Informationssicherheit und IT-Forensik

4-02 – IT-Forensik

Lernziele dieser Einheit

- Grundbegriffe und Grundprinzipien kennenlernen
- Die juristische Komponente einschätzen (insbesondere: nicht alles was technisch möglich ist, ist auch erlaubt)
- Die verschiedenen Kopierarten kennen (logisch, physisch, …)
- Die Locard‘sche Regel und ihre Bedeutung kennen
- Prinzip und Bedeutung „gelöschter Dateien“ kennen
- Forensic Readiness kennen

HSH Nordbank entschuldigt sich bei ehemaligem Manager

- 20.03.2011, FAZ
- September 2009: Ein Team der Bank findet auf dem PC des New Yorker Filialleiters E-Mails, die zu Kinderporno-Bildern führen.
- Taggleich: Fristlose Entlassung des Mitarbeiters.
- September 2010: Staatsanwaltschaft erkennt und teilt mit, dass Dritte mit kriminellen Handlungen das Material untergeschoben haben.
- März 2011: HSH Nordbank kommt zum gleichen Schluss und entschuldigt sich öffentlich.
- Währenddessen: Ablehnung bei Bewerbungen!
- http://www.faz.net/-01pzyv

Was ist IT-Forensik?

Klassische Vorstellung eines Forensikers:

Quelle linkes Bild: Ralf Roletschek, publiziert unter GFDL 1.2

IT-Forensik

Ursprung

(lateinisch forum = Marktplatz [auf dem insbesondere eine Gerichtsverhandlung stattfindet])

bezieht sich auf Arbeitsgebiete, in denen
z.B. (kriminelle) Handlungen untersucht werden, typischerweise in Bezug auf Gerichtsverfahren und Strafvollzug, aber auch privatwirtschaftlich, zivilrechtlich oder in Bezug auf Non-Compliance

z.B.

- Rechtsmedizin
- Forensic Services von Rechtsanwälten und Wirtschaftsprüfern

IT-Forensik

Definition: IT-Forensik, Digitale Forensik, Computerforensik

- Teilgebiet der Forensik, bezogen auf digitale Datenspuren
- Gegenstand: Untersuchung und Beurteilung verdächtiger Vorfälle / Handlungen im Zusammenhang mit IT-Systemen
- Grundlage: digitale Spuren, die erfasst, gesichert, aufbereitet, analysiert bzw. interpretiert und sachverständig beurteilt werden
- Stellt Sachverhalte, insbesondere Abläufe, Tatbestände, Tatmuster und, so möglich, handelnde Personen fest – **Klärung von W-Fragen**
- Beantwortung von **Beweisfragen** zu digitalen Datenspuren mit dem Ziel zusätzlicher Erkenntnisgewinn, der anders nicht zu erlangen wäre
- Dabei werden **Hypothesen** aufgestellt und sowohl belastende als auch **entlastende** Anzeichen berücksichtigt

IT-Forensik

Definition: IT-Forensik, Digitale Forensik, Computerforensik (weitere)

- Anwendung von Untersuchungs- und Analysetechniken, um Beweise von bestimmten IT-Systemen/-Geräten zu sammeln und zu bewahren auf eine Weise, die für eine Präsentation vor Gericht geeignet ist
- Ziel ist eine strukturierte Untersuchung unter Erhalt einer dokumentierten Beweismittelkette, um genau herauszufinden, was auf dem System passiert ist und wer/was dafür verantwortlich ist

Quelle z.B.: Bhadane & Patil (5/2016): A Review on Computer Forensics, in: International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), 4(5), 173-178 (meine Übersetzung), siehe auch http://searchsecurity.techtarget.com/definition/computer-forensics

IT-Forensik

Definition: IT-Forensik, Digitale Forensik, Computerforensik (weitere)

Untersuchung entscheidend verbessern können. Es wird deshalb für den vorliegenden Leitfaden festgelegt:

> IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.

Quelle: Leitfaden IT-Forensik (2011), S. 8, S. 13, BSI

IT-Forensik

Weitere Begriffe: IT-Systeme, Taten und Datenspuren

IT-Systeme können bezogen auf einen Vorfall sein:

- **Tatwerkzeug** (z.B. Nutzung von IT entgegen Richtlinien, Fälschung von Buchungen oder Dokumenten)
- **Spurenträger** (z.B. Webproxy) oder
- **Tatziel** (z.B. lahmgelegter Webshop, entwendete Kundendaten, übernommene Rechner)

IT-Forensik

Gedankenspiel Erkenntnisquelle: Methoden je nach Vorfall (Auswahl)

- **Tat einer Person:** Daten vom Client und Server inklusive Backups sichern: Endgerät (PC oder Laptop) physisch sichern, ggf. Mobilgerät sichern, ebenso je nach Handlung Mails vom Mailserver, Dokumente vom Fileserver
- **Wirtschaftskriminalität:** z.B. Buchhaltungssystem sichern, Projektverzeichnis, E-Mails und Dokumente, eDiscovery
- **„Diebstahl“ von Software:** Vergleich von Code in Code-Repositorys, Funktionsweise vergleichen
- **Gerichteter Malware-Befall:** Reverse Engineering, Verhaltensbeobachtung
- **Zeitliche Korrelation von Datenspuren zwischen Artefakten:** Zeitleistenanalyse, Zeitstempelanalyse

IT-Forensik

Gedankenspiel Erkenntnisquelle: Methoden je nach Vorfall (Auswahl)

- **Eindringling im Netzwerk:** Schattennetzwerk, Netzwerkforensik, Logfileforensik, Virtualisierungsforensik, IT-Forensik auf Honigtopf
- **Abfluss vertraulicher Daten:** IT-Sicherheit von IT-Systemen, Mail- und Fileserver, Netzwerk, angeschlossene USB-Geräte / Datenträger, Inhalte von Mails / Anhänge, auch Webmailer-Reste, Netzwerkverbindungen in Cloud-Dienste
- **Untersuchung einer Festplatte:** Intellektuelle Sichtung, Dateisystem und Partitionen, Betriebssystem, Programme, zuletzt genutzte Dokumente, Einstellungen, Netzwerke, auffällige Dateien und weitere Datenspuren, Internet-Forensik, zahlreiche Spezialauswertungen möglich

Beispiele für Computerkriminalität

Tabelle 15.6

Computer als Ziel krimineller Handlungen	Computer als Instrument krimineller Handlungen
Verletzung der Vertraulichkeit geschützter elektronischer Daten	Diebstahl von Geschäftsgeheimnissen und nicht autorisierte Kopien von Software oder durch Urheberrecht geschütztem geistigen Eigentum, wie Artikel, Bücher, Musik und Videos
Nicht genehmigter Zugriff auf ein Anwendungssystem	Maßnahmen zur Unterschlagung
Bewusster Zugriff auf einen geschützten Computer für Betrugsdelikte	E-Mails mit Drohungen oder für Belästigungen
Vorsätzlicher Zugriff auf einen geschützten Computer und fahrlässige oder absichtliche Verursachung von Schaden	Vorsätzlicher Versuch, die elektronische Kommunikation zu unterbinden
Bewusste Übermittlung eines Programms, Programmcodes oder von Befehlen, die vorsätzlich einen geschützten Computer schädigen	Illegaler Zugriff auf gespeicherte elektronische Kommunikation, einschließlich E-Mails und Voice-Mails
Androhung der Schädigung eines geschützten Computers	Verbreitung oder Besitz von Kinderpornografie über einen oder auf einem Computer

Quelle: Laudon/Laudon/Schoder (2015), Tabelle 15.6

IT-Forensik

Teilgebiete (Auswahl)

- Datenträger (z.B. Festplatte, SSD): **Datenträgerforensik, Festplattenforensik, Disk-Forensik**
- Speicherinhalte (Hauptspeicher, Prozessspeicher): **Speicherforensik**
- Analyse von Massendaten (z.B. strukturiert aus Datenbanken, oder große Mengen „loser“ Dateien einschließlich E-Mails → e-Discovery): **Datenforensik, Forensische Datenanalyse**
- Zahlreiche Bereiche und Methoden, z.B. nach IT-System/Gerät (Netzwerkforensik, Mobilforensik, Videoforensik), nach Betriebssystem (Windows-Forensik), nach Anwendung (Mailforensik), nach Artefakt (Logfile-Forensik, Webbrowser-Verlaufsforensik), …
- Nach dem Vorgehen: **post mortem** (klassisch) vs. **live** (im Rahmen von **Incident Response**, dabei zu untersuchende Systeme notwendig und dokumentiert verändernd)

IT-Forensik

(Ein mögliches) Prozessmodell und exemplarische Tätigkeiten

Totforensik (post mortem)

Live-Forensik

Netzwerkforensik

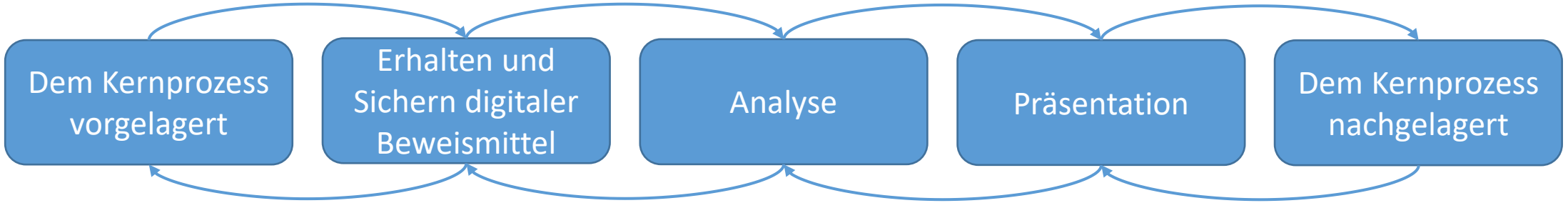
Sachverständigengutachten

eDiscovery

Sicherheitsvorfall

Datenabfluss

Compliance-Verstoß



IT-Forensik

(Ein mögliches) Prozessmodell und Zuordnung zu COBIT und ITIL

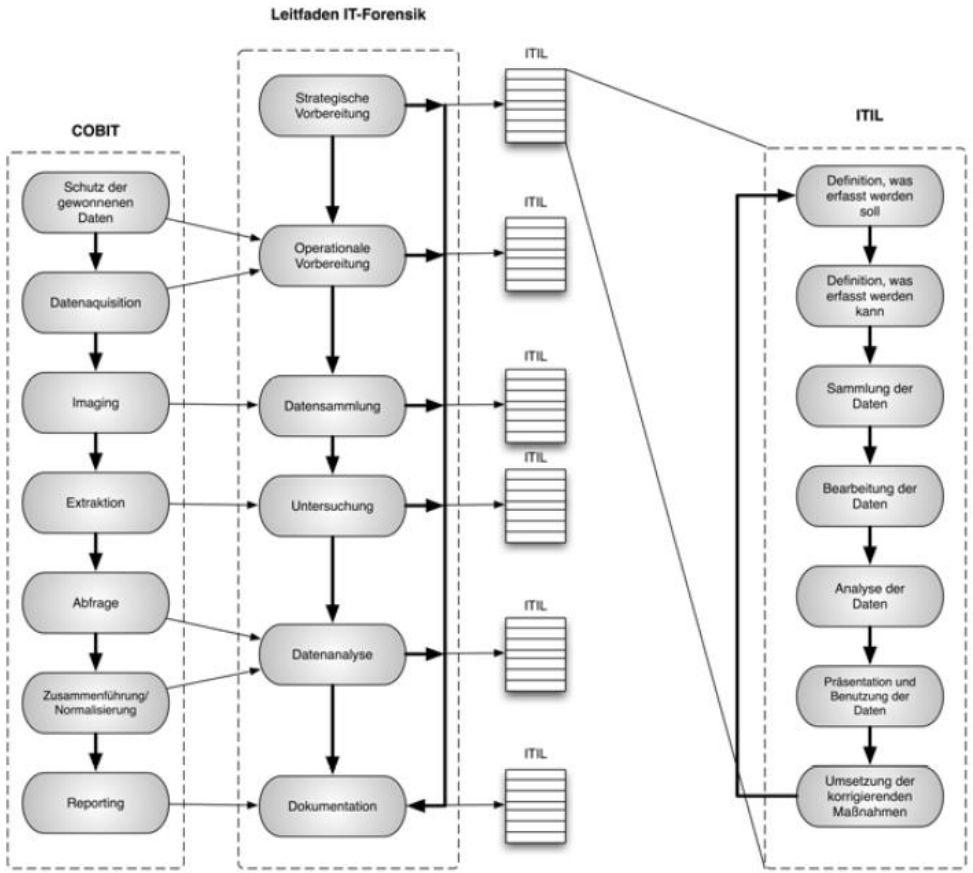
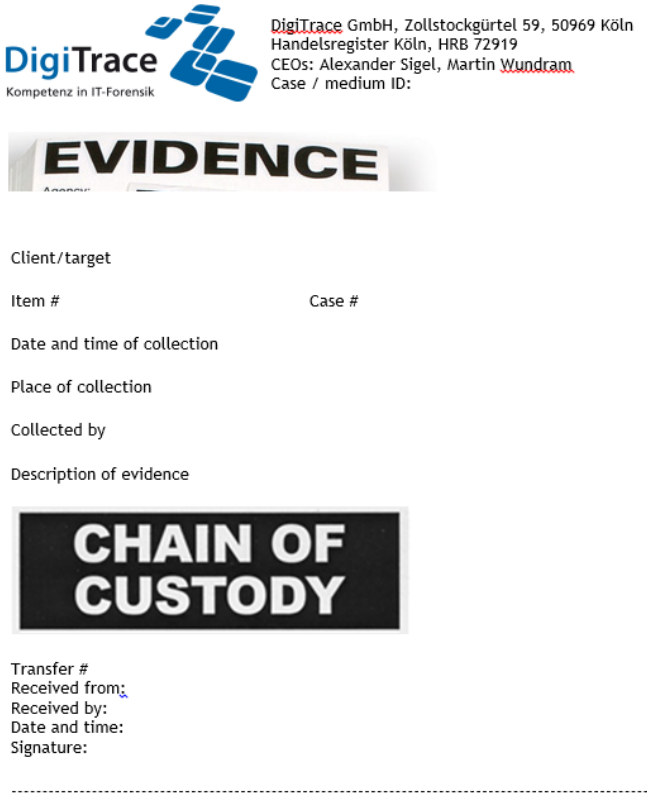


Abb. 3: Der forensische Prozess in Zusammenspiel von COBIT und ITIL

Quelle: BSI-Leitfaden IT-Forensik, S. 14

Erhalten und Sichern digitaler Beweismittel: Beweismittelmanagement / Beweismittelkette



DigiTrace Kompetenz in IT-Forensik

DigiTrace GmbH, Zollstockgürtel 59, 50969 Köln
Handelsregister Köln, HRB 72919
CEOs: Alexander Sigel, Martin Wundram
Case / medium ID:

EVIDENCE

Client/target

Item # Case #

Date and time of collection

Place of collection

Collected by

Description of evidence

CHAIN OF CUSTODY

Transfer #
Received from:
Received by:
Date and time:
Signature:

IT-Forensik

Erhalten und Sichern digitaler Beweismittel: Datenträger kopieren

- Hardware-Writeblocker sollen Schreibzugriff auf Originaldatenträger unterbinden
- Zahlreiche Hersteller z.B. Tableau, Wiebetech, Logicube
- Eine neue Herausforderung stellen SSDs dar

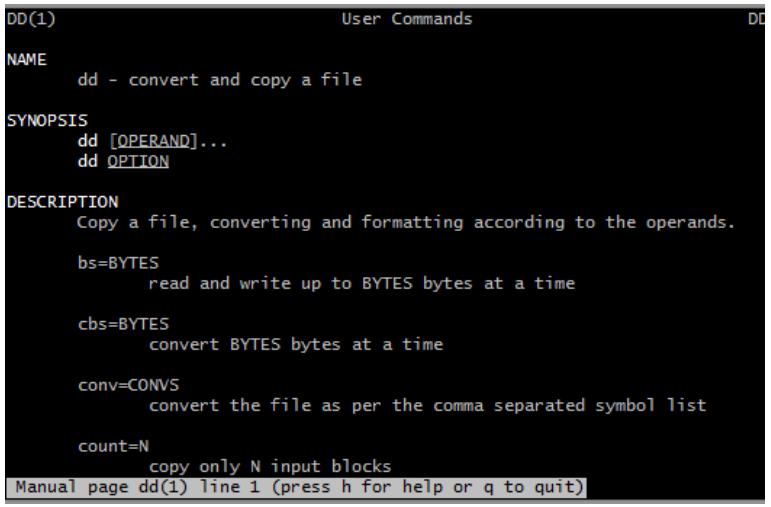
Erhalten und Sichern digitaler Beweismittel: Methode blockweise Sicherung (Imaging)

dd (disk dump) als bekanntestes Werkzeug für blockweises Kopieren von Datenströmen in der Linux-Welt:

Manuell auf der Kommandozeile

```
dd if= … of= …
```

von if (input file) nach of (output file)



Liest (hier) das sogenannte Block-Device aus

IT-Forensik

Locard‘sche Regel / Locard‘sches Prinzip

- Kontakt zwischen zwei Objekten (Täter, Opfer, Tatort, …) nicht möglich ohne wechselseitige Spuren
- Gilt in der Praxis auch in der IT:
  - Täter hinterlässt Logdatei-Einträge
  - Täter löscht Logdatei, hinterlässt aber gelöschte Datei im Dateisystem
  - Täter überschreibt Datei vorher, hinterlässt dadurch aber wieder Einträge in anderer Logdatei

IT-Forensik

- Achtung:
  - IT-Forensik ist nicht nur bei IT-Sicherheitsvorfällen notwendig

- (anlassunabhängige) Compliance-Prüfungen
- Verdacht auf Datenabfluss
- Fraud Investigation (Schmiergeldzahlungen, Betrugsversuche)
- Unterstützung von Insolvenzverwaltern
- …

- Daher: Forensic Readiness ist nicht nur als präventive Maßnahme gegen IT-Angriffe („Hacker“) wichtig und notwendig

IT-Forensik

BSI-Leitfaden IT-Forensik

- BSI-Leitfaden IT-Forensik
- Grundlagen- und Nachschlagewerk

- praxisbezogen
- erklärt, was IT-Forensik ist, wie sie in Unternehmensprozesse eingebettet werden kann, wie vorgegangen wird, was erwartet werden kann, …
- gibt auch praktische Erläuterungen zu einzelnen forensischen Artefakten
- Problem: Technik schreitet rasant voran, Leitfaden ist von 2011:

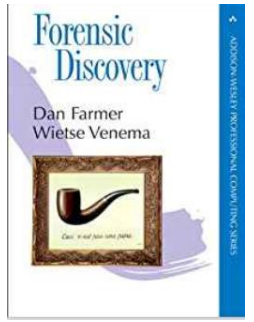
> „Die grundlegende Methode ‚Betriebssystem‘
> – Das Betriebssystem MS Windows XP“

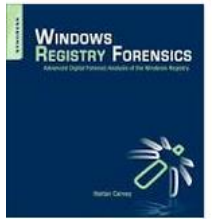
- Wichtig: Grenzen/Einschränkungen der genutzten Ressourcen müssen klar sein

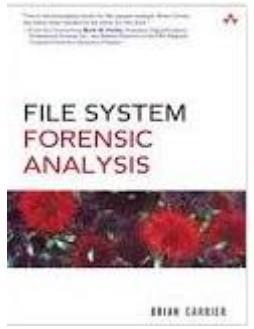
IT-Forensik

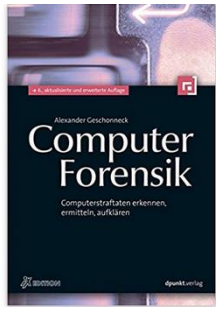
Literatur (Beispielhafte Auswahl)

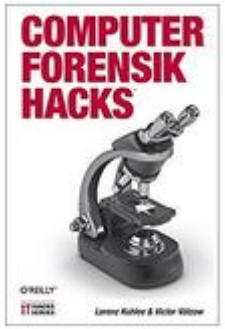
- **Prinzipien**: Farmer / Venema: Forensic Discovery
- **Dateisysteme**: Carrier: File System Forensic Analysis
- **Grundlagen, Vorgehensweise**:
  - Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären, 6. Aufl. 2014
  - Kuhlee & Völzow: Computer Forensic Hacks
  - Willer: PC-Forensik: Daten suchen und wiederherstellen
- **Windows-Analyse**: Carvey: Windows Forensic Analysis; Windows Forensic Analysis Toolkit, Windows Registry Forensics











IT-Forensik

„Empfindliche“ Datentypen (Geschonneck, 2006)

- **Flüchtige Daten** (weg, sobald PC aus, ändern sich aber auch im Laufe der Zeit „von selbst“, z.B. Hauptspeicher)
- **Fragile Daten** (können sich beim Zugriff ändern, z.B. Zeitstempel)
- **Temporär zugreifbare Daten** (nur zu bestimmten Zeitpunkten zugänglich, z.B. verschlüsseltes Dateisystem, Inhalte einer Anwendung)

IT-Forensik

Beweissicherung in der Reihenfolge abnehmender Flüchtigkeit der Datenspuren

- Ziel: alle bzw. möglichst viele beweisrelevante Daten sichern
- Daten sind teilweise flüchtig, fragil bzw. nur temporär verfügbar, d.h. bei Nichthandeln irgendwann verloren
- Beweissicherung darf Daten nicht verändern / vernichten
  - Falls es nicht anders geht, dann „sauber“ dokumentieren
- Täter können eventuell Daten weiterhin verändern oder löschen oder Werkzeuge auf dem zu untersuchenden System kompromittieren
- **Daumenregel: Daten grundsätzlich in der Reihenfolge erwartbar zunehmender Dauerhaftigkeit sichern**
  - Z.B. erst Hauptspeicher, dann offene Dateien und Netzwerkverbindungen, dann temporär verbundene oder entschlüsselte Dateisysteme, dann Massenspeicher, dann Logfiles / Backups
- Es kann jedoch andere, auch konfligierende Ziele geben
  → Einzelfallbetrachtung

Quelle: RFC 3227

IT-Forensik

Arten von Kopien

- **Logische Kopien**
- **Physische Kopien**
- **Mischformen**

Arten von Kopien: Logische Kopien

- **Logisch**: wie mit Dateiexplorer
  - Kann ausreichen, aber gelöschte Dateien so nicht wiederherstellbar
  - Kopiert nur den Inhalt von im Dateisystem sichtbaren Dateien, und dort auch nur den von der Datei wirklich verwendeten Teil (ohne Schlupfspeicher = slack space)
  - Z.B. Logfiles, Konfigurationsdateien, Sicherung temporär entschlüsselter Dateisysteme

Arten von Kopien: Physische Kopien

- Wirkliche **physische Kopien** (1:1 bitgenaue IT-forensische Images): Datenträger wird blockweise ausgelesen, unabhängig vom Dateisystem (wie mit dd = disk dump)
  - Grundsätzlich: Einsatz von Schreibschutz (Writeblocker), um Originaldaten nicht zu verändern
  - Vollständigkeit? Fehlerbehandlung? Nachweis der Identität mit dem Original? (Hash)
  - Günstigenfalls können so gelöschte, aber noch nicht überschriebene Dateien zumindest teilweise wieder hergestellt werden
  - Bereits für SSDs schwierig, deren Firmware eigenständig Optimierungen und damit Datenveränderungen vornimmt

Arten von Kopien: Mischformen

- **Mischformen**
  - „Halb-physische“ Kopien bei Mobiltelefonen
    z.B. Kopie erreichbarer Dateien aus dem Dateisystem über verschiedene Wege, Jailbreak = Rooting. Bestimmte geschützte Bereiche können dabei nicht gesichert werden, z.B. bei neueren Apple-Versionen E-Mails, bestimmte Sandboxen ohne Zugriff
  - Ältere Versionen, die möglicherweise gelöscht wurden, können z.T. über Abgleiche mit Schattenkopien (VSC), Dateijournale, Backups oder Gegenspuren auf verbundenen Systemen rekonstruiert werden
  - Images mancher Imaging-Programme enthalten nicht alles, was ein volles physisches Image enthalten würde
  - Auch logisch kopierte Datenbanken enthalten möglicherweise noch nur zur Löschung vorgemerkte Einträge

IT-Forensik

Gelöschte Daten: Warum kommt es zu gelöschten Dateien?

- Verursacht vom Betriebssystem oder Anwendungen
  - Updates
  - Geänderte Konfiguration
    (z.B. Windows: Systemwiederherstellung wird ausgeschaltet)
  - Löschen nicht mehr benötigter Dateien
    (z.B. alte Logfiles nach Log-Rotation)

- Aktive Handlung eines Benutzers
  - Gewöhnliche Nutzung (Datei erstellen, dann umbenennen, nicht mehr benötigte Datei löschen)
  - Datenschutz-konformes Handeln oder Verschleierung von Handlungen (Cleaning-Programme, Nulling)
  - Deinstallationen

IT-Forensik

Gelöschte Daten: Was passiert beim Löschen einer Datei?

- Die Datei ist nach der Löschung (Eintrag z.B. in der „Inhaltsliste“ MFT eines NTFS-Dateisystems: jetzt nicht mehr alloziert) nicht mehr im Dateisystem
- Sie ist damit im freien Speicher
- Sobald das Betriebssystem Platz braucht, kann der Speicherplatz der ehemaligen Datei überschrieben werden
- Solange der Platz noch nicht wiederverwendet wurde, kann sie (ggf. teilweise) wiederhergestellt werden

IT-Forensik

Gelöschte Daten: Carving – eine von verschiedenen Möglichkeiten zur Wiederherstellung

- Daten sind nicht mehr im Dateisystem enthalten
- Man muss sie nun „von der Platte kratzen“
- Dazu werden freie Speicherbereiche sequenziell durchlaufen mit einer Heuristik
- Diese kennt Charakteristika zu Dateien verschiedenen Typs, insbesondere bekannte Dateisignaturen (Köpfe, gelegentlich auch Rümpfe) und erwartbare Längen
- Trifft das Suchmuster zu, wird der Block des Musters als Dateikandidat herausgeschrieben
  → viele **falsch-positive** Ergebnisse
  → generischer Ansatz, der immer möglich ist

IT-Forensik

Übersicht über wichtige Grundsätze IT-forensischer Arbeitsweise

- Rechtskonforme Sicherung
  (Vermeidung Beweisverwertungsverbot, Compliance-Problem darf durch die Untersuchung nicht größer werden …)
- Keine Arbeit auf Originaldaten: Erst unveränderte Kopie sicherstellen, dann auswerten
  (nicht möglich bei Live-Forensik, dann möglichst wenig verändern und Veränderungen dokumentieren)
- Lückenlose Nachvollziehbarkeit, Beweisbarkeit, Beweismittelkette, Dokumentation, Sorgfalt
- Reihenfolge der Sicherung (Prinzip abnehmender Flüchtigkeit)

Zeitleisten

- Zeitleisten stellen graphisch oder tabellarisch zeitliche Abläufe dar
- Ereignisse werden zeitlich eingeordnet
- Zeitpunkte und Zeiträume
- Vorteile:
  - ermöglichen oft, zeitliche Zusammenhänge besser zu verstehen und besser zu erkennen
  - Können im Laufe einer Untersuchung kontinuierlich vervollständigt werden
  - Ermöglichen obere und untere Zeitschranken leicht zu erkennen („Erst der Mord, dann die Leiche. Mord kann nicht vor Tag x erfolgt sein, weil …f“)
  - Können auch als Dokumentationstechnik verwendet werden, um Dritten einen schnellen Überblick zu ermöglichen

IT-Forensik

Kurzvorstellung (Nennung) verbreiteter Werkzeuge

- Autopsy und The Sleuth Kit
- X-Ways Forensics
- Encase
- FTK
- Cellebrite UFED
- …

Gabelungssituationen

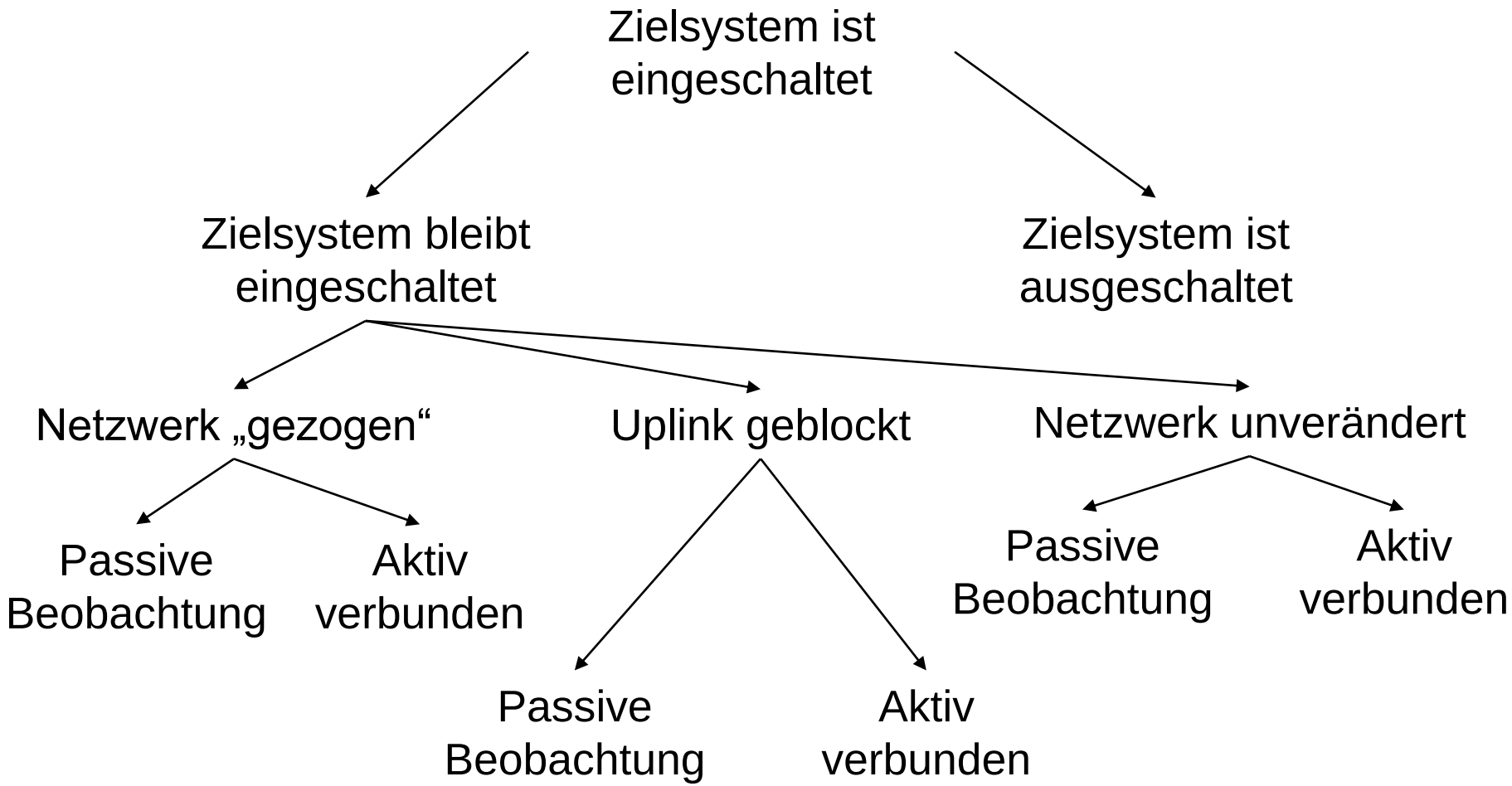
- Was sind **Gabelungssituationen** in der IT-Forensik?
  -> Konkrete Entscheidungen
  mit (unbekannten) Folgen
- Etwa: „mache A oder B, nur eines davon ist möglich“
- Beispiele:
  - System ausschalten, oder laufen lassen
  - Aktive Verbindung oder passives Beobachten
  - Netzwerk „kappen“/jammen oder unverändert lassen

Gabelungssituationen

- **Strategische** Gabelungen:
  - Ermitteln vs. Absichern
  - Proaktiv vs. abwartend
  - …
- **Taktische** Gabelungen:
  - Materialauswahl, welche Ausrüstung wird mitgenommen
  - Schwerpunkte setzen (etwa Fokus auf Netzwerkverbindungen)
  - …
- **Operative** Gabelungen:
  - Konkrete technische Entscheidungen im Einsatz „an der Maschine“

Gabelungssituationen

- Beispiel für **mehrstufige operative Gabelungen**:



IT-Forensik

Rechtliche Einschränkungen

- Ermittlungsmaßnahmen bzw. Maßnahmen, bei denen (private) IT-Forensiker involviert sein können, stellen oftmals einen Eingriff in Grundrechte des Betroffenen dar:
  - Menschenwürde
  - Datenschutz
  - Fernmeldegeheimnis
  - Schutz des Eigentums
  - …
- **Je intensiver der Eingriff, desto höher die Anforderungen an die Rechtfertigung**

Rechtliche Einschränkungen

Wer hat welche Befugnisse?

staatliche Ermittlung

- Umfassende Befugnisse:
  - Durchführung von Durchsuchungen
  - Beschlagnahme von Beweismitteln
  - Überwachung (TKÜ, Wohnraumüberwachung, …)
  - Vernehmung von Beschuldigten oder Zeugen
  - …

Rechtliche Einschränkungen

Wer hat welche Befugnisse?

private Ermittlung

- *„Der Gesetzgeber behandelt den Privatermittler wie jeden Privatmann, d.h. es gibt keine hoheitlichen oder quasi-hoheitlichen Rechte zur Vornahme von vertraglich vereinbarten Ermittlungsmaßnahmen“* (Grüner, Der Ermittlungsauftrag durch Unternehmen zur Überwachung von Mitarbeitern und Organen)

- Keine Befugnis, Zwangsmaßnahmen anzuwenden, etwa wegen eines Verdachts zum Zwecke einer Untersuchung die Datenverschlüsselung eines Mitarbeiters ohne dessen Zustimmung zu überwinden -> Gefahr der Strafbarkeit eigener Handlung
- **Notwehr, Nothilfe** gelten grundsätzlich, aber: besondere Stellung eines externen IT-Forensikers als „Profi“
- Besonders „brisant“: Geheimes/verdecktes Vorgehen – mögliche Strafbarkeit des Ermittlers inkl. zivilrechtliche Schadensersatzklagen usw. (Haftung)!

- **Deshalb: für eine Untersuchung sollte die Einwilligung des Betroffenen vorliegen!**

Rechtliche Einschränkungen

Wer hat welche Befugnisse?

Einwilligung durch Betroffene

- grundsätzlich zwei Varianten möglich:
  - Einwilligung **vor dem Vorfall**, etwa durch Betriebsvereinbarungen, IT-Richtlinien, …
  - Einwilligung **nach dem Vorfall** und bezogen auf den jeweiligen Einzelsachverhalt:
  - *„Erklären Sie sich damit einverstanden, dass wir Ihr (auch) dienstlich verwendetes iPhone auswerten? Bitte stellen Sie uns dieses zur Verfügung und teilen uns auch den PIN zum Entsperren mit.“*
  - Alternativ: mit Rechtsbeistand prüfen, ob/wie Maßnahmen ohne Einwilligung möglich sind

Live-Analyse

Motivation

- Daten, die nur Live verfügbar sind (z.B. Prozesse im RAM, Zugriff auf Dropbox-Share)
  - Als einzige Quelle („Gibt es eine nicht-persistente Kompromittierung im System?“)
  - Als erster Schritt („Erst FDE-Passphrase, dann Zugriff auf HDD)
  - Ergänzend („was man hat, das hat man“/“doppelt genäht…“)
- Aus wirtschaftlichen Gründen (Live-Triage)
- Wenn persistente Daten viel zu umfangreich sind (SAN mit 10 PB Daten)
- Oder schlicht: das zu untersuchende System darf/soll/kann nicht ausgeschaltet werden

Live-Analyse

Definition

- Es gibt im Gegensatz zur Tot-Analyse bisher kein allgemein akzeptiertes Schema für das allgemeine Vorgehen
  - Sowohl die Sicherungs- als auch die Analysemethoden sind stark abhängig von der Situation
  - Auch die Reihenfolge der Anwendung von Sicherung und Analyse kann unterschiedlich sein
- Die Frage ist immer: Welche Spuren benötigt man?

- Es gibt aber auch „Standardsituationen“ die oft ähnlich ablaufen und ähnliche Vorgehensweisen ermöglichen

Live-Analyse

Planung

- Vor einer Live-Analyse sollte man sich einen Sicherungs- und Analyseplan zurecht legen
  - Welche Spuren suche ich?
  - In welcher Reihenfolge möchte ich die Spuren sichern?
  - Muss ich bestimmte Spuren am laufenden System sichern?
  - Benötige ich einen Hauptspeicherabzug?
  - Falls ja, welche Methode möchte ich dafür einsetzen?
  - Besteht die Gefahr von logischen Sprengfallen oder Rootkits?
  - Falls ja, wann und wie prüfe ich darauf?

Live-Analyse

Grobes Schema

- Falls notwendig, erst schnell flüchtige Daten am laufenden System sammeln (unter Zuhilfenahme der HW und der SW des Systems)
  - Was man hat, das hat man
  - Ggf. auch offene Kryptocontainer oder Netzwerklaufwerke inspizieren
- Davor oder danach einen Hauptspeicherabzug machen mit einer geeigneten Methode
  - Gewählte Methode hängt vom Einzelfall ab
  - Man sollte generell versuchen, die Methode zu wählen, mit der die zuverlässigsten Ergebnisse erzielt werden
- Dann später am Analyserechner den Hauptspeicherabzug analysieren (mit Tools wie volatility)

IT-Forensik

Live-Analyse: Von Strom und/oder Netz trennen?

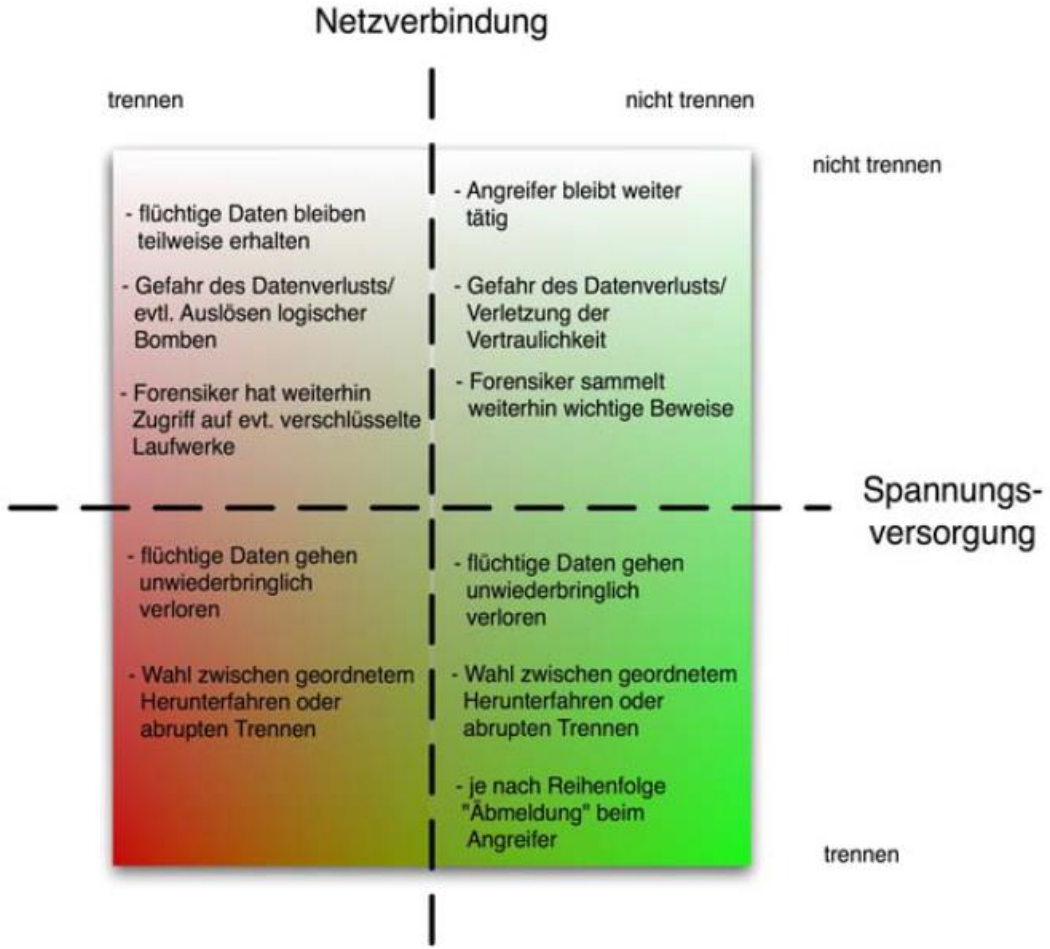


Abb. 6: Wichtige Fragestellungen beim Eintreffen am betroffenen Computersystem

= BSI-Leitfaden IT-Forensik, S. 37

Live-Analyse

Beispiel für Live-Analyse in Analyse-Station

- Cuckoo Sandbox
- „Automated Malware Analysis“
- Open-Source
- Kann Eigenschaften ausführbarer Dateien in Windows, OS X, Linux und Android durch Verhaltensanalyse erkennen und darüber einen Report erstellen
- Interessant z.B. in folgender Prozessreihenfolge: Live-Analyse -> Tot-Forensik -> Live-Analyse

Live-Analyse

Erster Beispielfall zur gemeinsamen Bearbeitung

- Die Geschichte:
  - Der Betreiber eines PC-Ladens steht im Verdacht, Mitglied der **Hackergruppe "Krümelmonster"** zu sein und DDoS-Tools, sowie **Trojaner** entwickelt und verbreitet zu haben. Bei einem anonymen Besuch im PC-Laden und einer abendlichen Observation konnte entdeckt werden, dass der Verdächtige auch Abends an seinem Laptop sitzt und daran arbeitet. Er nimmt diesen Laptop anschließend auch immer mit nach Hause. Durch einen Fensterblick in seine Wohnung konnte erkannt werden, dass er dort außer dem **Laptop** keinen Computer verwendet.
  - Es konnte unauffällig ein Foto des Arbeitsplatzes im Laden erstellt werden (nächste Folie)
- Was tun? Wie würden Sie vorgehen? Wie würden Sie den Einsatz vorab planen?

Live-Analyse

Erster Beispielfall zur gemeinsamen Bearbeitung

Live-Analyse

Zweiter Beispielfall zur gemeinsamen Bearbeitung

- Die Geschichte:
  - Die Vorstandssekretärin beklagt sich über ihren **lahmenden PC**. Der herbeigeeilte Administrator will sich auch einmal den PC selbst anschauen und bemerkt dabei, dass ein **zweites Netzwerkkabel** in den Computer hineingeführt ist. Misstrauisch öffnet er das PC-Gehäuse und findet darin einen **Raspberry Pi**. Der Administrator erkennt einen möglichen Spionageangriff und ruft die IT-Forensiker des Konzerns mit der Bitte um Aufklärung des Falles.
  - Keine angeschlossenen Devices, außer MicroSD-Karte, USB-Kabel an das Mainboard und LAN
  - Siehe Fotos auf folgenden Folien
- Was tun? Wie würden Sie vorgehen? Wie planen Sie den Einsatz und welche Strategie wählen Sie?

Live-Analyse

Zweiter Beispielfall zur gemeinsamen Bearbeitung

Live-Analyse

Zweiter Beispielfall zur gemeinsamen Bearbeitung

Forensic Readiness

Definition

- „die Maximierung der Verarbeitungsfähigkeit digitaler Beweise bei gleichzeitiger Minimierung der Ermittlungskosten“
  (frei übersetzt nach Robert Rowlingson, “A Ten Step Process for Forensic Readiness”, International Journal of Digital Evidence Winter 2004, Vol. 2, Iss. 3)

- „Erreichen eines angemessenen Niveaus an Fähigkeiten durch eine Organisation, damit diese in der Lage ist, digitale Beweise zu erheben, zu bewahren, zu schützen und zu analysieren. Zweck: diese Beweise in Rechtssachen, insbesondere in Disziplinarangelegenheiten, vor einem Arbeitsgericht oder Gericht wirksam verwenden können“
  (frei übersetzt nach CESG Good Practice Guide No. 18, Forensic Readiness)

Forensic Readiness

Grundüberlegungen

- **Forensic Readiness ist komplex**: hier nur eine Einführung in die wichtigsten Aspekte und Fallstricke
- **Forensic Readiness ist individuell**: während ein Unternehmen seine geheimsten Produktionszeichnungen schützen muss, ist für ein anderes Unternehmen ein langfristiger Ausfall der Produktionskette das schlimmste Szenario
- **Forensic Readiness zahlt sich aus**: die eigene Erfahrung der Workshopleiter zeigt, dass immer wieder wertvolle Zeit verloren geht und vor allem, dass essenzielle Spuren mit besserer Vorarbeit auswertbar gewesen wären
- **Recht-technisch**: es ist zwingend notwendig, vorab juristische und technische Aspekte gemeinsam zu betrachten
  -> Interdisziplinär: Geschäftsführung, IT, Compliance, …

Forensic Readiness

Typische Fehler

1. Sicherheit wurde in der IT-Landschaft bisher noch gar nicht berücksichtigt.

2. Auf einem Server wird Schadsoftware gefunden. Es ist völlig unklar, was für Auswirkungen dies haben könnte. Es gibt keinerlei Informationen über den Server und dessen Verwendung im Unternehmen. Altlast? Kundendaten?

3. Mitarbeiter erhält eine E-Mail und öffnet die vermeintliche Rechnung im Anhang. Ein schwarzes Fenster erscheint, der Mitarbeiter traut sich nicht, dies der IT mitzuteilen.

4. Ein PC meldet einen IP-Adresskonflikt im Netzwerk. Die IT-Abteilung weist dem Rechner eine neue Adresse zu und prüft nicht, wieso es zu dem Konflikt kommt.

Forensic Readiness

Typische Fehler

5. Der IT-Forensiker muss im Ortstermin mehrere Stunden warten, da sich die Rechtsabteilung noch nicht sicher ist, ob die Untersuchung des fraglichen Laptops überhaupt zulässig ist.

6. Auftrag an den IT-Forensiker ist unpräzise formuliert / der Forensiker muss erst im Ortstermin herausfinden, was der Auftraggeber eigentlich für einen Bedarf hat.

7. IT-Forensiker bekommt zum Ortstermin keine IT-Dokumentation. Nach dem Login auf ein System stellt er fest, dass der PC zwei IP-Adressen hat; offenbar stecken zwei Netzwerkkabel. IT-Administrator kann auf Rückfrage keine Antwort geben: „das hat mein Vorgänger gemacht“.

Forensic Readiness

Typische Fehler

8. Nach der durchgeführten Untersuchung wird bekannt, dass es noch ein Backup von dem Mailserver gegeben hätte, auf dem sich eventuell weitere Daten befunden hätten.

9. Ein Backup existiert zwar, für dieses muss aber eine gesonderte rechtliche Genehmigung eingeholt werden (Funktionsänderung der Daten).

10. Logins von Benutzern können nicht mehr nachvollzogen werden, da der zu untersuchende Zeitraum drei Monate zurückliegt. Der Domaincontroller speichert seine Logdateien aber nur für zwei Tage.

11. Der Auftraggeber ist völlig schockiert, als der IT-Forensiker ihm mitteilt, dass die Sicherung von drei 2 Terabyte-Platten und einem Mobilgerät ca. einen Arbeitstag dauert. Er beauftragt nicht und will den Fall aussitzen.

Forensic Readiness

Vorgehensvorschlag

1. **Prävention**
2. **Bedarf festlegen und Szenarien entwickeln**
3. **Awareness**
4. **Rechtliche Absicherung**
5. **Partner suchen**
6. **Planung zukünftiger IT-Forensik-Einsätze**
7. **IT-Dokumentation pflegen**
8. **Datensicherungen berücksichtigen**
9. **Konfiguration der IT**
10. **Re-Evaluation**

Anti-Forensik

Definition

- ***Jeder Kompromittierungsversuch zur Reduktion der Verfügbarkeit oder Nützlichkeit von Beweisen für den IT-forensischen Auswerteprozess***
  (angelehnt an Definition von Ryan Harris)

- Es gibt im Wesentlichen Maßnahmen der **Datenvermeidung** und **Datenverschleierung/Datenvernichtung** (können unbemerkt und unbemerkbar bleiben) und **aktive Angriffe** (können und führen oft zu erkennbaren Unregelmäßigkeiten)

Anti-Forensik

Angriffsziele / Zielsetzung aus Tätersicht

Angriffsziel / Zielsetzung	**Untersuchung vermeiden/verhindern**	**Untersuchung verzögern**
Auf das Asservat bezogen	Festplatte wipen; Registry wipen; Steganographie; full disk encryption; ...	Große Mengen Pr0n, ungewöhnliche Hardware, ...
Auf den Auswerter bezogen	Präkontamination mit Auswerterdaten	Zeitstempel manipulieren
Auf das Auswertesystem bezogen	Code injection Angriffe; buffer overflows; directory loop Angriffe	ZIP-Bomben, Hashes von Dateien verändern (Hash-Datenbanken!)

Anti-Forensik

„Self-Anti-Forensik“ bzw. allgemein Verlässlichkeit von IT-Forensik-Werkzeugen

- **Produkt A (Web-History-Tool)**: ~30% der Firefox-History (SQLite-Datenbank!) wurden kommentarlos übersehen
- **Produkt B (Standard-Suite)**: „Fehler 42 in Komponente XY bei Auswertung MFT. OK klicken für Weitermachen“ → großer Teil der Dateien wurde nicht angezeigt, unter anderem die Outlook-.PST mit entlastenden Spuren!
- **Produkt C (Live-Forensik-Tool)**: Reproduzierbarer Absturz bei Sicherung des DNS-Cache, weitere Auswertung nicht möglich
- **Produkt D („Mächtiges“ Artefakt-Tool)**: Neueste Version findet in eigenem Case-Dataset von älterer Version plötzlich eine Vielzahl neuer protokollierter Webseitenaufrufe
- **Produkt E (Anti-Forensik- / Datenlöschungs-Tool)**: Wurde verwendet, um Spuren gründlich zu vernichten, hat aber innerhalb einer SQLite-Datenbank nicht alle Einträge überschrieben, sondern einzelne Einträge „übersehen“

Anti-Forensik

Gegenmaßnahmen

- Aufmerksamkeit
- Zeit
- Vorbereitung
- Robustere Tools!
- Tools mit mehr Logging
- Logs auswerten
- Erfahrung mit Anti-Forensik (was kann passieren?)

Ein Auftrag an Sie: unser Musterfall

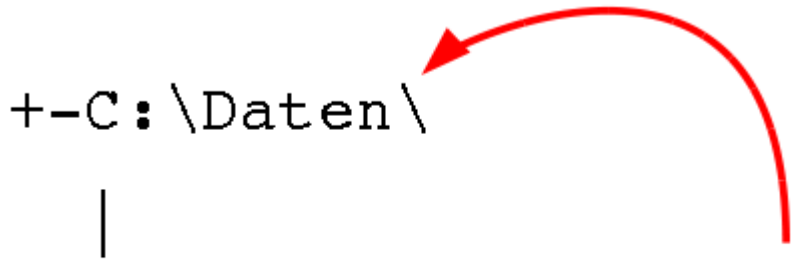
Wiederkehrende, vorlesungs- und übungsbegleitende Übungsaufgabe

- Überarbeiten Sie Ihre Planung für die Errichtung einer „smarten“ Einbruchmeldeanlage 2.0 für das Handwerksunternehmen Ihrer Eltern
- Nehmen Sie sich dafür jetzt 5 Minuten Zeit
- Beantworten und begründen Sie unter eigenen Annahmen z.B. folgende Fragen:
  - Ändern Sie Ihre bisherige Planung?
  - Welche Maßnahmen fallen Ihnen ein, um eine gute „Forensic Readiness“ zu erreichen, also für zukünftige IT-forensische Untersuchungen an Ihrer EMA gut vorbereitet zu sein? Was glauben Sie, könnten typische Fragestellungen sein, z.B. nach einem Einbruch?
  - Skizzieren Sie mögliche Problemstellen. Wo könnten Probleme lauern?

Live-Hack

Anti-Forensik an einem laufenden System und anschließende Aufklärung

- ACHTUNG:
  - Verwendung ist außerhalb des eigenen Systems grundsätzlich illegal
  - Z.B. Verändern von Daten, Computersabotage




```
+-C:\Daten\
  |
  +-Unterverzeichnis\
  | |
  | +-Unterverzeichnis\
  | | |
  | | +-Unterverzeichnis\
  | | +-Inhalte.txt
  | |
  | +-Inhalte.txt
  |
  +-Inhalte.txt
```