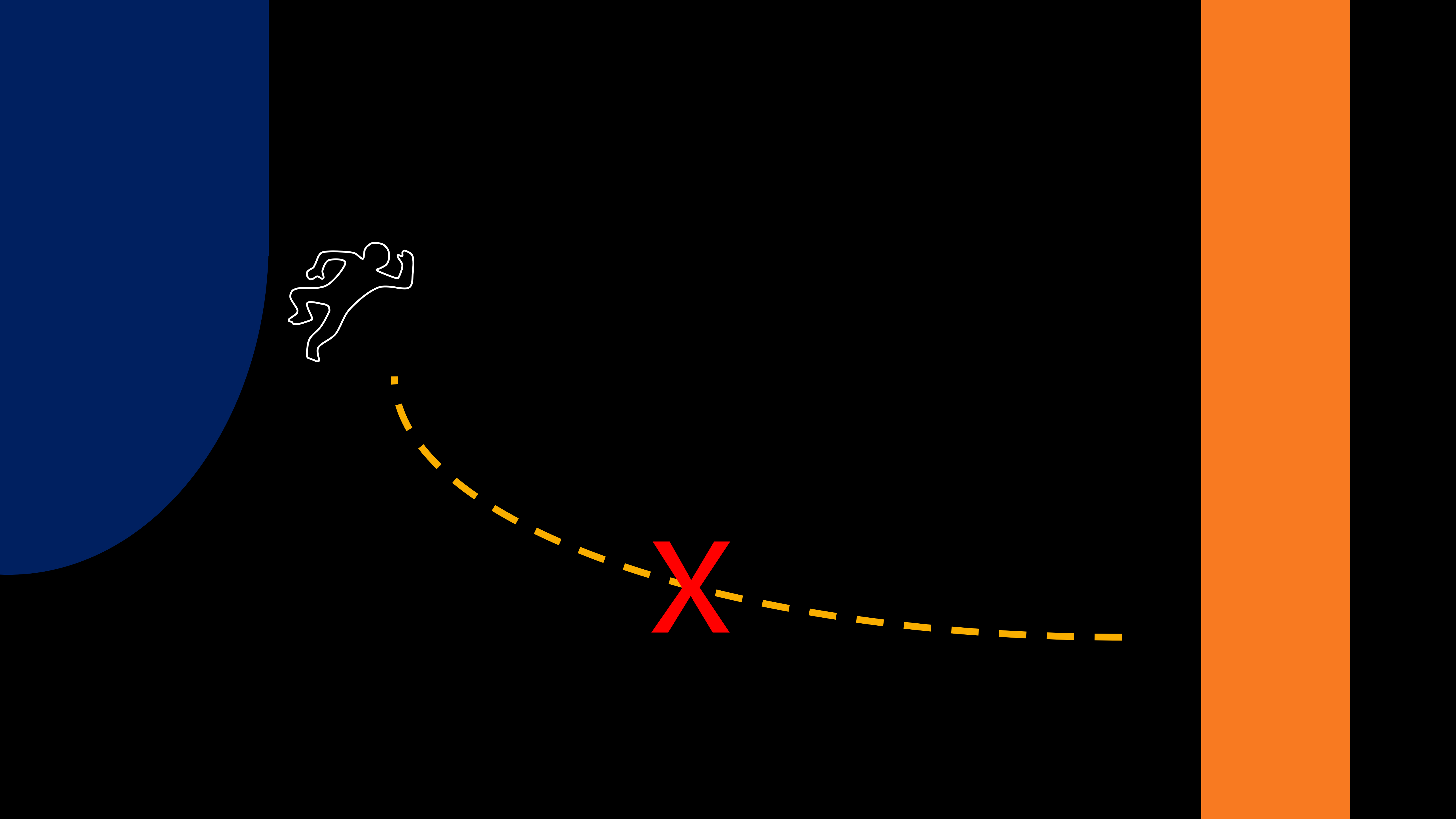
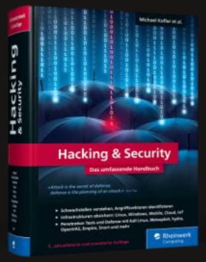


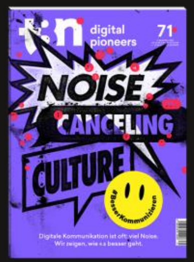
IT-Forensik – Aufklärung von IT-Sicherheitsvorfällen

VDI Zollern-Baar 05. April 2023

Über mich

- 1999 GeoCities, 2000 Domain, 2001 Kundenprojekte & ab 2010 eigener Blog
- 2009 bis 2012: Softwareeingenieur im Bereich Web Development (Gute Aussicht)
- Seit 2012: Akademischer Mitarbeiter (Hochschule Albstadt-Sigmaringen)
- Autor, Blogger, Referent & Dozent





Agenda

01. Die Methoden der IT-Forensik

02. Fall A: Die verschwundenen Logfiles

03. Fall B: Geknacktes Passwort eines Servers

04. Fall C: Industriespionage durch Innentäter

01. Die Methoden der IT-Forensik

IT-Sicherheit vs. IT-Forensik

IT-Sicherheit	IT-Forensik
Was könnte passieren?	Was ist passiert?

IT-Forensik

Zielsetzungen

- Bei der IT-Forensik geht es um die Untersuchung nach einem Vorfall.
- Das Ziel ist die Analyse und Auswertung von digitalen Spuren zur Aufklärung von Vorfällen.
- Es geht darum, rechtswidrige oder schädliche Handlungen zu verstehen und nachzuweisen.

Strikter Prozess

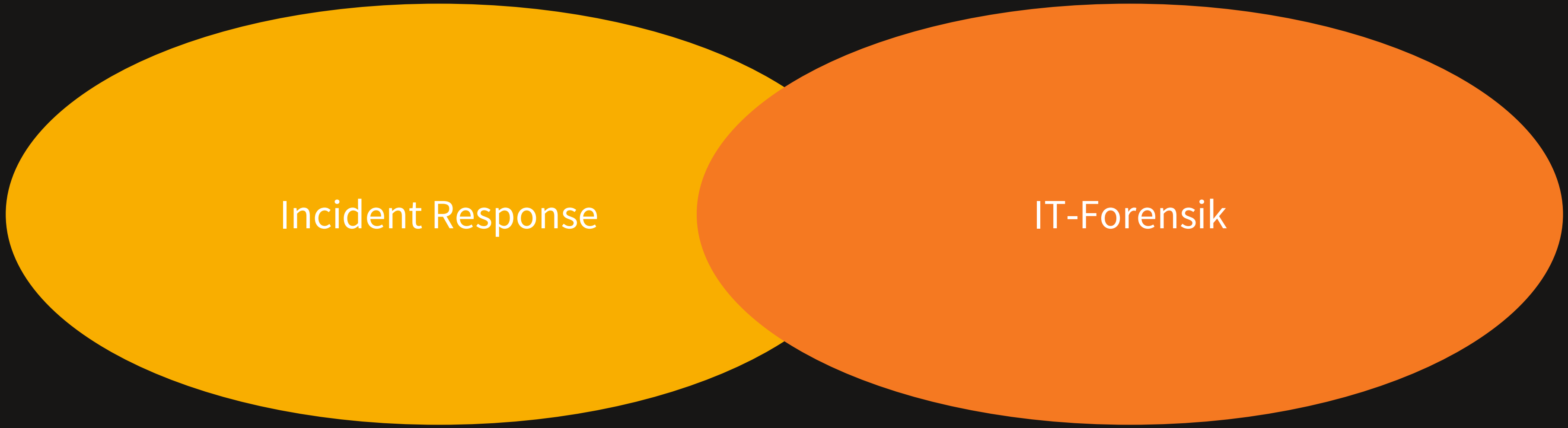
- Nachvollziehbarkeit
- Wiederholbarkeit
- Integrität
- Vollständigkeit

Quelle: flickr.com (1)

Forensische Untersuchungen

- Wie bei anderen Untersuchungen im Ermittlungsbereich können auch hier die 7 W-Fragen der Kriminalistik angewendet werden. Damit soll ein behaupteter Vorgang bewiesen oder widerlegt werden.
  Wer? Was? Wo? Wann? Womit? Wie? Weshalb?
- Zur gerichtsverwertbaren Sicherung digitaler Spuren muss die Untersuchung nach etablierten Standards streng methodisch und jederzeit nachweisbar erfolgen.
- Ermittlungen wegen: Tötungsdelikten, Terrorismus, Kinderpornographie, Betrug, Diebstahl, Copyright-Verletzung, Datendiebstahl, Schadsoftware, Garantiefälle, Versicherungsnachweis, Audits, …

Spannungsfelder



- Möglichst schnelle „Beseitigung“ des Vorfalls und seiner Folgen
- Möglichst rasche Absicherung der Systeme, Beseitigung der Ursache des Vorfalls

- Keinerlei Veränderung digitaler Spuren
- Systematische Sicherung der Spuren benötigt Zeit / Betriebsunterbrechung
- Aufarbeitung der gefundenen Spuren

02. Fall A: Die verschwundenen Logfiles

Die verschwundenen Logfiles

Fall

- Logfiles sind verschwunden, es wird vermutet, dass ein Angriff dahinter steckt

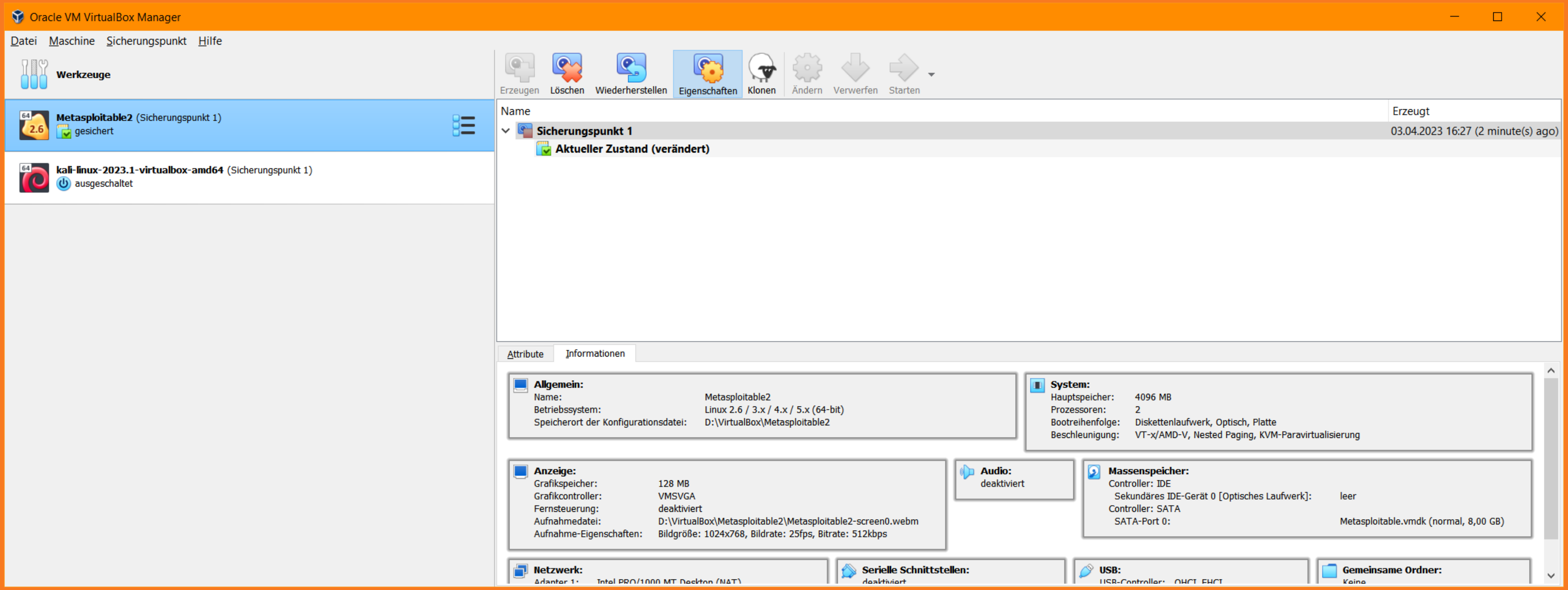
Zielsetzung

- Herausfinden, ob die Logfiles wiederhergestellt werden können
- Analysieren, welcher Prozess die Änderungen vornimmt

File-Carving

- Die Suche nach Dateien auf Datenspeichern auf Basis einer inhaltlichen Analyse der Datenblöcke anhand von Mustern (Header, Signaturen, u. a.)

LIVE File-Carving



03. Fall B: Geknacktes Passwort eines Servers

Geknacktes Passwort eines Servers

Fall

- Intensiver Scan eines Servers
- Angreifende testen verschiedene Passwörter

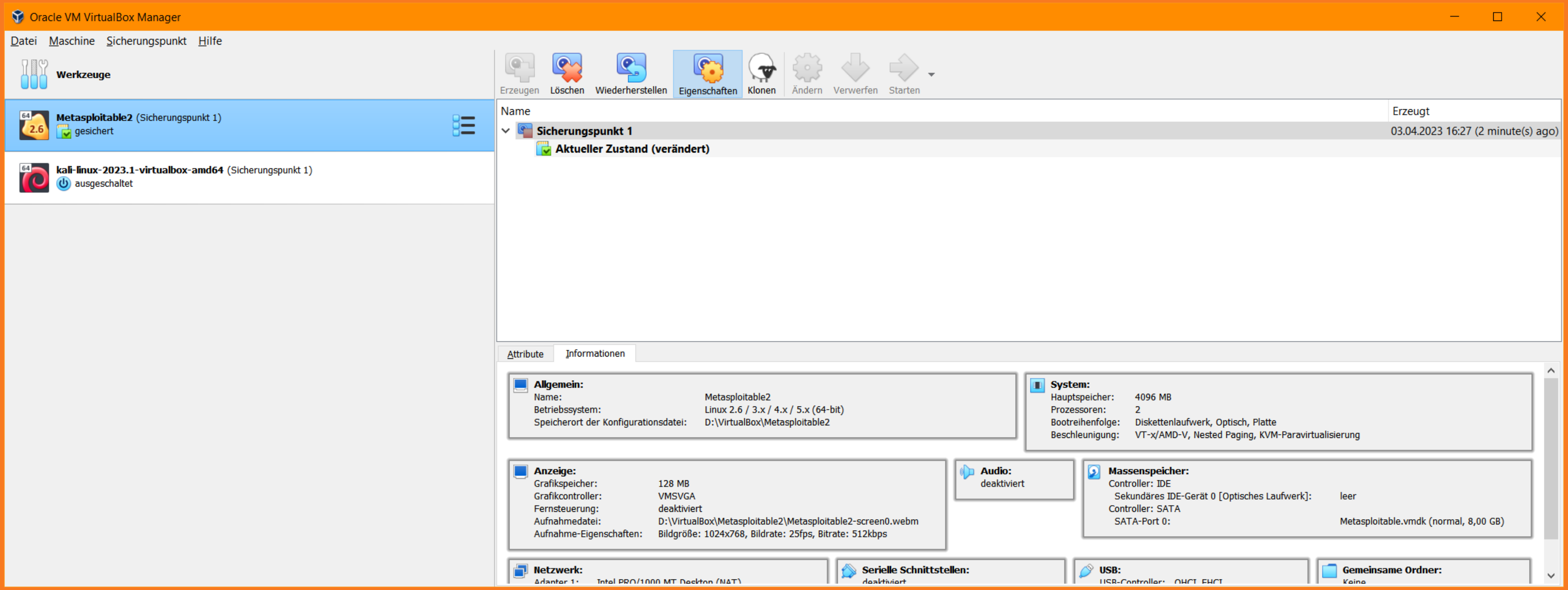
Zielsetzung

- Analysieren, welche Dienste von den Angreifern untersucht wurden
- Herausfinden, ob ein unautorisierter Zugriff möglich war

Post-Mortem-Analyse

- Beschreibt die Untersuchung eines Rechnersystems im ausgeschalteten Zustand

LIVE Logfiles Auswertung



04. Fall C: Industriespionage durch Innentäter

Industriespionage durch Innentäter

Fall

- Daten eines Unternehmens wurden entwendet
- Die bisherigen Analysen führen zu einem spezifischen Rechner

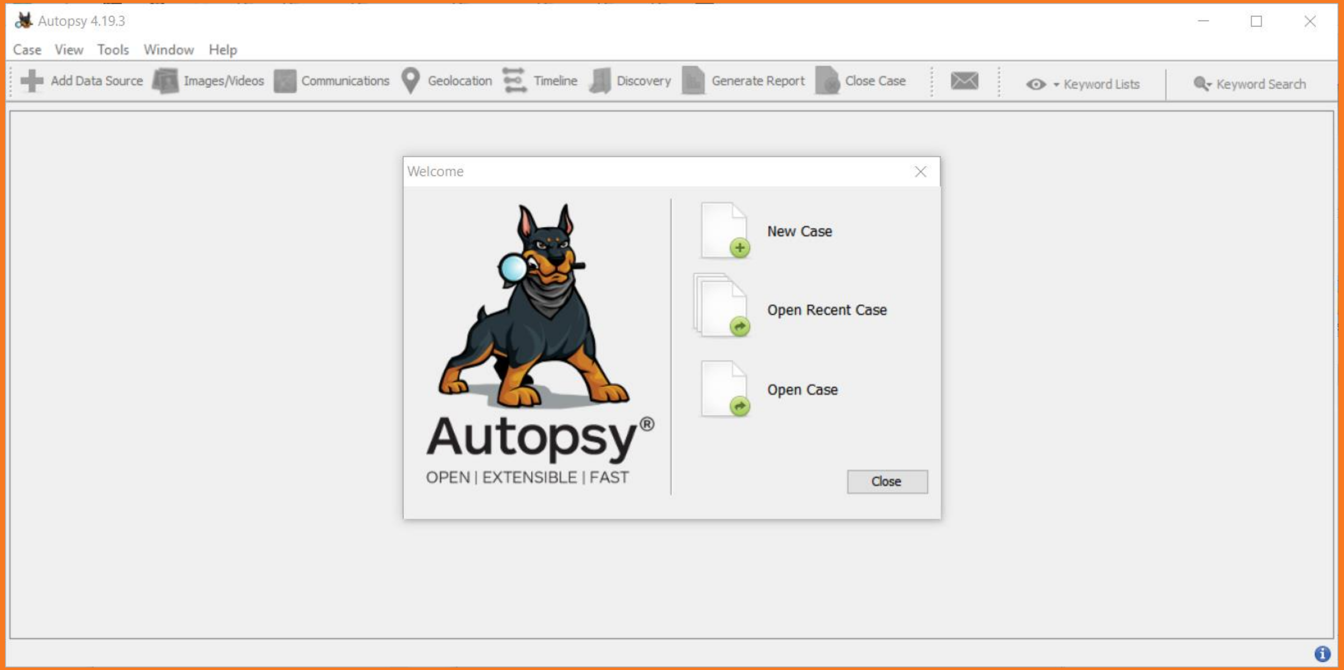
Zielsetzung

- Herausfinden, wie die Daten von diesem Rechner kopiert wurden

Post-Mortem-Analyse

- Beschreibt die Untersuchung eines Rechnersystems im ausgeschalteten Zustand

LIVE System Analyse



IT-Forensik

Zusammenfassung

Kern-elemente

+ Zielsetzung
+ Digitale Spuren
+ Forensische Untersuchung
+ Spannungsfelder

Vorgehens-weise

+ Secure
+ Analyse
+ Present

Untersuchungs-methoden

+ Post-Mortem
+ Live-Analyse

Einsatz-szenarien

+ Computerkriminalität
+ Straftaten
+ Fehlfunktionen
+ Systemanalysen

IT-Forensik

Noch Fragen?

Nächste Veranstaltungen

Vorträge

- Mit Low-Code Technologie zu papierlosen Prozessen in Fertigung und Lager [VDI]
  19.04.2023
- Offensive IT-Sicherheit – Kali Linux [VDI]
  07.06.2023

Workshops

- Keylogger und BadUSB-Angriffe über die USB-Schnittstelle [VDI]
  13.05.2023
- Hacking- und Pentest-Hardware Workshop
  24.05.2023

Digitale Spurensuche

Experimentieren Sie mit freien Anwendungen,
um ein Gefühl für digitale Spuren zu bekommen.

Machen Sie sich in Unternehmen und als Entwickler
Gedanken zum Thema Forensic Readiness.

Neugierig? Online-Vorträge & Workshops:

www.scheible.it