Grundlagen und Anwendungen der IT Forensik

KNF-Kongress 2019

Roland Wagner
roland@datevnet.de

File Carving

„Foto-Exkurs“

File Carving

file signatures

„magic numbers“

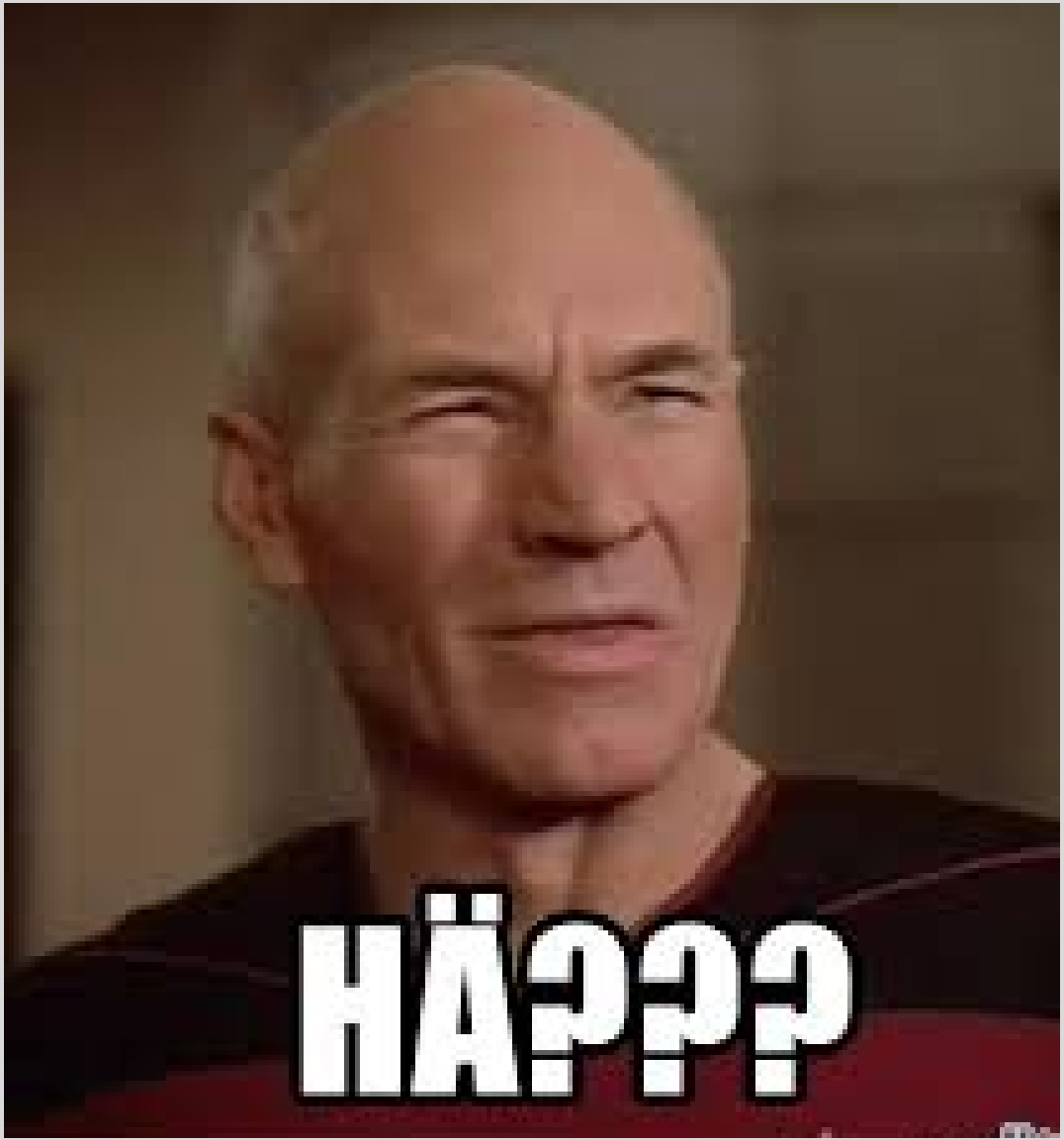
File Carving - Quiz

HEX	CHAR	Datei
4D 5A	MZ	DOS ausführbar .exe
47 49 46 38 39 61	GIF89a	Bild im GIF-Format
25 50 44 46 2d	%PDF-	PDF Dokument
FF D8 FF DB	ÿØÿÛ	Bild im JPEG-Format (JFIF, EXIF)
21 3C 61 72 63 68 3E	!<arch>.	Linux DEB-Datei
49 44 33	ID3	MP3 Datei
50 4B 03 04	PK..	ZIP-Datei (apk, docx, epub, jpa, jar, ...)
3A 29 0A	:).	SMILE (Datenautauschformat, JSON)

Gundlagen IT-Forensik

Wikipedia:

„… wissenschaftliche Expertise, die eine Beurteilung und Würdigung von Informationstechnik durch die Öffentlichkeit oder innerhalb eines Gerichtsverfahrens ermöglicht.“


HÄ???

Gundlagen IT-Forensik

BSI:

„… streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen, unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung, insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“

Gundlagen IT-Forensik

Meine Definition:

„Analyse von Daten

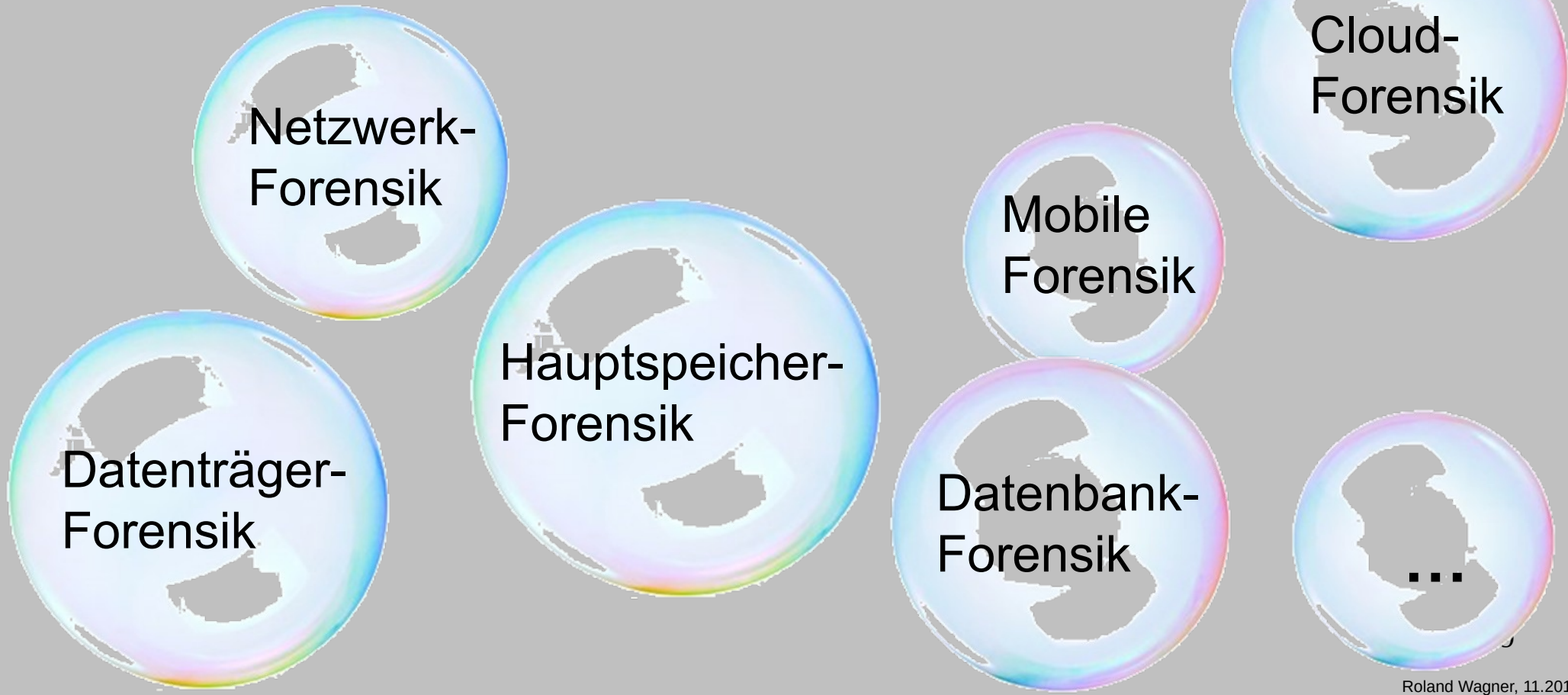
(auf Datenträgern, Geräten oder in Netzwerken),

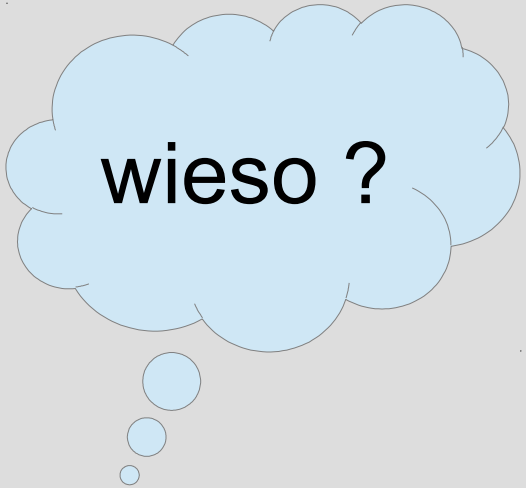
um zu ermitteln, wodurch welche Manipulationen

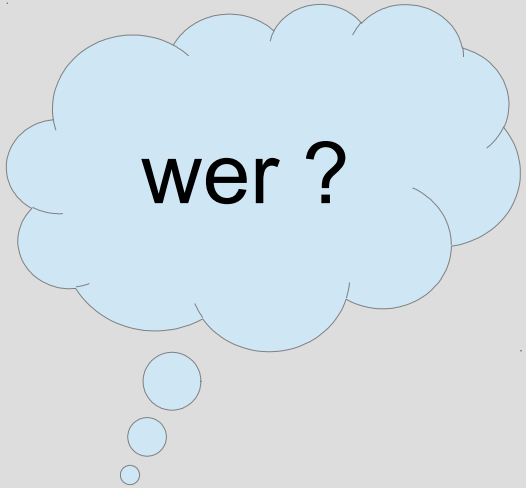
(am DV-System)

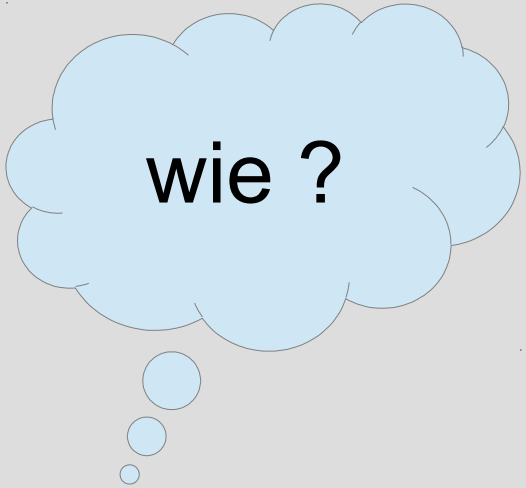
vorgenommen wurden.“

Begriffe


Netzwerk-
Forensik
Cloud-
Forensik
Mobile
Forensik
Hauptspeicher-
Forensik
Datenträger-
Forensik
Datenbank-
Forensik
...

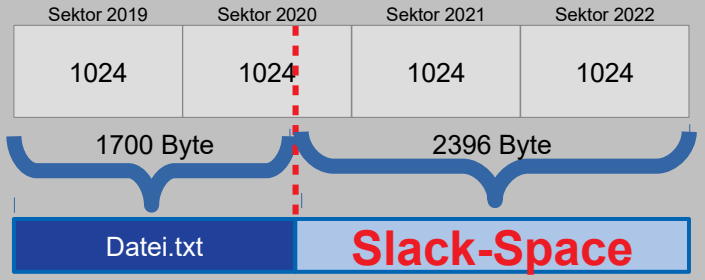

wieso ?

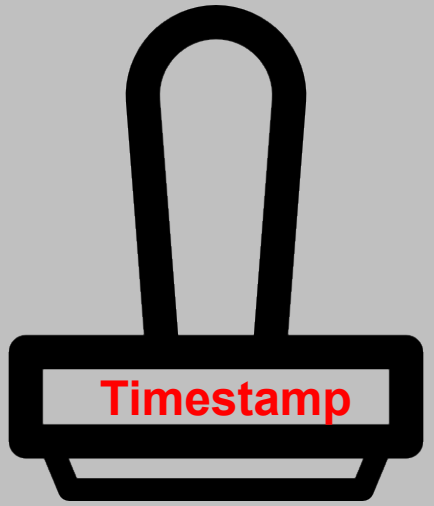

wer ?


wie ?

… ausgewählte Kapitel ...

File-Carving

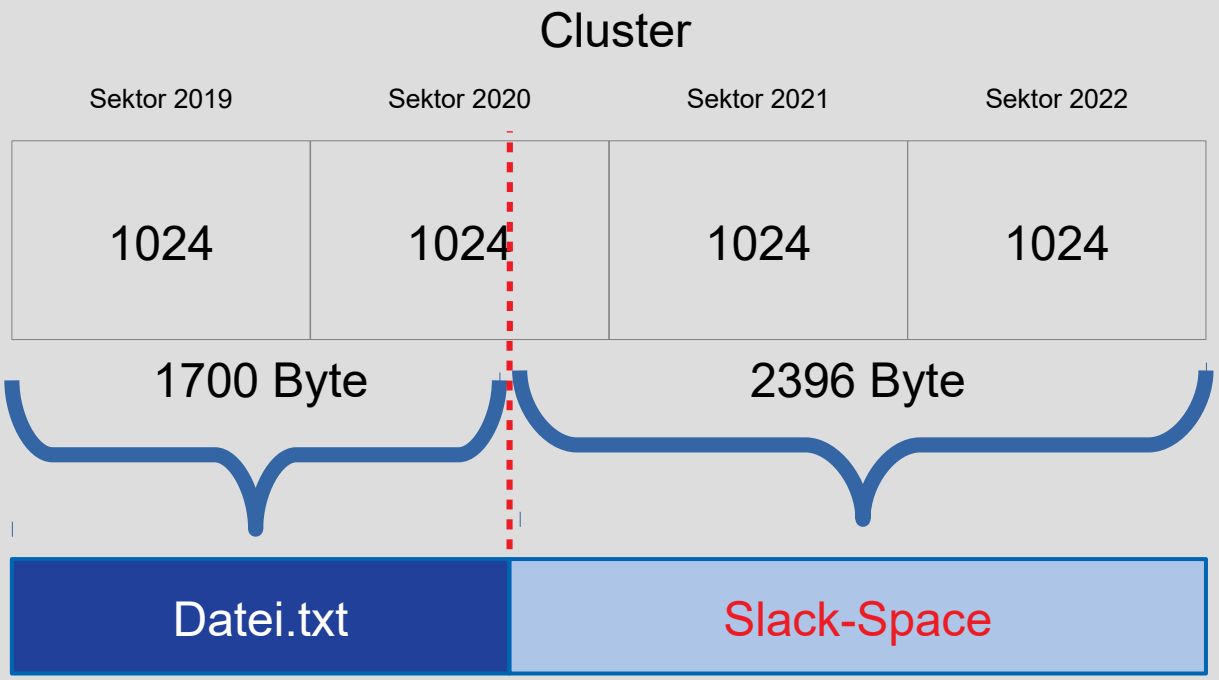




Slack Space

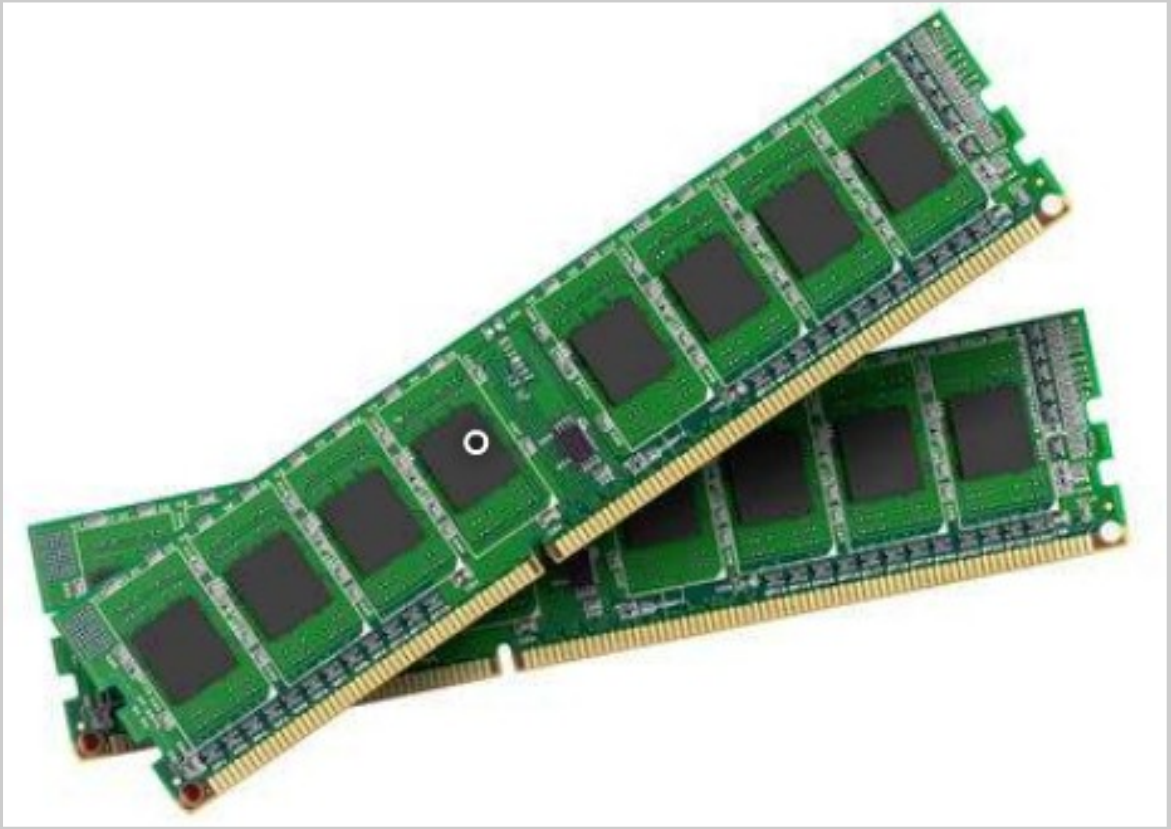
Slack Space

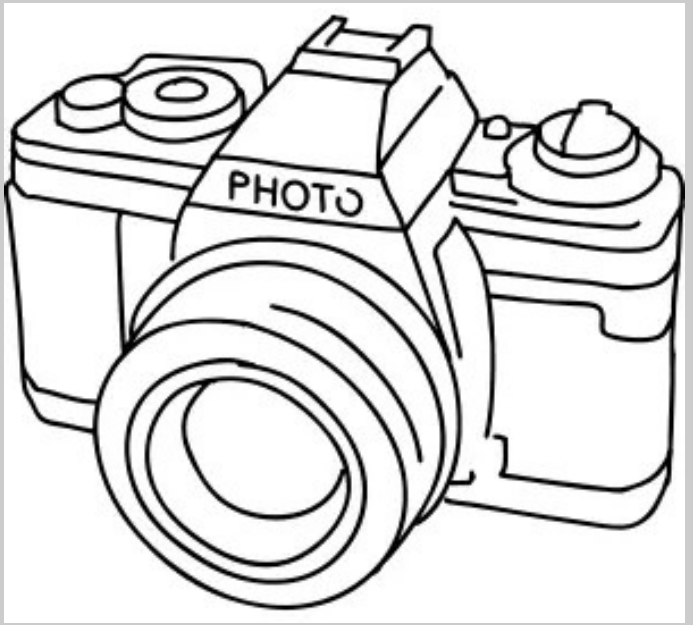
- Drive-Slack (RAM-Slack, MFT-Slack)



Memory-Forensik

Memory-Forensik





Memory-Forensik

pagefile.sys

swap

crash-file

core dump

hyperfil.sys

Memory-Forensik

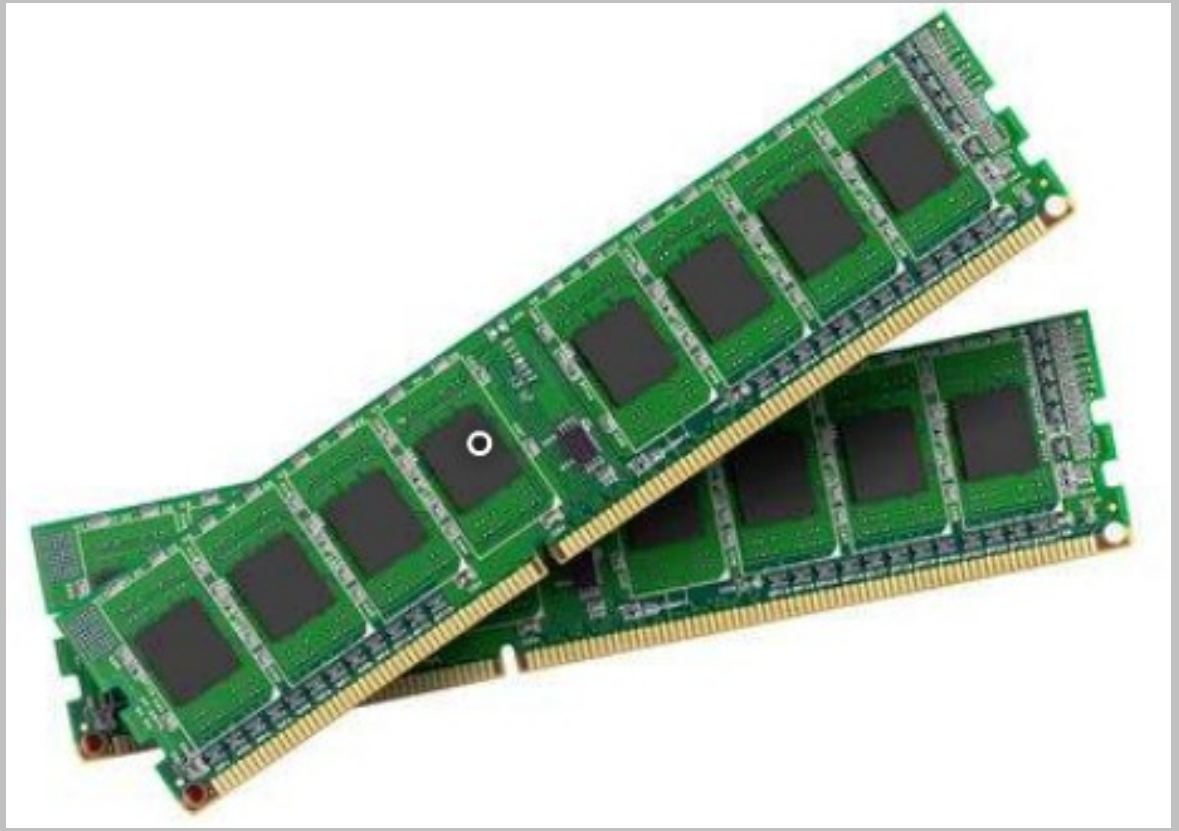
Komplettes Speicherabbild !

Früher:

- Firewire + /dev/mem

Heute:

- Virtuelle Systeme ,
- Tools



Memory-Forensik: Tools

FTK-imager

LIME

MAC Memory Reader

dumpit

linpmem

winpmem

osxpmem

… oder ...

„Cold Boot Attack“

https://youtu.be/TQP2IMnPw9c

Memory-Forensik
„Cold Boot Attack“

https://youtu.be/TQP2IMnPw9c

Anti-Forensik

Anti-Forensik - Manipulationen

- Einbruch im System
  - Aufruf von Webseiten
    - Aufruf von Programmen
      - Diebstahl von Daten
        - Besitz von strafrechtlich relevanten Daten
          - Verändern von Zeitstempeln
- ...

Manipulation Zeitstempel

„… war das alles ?“

- Handarbeit ? Werkzeuge !


Any
Questions