Digitale Forensik

Gerhard Klostermeier

Hochschule für Technik und Wirtschaft Aalen

18. Juli 2013

Inhalt

Definition

Unter dem Begriff Forensik werden die wissenschaftlichen Arbeitsgebiete zusammengefasst, in denen kriminelle Handlungen systematisch identifiziert beziehungsweise ausgeschlossen sowie analysiert oder rekonstruiert werden. [a]

[a] Quelle: Wikipedia

Definition

Forensic science (often shortened to forensics) is the practical application of science to matters of the law. In criminal law, forensics science can help prove the guilt or innocence of the defendant. In civil actions, forensics can help resolve a broad spectrum of legal issues through the identification, analysis and evaluation of physical evidence. [a]

[a] Quelle: Sally Kane

Forensik

Ziele

- Identifizieren
- Analysieren
- Rekonstruieren
- (Ausschließen)

Inhalt

Definitionen

Definition

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. [a]

[a] Quelle: Leitfaden „IT-Forensik“ (BSI)

Forensik vs. Digitale Forensik

- Digitale Forensik ist ein Teilgebiet der Forensik
- Beschränkt sich auf IT-Systeme
- Beweise/Artefakte/Spuren sind virtuell

Bestandteile

- Network Forensics
- Multimedia Forensics
- Image Forensics
- Mobile Device Forensics
- etc.

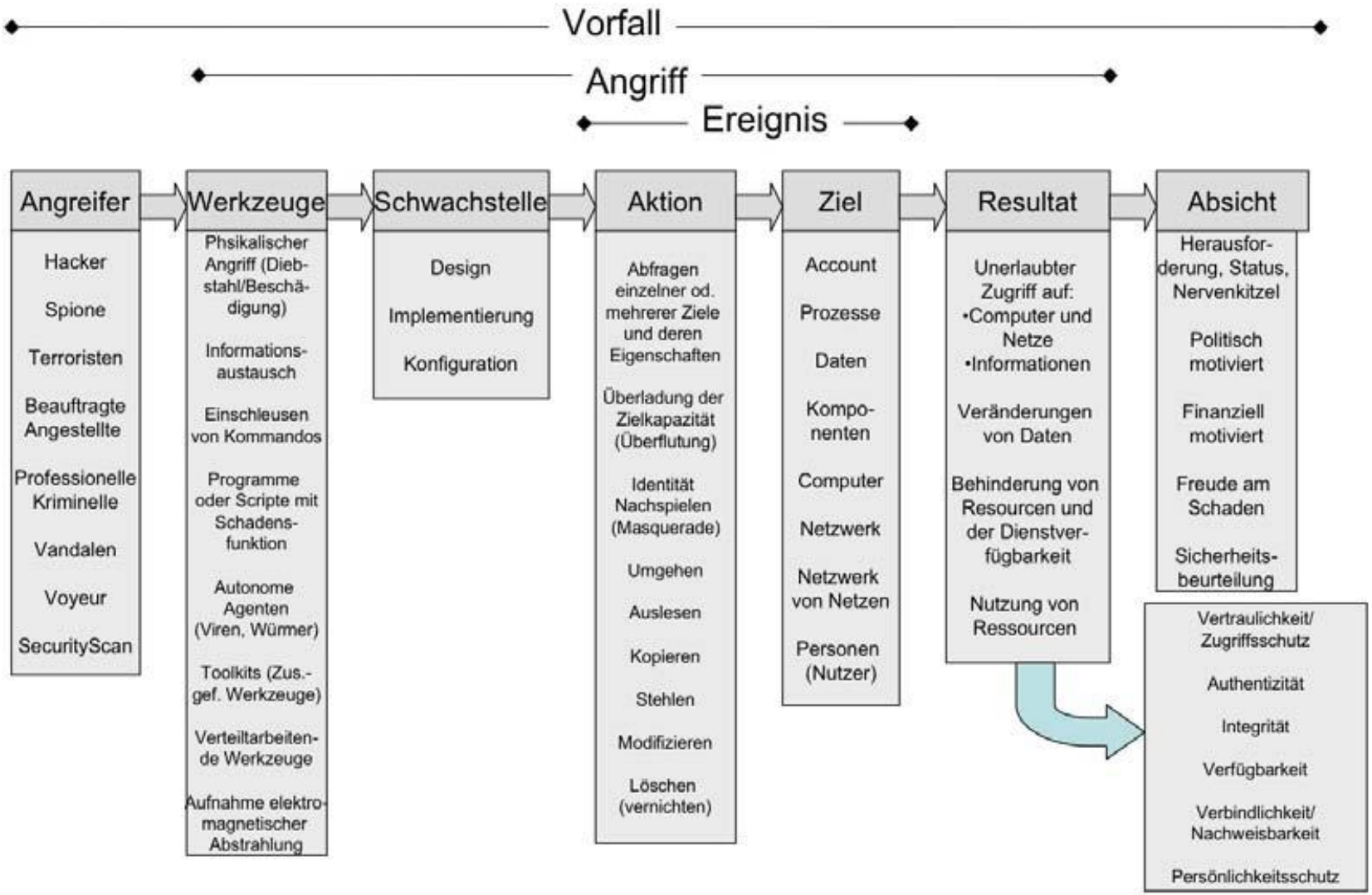
Problem

Beweise/Artefakte/Spuren sind virtuell und können manipuliert werden, ohne Spuren zu hinterlassen.

Abhilfe:

- Write Blocker (Zertifiziert)
- Dupplicator/Imager (Zertifiziert)
- Zeugen
- Sicherheitsüberprüfung des Forensikers (Ü1, Ü2, Ü3)

Vorgehensweise



1

[1] Quelle: Jana Dittmann, IT-Security

Vorgehensweise

Fragestellungen

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Eventuell auch:

- Wer hat es getan?
- Was kann dagegen getan werden?

Inhalt

Tools

Hardware

Tools

Hardware

Betrachtungsmöglichkeiten:

- Betriebssystemebene
- Dateisystemebene
- Dateiebene
- Netzwerkebene
- etc.

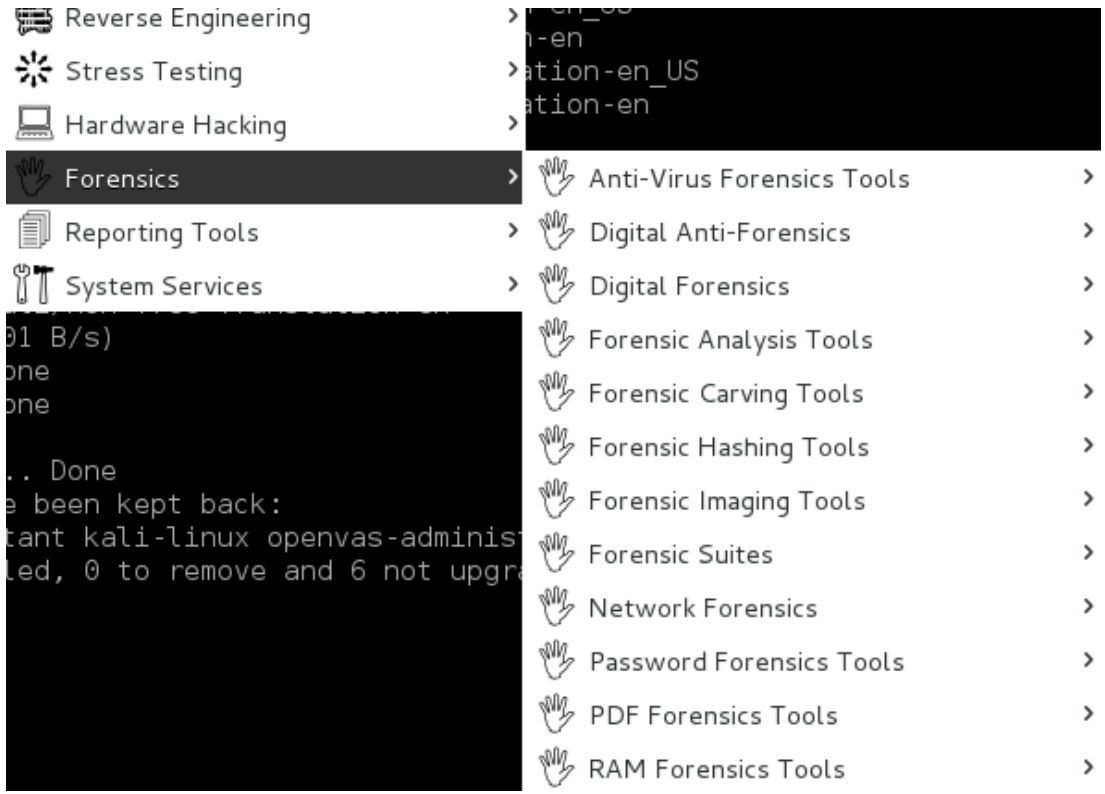
Richtiges Tool

- Die Wahl des „richtigen“ Tools hängt ab vom Betrachtungswinkel auf das Problem.
- Die Betrachtung des Problems sollte aus allen möglichen Richtungen Erfolgen.

Software

Ein kleiner Auszug

- Betriebssystemebene
  - log2timeline
  - RegRipper
- Dateisystemebene
  - wisp
  - foremost
- Dateiebene
  - ImageExifTool
  - pdf-parser
- Netzwerkebene
  - Wireshark
  - tcpxtract
- etc.



ExifTool

- Image Exiftool (von Phil Harvey)
- Zweck: Anzeigen und Manipulieren von Exif (Meta) Daten
- Typische Exif Daten:
  - Datum und Uhrzeit
  - Brennweite
  - Belichtungszeit
  - Kameramodell
  - Firmware Version
  - Autor
  - Firma
  - Erstellungs–/Bearbeitungsprogramm
  - GPS-Koordinaten
  - ...und viiiiiele weitere!

RegRipper

- RegRipper/rr (von Harlan Carvey)
- Zweck: Windows Registry (hive files) parsen und aufbereitet anzeigen
- Modularer Aufbau (Plugin-System)
- Windowstool $\rightarrow$ Ausführung unter Linux mit `wine` möglich
- Registry hives:
  - HKEY_USERS:
    `\Documents and Setting\User Profile\NTUSER.DAT`
  - HKEY_USERS\DEFAULT:
    `\Windows\system32\config\default`
  - HKEY_LOCAL_MACHINE\SAM:
    `\Windows\system32\config\SAM`
  - HKEY_LOCAL_MACHINE\SECURITY:
    `\Windows\system32\config\SECURITY`
  - HKEY_LOCAL_MACHINE\SOFTWARE:
    `\Windows\system32\config\software`
  - HKEY_LOCAL_MACHINE\SYSTEM:
    `\Windows\system32\config\system`

log2timeline

- log2timeline (von Kristinn Gudjonsson)
- Neues log2timeline: plaso (Achtung: Alpha)
- Zweck: Logfiles und Artefakte parsen um sie auf einen Zeitstrahl abbilden zu können
- Mögliche Quellen:
  - Apache Logs
  - Brwoser History
  - PCAP Datein
  - Windows 2k/XP Event Log
  - PDF Metadaten
  - Papierkorb
  - etc.

wisp

- Windows INDX Slack Parser (von TZWorks LLC)
- Zweck: NTFS INDX Records parsen und Eigenschaften (Attribute) extrahieren
- Typische Eigenschaften:
  - Dateiname
  - Dateigröße
  - Flags (z.B. gelöscht)
  - Erstellungszeitpunkt
  - Letzte Modifizierung (Zeitpunkt)
  - etc.

Fragen

Danke. Fragen?