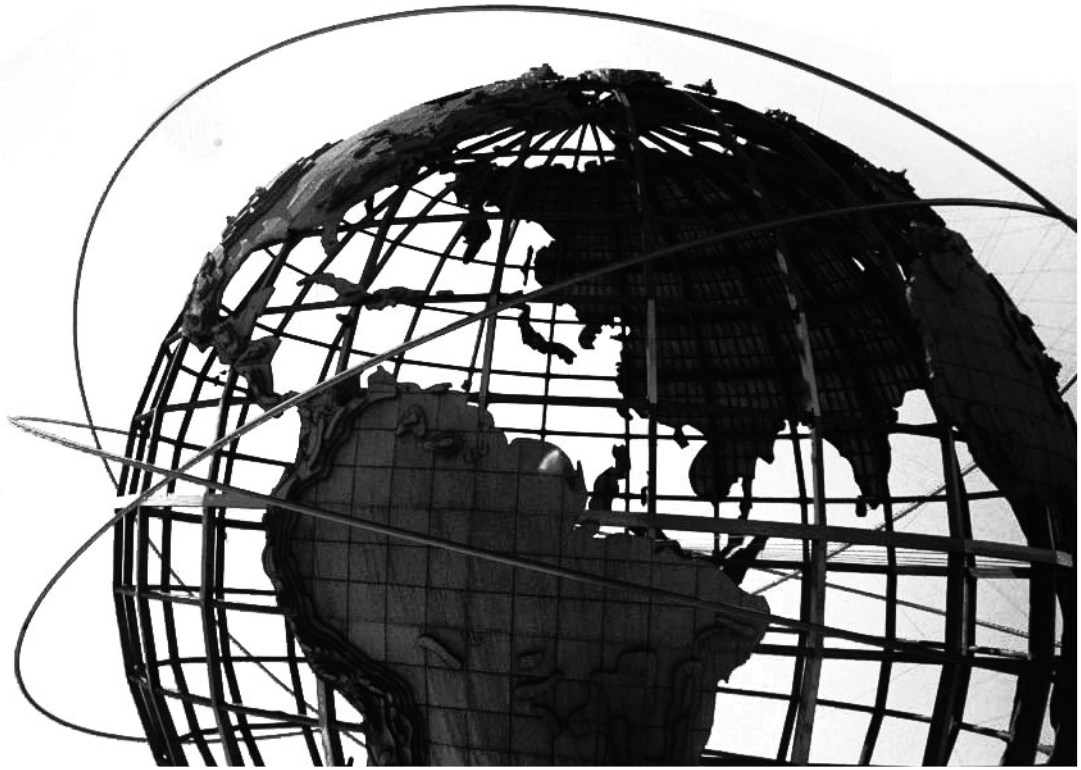
BAKER & MCKENZIE

Cyber Forensics

Die Sicherung digitaler Beweismittel

Dr. Lukas Feiler, SSCP
Erich Fried Realgymnasium
18. Februar 2014



Themen

1. Einsatzgebiete & Grundsätze von Cyber Forensics
2. Web Browser-Spuren
3. Meta-Daten in Office-Dokumenten
4. Dateisystem-Forensik
5. Beweismittel im laufenden System
6. Logfiles
7. Temporäre Dateien
8. Maßnahmen gegen den Missbrauch von forensischen Methoden

Einsatzgebiete für Cyber Forensics

- Untersuchungen der Strafverfolgungsbehörden
  - zB jemand wird verdächtigt, ein aktives Mitglied von Anonymous zu sein
  - zB jemand wird verdächtigt, mit Insider-Informationen zu handeln
- Unternehmens-interne Untersuchungen
  - zB der Eigentümer des Unternehmens will herausfinden, wer in Absprachen mit Wettbewerbern verwickelt war
  - zB das Unternehmen will herausfinden, ob ein Mitarbeiter Industriespionage begangen hat
- Geheimdienstliche Informationsbeschaffung
  - zB NSA / GCHQ interessieren sich für den Inhalt der Festplatte einer Geschäftsfrau bei der Einreise in die USA / UK

Grundsätze der Beweismittelsicherung

- Erhaltung des Zustandes des ursprünglichen Beweismittels
  - Bereits das Einschalten eines PCs verändert dessen Zustand
  - → zB zu analysierenden Datenträger kopieren und nur die Kopie analysieren
- Sicherung der Datenintegrität im forensischen Prozess
  - Wie kann sichergestellt werden, dass die Daten während der Analyse nicht verändert werden?
  - → Erster Schritt vor Beginn der Analyse: Kryptographische Checksum der Daten berechnen (zB md5sum)
- Dokumentation
  - Jeder Schritt muss dokumentiert werden

Web Browser-Spuren – 1 von 2

- Browser History (Ctrl-H)
  - Wann wurde welche URL aufgerufen?
  - Tools:
    - http://www.nirsoft.net/utils/mozilla_history_view.html
    - http://www.nirsoft.net/utils/iehv.html
- Download History (Ctrl-J)
- Browser Cache
  - Firefox: about:cache
  - Tools:
    - http://www.nirsoft.net/utils/mozilla_cache_viewer.html
    - http://www.nirsoft.net/utils/ie_cache_viewer.html

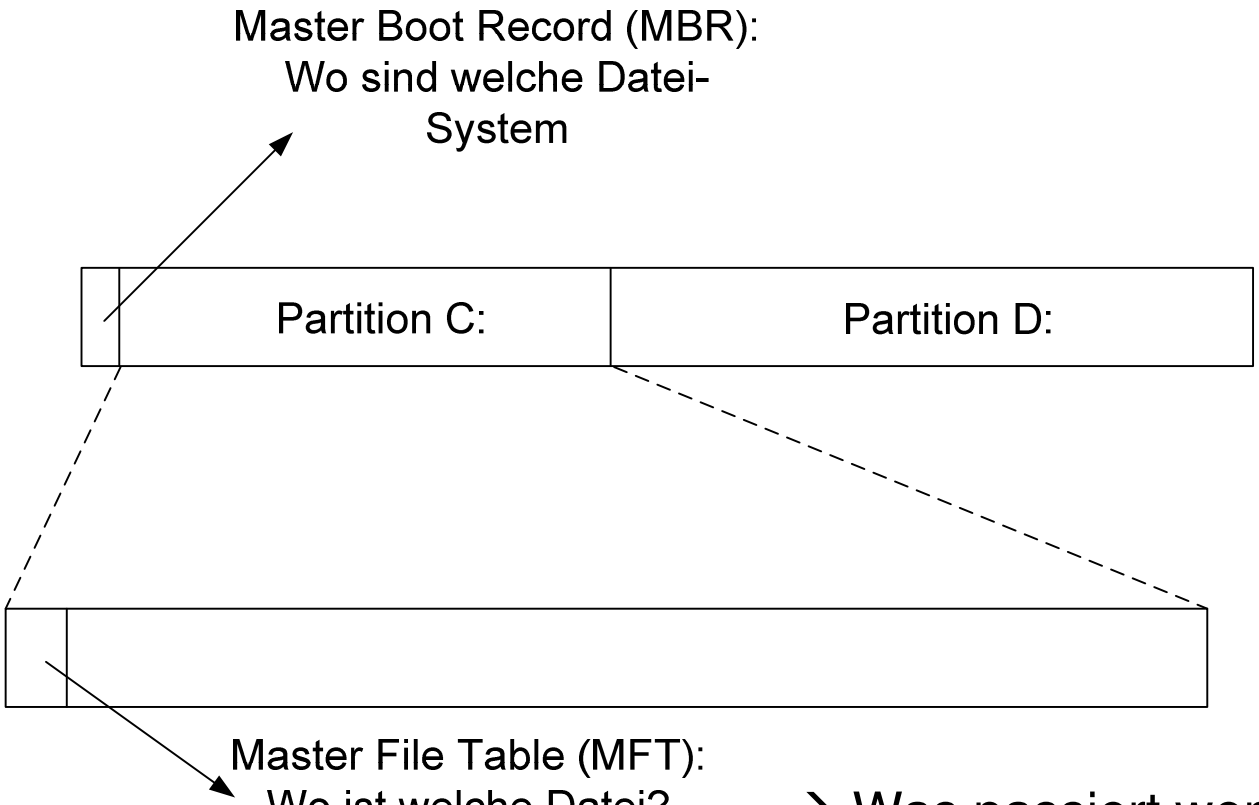
Web Browser-Spuren – 2 von 2

- Form History
  - Browser speichert by default was man in Textfelder eingibt
  - zB Firefox:
    - %UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random>.default\formhistory.sqlite
    - SQLite-Client nötig: zB http://sourceforge.net/projects/sqlitebrowser/files/latest/download
- Cookies
  - Werden von fast jeder Website verwendet
  - Tools:
    - http://www.nirsoft.net/utils/mzcv.html
    - http://www.nirsoft.net/utils/iecookies.html

Meta-Daten in Office-Dokumenten

- Office/Excel/PowerPoint
  - Bei geöffnetem Dokument: Datei | Eigenschaften
  - Meta-Daten entfernen:
    - Office 2003: http://www.microsoft.com/de-de/download/details.aspx?id=8446
    - Office >2010: File | Infos | Check for Issues | Inspect Document
- PDF-Dateien
  - File | Properties
  - Meta-Daten entfernen
    - zB Adobe Acrobat Pro

Dateisystem-Forensik - 1 von 4



→ Was passiert wenn eine Datei gelöscht wird?

Dateisystem-Forensik - 2 von 4

- Wiederherstellen „gelöschter“ Files
  - Datei ist im MFT nicht mehr enthalten
  - Solange sie nicht überschrieben ist, gibt es sie aber noch
  - Zahlreiche Tools suchen im nicht-allozierten Bereich einer Partition
- Schnell-Formartierte Partition
  - Es wurde nur der MFT gelöscht
- Glöschte Partition
  - Die Partition wurde aus dem MBR gelöscht
  - Die Daten der Partition einschließlich MFT gibt es so lange, bis sie nicht überschrieben sind

Dateisystem-Forensik - 3 von 4

- Wie lösche ich eine Datei „richtig“?
  - → zuerst mehrmals überschreiben, erst dann „löschen“
  - Windows: sdelete
    - http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx
  - Linux: shred

Dateisystem-Forensik - 4 von 4

- MAC-Zeiten
  - Last Modified
  - Last Accessed
  - Metadata last Changed (UNIX) od. Creation Time (Windows)
  - → Betrachtung der MAC-Zeiten aller Files auf einem System auf einer Zeitachse oft Aufschlussreich

- MAC-Zeiten bei Directories
  - Last modified: Wann zuletzt eine Datei in dem Verzeichnis erstellt oder gelöscht wurde

Beweismittel im Laufenden System - 1 von 2

- Laufende Prozesse
  - Windows:
    - Task Manager
    - Process Explorer
  - Linux/Unix
    - ps –aux
- Offene Netzwerk-Verbindungen
  - Windows:
    - TCPView
  - Linux/UNIX
    - Netstat
- Inhalt des Arbeitsspeichers (zB /dev/mem unter Linux)

Beweismittel im Laufenden System - 2 von 2

- Problem 1: Order of Volatility
  - Arbeitsspeicher
  - Netzwerk-Status
  - Laufende Prozesse
  - Festplatteninhalt
- Problem 2: Kann man dem laufenden System noch trauen?
  - Kompromitiertes System liefert uU falsche Ergebnisse
  - zB Rootkits

Logfiles

- System-Logfiles
  - Wann hat sich wer eingelogged/ausgelogged?
  - Wann wurde das System gestartet/heruntergefahren/in den Ruhezustand versetzt?
  - Windows:
    - eventvwr.msc
  - Linux/UNIX
    - Syslog files unter /var/log/*
- Applikations-Logfiles
  - zB Sype: Call History; Chat-Protokoll; zB mittels http://www.nirsoft.net/utils/skype_log_view.html

Temporäre Dateien

- Tempfiles werden von diversen Programmen angelegt …
  - … aber uU niemals gelöscht
  - Unter Windows: C:\Windows\Temp (ua)
  - Unter Linux/UNIX: /tmp/

Maßnahmen gegen den Missbrauch von forensischen Methoden

- Physische Sicherheit: physischen Zugriff auf Gerät verhindern
- Private Browsing
  - Privatspähre-Einstellungen des Browsers nutzen!
- Sicheres Löschen von Dateien
- Vorsicht vor dem Ruhezustand
  - Inhalt des Arbeitsspeichers wird unverschlüsselt auf die Festplatte geschrieben

Maßnahmen gegen den Missbrauch von forensischen Methoden #2

- Verschlüsselung im Allgemeinen
  - Keine Verschlüsselung ist (für die NSA) unknackbar
  - Weakest Link ist meistens das Passwort
- Verschlüsselung einzelner Dateien
  - Werden temporäre Dateien unverschlüsselt gespeichert?
  - Werden die entschlüsselten Daten unverschlüsselt in den Hauptspeicher kopiert?
- Festplattenverschlüsselung
  - Sicheres Backup – Verfügbarkeit vs. Vertraulichkeit

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

Dr. Lukas Feiler, SSCP
lukas.feiler@bakermckenzie.com