Forensik: Wie holen wir das Maximum aus den verfügbaren Daten

HiSolutions Know-how to go

HiSolutions AG

Dania Blum

Dania Blum

Senior Consultant

E-Mail: blum@hisolutions.com

Fachliche Schwerpunkte:

- Definition, Implementierung und Weiterentwicklung von vollumfänglichen Business Continuity & Crisis Management Systemen
- Umsetzung von Anforderungen aus BSI IT-Grundschutz 200-4
- Planung, Durchführung und Nachbereitung von Notfall- und Notfallstabsübungen
- Incident Response

Zertifikate:

- Business Continuity Manager mit TÜV Rheinland geprüfter Qualifikation

„Überall dort, wo er geht, was er berührt,
was er hinterlässt, auch unbewusst,
all das dient als stummer Zeuge gegen ihn."

Edmond Locard

Was ist IT-Forensik?

IT-Forensik (oder auch Computer-Forensik, Digitale Forensik):

- Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität
- Nachweis und Aufklärung von anderen strafbaren Handlungen durch Analyse von digitalen Spuren

- Computer-Forensik ist digitale Kriminalistik.

Mögliche Ziele der Ermittlung

- Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,
- Ermittlung des entstanden Schadens nach einem Systemeinbruch,
- Identifikation des Angreifers,
- Sicherung der Beweise für weitere juristische Aktionen.

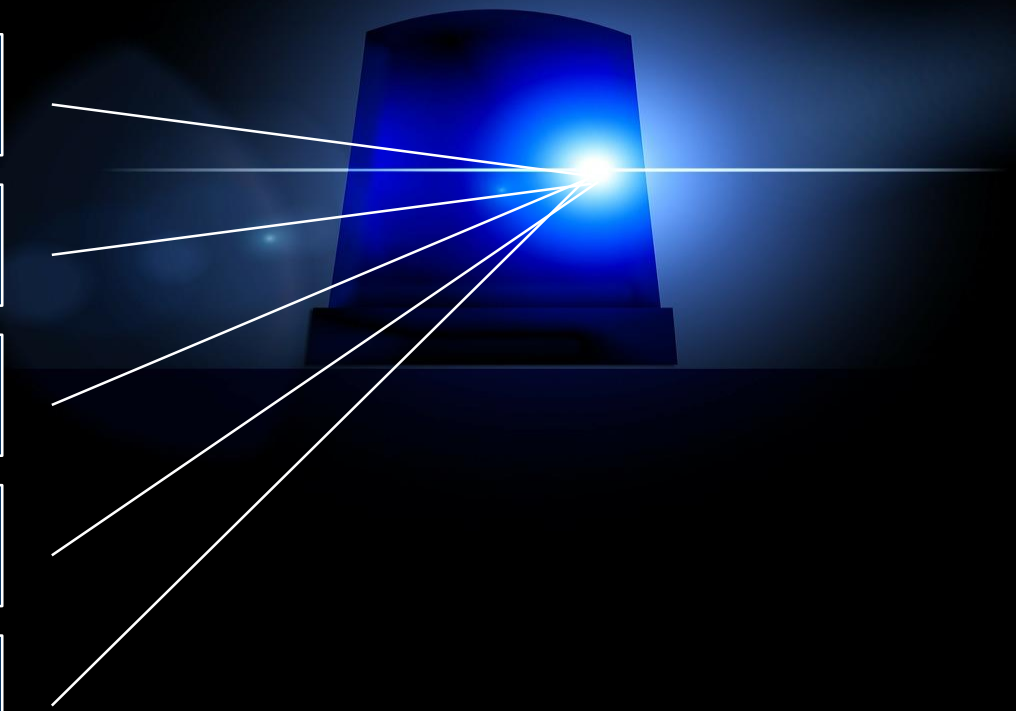
Was ist geschehen?

Wo ist es passiert?

Wann ist es passiert?

Wie ist es passiert?

Wer hat es getan?



Erkenntnisse in der IT-Forensik

Was ist geschehen?	———	Kompromittierung
Wo ist es passiert?	———	Betroffene Systeme
Wann ist es passiert?	———	Angriffszeitpunkt
Wie ist es passiert?	———	Einfallsvektor
Wer hat es getan?	———	Attributierung

Strategien zur Vorgehensweise: Forensische Fragestellung

Ziel der Arbeiten muss immer definiert sein:
Forensische Fragestellung

Früh erste Fragestellung definieren
- Möglichst konkret definieren, was untersucht werden soll
- Kann ggf. im Verlauf angepasst und verfeinert werden

Vorgehensweise davon abhängig
- Auch schon bei der Sicherung und den ersten Schritten
- Spätestens für die Analyse und Bewertung benötigt

Forensische Fragestellung (Beispiele)

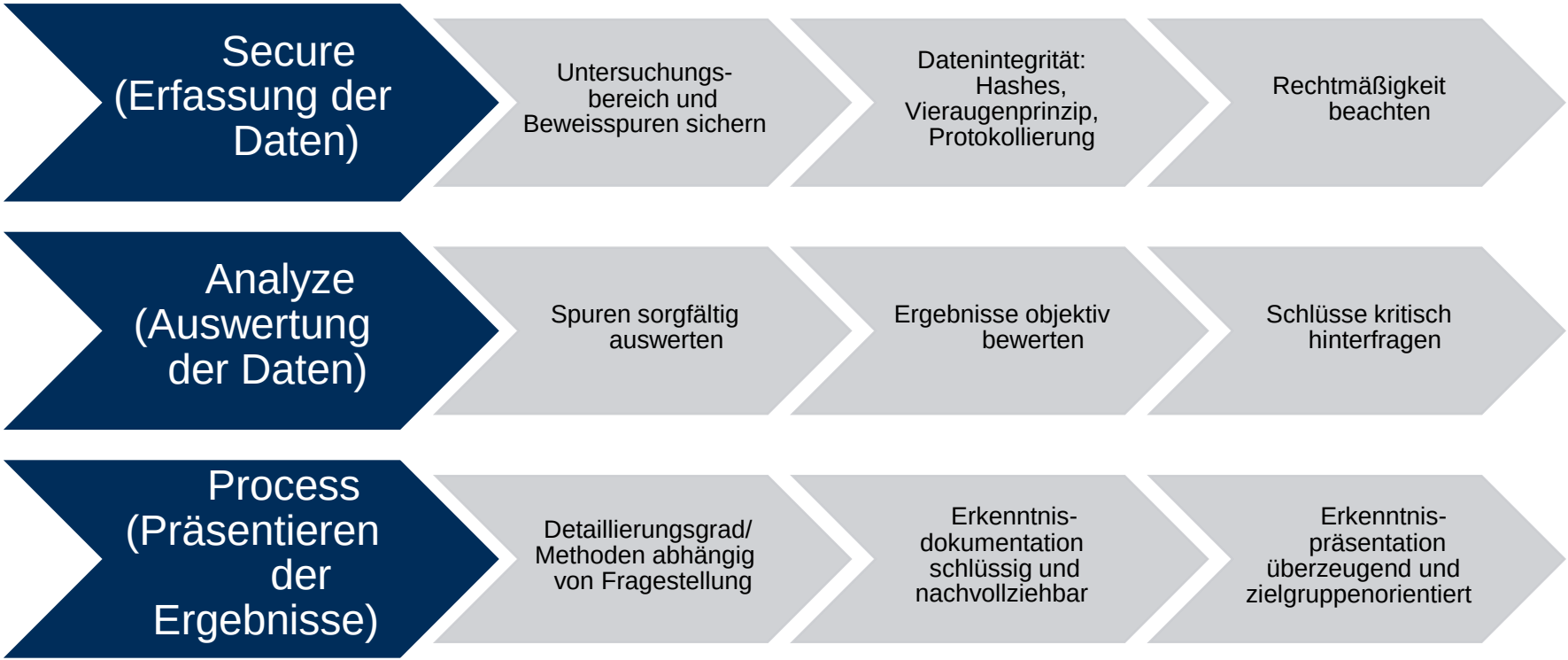
Ziel der Arbeiten muss immer definiert sein:
Forensische Fragestellung

Beispiele:

- Hat Mitarbeiter X in der letzten Woche Unterlagen zur Ausschreibung Y von seinem Rechner auf einen USB-Stick kopiert?
- Hat sich der Angreifer am 06.09.2024 über die Webanwendung Zugriff auf die Datenbank verschafft?
- Wie ist die Malware auf den PC gelangt und welche Kommunikationsverbindungen hat sie genutzt?

Ablauf einer forensischen Analyse

Strategien zur Vorgehensweise: Grundsätzlich gilt: S.A.P. Modell



Anforderungen an eine forensische Analyse

Akzeptanz

Integrität

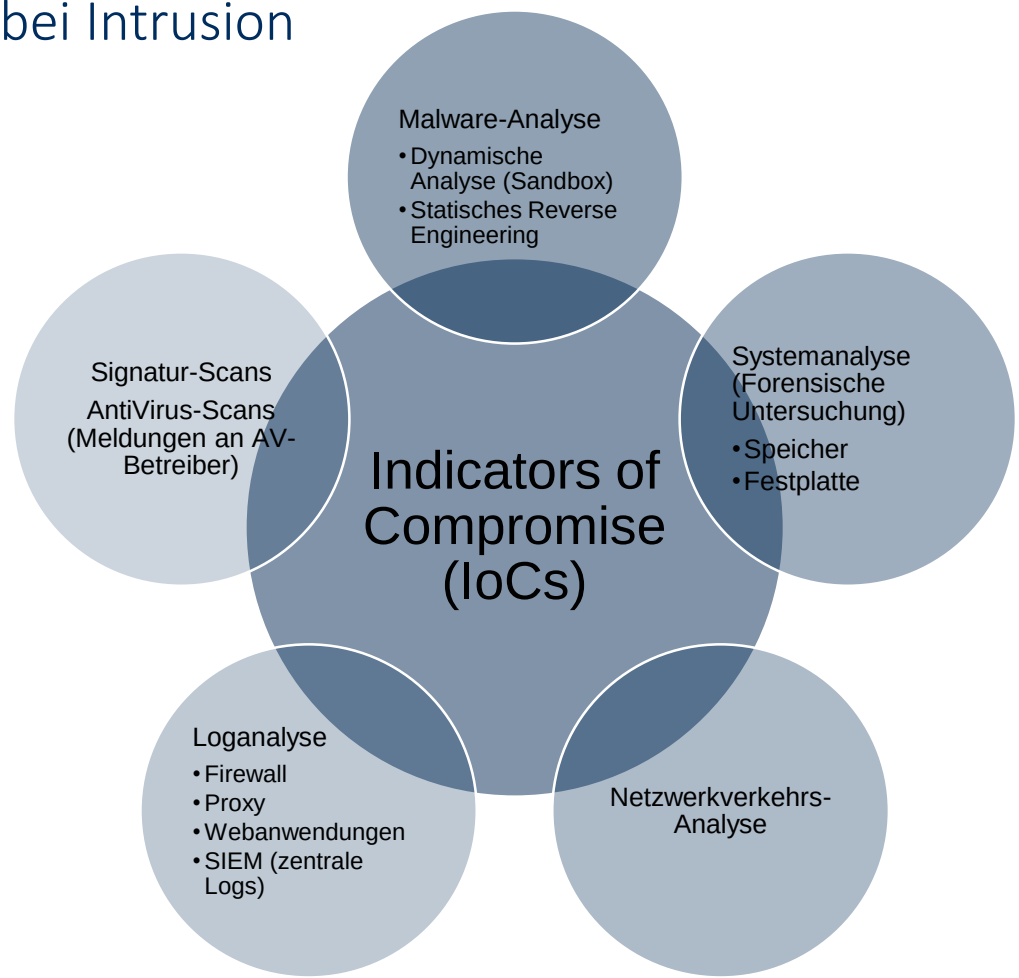
Glaubwürdigkeit

Ursache und Auswirkungen

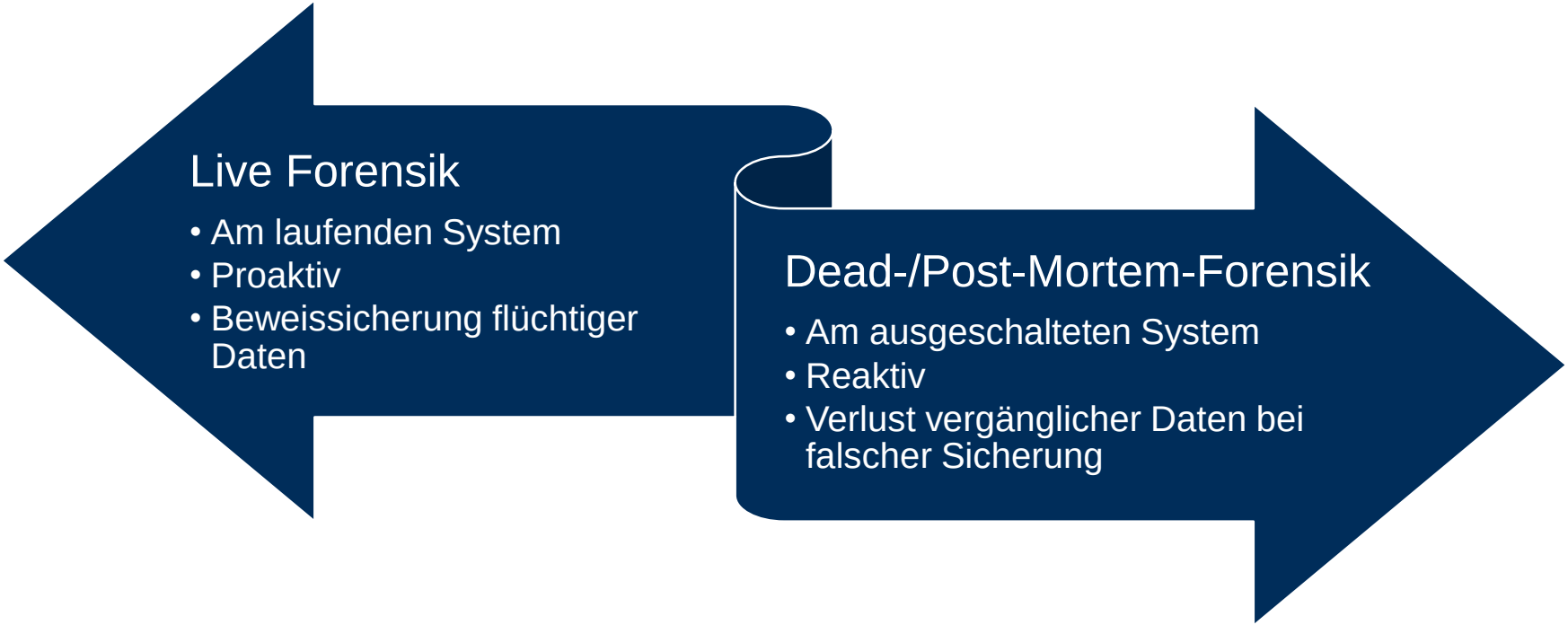
Wiederholbarkeit

Dokumentation

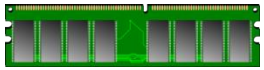
Ermittlung bei Intrusion



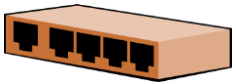
Unterschiedliche Ansätze



Fundorte digitaler Spuren



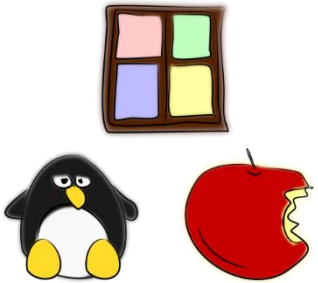
Arbeitsspeicher



Netzwerk

Datenbanken

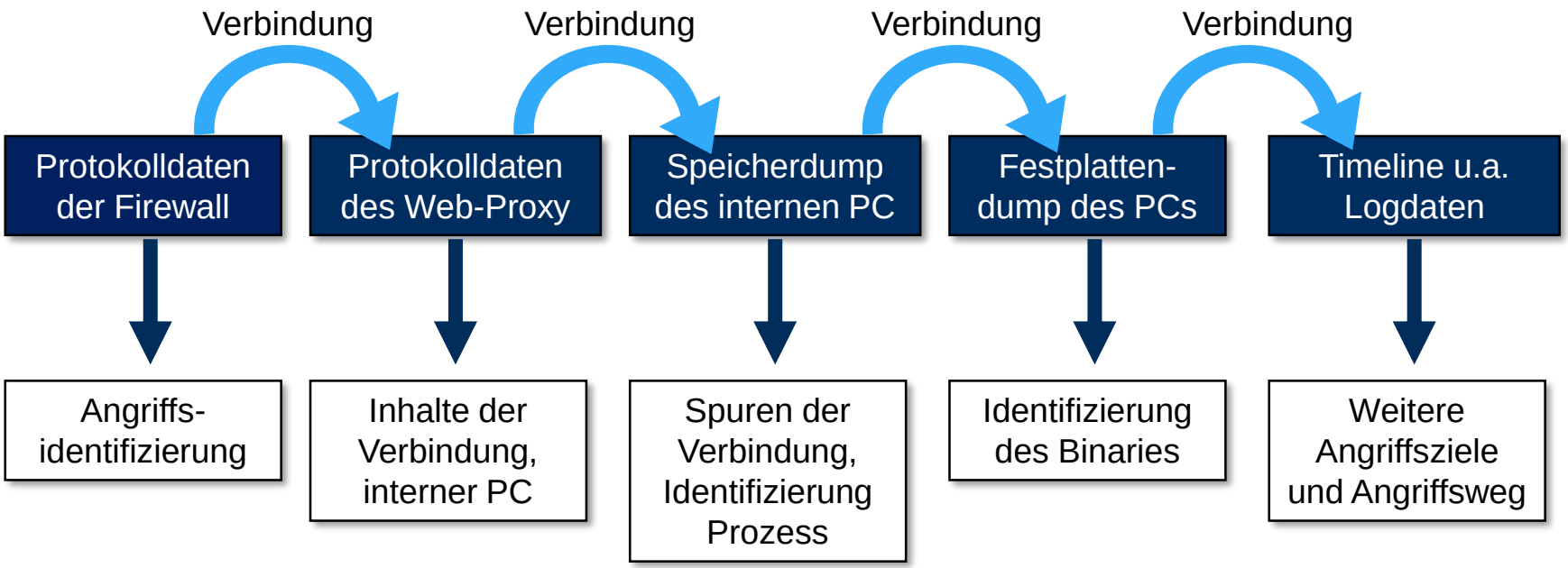
Dateisystem



OS-Artefakte

Protokolldateien

Beispiel: Zusammenhang der vorhandenen Logdaten herstellen



Forensik

Es muss sichergestellt werden, dass soviel Informationen wie möglich von einem kompromittierten System gesammelt werden können, ohne dabei den aktuellen Zustand bzw. Status dieses Systems zu verändern.

Strategien zur Vorgehensweise: Welche Daten können verloren gehen?

Unabhängig von der konkreten Fragestellung und dem zu untersuchenden System lassen sich grundsätzlich einige empfindliche Datentypen, die für die Ermittlung von Interesse sind, finden:

- **Flüchtige Daten**
  Informationen, die beim geordneten Shutdown oder Ausschalten verloren gehen (Inhalt von Cache und Hauptspeicher, Status der Netzverbindungen, laufende Prozesse und deren Speicherbelegung, angemeldete User etc.)
- **Fragile Daten**
  Informationen, die zwar auf der Festplatte gespeichert sind, aber deren Zustand sich beim Zugriff ändern kann
- **Temporär zugängliche Daten**
  Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z.B. während der Laufzeit einer Anwendung.

Die Halbwertszeit der Daten bestimmt die Reihenfolge der Datensammlung.

Exkurs Forensik - Sicherungsreihenfolge

Die Halbwertzeit der Informationen bestimmt die Sicherungsreihenfolge

- Routingtabellen, ARP-Cache, Prozessliste, angemeldete User, Netzstatus, Kerneldaten, Hauptspeicherinhalt (durch Prozesse belegt)
- Temporäre Dateisysteme, SWAP-Bereiche, etc
- Der komplette Inhalt der Datenträger
- Relevante Logging und Monitoringdaten auf zentralen Loggingservern
- Physische Konfigurationen und Netzwerktopologien
- Archivierte Medien

Assess It All, Or Lose It All

Reihenfolge der Sicherung flüchtiger Daten: Windows

Flüchtigkeit der Informationen

Beweisquelle	Werkzeuge
Aktuelle Systemzeit/Datum	time, date, now, psinfo, systeminfo
RAM	dd, userdump, mem, pmdump
laufende Prozesse	pslist, pstat, tlist, cmdline, handle
Angemeldete Benutzer	psloggedon, ntlast, netusers
Status der Netzwerkverbindungen	ipconfig, arp, route, netstat, fport, nbtstat, net, hunt, promiscdetect
Zeitstempel aller Dateien	dir
Auslagerungsdatei	Nur offline Analyse möglich, zur Laufzeit gesperrt
geladene Treiber	sc.exe, psservice.exe, drivers.exe,
Registry	reg, regdmp, autorunsc
Ereignisprotokolle	dumpel, psloglist
Command History	doskey /history, reg
Gruppenrichtlinien	gplist.exe, gpresult.exe
Zwischenablage	pclip

Reihenfolge der Sicherung flüchtiger Daten: Linux

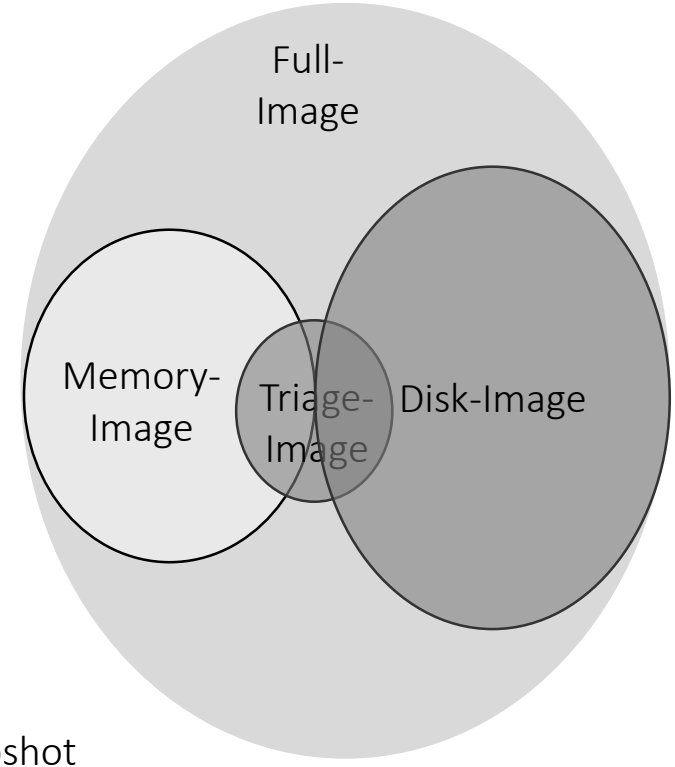
Flüchtigkeit der Informationen

Beweisquelle	Werkzeug
Aktuelle Systemzeit/Datum	date
RAM	dd, pcat (teilweise bei modernen Kernel nur mit Anpassungen möglich!)
laufende Prozesse	ps –aux, lsof –n –P –l
Angemeldete und zuletzt angemeldete Benutzer	w, last
Netzwerkverbindungen	ip a, netstat –an(p), arp –an, route –Cn, lsof -i
Zeitstempel aller Dateien	ls
Systeminformationen	tar cf - /proc
Alle geöffneten Dateien	lsof
geladene Module	cat, lsmod
Bash-History	cp, history

Datensammlung

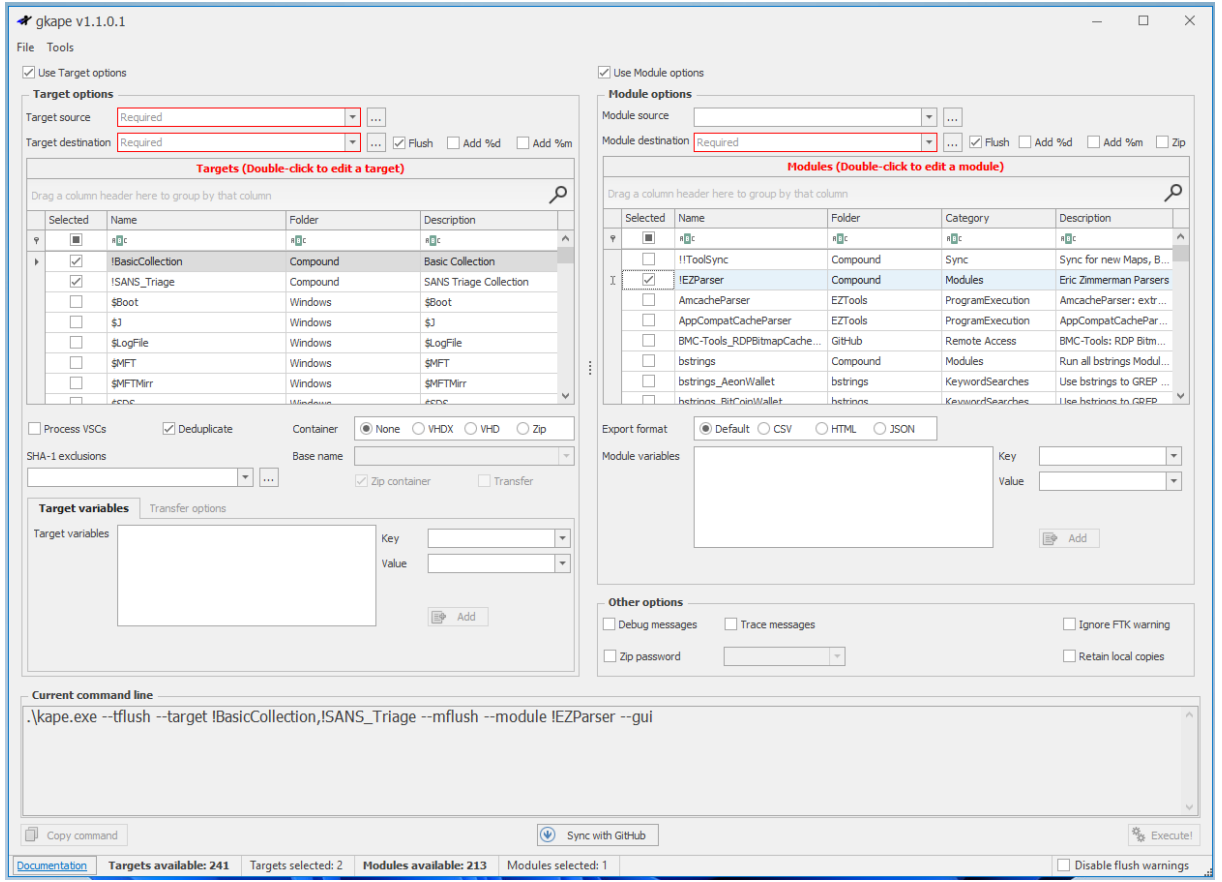
- Disk-Image
  - Vollumfängliche bitweise Kopie von Festplatte/SSD
- Memory-Image
  - Kopie des RAM-Speichers
- Triage Forensik
  - Zielgerichtetes Sammeln geeigneter, wichtiger Daten

- Full Image:
  - Kombination aus RAM und Festspeicher, z.B. VM-Snapshot



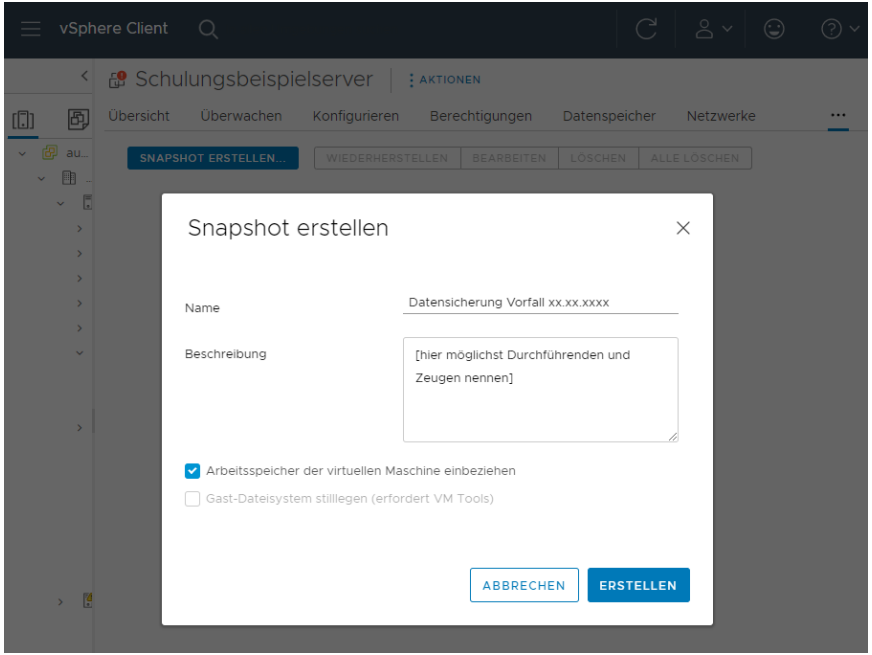
Triage

Tools wie Gkape Gkape / KAPE
https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
Oder Velociraptor um gezielt Artefakte zu sichern



Speicher sichern – Beispiel virtuelle Maschine

- Keine Zerstörung von Beweismitteln und Analysemöglichkeit durch Herunterfahren von (potentiell) betroffenen Systemen
- Herunterfahren erst nach erfolgter Beweissicherung
  - Sicherstellung der Integrität forensischer Daten durch Erstellung von Snapshots(mit Arbeitsspeicher)
    - **Betroffene Systeme:**
    - **Virtualisierte Server**: Alle virtualisierten Systeme, die potenziell betroffen sind.
    - **Virtualisierte AD-Controller**: Speziell alle Domain-Controller in der virtualisierten Umgebung.
- Kompromittierte Systeme hart ausschalten! (Strom trennen, nicht herunterfahren).



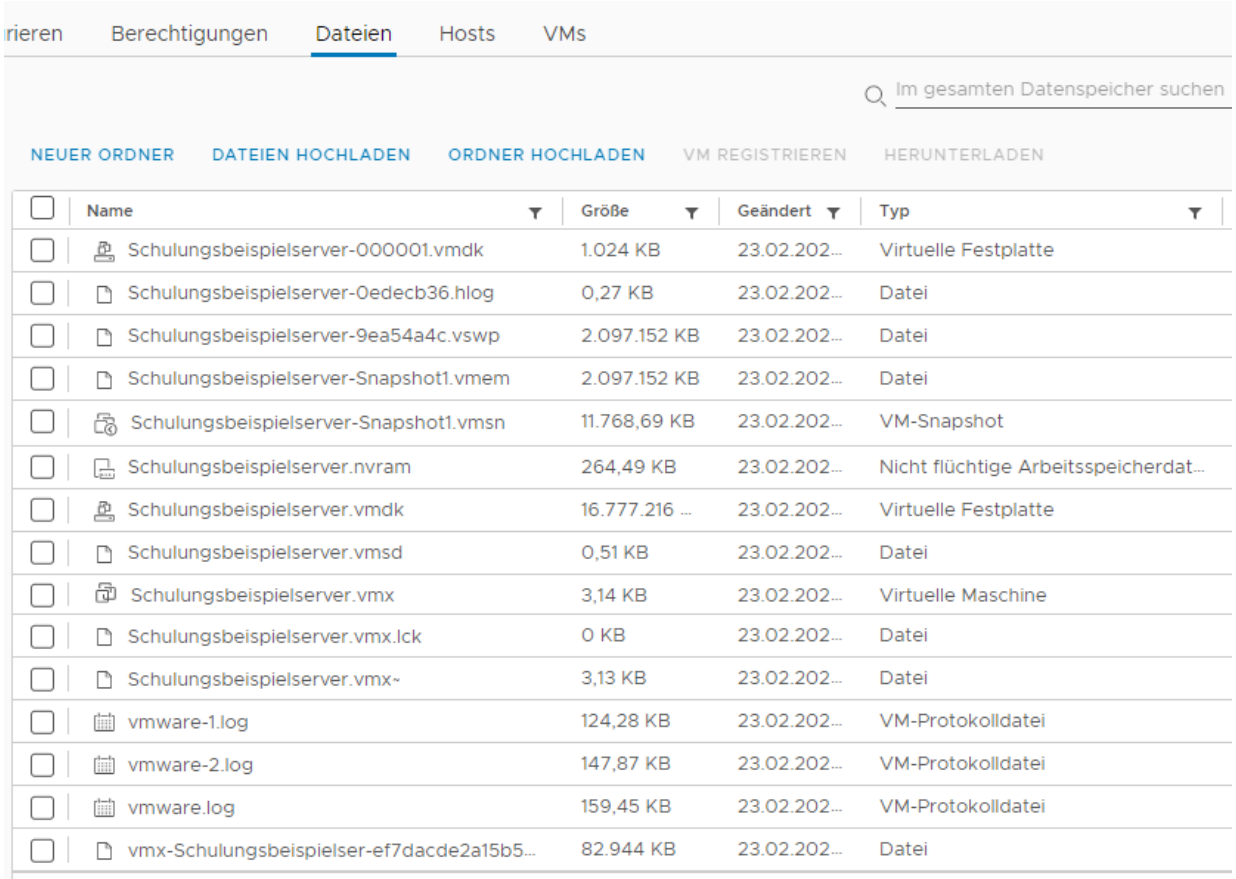
Speicher sichern – Beispiel virtuelle Maschine

Virtueller Server?

→Snapshot

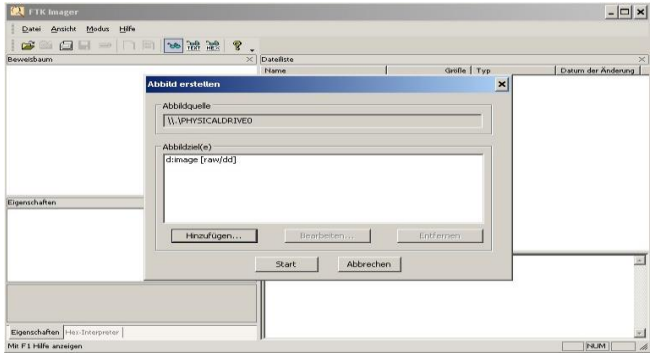
Dateien:

- .VMDK
  - Festplatte
  - Außer -00000x.VMDK (Snapshot, gelockt)
- .VMSN – Snapshot
- .VMSS – Suspend
  - u.a. RAM
- .LOG
- .VMX



Forensische Duplikation:
Duplizierung über Hard- und/oder Software

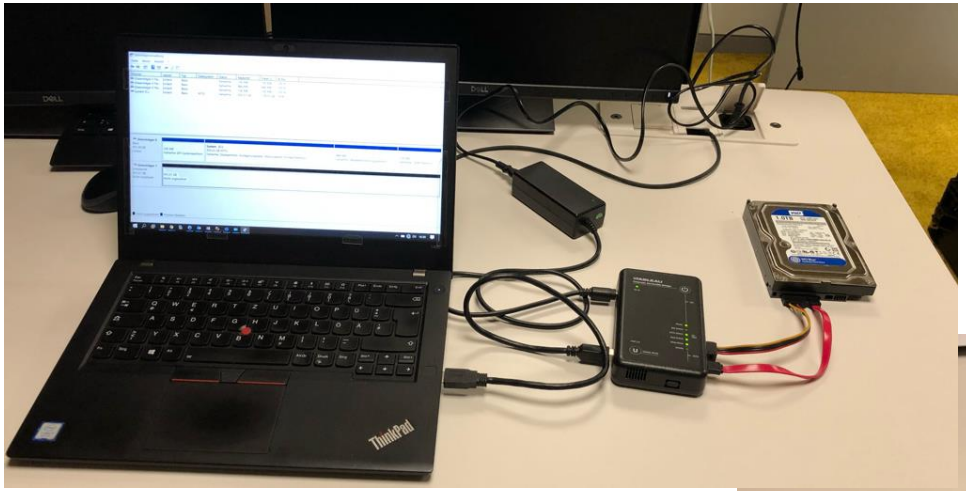
Tableau TX1



FTK-Imager

Forensische Duplikation in der Praxis

Unbedingt Writeblocker für die verdächtigen Datenträger verwenden!



Strategien zur Vorgehensweise: „Eisberg“ der Daten

Daten, die von normalen Tools gefunden werden

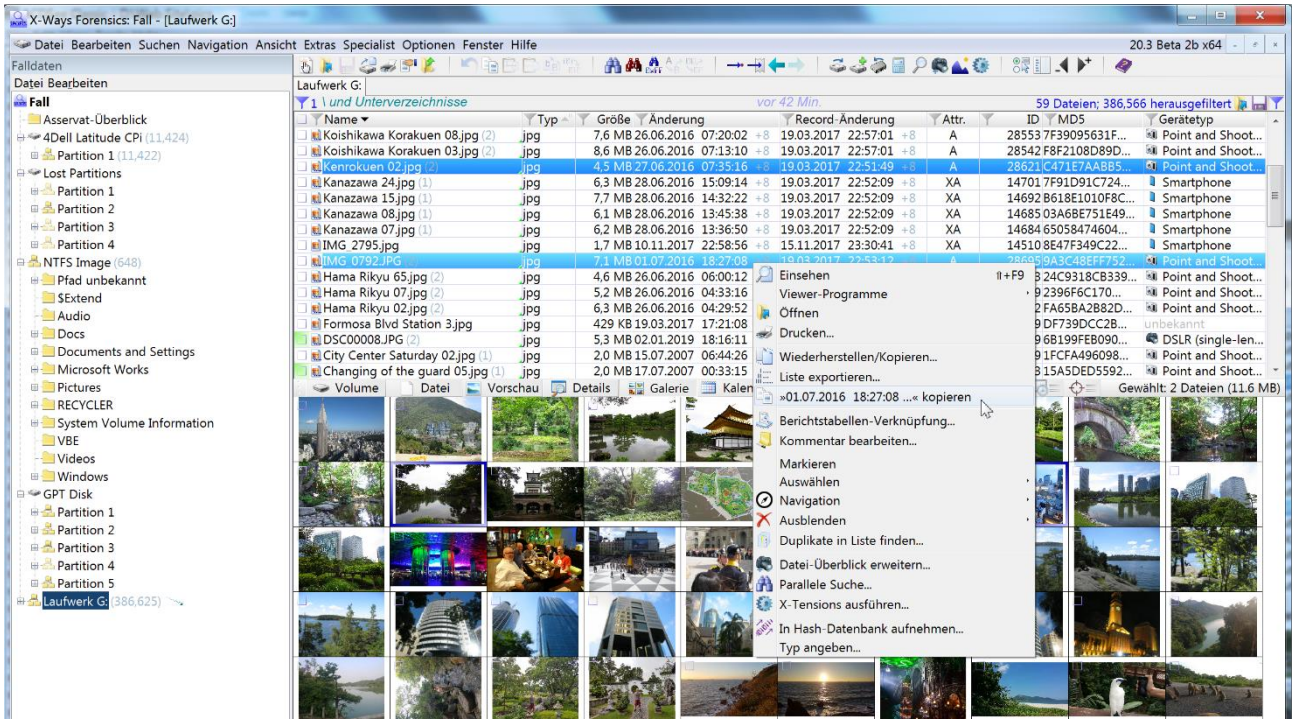
(z.B. Windows Explorer)

Zusätzliche Daten, die nur durch Spezialwerkzeuge gefunden werden können

(gelöscht, umbenannt, versteckt, unvollständig, schwer aufzufinden)

X-Ways

- https://www.x-ways.net/forensics/index-d.html
- findet gelöschte Dateien
- Bereitet Windows-EVT-Logs auf
- Regristry-Betrachter

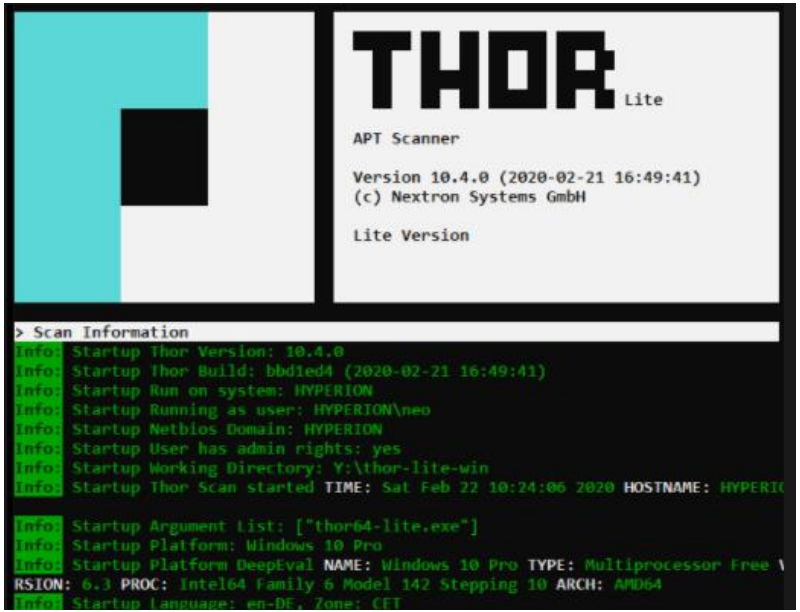


c‘t Desinfec‘t AV Scan
VM oder Live-System

- Desinfec't 2021/22
  https://www.heise.de/download/product/desinfect-71642
- Linuxbasiertes Live-System
- Quickwin in der Forensik:
  - Image oder System scannen und schnelle Ersteinschätzung erhalten
  - Bekannte Schadsoftware einfacher identifizieren.
- Ohne Dateien z.B. nach Virustotal hochzuladen kann man prüfen, ob diese von Virenscannern mit aktuellen Signaturen erkannt werden.
- Im IR-Einsatz kann man Datenträger z.B. USB-Sticks über die VM schnell prüfen

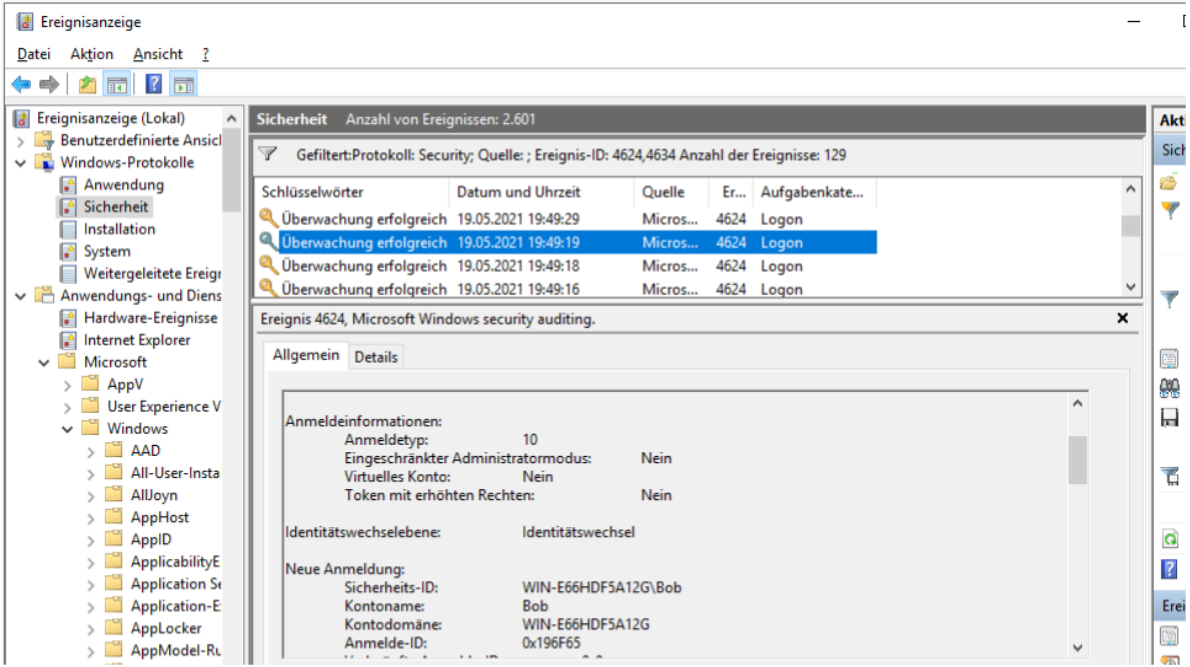
Thor Lite Scanner

- https://www.nextron-systems.com/thor-lite/
- 3 ähnliche Produkte des Herstellers:
  - LOKI – Open Source Version (Python)
  - Thor – Kommerzielle Version (Go)
  - Thor Lite – Freie abgespeckte Version von Thor
- Wird bereits mit vielen YARA-Regeln ausgeliefert
  - Benötigt beim ersten Start Internet für Regel-Download
- Ergebnisse sollten händisch geprüft werden:
  - False Positives leicht möglich
- Sowohl einzelne Dateien (bspw. Logfiles), als auch Images können gescannt werden. Letztere müssen vor dem Scan gemountet werden.



Log Analyse – kleiner Einblick

- Folgende Logdateien werden benötigt:
  - Firewalls,
  - Proxys
  - und AD-Controllern (C:\Windows\System32\winevt\Logs*.evtx)
- System32\winevt\logs\Security.evtx als Betrachtungsgegenstand
- 4624 – Successful Logon
- Anmeldetyp 10 Remote interactive logon (RDP)



Zusammenfassung – Was ist möglich?

- Wiederherstellung von gelöschten **Dateien** – gelöscht durch
  - „Löschen“ mit dem Betriebssystem,
  - „Formatieren“ mit Systemtools (Schnell-Format) oder
  - Neu partitionieren

- Wiederherstellung von gelöschten **Daten**
  - Gelöschte temporäre Kopien, Schattenkopien, Cache,(…)

- Erkennen, zu welchem Zeitpunkt Dateien erzeugt, verändert, aufgerufen/angesehen oder gelöscht wurden (meistens)
  - Unterschiede je nach Dateisystem / Betriebssystem

- Auslesen von Anwendungsdaten, z.B. Browser- und Emailprogramm
  - Welche Webseiten wurden besucht? Welche Suchen wurden ausgeführt?
  - Welche Emails wurden wann empfangen/versendet?
  - … (und vieles mehr)

Zusammenfassung – Was ist möglich?

- Auslesen von detaillierten Nutzungsdaten (z.B. Windows Registry, Logfiles)
  - Welche Anwendungen sind / waren installiert?
  - Welche Nutzer gibt es / gab es auf dem System?
  - Wann wurden die Anwendungen installiert / genutzt / wie oft?
  - Welche Dokumente wurden in letzter Zeit geöffnet? Von wem?
  - Welche externen Speichergeräte waren jemals angeschlossen?
  - Welche WLAN-Hotspots wurden genutzt?
  - … (und vieles mehr)

Was ist nicht möglich?

- Wiederherstellung des Zustands vor dem Angriff
- Daten auf physisch zerstörten Datenträger
  - Datenretter können teilweise Festplatten reparieren, aber nur wenn das Medium selbst nicht beschädigt ist.
- Sicher gelöschte und/oder überschriebene Daten wiederherstellen
  - Wurden die Daten mit „0“ überschrieben, können sie theoretisch wiederhergestellt werden, praktisch meist nicht
- Verschlüsselte Datenträger / Dateien können bei aktuellen Verfahren ohne Schlüssel nicht ausgewertet werden
- Nur Aktionen erkennbar, die explizit oder implizit aufgezeichnet wurden
- Nur bestimmten Zeitraum zurück:
  - Protokolle werden meist zyklisch überschrieben/gelöscht
  - Artefakte werden durch weitere Nutzung überschrieben

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com