Informationssicherheit und IT-Forensik

– Übung –

UEB-05 – Forensik

Forensische Datenspuren

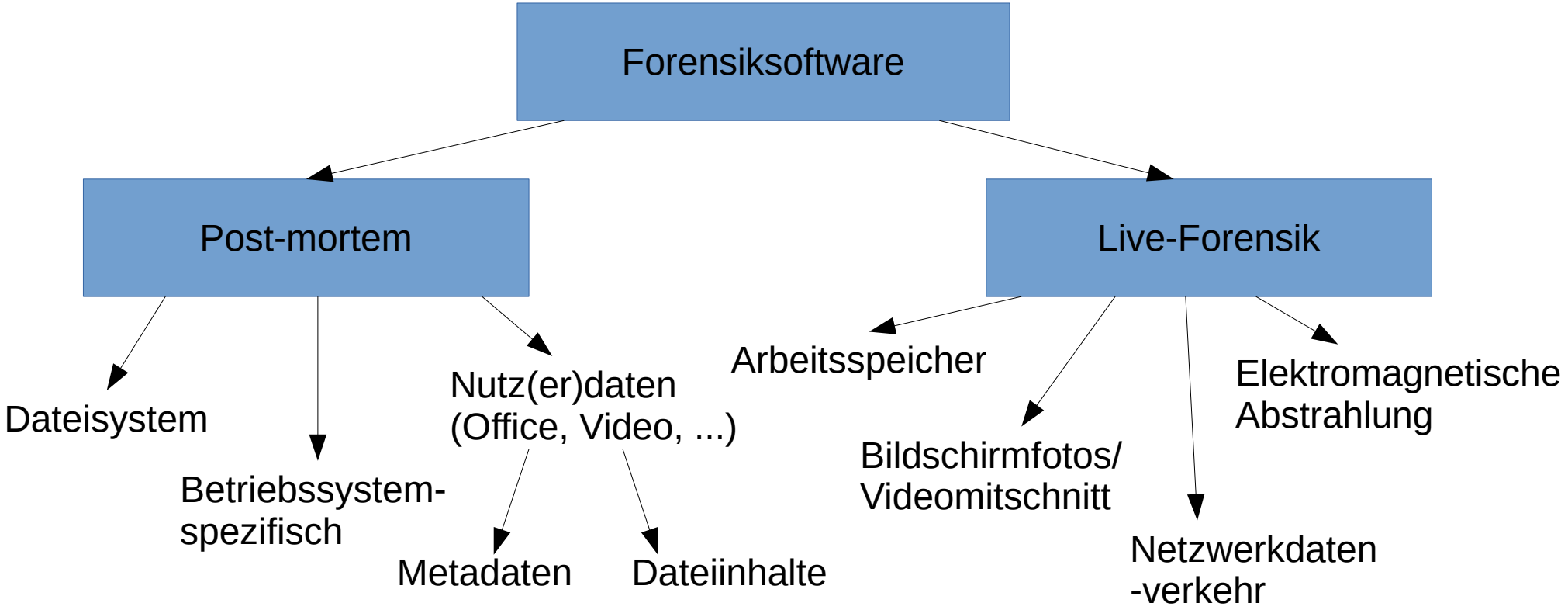
Wir haben im Laufe der Übung (mehr oder weniger erfolgreich) mit einer Kali-VM gearbeitet. Was bedeutet das aus Sicht der Forensik? Angenommen, jemand hätte gestern „versehentlich“ in der Übung den Bundestag gehackt?

- Wo fallen Spuren an?
- Wo fallen explizit keine Spuren an?
- Was wäre, wenn Sie die Kali-VM gestern nach der Übung von Ihrem System gelöscht hätten?

Grundlagen

- In der Vorlesung wurde schon einiges über IT-Forensik erzählt
- Hier möchte ich (kurz) einen Weg vorstellen, Forensiksoftware in Kategorien einzuteilen (aus Bachelorarbeit Phil Knüfer, 2014)
- Diese Kategorien geben uns gleichzeitig eine gute Indikation, welche verschiedenen Bereiche der IT-Forensik es gibt

Arten von Forensiksoftware



Forensische Auswertung: Praxisbeispiel

- Auf dem Desktop der Kali-VM findet sich der Ordner `Aufgaben/forensik`
- Darin liegt ein „Festplattenabbild“. Ein anderer Forensiker hat bereits eine Kopie der Beweisfestplatte mit der Linux-Software `dd` durchgeführt.
- Behandeln Sie diese Datei wie eine Festplatte.
  - Lesbar darauf zugreifen
  - Untersuchung dazu anstellen
- **Untersuchungsfrage 1:** „Der Benutzer john hat ein Bild gelöscht, können Sie das wiederherstellen?“
- **Untersuchungsfrage 2:** „Ein Webserver wurde per SQL-Injection gehackt. Wann wurde der Hack durchgeführt? Wir haben schon einmal ein bisschen recherchiert. Der SQLi-anfällige URL-Parameter lautet ‚debug‘.“

Forensische Auswertung: Praxisbeispiel

Allgemein:

- Einbinden einer Festplatte: `mount` (Standard-Linuxsoftware)
- Minimaler(!) Befehl für das Einbinden:
  - `sudo mount /pfad/zu/festplatte.dd /mnt`
  - Festplatte ist danach unterhalb des Ordners /mnt eingebunden und kann so verwendet werden, als wäre sie Teil des Kali-Dateisystems.
  - Überlegen Sie vor dem Einbinden des Festplattenabbilds, ob Sie den minimalen mount-Befehl um weitere Optionen ergänzen wollen (man-Page, Webrecherche, ...)

Forensische Auswertung: Praxisbeispiel

Untersuchungsfrage 1: „Der Benutzer john hat ein Bild gelöscht, können Sie das wiederherstellen?“

- Schnellauswertung – Software für Dateicarving: `foremost` („Spezialsoftware“)
  - man-Page oder Webrecherche für Details
- Gründlich – Open-Source-Forensiksoftware: `autopsy`
  - `$ sudo autopsy`
  - Dann im Webbrowser: `http://localhost:9999/autopsy`
  - Mit `„New Case“` einen neuen Fall anlegen, beliebigen Namen eingeben
  - Mit `„Add Host“` ein auszuwertendes System hinzufügen, beliebige Informationen eingeben
  - Mit `Add Image → Add Image File` ein Festplatten-Abbild angeben. Als Pfad `/home/user/Schreibtisch/aufgaben/04_forensik/festplatte.dd` eingeben, Typ `„Partition“` auswählen
  - `Next → Add → OK → Analyze → File Analysis` führt zu einer Ansicht, in der das Dateisystem graphisch wie in einem Dateiexplorer besichtigt werden kann

Forensische Auswertung: Praxisbeispiel

Untersuchungsfrage 2: „Ein Webserver wurde per SQL-Injection gehackt. Wann wurde der Hack durchgeführt? Wir haben schon einmal ein bisschen recherchiert. Der SQLi-anfällige URL-Parameter lautet ‚debug‘.“

- Wo dokumentiert ein Webserver die Zugriffe?
- Wie kann man die erhobenen Daten durchsuchen?

Forensische Auswertung: Bericht

Aufgabe:

- Formulieren Sie einen forensischen Bericht (Stichpunkte).
- Dieser soll dem Auftraggeber gegenüber klar nachvollziehbar beschreiben, welche Tätigkeiten mit welchen Ergebnissen durchgeführt wurden.
- Dabei die W-Fragen beachten:

  Was würde Wundram wissen wollen?

Forensische Auswertung: Bericht

Gemeinsame Besprechung / Diskussion: Was gehört in so einen Bericht? Wie geht man forensisch sauber vor?