Forensikbericht

Datum der Untersuchung: [Datum der Untersuchung]

Untersuchungsprofil:

* Fallidentifikation: [Fallnummer]
* Geräteanalyse: [Liste der untersuchten Geräte/Systeme]
* Umgebungsbeschreibung: [Beschreibung der Umgebung, z.B. Betriebssystemtyp, Netzwerkkonfiguration]

Forensische Instrumente und Taktiken:

* Werkzeugauswahl: [Aufzählung der forensischen Werkzeuge und deren Versionen]
* Anwendungsstrategien: [Beschreibung der angewandten forensischen Methoden]

Beweissicherungsprozess:

* Sicherungsmethoden: [Beschreibung des Prozesses zur Beweissicherung]
* Beweisfund: [Aufzählung der identifizierten Beweise, einschließlich Beschreibung und Herkunft]

Datenanalyse:

* Extraktionsergebnisse: [Art der extrahierten Daten und deren Relevanz für die Untersuchung]
* Analysezusammenfassung: [Zusammenfassung der analysierten Daten und ihrer Implikationen]

Ergebnisübersicht:

* Beweisfunde: [Beschreibung der gefundenen Beweise und deren Bedeutung für den Fall]
* Fazit: [Schlussfolgerungen basierend auf den Untersuchungsergebnissen]

Ergebnisdiskussion:

* Ergebnisinterpretation: [Diskussion möglicher Interpretationen der Ergebnisse]
* Begrenzungen: [Identifizierte Einschränkungen der Untersuchung]

Abschließende Schlussfolgerungen und Vorschläge:

* Fazit: [Zusammenfassung der wichtigsten Erkenntnisse]
* Empfehlungen: [Empfohlene Maßnahmen oder weitere Schritte]

Unterschrift und Datum: Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Datum:

Forensikbericht

Datum der Untersuchung: 26.03.2024 17:00 Uhr - 18:30 Uhr GMT +1

Beteiligte Mitarbeiter:

* Pesch, Dylan (Matr.Nr: 2123049)
* Rück, Alexander (Matr.Nr: 2120676)
* Steelandt, Jonathan (Matr.Nr: 2124503)

Untersuchungsprofil:

* Übung 1
* Zu bearbeitendes Dokument: U1.pdf
* Umgebungsbeschreibung: Computerpool A008

Forensische Instrumente und Taktiken:

* Werkzeugauswahl: Vorwissen und Internetrecherche via Brave Browser

Beweissicherungsprozess:

* Sicherungsmethoden: Dokumentation in einem Google Dokument

Datenanalyse:

* Extraktionsergebnisse: [Art der extrahierten Daten und deren Relevanz für die Untersuchung]
* Analysezusammenfassung: [Zusammenfassung der analysierten Daten und ihrer Implikationen]

Ergebnisübersicht:

* Ergebnisse:

Aufgabe 1

1. Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, die sich mit der systematischen Untersuchung krimineller Handlungen befassen.

* Computer-Forensik
* Forensische Psychiatrie und Psychologie
* Rechtsmedizin

1. Spuren sind physische Hinweise auf eine Straftat, wie Fingerabdrücke oder Blutspuren. Indizien sind mittelbare Hinweise, die auf eine Straftat schließen lassen, aber nicht direkt beweisen. Beweise sind direkte und unmittelbare Hinweise, die eine Straftat beweisen.
2. Das Locardsche Austauschprinzip besagt, dass bei jedem Kontakt zwischen zwei Objekten Spuren übertragen werden. Es ist ein grundlegendes Prinzip der Forensik, das besagt, dass keine Spuren ohne Spurenübertragung existieren können.
3. c) 255
4. b) 10010111
5. c) 218
6. a) 0x2100
7. a) 0010 0001 0000 0001
8. c) 1000101
9. Das Dezimaläquivalent des Hexadezimalwerts 0x33FACC00 ist 569614080, unabhängig davon, ob in Big-Endian oder Little-Endian interpretiert.

Aufgabe 2

1. Kali linux wurde als VM eingerichtet
2. Die wichtigsten tools sind hier zusammengefasst: <https://medium.com/@mailtodevens/deciphering-digital-mysteries-a-comprehensive-guide-to-kali-linux-forensic-tools-6cbe429c73de>

Aktuelles Arbeitsverzeichnis: /home/kali

Aktuelles Verzeichnis: pwd

Allen anweisungen wurde folge geleistet

1. Die Bezeichnungen “-rw -rw -r-- 1 donald staff 6,1K 28 Sep 2022 datei.txt” in einer Unix- oder Linux-Dateiliste geben verschiedene Informationen über die Datei datei.txt wieder:

Das erste “-rw” steht für den Dateibesitzer (user) und bedeutet, dass er lesen und schreiben kann.

Das zweite “-rw” steht für die Gruppe (group) und bedeutet, dass sie ebenfalls lesen und schreiben kann.

“-r–” steht für andere Benutzer (others) und bedeutet, dass sie nur lesen können.

“1” zeigt die Anzahl der Links zur Datei an, normalerweise 1 für eine einzelne Datei.

“donald” ist der Benutzername des Dateibesitzers.

“staff” ist der Name der Gruppe, zu der der Dateibesitzer gehört.

“6,1K” ist die Größe der Datei (hier: 6,1 KB).

“28 Sep 2022” ist das Datum der letzten Änderung der Datei.