IT-Forensik

Mark Bröcker, B.Sc.

Quintalog Systemhaus GmbH

broecker@quintalog.de

Mein/unser Bezug zum Thema:

- IT-Forensik für Insolvenzverwalter,
- Datenrettung, IT-Sicherheit,
- Externer Datenschutzbeauftragter

und ...

- IT- und TK-Administration für Windows, Mac, UNIX/Linux
- Datenbankentwicklung
- Virtualisierung
- SAN/RZ-Betrieb

Inhalt & Ablauf

- Prinzipien und Abläufe in der IT-Forensik
  mit dem Fokus auf dauerhaften Medien (HDD, DVD, SSD)
  (nicht den Spuren im Hauptspeicher, also „offline“/„kalt“)
  und Nachweis von Nicht-IT-Straftaten,
  d.h. insbesondere Vermögensdelikten
- Nebeneffekt: Methoden zur (privaten) Datenrettung
- abwechselnd mit technischen Details,
  Praxiserfahrungen und Empfehlungen

- Live-Vorführung einzelner Schritte
- Fragen – gerne auch mittendrin!

IT-Forensik, **die reine Lehre**

1. Identifikation und **Sicherstellen**
   alles relevante (?!), kein zweiter Versuch...
2. **Analysieren**
   Anlegen von Indizes, Fundstück-Sammlung,
   Vergleich der Belege – ohne Meinung/Wertung
3. Aufbereitung und **Präsentieren**
   Verfahren und Ergebnisse so aufbereiten,
   daß Laien die Herangehensweise und die
   Ergebnisse nachvollziehen können,
   Schlußfolgerungen überlassen wir Dritten.

[Quelle z.B. Wikipedia]

Sicherstellen

- **Was?**
  Server (klar!), aber auch Arbeitsplatz-PCs, Notebooks, USB-Sticks, CDs, Ordner (Passworte?), Dongle, Online-Bestände?
  >> alles, was das Wiederherstellen später ermöglicht, also Medien und eventuell **Teile der Arbeitsumgebung**
- **Wie?**
  Original mitnehmen (19“-Rack?, RZ), Betriebsfortführung?!
  oder Kopie erstellen (6 TB bei 20 LUNs im SAN?)
  aber auch Arbeitsplatz-PC mit 1TB-Platte – alles wichtig?

  Praxis: Methode, die hinterher plausibel erklärbar ist
  ⟶ nur die Dateien/belegten Blöcke ???
  aber: es gibt keinen zweiten Versuch
  (doch lieber **dd und Original mitnehmen**?)

  Prüfsummen und Inhalte bei defekten Originalen ändern sich.
- **Bei SSDs ändern sich die „gelöschten“ Blöcke der Originale laufend!**

Sicherstellen 2

- **Regel**: Die Medien müssen revisionssicher, d.h. ***beweisbar*** unveränderbar sichergestellt werden, wenn man sich später darauf berufen möchte.
- **praktisch**: Medien-Liste (handschriftlich!), einfaches Duplizieren, z.B. dd & SHA-1(-2-3)-Ermittlung vom Polizisten vor Ort unterschreiben lassen.
- **Realität** in der Insolvenz-Forensik:
  lieber alles schnell mitnehmen, man kommt eh' nicht im Zivil-Prozess für die Gläubiger noch an Geld, Staatsanwaltschaft kommt erst Jahre später.
  Zum Glück: ***Freie Beweiswürdigung*** durch Richter

Analysieren (Ziele, Zeit, Geld)

- **Ach so:** spätestens jetzt Prüfsummen und 1:1 Backups, wegen eigener Paddeligkeit!
- **Ziele definieren**, wonach suche ich überhaupt, widerspricht aber der reinen Lehre der Neutralität, **Insolvenz-Forensik → Geld!**
- Suchen in
  - Anwendungsprogrammen/Datenbanken und/oder
  - in den Filesystemen/Dateien und/oder
  - auf den blockbasierten Medien und/oder
  - den Molekülen der Medien nach früheren Inhalten ;-)
- Für vereinfachte erneute Suche Indizes und Fundlisten (>> Fallverwaltungssoftware)

Analysieren 2 - wo noch und womit?

- Suche in vermeindlich gelöschten Bereichen/Dateien, Blöcken
- Suche in Verschnitt-Bereichen (Zufallsfunde) von Dateien (am Ende von Dateien)
- Suche in Hybernate- und Swap-Partitionen/Dateien
- z.B. Magic-Code-Suche: Photorec ⟶ Empfehlung
- In-Place-Carving: CarvFS mit Scalpel
  (auch bei verschachtelten Dokumenten)
- (Vielleicht mit Festplatten-Tools in defekten Bereichen)

Analysieren 3 - Techniken

- Mounten von dd-Images mittels Loop-Device unter Linux: mount chef-sda1.dd /taeter -o loop,ro
- Testdisk, Photorec
- Autopsy, PTK, mit NSRL/NIST bekanntes ausblenden
- CarvFS, Foremost, Scalpel
- Virtualisierung für das Darstellen kompletter Anwendungsumgebungen → z.B. Suche nach Buchhaltungstransaktionen
- Heute schon parallel: Spurensuche im Internet: Google, Facebook, zukünftig: Bildersuche
- Praktisch nicht gelöst: Verschlüsselung (Trojaner vorher?)

Analysieren 4 – wie Taten erkennen?

- E-Mails & Dokumente wurden gelöscht: z.B. Belege für das Wissen um die finanzielle Situation der Firma ⟶ Insolvenzverschleppung und persönliche Haftung von Geschäftsführern und Gesellschaftern
- Unterschiede der Papierbuchhaltung zur IT
- Zahlungsströme mit statistischen Anomalien:
  Endziffern kommen falsch häufig vor
- Zahlungsströme zu bestimmten Daten: Freitag abend / Wochenende
- IT-Buchhaltungs-Lage der Firma stimmt nicht mit der Buchhaltung des Kunden überein (Scheinrechnungen, ...)
- Alles stimmt buchhaltärisch, nur juristisch hätte die Zahlung gar nicht erfolgen dürfen. (nun wissen wir, welche Zahlung wann genau)
- **Zweck:** im Verlauf der Insolvenzabwicklung bekommen die Gläubiger mehr Geld, z.B. von den Gesellschaftern – **deshalb** (nicht *nur* wegen des „Thrills“ ;-) macht man die IT-Forensik, daß die bösen bestraft werden, kommt vielleicht erst viel später – wenn überhaupt ...

Strukturieren, Präsentieren

- Fall-Software sollte uns ein Ablaufprotokoll liefern
- Schriftlicher Bericht: was wurde wann womit wie gemacht?
- Powerpoint für Richter und die Presse ;-)
- Managementzusammenfassung ⟶ Dilbert

  (MA 1. entlassen und auf Schadenersatz verklagen, 2. weiß zuviel: befördern oder 3. abfinden)
- Abrechnung (+++), dauerhafte Archivierung

- Bedenke: Staatsanwaltschaft kommt erst nach zwei Jahren!

Die Zukunft der IT-Forensik?

Längst da: iDingse, anDroids und die Cloud müssen analysiert werden – Widerstand ist zwecklos...

Quellen, beide Cubes: http://searchengineland.com/meet-the-new-borg-google-facebook-apple-54969, Picard: http://miquelpuig.wordpress.com/2010/01/27/jobbs-llega-20-anos-tarde-jean-luc-picard-ya-tenia-tablets-2/, Rechte nicht geklärt.

Ein paar Quellen und Verweise

- Wikipedia ⟶ IT-Forensik
- Wikipedia ⟶ SHA256 etc.
- Computer-Forensik - Sachbuch, nett, einfach auf deutsch
- AFF – Advanced Forensic Format, neues Standard-Format für forensische Datenerhebung (Container)
- Carving – Theorie auf deutsch aufgearbeitet
- SysRescCD – viele Kommandozeilen-Tools (u. SPARC!) (GPL)
- Helix3 – früher DIE Forensik-CD, hier noch eine freie Version mit Fall-Bearbeitungs-Software und Windows-Live-Teil
- BackTrack (5R2) – heute Linux-Forensik-Standard, alle Tools aber DVD
- Encase, Ältere Demo-Version – für Klicki-Bunti-Fensterln, Defacto-Forensic-Standard EFW-Format ($)
- X-Ways-Forensics – deutschsprachige Windows-Software ($)
- CarvFS – hier Doku und Sourcen, sonst Live-CDs (GPL)
- NSRL/NIST – u.a. MD5-Summen zum Ausblenden unwichtiger Dateien
- Photorec / Testdisk – sucht nach Datei(-Stücken), bzw. Partitionen auf dem Block-Device mittels bekannter Signaturen (GPL)
- IDEA - suche nach Ziffernmustern u. Zahlungsströmen ($)
- SSDs bedürfen möglicherweise – je nach Dateisystem einen extra TRIM-Befehl zum sicheren Löschen
- ein Podcast liefert für die SSDs technische Grundlagen
- xmount - neueres Tool (GPL) (->Link auch auf ForensicWiki: Tools im Überblick)
- DFF – Digital Forensic Framework (GPL) – es geht weiter
- Maltego CaseFile – doch etwas CSI ...