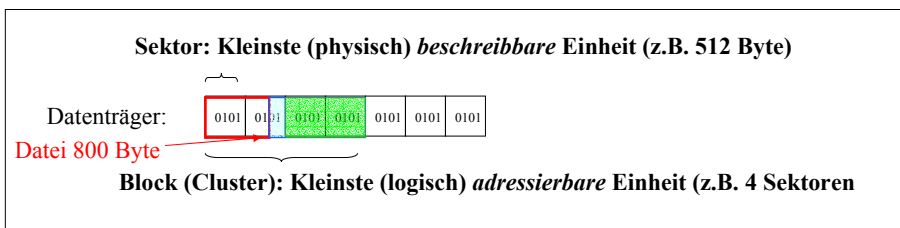
- Inhalt der Datei (selbstverständlich)
 - Metainformationen über Dateien
 - Erstellungszeit, Ersteller
 - Letzte Modifikation, Ausdruck
 - Dateigrösse
(effektiv und belegter Platz auf Datenträger)
- Woher stammt der Unterschied bei den beiden Grössenangaben?

Vergleich Filesize / Diskpace



Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -5

„Freier Platz“ auf Datenträgern (slack space)



Daten werden sektorweise gelesen/geschrieben, im obigen Bsp. werden also 1024 Byte für die Speicherung der 800 Byte grossen Datei geschrieben:

Überreste / „alte“ Daten in:

- Sektorresten (z.B. 801.-1024. Byte mit zufälligem RAM-Inhalt [**RAM-Slack**])
- Blockresten (Sektoren seit letztem Beschreiben dieses Clusters [**Cluster-Slack**])

Vorstellungshilfe:

(teilweise) besetzte oder leere Wohnungen in einem Hochhaus

Zimmer als Sektoren, Wohnungen als Cluster, Klingeltafel am Hauseingang als FAT

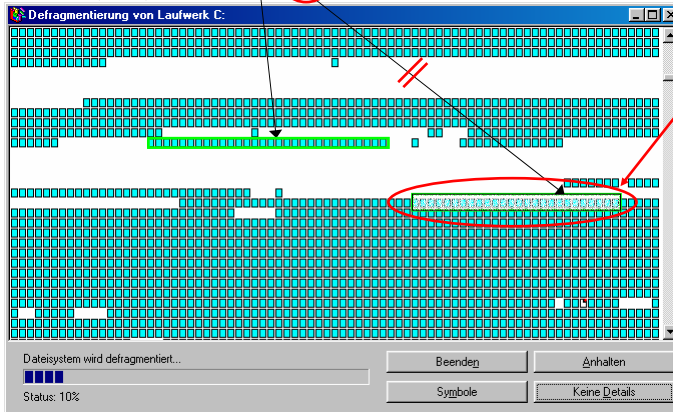
Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -6

„gelöschte Dateien“

File Allocation Table (FAT)

...	...	Name	Name
...	...	Ort	Ort

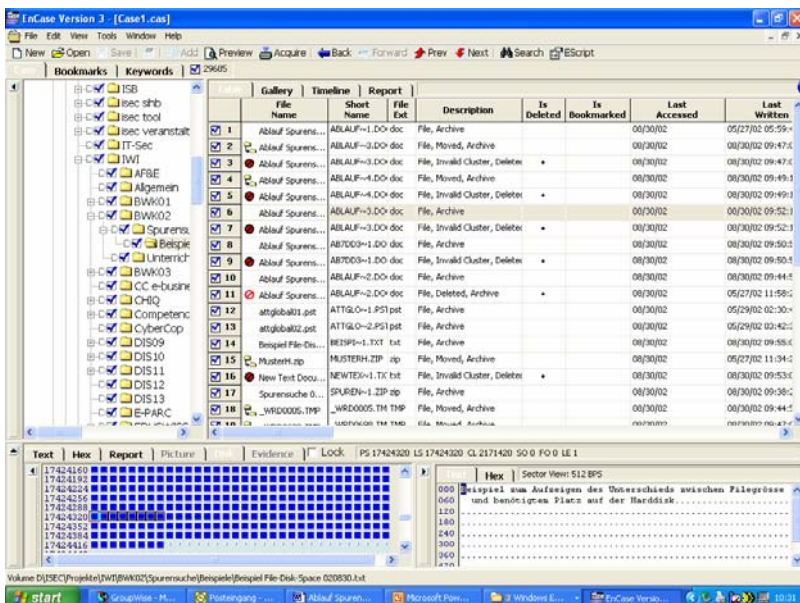
Löschung findet im Verzeichnis statt (Zuordnung aufheben)



Der Bereich wird zwar freigegeben, die Daten bleiben aber erhalten!!

Abhilfe: Explizites Auswischen (wipe) oder vollständiges Formatieren!

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -7



Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -8

Datensicherung

- Dateiweise (Dateien einzeln lesen und schreiben)
 - Cluster-Slack nicht erhalten
- Blockweise (Clone des Datenträgers)
 - Unter Umständen auch Cluster-Slack cloned
- Sicherungsmedium kann einmal oder mehrmals beschrieben werden
 - Offensichtliche Unterschiede zwischen HDU, CD/R, Tape

Logfiles des Betriebssystems

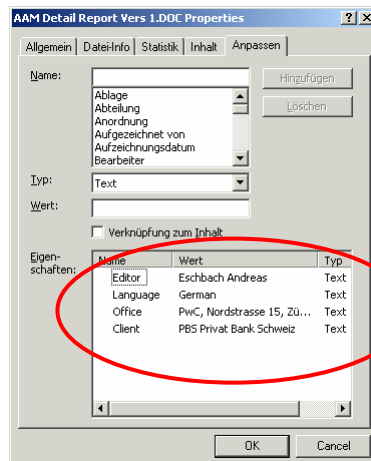
- Systematisches Erfassen der Manipulationen an Dateien durch das Betriebssystem
 - „wer“
 - „wann“
 - „was“
 - aber in der Regel nicht Inhalte der Dateien

Temporäre Dateien

- Office-Dokumente, die gerade bearbeitet werden
- Lokaler Cache des Webbrowsers (Zwischenspeicher zur schnellen Wiederholung eines kürzlich erfolgten Aufrufes)
- Hilfsdateien zur Zwischenablage bei der Verarbeitung von Dateien (z.B. auch bei der Verschlüsselung!)
- Cookie-Datei(en), die Rückschlüsse auf besuchte Websites zulassen, oder Benutzerkennndaten zur bequemen Identifikation bei einem WWW-Server speichern

Spuren im Microsoft Word

- Temporärdateien
- Sicherungskopien / Wiederherstellung
- Eigenschaften



Benutzerunterstützende Funktionen

- History-Daten:
 - Letzte benutzte Dateien in Office-Programmen
 - Letzte aufgerufene URLs
 - Adressaten der letzten 10 versandten e-Mails
- Eingabehilfen:
 - (seitenbezogen) zwischengespeicherte Benutzerkennungen für die bequeme Benutzung des Webbrowsers.



Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -15

Nochmals: Log-Files

- Verschiedenste Applikationen schreiben Log-Files, was nicht immer bedacht wird.
 - (z.B. „Änderungen verfolgen“ in Word)
- Vor allem im Zusammenhang mit Datenbanken
- Möglichkeit Nachweise zu erbringen, die eine Rekonstruktion der zeitlichen Abfolge erfordern

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -16

Undelete

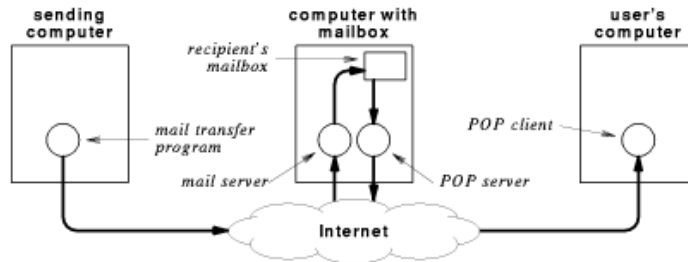
- Mit den geeigneten Werkzeugen können gelöschte Daten „gerettet“ werden
- Undelete, www.winternals.com,
US\$ 39.00

Richtig löschen

- Wipe
 - Löschmuster
- Wipe von vertraulichen Daten
- Wipe des freien Festplattenbereichs
- SafeGuard PrivateCrypto, www.utimaco.com

Kommunikation

Grundsatz: Weiterleitung bedingt oft Zwischenspeicherung
Zustellen einer e-Mail an Postfach



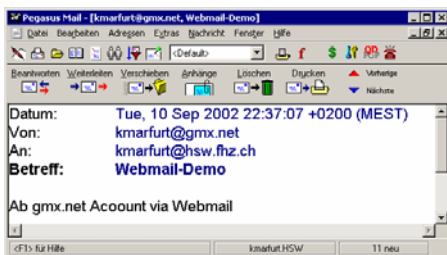
Versand einer e-Mail via SMTP

Zwecks Verständlichkeit ist nur ein einziger Message Transfer Agent (MTA) eingezeichnet

In der Realität liegen zwischen dem sendenden Computer und dem Zielhost mit dem Postfach mehrere MTAs

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -19

Mail-Beispiel:



Keine Standard-Header,
aber sehr hilfreich!

```
Received: from SpoolDir by HWNS02 (Mercury
1.47); 10 Sep 02 22:37:16 +0100
Return-path: <kmarfurt@gmx.net>
Received: from mx0.gmx.net (213.165.64.100)
by hsw.fhz.ch (Mercury 1.47);
10 Sep 02 22:37:06 +0100
Received: (gmail 32722 invoked by uid 0); 10
Sep 2002 20:37:07 -0000
Date: Tue, 10 Sep 2002 22:37:07 +0200 (MEST)
From: kmarfurt@gmx.net
To: kmarfurt@hsw.fhz.ch
MIME-Version: 1.0
Subject: Webmail-Demo
X-Priority: 3 (Normal)
X-Authenticated-Sender: #0011112222@gmx.net
X-Authenticated-IP: [147.88.186.131]
Message-ID: <19664.1031690227@www54.gmx.net>
X-Mailer: WWW-Mail 1.5 (Global Message
Exchange)
X-Flags: 0001
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: 7bit
X-PMFLAGS: 34078848 0 1 YOC056.CNM

Ab gmx.net Account via Webmail
```

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -20

Nochmals Mail: Header Informationen einer SMTP-Übertragung

Received: from SpoolDir by **HWNS02** (Mercury 1.47); 22 Feb 02 08:42:30 +0100
Return-path: <markirgendwer@dplanet.ch>
Received: from **dubb05h09-0.dplanet.ch** (212.35.36.9) by hsw.fhz.ch (Mercury 1.47) with ESMTP; 22 Feb 02 08:42:27 +0100
Received: from pcmark (**dialup-60-118.dplanet.ch** [212.35.60.118]) by dubb05h09-0.dplanet.ch (8.9.3/8.9.3/1.01dplanet-smtp) with SMTP id IAA13133 for <kmarfurt@hsw.fhz.ch>; Fri, 22 Feb 2002 08:42:28 +0100
Message-ID: <000801c1bb74\$495c7100\$763c23d4@pcmark>
From: "Mark Irgendwer" <markirgendwer@dplanet.ch>
To: "Konrad Marfurt" <kmarfurt@hsw.fhz.ch>
Subject: Beispiel-Adresdatenbank
Date: Fri, 22 Feb 2002 08:40:49 +0100
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Content-Transfer-Encoding: quoted-printable
X-MIME-Autoconverted: from 8bit to quoted-printable by dubb05h09-0.dplanet.ch id IAA13133
X-PMFLAGS: 35127424 0 1 Y0C412.CNM
Hoi Koni
Sorry f=F6r die St=F6hrung von vorher. (Ich war schon ziemlich verzweifelt= ...) K=F6nntest Du mir mal Eure Beispieldatenbank schicken? Schon jetzt herzlichen Dank!!!
Gruss und sch=F6nes Wochenende
Mark

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -21

FACHHOCHSCHULE ZENTRALSCHWE
HSW
IWI → INSTITUT FÜR
WIRTSCHAFTSINFORMATIK LUZERN

Grundsätzliches zur Datenübertragung

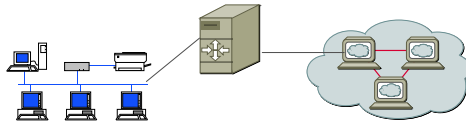
- Kurzfristige Zwischenspeicherung auf Gateways (Übergängen zu anderen Netzen) oder Routern (für die Bestimmung des Übertragungsweges) (Quell- und Zieladresse, Verbindungstyp)
- Überwachungsprogramme auf Firewalls mit Application-Gateways zur Analyse des Datenverkehrs zwischen zwei Netzwerken unterschiedlicher Sicherheitsstufe (evtl. Benutzerangaben und Zeitpunkt, Quell- und Zieladresse, Verbindungstyp)

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -22

FACHHOCHSCHULE ZENTRALSCHWE
HSW
IWI → INSTITUT FÜR
WIRTSCHAFTSINFORMATIK LUZERN

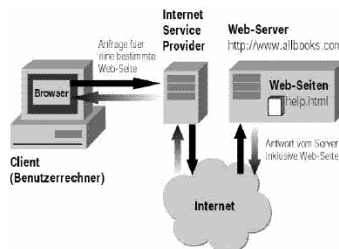
Proxy-Server für WWW-Zugang

- Je nach Installation werden Benutzerangaben und Zeitpunkt der Verbindung festgehalten
- Quell- und Zieladresse sowie Verbindungstyp
- Kopie der übertragenen Daten (zur Steigerung der Performance bei wiederholtem Zugriff) im sogenannten „Cache“
(bei korrekt konfiguriertem caching werden die Daten von verschlüsselten Verbindungen nicht zwischengespeichert)



Internet Service Provider (ISP)

- Logfiles der ISPs bei Dial-Up Zugängen
Einwahlmöglichkeit von Privatkunden via Modem zwecks temporärem Aufbau einer Verbindung
- Bei einigen Telecom-Anbietern auch anonym möglich
(dann wird bestenfalls die Telefonnummer des Anrufenden zu dessen Identifikation beitragen)
- ISPs betreiben in der Regel auch Mailserver und WWW-Proxies (vgl. oben)



„Roaming“ in Funknetzen

- Drahtlose Netzwerkzugänge funktionieren derzeit nur auf kurze Distanzen mit befriedigender Datenrate
- Funknetze werden in Zellen unterteilt (räumlich viel kleiner als beim GSM-Netz für Mobiltelefonie)
- Roaming, d.h. das verschieben des mobilen Computers in den Funkbereich einer anderen Antenne / Zelle, ist im Prinzip nachvollziehbar

Zurückverfolgen von Angriffen

Lokale Spuren eines Angriffes auf einen Webserver:

1a) Apache errorlog:

```
[Sat Sep 07 22:49:07 2002] [error] [client 210.178.130.193]  
Client sent malformed Host header
```

1b) Apache accesslog (Code Red II):

```
210.178.130.193 - - [07/Sep/2002:22:49:07 +0200] "GET  
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%  
u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b  
00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 400 309
```

Was „erhält“ der Server, der den inkorrekten Header akzeptiert (Programm: Listen Port 80)

Content-type: text/xml

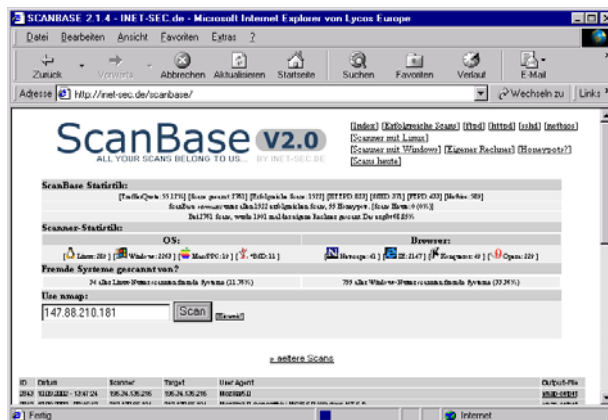
Content-length: 3379

CodeRedII <--- Daher der Name: Code Red II

```
F4)ETh~f Th~f ;Mzu KERNu EL32u GetPu rocAu D$$dg LoadLibraryA
CreateThread GetTickCount Sleep GetSystemDefaultLangID
GetSystemDirectoryA CopyFileA GlobalFindAtomA GlobalAddAtomA
CloseHandle _lcreat _lwrite _lclose GetSystemTime WS2_32.DLL
socket closesocket ioctlsocket connect select send recv
gethostname gethostbyname WSAGetLastError USER32.DLL ExitWindowsEx
\CMD.EXE d:\inetpub\scripts\root.exe
d:\progra~1\common~1\system\MSADC\root.exe hT @ hH @ hX @ t6Ff
%`0@ %d0@ %h0@ %p0@ %t0@ %x0@ %|0@ \EXPLORER.EXE
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SFCDisable
SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots
/Scripts /MSADC c:\,217 d:\,217 KERNEL32.dll ADVAPI32.dll Sleep
GetWindowsDirectoryA WinExec RegQueryValueExA RegSetValueExA
RegOpenKeyExA RegCloseKey d:\explorer.exe
```

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -27

Zurückverfolgen von Angriffen

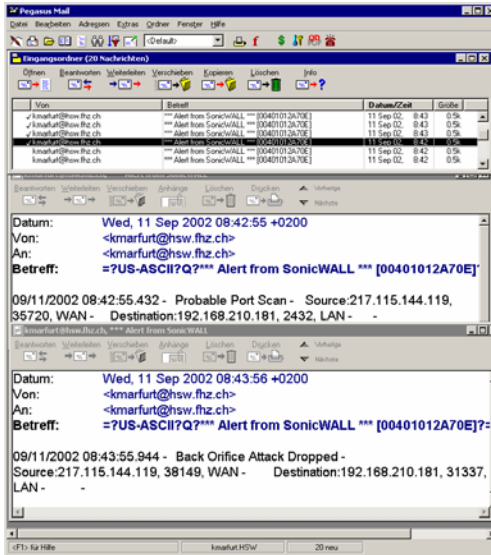


Demonstration:

- Simulierter Port Scan
- Nur auf eigene IP Adresse!!
- inet-sec.de

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -28

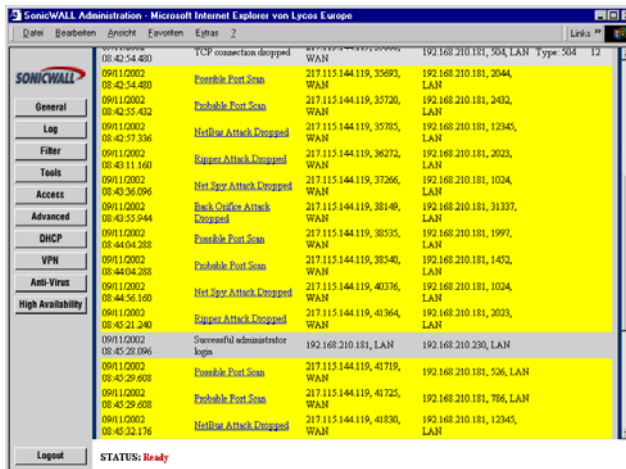
Alerts von der Firewall



- Je nach Regel löst ein Vorkommnis eine Mail aus
- Differenzierte Information über Details (Source-IP, Zeitpunkt und Typ des ausgelösten Alarms)

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -29

Logfile der Firewall



- „Bekannte“ Ports erzeugen kommentierte Fehlermeldungen
- Serien von „wilden“ Syncs werden als mögliche Scans registriert

Forensics im IT-Umfeld
Spurensuche – Konrad Marfurt / Carlos Rieder - August 2002 -30

Diagnose und Massnahmen

- Sofortmassnahme: Absenderadresse sperren
- Nur IP-Adresse bekannt: Nachforschen bei Registrierern (z.B. www.arin.net) oder bei „Privatdetektiven“ wie www.sampade.org
 - Domain name: hswlu.ch
 - Holder of domain name: Hochschule fuer Wirtschaft Luzern, Konrad Marfurt, Luzern
- Kontaktaufnahme mit Betreiber
 - Beachten: Zeitverschiebung, Sprache, selten richtige Ansprechperson
- Spurensicherung an der „Quelle“, sofern kooperativer Betreiber
- Führt leider oft nur auf Relais-Station (im schlechteren Fall offshore)

Spuren auf Applikationsebene

transaction monitor

- Laufende Überwachung der An- und Abmeldevorgänge und der Benützung bestimmter Applikationen
- Überwachung und Protokollierung von Zugriffen auf ein Datenbanksystem zwecks Rollback im Falle des Abbruchs einer Transaktion
- Bei Datenbanksystemen werden Inhalte der Änderungen auch zwischengespeichert

Spurensuche - Prinzipielles

- e-Information ist nicht an ein Medium gebunden
→ Kopierbarkeit, Veränderung ohne sichtbare Spur
- Nachvollziehbarkeit der Beweisführung bedingt Nachweis der Authentizität des (kopierbaren) Beweismittels
- Korrektes Vorgehen dokumentieren. Muss ggf. nach langer Zeit nachvollziehbar sein
- 4-Augen Prinzip bei Ermittlungen (rechtlich korrekt)
- Sorgfältige Behandlung der Beweismittel (Schutz vor (unsichtbar bleibenden) Manipulationen)

Phase 1: Sichern (stark situationsbedingt)

- Am laufenden Rechner (sofern möglich):
 - Systemzeit, angemeldete Benutzer dokumentieren
 - Laufende Prozesse identifizieren und dokumentieren (z.B. bei einem Web-Server, Router, Firewall)
 - Rechner stoppen (zur Momentaufnahme mittel Image)
- Hardwarekonfiguration dokumentieren
 - Datenträger identifizieren (auf Backup-Systeme achten)
 - System überwachen
- Bitweise Kopie des Systems (sofern möglich):
 - Ohne Änderung am System (Beweisqualität)
 - Digitale Signatur über Original und Kopie anfertigen
 - unter mindestens 4 Augen
- IT-Security Lab: „Spurensuche im IT-Umfeld“

Phase 2: Aufarbeiten

- Arbeitskopien der zu analysierenden Daten erstellen
- Zusammenstellung der vorhandenen Datenträger und deren Inhalte (Verzeichnisse) anfertigen
- Bei Bedarf / Verdacht nach versteckten Aufzeichnungen suchen
 - unbenutzte Bereiche von Backupmedien
 - spezielle Speicherbereiche (vgl. „Datenspeicherung“)
 - „gelöschte“ Daten soweit möglich rekonstruieren

Phase 3: Analysieren

- Erstellen einer Liste von Suchwörtern oder Signaturen gesuchter Muster (z.B. Bilder, Programme, ...)
- Analyse der zugänglichen Bereiche bezüglich dieser Kriterien
- Zusammenhänge sowie Anomalien (z.B. Filetyp / Extension) suchen und dokumentieren (z.B. „4d 5a“ bzw. „MZ“ am Anfang eines ausführbaren .DLLs)
- Einsatz von geeigneten Werkzeugen (Demonstration)
- IT-Security Lab: „Spurensuche im IT-Umfeld“

Professionelle Werkzeuge (z.B. Encase)

- Zuverlässige Sicherstellung der Daten
- Beweisbare Unverändertheit
- Preview Möglichkeit
- Leistungsstarke Suchmöglichkeiten
 - Files
 - Bilder
 - Schlüsselwörter
- eScript-Sprache zum Programmieren von Suchsequenzen
 - Alle WEB-Adressen
 - Spezielle Dateitypen
- Details unter www.encase.com



Verhindern von Spuren

- Verschlüsselung
 - Wirksamer Algorithmus
 - Langes Passwort
 - Gesamte Disk verschlüsseln
- Richtig löschen
 - Daten
 - Temporär Verzeichnis
 - Internet Temporär Files
- Wipe Free Disk Space (regelmässig)

Verhindern von Spuren

- Nur verschlüsselte Dokumente per E-Mail
 - Pretty Good Privacy (PGP)
 - Privat Crypto (www.utimaco.com)
- PDA verschlüsselt
 - Beim Palm genügt „privat“ nicht
- Natel
 - Keine vertraulichen Daten

Links

- www.fbi.gov
- www.interpol.int/Public/TechnologyCrime
- www.encase.com
- www.vogon.de
- www.evidence-eliminator.com
- www.forensic-computing.ch
- www.securityfocus.com
 - Mailing list: forensics