Forensik-Playbook: Untersuchung eines Guymager-Images mit NirLauncher

Dieses Playbook beschreibt die systematische Vorgehensweise, um ein mit Guymager erstelltes Forensik-Image (.E01 oder .dd) unter Windows zu analysieren. Als Werkzeug dient dabei die NirLauncher-Toolsammlung, die zahlreiche portable Analyse-Utilities von NirSoft enthält. Das Playbook legt Wert auf forensische Best Practices: Hash-Prüfung, Chain-of-Custody, Read-Only-Mounting, Exporte und Dokumentation.

Schritt A — Vorbereitung

- Arbeitsumgebung einrichten (Forensik-VM oder isolierte Workstation).
- Tools bereitstellen: NirLauncher, FTK Imager (oder OSFMount/Arsenal), Hash-Tools.
- Ordnerstruktur für Originals, Working Copies, Exports, Logs anlegen.
- Untersuchungsprotokoll mit Case-ID, Datum, Bearbeiter beginnen.

Schritt B — Integritätscheck des Original-Images

- Berechne SHA256-Hashwerte aller Image-Segmente (E01, E02, …).
- Vergleiche mit von Guymager erzeugten Hashwerten (falls vorhanden).
- Dokumentiere Hashes in Chain-of-Custody.
- Stelle sicher, dass alle Segmente vorhanden sind und korrekt benannt.

Schritt C — Sichere Kopie / Arbeitskopie

- Arbeite niemals auf den Original-Dateien.
- Erstelle eine geprüfte Kopie auf dein Arbeitsmedium.
- Prüfe erneut die Hashes der Kopien.

Schritt D — Mounten des Images (Read-Only)

- Starte FTK Imager als Administrator.
- File → Image Mounting → Image File auswählen.
- Mount Type: Physical & Logical, Mount Method: Read-Only.
- FTK zeigt die neuen Laufwerksbuchstaben (z. B. G:, H:).
- Dokumentiere Zeit und Buchstaben.

Schritt E — Exporte vorbereiten

- Ordner `exports\nirsoft` anlegen.
- Dateinamenskonvention: ___.csv.
- Hashes für Exporte im Log dokumentieren.

Schritt F — Analyse mit NirLauncher

- BrowsingHistoryView: Browserverläufe aus Profilordnern extrahieren.
- BrowserAddonsView: Extensions/Add-ons auflisten.

- WebBrowserPassView/ChromePass: Gespeicherte Passwörter prüfen (DPAPI-Beschränkung beachten).
- ChromeCookiesView: Cookies und Cache-Einträge sichern.
- UserProfilesView: Benutzerprofile anzeigen.
- LastActivityView: Chronologische Aktivitäten rekonstruieren.
- WinPrefetchView: Prefetch-Dateien auswerten.
- RegistryChangesView/RegScanner: Registry-Hives vergleichen und durchsuchen.
- WirelessKeyView/NetworkInterfacesView: WLAN-Keys und Netzwerkschnittstellen sichern.
- SearchMyFiles: Dateien gezielt nach Typ, Zeit, Inhalt durchsuchen.

Schritt G — Dokumentation

- Jeden Export als CSV/HTML sichern.
- SHA256-Hash für jede Exportdatei berechnen.
- Hashes in Log-Datei schreiben.
- Screenshots nur ergänzend verwenden.

Schritt H — Vertiefte Forensik (optional)

- MFT-Analyse (MFTECmd, AnalyzeMFT).
- Timeline-Erstellung (plaso/log2timeline).
- File Carving (bulk_extractor, scalpel).
- Memory-Analyse (Volatility), falls Dump vorhanden.

Schritt I — Abschluss

- Report erstellen (Executive Summary, Methode, IOCs, Evidenzverzeichnis).
- Gemountetes Image im FTK Imager sauber unmounten.
- Arbeitsumgebung sichern, Logs finalisieren.

Beispiel: Hash-Berechnung mit PowerShell

```
Get-FileHash -Path "D:\Cases\CASE-001\originals\case01.E01" -Algorithm SHA256
```

Beispiel: Hashes aller Exporte in CSV schreiben

```
Get-ChildItem -Path "D:\Cases\CASE-001\exports\nirsoft" -Recurse -File |
  ForEach-Object { Get-FileHash $_.FullName -Algorithm SHA256 |
    Select-Object @{Name='Path';Expression={$_.Path}},Hash } |
  Export-Csv -Path "D:\Cases\CASE-001\logs\export_hashes.csv" -NoTypeInformation
```