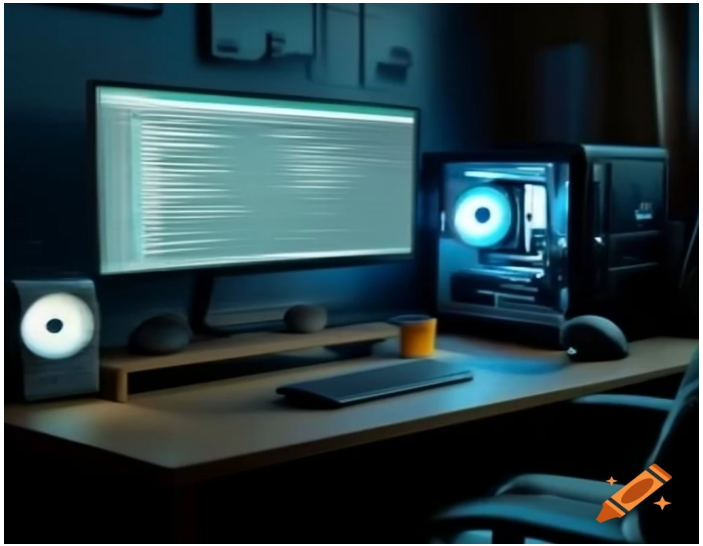
forensische IT-Ermittlung

Szenario: Ein Mitarbeiter könnte heimlich Daten von einer internen Festplatte auf einen externen Datenträger kopiert haben. Möglicherweise hat er Programme oder Skripte installiert, um bestimmte Sensorwerte auf dem Mainboard oder das BIOS des Rechners zu manipulieren. Die Geschäftsführung wünscht nun eine lückenlose Dokumentation, damit eine interne IT-Forensik- Abteilung oder, falls nötig, die Strafverfolgungsbehörden den Vorfall aufklären können.



5 Phasen der Ermittlung

- **Phase1 : Identifizierung**
- **Phase2 : Abholung**
- **Phase 3 : Analyse**
- **Phase 4: Berichterstattung**
- **Phase 5: Präsentation**

Ermittlungen am Tatort

Identifizierungsphase

- **Geräte Identifizieren**
- **Foto Dokumentieren**
  - wie sieht der Tatort aus
  - wo lag die Hardware
  - sind geräte und steckverbindungen getrennt worden
  - gibt es physische Anzeichen für Manipulation

- **Katalogisieren der einzelnen Komponenten (Hardware, Ablagen und etc.)**

Abholungsphase

- Datenerfassung (Image des Gerätes)
- der Ermittler muss spezielle Tools und Techniken verwenden
- der Prozess muss Dokumentiert werden

Software der Forensik

-Adepto	dient zum erstellen von Datenträger-images
-Autopsy Forensic Browser	Auswerten von Datenträger-Images, Extraktion von Daten
-Captain Nemo	Auslesen diverser Dateisysteme
-Chkrootkit	Suche nach Spuren von gebräuchlichen Rootkits
-Filemon, Regmon	Analyse von Registry- und Filesystemzugriffen von Applikationen
-FPort	Anzeige,welche Applikationen Ports geöffnet haben

……..

Analyse

- werden die gesammelten Daten untersucht
- beweise identifizieren
- spezielle Techniken können gelöschte Dateien wiederherstellen
- der ermittler muss in der Lage sein, die Daten strukturiert zu analysieren, um sicherzustellen, dass alle relevanten Beweise identifiziert sind
- Analysephase kann der Ermittler mehrere Beweisstücke identifizieren
- es ist wichtig, jedes Beweisstück und die Schritte zu seiner Identifizieren und dokumentieren

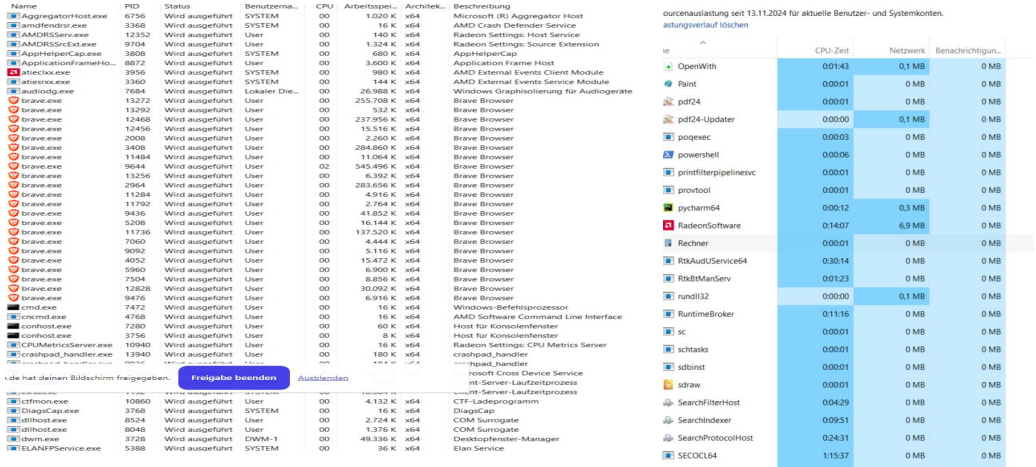
Überprüfung der Schnittstellen

Durch zugriff auf dem Geräte Image:

-überprüfen der Verlaufsdatei und Zugriffe auf dem pc

- zuletzt verwendete Dokumente, internetseiten (Browserverlauf)

-Taskmanager App (verlauf)



Hardware Prüfen

- Festplatten prüfen durch Analysetools, gegebenenfalls Daten wiederherstellen.
- Schauen ob alles internen Hardwarekomponeten funktionieren und nicht manipuliert worden.
- sind alle steckverbindungen korrekt etc .

Berichterstattung

- nach abschluss der Analysephase muss der Ermittler einen ausführlichen

  Bericht erstellen, ergebnisse zusammengefasst

- bericht sollte eine zusammenfassung der Untersuchung, der verwendeten Methoden, der gesammelten Beweise und der aus Analyse gezogenen Schlussfolgerungen enthalten
- bericht sollte klar und prägnant verfasst sein und keinen Fachjargon enthalten
- bericht sollte Empfehlungen für weiter Untersuchungen oder Maßnahmen enthalten

Danke Für eure Aufmerksamkeit