wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

FORENSIK@MMS

T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

FORENSIK

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

HERAUSFORDERUNG

- Strukturiertes und lückenloses Aufklären von Sicherheitsvorfällen in Anwendungen oder IT-Infrastrukturen
- Sichern von Beweismitteln
- Auffinden von Spuren und Nachvollziehen von Abläufen eines Sicherheitsvorfalls

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

BEGRIFFE

T · · Systems ·

FORENSIK

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

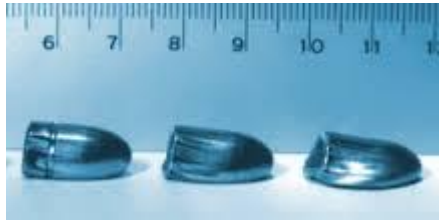
Rechtsmedizin

- Entomologie
- Osteologie
- Foren. Zahnmedizin

[...]

Toxikologie & Serologie

- Nachweis von Gift
- Auswertung von Blut, DNA oder anderen Sekreten



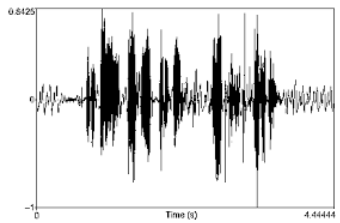
Ballistik

- Auswertung von Schusswaffen und Geschossen

Forensik

Phonetik

- Untersuchung von gesprochener Sprache

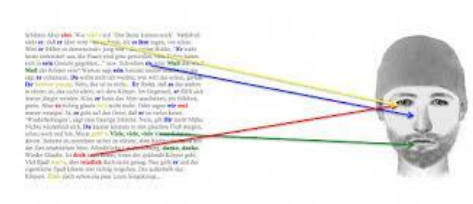


Tech. Formspuren

- Untersuchung von Abdrücken
- Daktyloskopie

Linguistik

- Untersuchung von geschriebener Sprache



IT-Forensik

- Aufdeckung von Computer-kriminalität

T · · Systems ·

IT-FORENSIK

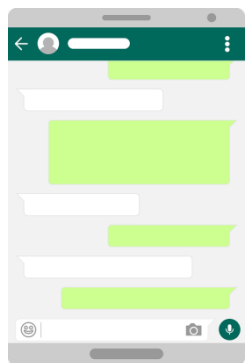
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Untersuchung von verdächtigen Vorfällen im Zusammenhang mit **IT-Systemen** und Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung **digitaler Spuren**
- Für das **Aufklären** eines Sicherheitsvorfalles, einer Straftat oder einer Verletzung von Richtlinien im IT-Umfeld ist eine **strukturierte und lückenlose Analyse** der betroffenen IT Infrastruktur notwendig
- Ziel der Analyse ist das **Auffinden von Spuren und Nachvollziehen von Abläufen** im IT-System
- Wesentliches Element der IT-Forensik ist die **Gerichtsfestigkeit** der digitalen Beweismittel und aller folgenden Aktivitäten

Anwendungsfelder:

Multimediaforensik

Mobilfunkforensik



T · · Systems ·

TATORT

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

„Ein Ort, an dem ein Täter vor, während oder nach der Straftat gehandelt hat“

Reale Welt

Digitale Welt

?

T · · Systems ·

SPUR

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

analoge Spuren

digitale Spuren

T · · Systems ·

DIGITALE SPUREN

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- In der Regel keine klassischen Beweismittel wie Fingerabdrücke, DNA-Spuren und ähnliche, die durch physische Interaktion zwischen Täter und Opfer entstehen
- Allerdings: „digitale Spuren“
- in den allermeisten Fällen sind Spuren zu finden, die technisch unvermeidbar sind und die der Forensiker erkennen und anschließend im Kontext der Untersuchung bewerten muss
- Viele der erzeugten Spuren sind nur temporär vorhanden
- Wo finden sich diese „digitale Spuren“
    - Betriebssystems
    - Dateisystems
    - IT-Anwendungen
    - Mitschneiden des Netzwerkverkehrs
    - .....

T · · Systems ·

DIGITALE SPUREN

wegweisend digital

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 6i3cb6owitcouepv.payoptvars.com/179zbgi
2. 6i3cb6owitcouepv.payforusa.com/179zbgi
3. 6i3cb6owitcouepv.paywelcomefor.com/179zbgi
4. 6i3cb6owitcouepv.payemarateslines.com/179zbgi

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. 6i3cb6owitcouepv.onion/179zbgi ◄Type in the address bar

T · · Systems ·

FEHLENDE SPUR BZW. ZU VIELE SPUREN ???

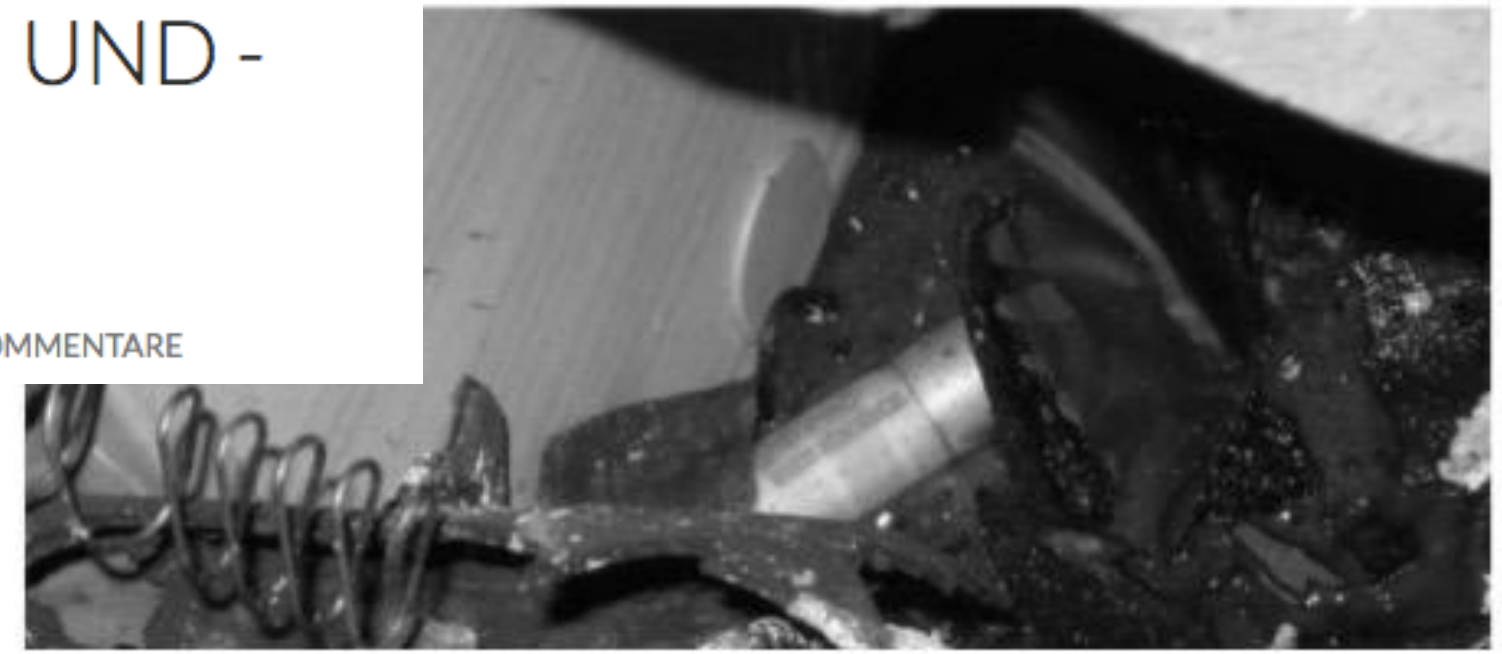
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

BEWEISMITTEL-MANIPULATION?

CHAOTISCHE BEWEISSICHERUNG LEERER PUMPGUN-HÜLSEN UND -PATRONEN IM NSU-WOHNMOBIL

SEPTEMBER 16, 2014 GEORG LEHLE 10 KOMMENTARE

dungslage Hülse Flintenlaufgeschoss Brenneke
rer linker Sitz



T · · Systems ·

FEHLENDE SPUR

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Häufigstes Vorkommen: Lücken in Logdateien
- Nutzen 1: Nachweis der Manipulation
- Nutzen 2: Widerlegen von Verdachtsmomenten

- Absichtliches Manipulieren Vernichten von Spuren wegen
  - Angst vor ...
  - Unwissenheit

T · · Systems ·

ZU VIELE SPUREN

CCC-Analyse des Staatstrojaners

Programmierter Verfassungsbruch

Die Analyse staatlicher Überwachungssoftware durch den Chaos Computer Club hat Erschreckendes zutage gefördert: Die eigentlich nur zur Überwachung von Kommunikation gedachte Software erlaubt einen Vollzugriff auf den Rechner des Betroffenen. Das aber hat das Bundesverfassungsgericht untersagt.

Von Christian Stöcker

DPA

Online-Durchsuchung: Mehr als das Verfassungsgericht erlaubt

Teilen Twittern E-Mail

Sonntag, **09.10.2011** 12:43 Uhr Drucken Nutzungsrechte Feedback Kommentieren

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

FORENSISCHER PROZESS/ VORGEHENSWEISE

T · · Systems ·

FORENSISCHER PROZESS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Zur Durchführung einer Analyse mittels *IT-Forensik* ist ein fester Prozess notwendig

Ziel ist die Beantwortung der folgenden Fragen:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie wurde vorgegangen? Welche Tools und/oder welche physikalischen Mittel wurden eingesetzt?

Gegebenenfalls werden diese Fragen noch durch (mindestens) zwei weitere ergänzt:

- Wer hat es getan?
- Was kann gegen eine zukünftige Wiederholung der Vorgänge getan werden?

→ Ablauf einer Untersuchung muss schon vor Beginn klar definiert und zum Zweck der späteren Überprüfung jederzeit reproduzierbar sein

T · · Systems ·

FORENSISCHER PROZESS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

(Nach BSI Leitfaden „IT-Forensik“)

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

STRATEGISCHE VORBEREITUNG

T · · Systems ·

FORENSISCHE UNTERSUCHUNGSABSCHNITTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Strategische Vorbereitung
  - Maßnahmen vor Eintreten eines Vorfalls
  - Maßnahmen beim Betreiber der IT
    - Aktivierung von Dokumentationsmechanismen (Logdaten),
    - Zeitsynchronisation,
    - Definition von Sicherheits- und Forensikkonzepten,
    - Einsatz von Erkennungswerkzeugen (IDS)
    - Definition von Meldewegen
    - Maßnahmen auf Seiten des Forensikers
    - Konzeptionierung und Ausstattung eines forensischen Labors (Vorgehensplanung, HW, Formblätter,...)
    - Auswahl und Test verschiedener Sicherungstools,
    - Vorbereiten von Boot-Images und Datenträgern zur Sicherung,

T · · Systems ·

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

OPERATIVE VORBEREITUNG

T · · Systems ·

FORENSISCHE UNTERSUCHUNGSABSCHNITTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Operative Vorbereitung
  - Maßnahmen nach Eintreten eines Vorfalls
  - Auswertung des Symptoms (Verdachtsfall) /Bewertung des Vorfalls und der Indizien
  - Definition der Vorgehensweise der forensischen Untersuchung
    - Suche, Identifikation und Beschriftung der in Frage kommenden Datenquellen (Computer, Handys, USB-Sticks, externe Festplatten, aber auch RAM, Routerkonfigurationen, Netzwerkstati, Logfiles, ...) und
    - Auswahl der geplanten Sicherungsmittel (Tools und Zieldatenträger)
  - Einleitung von Sofortmaßnahmen zur Schadensminimierung

T · · Systems ·

SOFORTMASSNAHMEN

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- BCM
  - Vorrangiges Ziel (für „Management“) des Incident Response Prozesses ist Minimierung von Kosten und (Ausfall-)Zeiten
  - Ziel Management: schnell wieder arbeitsfähig sein
  - Ziel Forensiker: Zeit gewinnen, in Ruhe analysieren
  - Idee: Analyse und BCM entkoppeln
    - Triage-Image erstellen
    - Bei virtuellen Umgebungen: VM anhalten (NICHT ausschalten/herunterfahren), ggf. umbenennen und VM-Backup als „neue“ Maschine wiederherstellen
    - Wiederherstellung aus Backups

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

DATENSAMMLUNG

T · · Systems ·

FORENSISCHE UNTERSUCHUNGSABSCHNITTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Datensammlung
  - Auswahl forensisch relevanter, zu sichernder Daten → eigentliche Sammlung der vorher festgestellten Daten
  - Erfassung von Systemparametern, laufenden Prozessen, Netzwerkverbindungen, Nutzern
  - Forensische Duplikation (Imaging) zur Beweissicherung
  - Absicherung der Images gegen unerkannte Veränderung
  - Ggf. Vier-Augen-Prinzip
- Chain of Custody: Beweiskette
- Ziel: Identität und Integrität von der Datensammlung bis hin zur Verwendung eines Beweisstücks vor Gericht
  - Wer hat das Beweismittel gesichert (Name und Kontaktinformationen)
  - Wann wurde es gesichert (Systemzeit und Ortszeit)?
  - Beschreibung des Beweismittels (make model, serial number, condition of the item (digital images))
  - Wo wurde es gesichert (physische Adresse, Foto der Fundszene)?

T · · Systems ·

MEMORY IMAGES

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Standard in der Forensik, Möglichkeit disk encryption zu umgehen
- Volatile Daten erfassen
  - RAM
  - Aktuelle Netzwerkverbindungen
  - Laufende Applikationen
  - Open/listening Netzwerkverbindungen

T · · Systems ·

ANALYZING MEMORY IMAGES

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Was findet sich alles im Memory?
  - Prozesse, Process space examination
  - Offene Files, Registry Keys, Devices
  - Encryption keys und Passwörter (Bitlocker, Truecrypt)
  - Netzwerkverbindungen
  - Konfigurationsparameter
  - Memory-only exploits/root kit technology, Malware (unencrypted)
  - Data stream Carving / String Search
    - Chat sessions
    - Internet history
    - Web Mail
    - String search

T · · Systems ·

SICHERUNG VON DATEN

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- einzig wirklich sinnvolle Methode der Priorisierung in der Digitalen Forensik ist die nach der Vergänglichkeit der Daten (Volatilität)
- Vorgeschlagene Reihenfolge:
  - CPU-Register, Cache-Speicher
  - Routingtabellen, ARP-Cache, Prozessliste, Netzwerkstatus, Kerneldaten, Hauptspeicherinhalt
  - Temporäre Dateisysteme, SWAP-Bereiche, andere temporäre Daten
  - Massenspeicherinhalte (logisch oder physikalisch)
  - Auf anderen Systemen verfügbare Log- und Monitoringdaten des untersuchten Systems
  - Physikalische Konfiguration, Netzwerkkonfiguration
  - Archivierte Medien (Datensicherungen)
- Bitte nicht:
  - Rechner herunterfahren bevor die Sammlung der Beweise abgeschlossen ist.
  - den Programmen und Tools vertrauen, die auf dem untersuchten Computer vorhanden sind
  - Programme starten, die großflächig Zugriffszeitstempel verändern können (z.B. ‚tar' oder ‚xcopy').

T · · Systems ·

DATENSCHUTZ

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Eingriff in die persönlichen Daten der von der Untersuchung Betroffenen
- betrifft es darüber hinaus aber fast immer auch Personen, die mit dem vorliegenden Fall überhaupt nichts zu tun haben
- im Bereich der Strafverfolgung durch die geltenden Gesetze weitgehend problemlos
- Aber: Datenschutz!
  - Vollmacht
  - Beteiligung relevanter Gremien

- Datenminimierung!!!

T · · Systems ·

DATENSAMMLUNG (1)

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

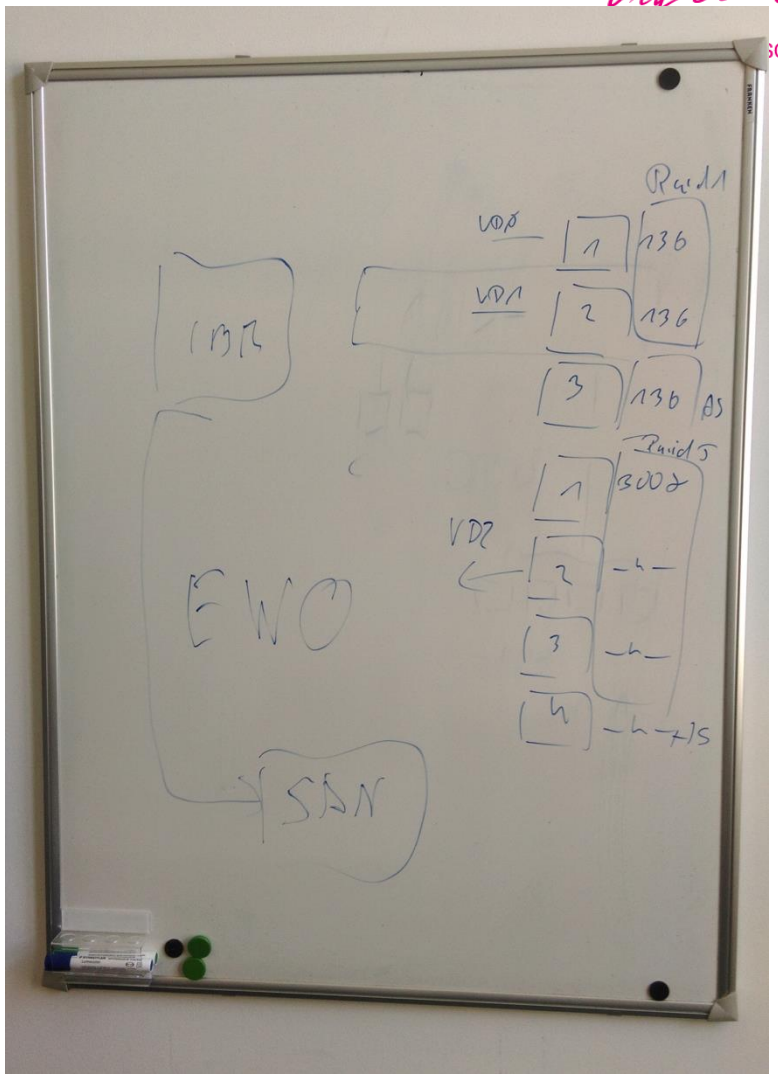
T · · Systems ·

DATENSAMMLUNG (2)

DATENSAMMLUNG (3)

wegweisend digital

SOLUTIONS



T · · Systems ·

DATENSAMMLUNG (4)

wegweisend digital
TIMEDIA SOLUTIONS

3 → Collection of data ¶

3.1 → Overview of analyzed evidence → ¶

Pos.	Description	Filename	Editor	Checksum
1	Autoruns file	SOL-PAL-S002.arn	Jan Starke	MD5: 2c02f5f5a7e1bce1b0210a056a622501
2	Forensic Image Notebook 1 (30349427221); Hard drive S/N: 43TRTJ2CT	First filename of image: TD2_IMG/2015-07-27 09-11-30/IMAGE.001	Jan Starke	SHA1: 9334fb710e34860ca040c589daa79ef62176afac ¶ MD5: 41a0d82c5cd2cd9a04c235dc013eb185
3	Forensic Image Notebook 2 (38724293233); Hard drive S/N: TF755AY9KRDEKM	First filename of image: TD2_IMG/2015-07-27 16-45-29/IMAGE.E01	Jan Starke	SHA1: 4ea9362a8670c34aa3d2db1dbcfd91708f017ee2 ¶ MD5: 1444160bf99a18fdfd99d6e29035badd
4	Screenshot of Process Explorer (svchost.exe processes)	svchost.exe.tiff	Jan Starke	MD5: ff6432c92947ecb19ea9d906eda988b3
5				
6				

Tabelle 3 Evidence ¶

T · · Systems ·

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

UNTERSUCHUNG / DATENANALYSE

T · · Systems ·

FORENSISCHE UNTERSUCHUNGSABSCHNITTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Untersuchung
  - Zwischenschritt vor der eigentlichen Datenanalyse
  - Identifizierung von forensisch relevanten Daten, d.h. „Identifikation und Reduktion“ der gesicherten Daten
  - Maßnahmen zur Extrahierung forensischer Daten

- Datenanalyse
  - Analyse der identifizierten Daten
  - Herstellung von Verbindungen zwischen Daten
  - Nachvollziehen zeitlicher Abläufe
  - Ggf. Live Analyse am laufenden System

T · · Systems ·

DATENANALYSE – CHAIN OF CUSTODY

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Chain of Custody: Beweiskette
- Ziel: Identität und Integrität von der Datensammlung bis hin zur Verwendung eines Beweisstücks vor Gericht
- Chronologische Dokumentation
  - Bei Übergabe eines Beweismittels:
    - Wer hatte das Beweismittel bisher (Name und Kontaktinformationen)
    - Wer übernimmt das Beweismittel (Name und Kontaktinformationen)
    - Datum und Uhrzeit der Übergabe
    - Zweck der Übergabe
    - Zustand des Beweismittels
  - Bei allen Aktionen:
    - Was für Aktionen wurden mit dem /auf dem Beweismittel durchgeführt?
    - Datum und Uhrzeit der Analyse
  - Nicht mit dem Original arbeiten, Kopie verwenden!

T · · Systems ·

INVESTIGATIVE PROCESS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Computer Forensics is as much of an art as it is a science!

- Forensische Untersuchung ist ein iterativer Prozess, keine statische Disziplin wie eine DNA-Analyse
- Kein statischer Prozess
- Aber: immer im Rahmen der Befugnisse bleiben
- Wichtige Skills:
  - Verständnis für das Betriebssystem und die Applikationen
  - User Aktionen und System Aktionen verstehen und interpretieren
  - Problem-Lösungsorientiertes Arbeiten
  - Analyse und nicht nur Daten Extraktion!
  - Hypothese über Vorgang aufstellen und nach Indizien zum Belegen UND Widerlegen suchen!
  - Nicht nur eine Hypothese: iterativer Vorgang!

T · · Systems ·

TIMELINE ANALYSIS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Manual Creation of a Super Timeline

Step 1 – Find Partition Starting Sector

- `# mmls image.dd`

Step 2 – Mount image for processing

- `# mount -o ro, noexec,show_sys_files,loop,offset=32256 image.dd /mnt/windows_mount`

Step 3 – Create Comprehensive Timeline

- `# log2timeline -p -r -f winxp -z CST6CDT /mnt/windows_mount -w timeline.csv`

Step 4 – Filter Timeline

- `# l2t_process -b timeline.csv -k keywords.txt MM-DD-YYYY..MM-DD-YYYY`

T · · Systems ·

TIMELINE ANALYSIS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992	Entry in log file: C:/Windows/
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/drivers/ndis.sys[MofResourceName](Thu Jun 18 22:30:26 2009.2998	Entry in log file: C:/Windows/
6/18/2009	22:36:15	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed	LOGON.SCR-7C80CA1C.pf - [L
6/18/2009	22:41:26	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM	[DELETED] SYSTEM
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed	DEFRAG.EXE-738093E8.pf - [
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F838A89.pf: DFRGNTFS.EXE was executed	DFRGNTFS.EXE-4F838A89.pf
6/18/2009	22:41:59	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE	[DELETED] emRoot/System32/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/	[DELETED] ???/0000000E/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/	[DELETED] ???/{83da6326-97a
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/	[DELETED] ???/00000003/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/	[DELETED] ???/00000008/000
6/18/2009	23:34:09	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed	PKMAILER.EXE-83FAD500.pf
6/18/2009	23:34:35	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats	Key name: HKEY_USER/Softwa
6/18/2009	23:34:36	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp	Key name: HKEY_USER/Softwa
6/18/2009	23:34:50	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed	IPODSERVICE.EXE-FE1A6FF7.p
6/18/2009	23:34:59	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed	RUNDLL32.EXE-2E65B341.pf
6/18/2009	23:34:59	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe	UEME_RUNPATH:C:/Windows
6/18/2009	23:35:05	EST5EDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences	LSO created -> File: C://mnt/v
6/18/2009	23:35:07	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc	Key name: HKEY_USER/Softwa
6/18/2009	23:35:38	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk	UEME_RUNPATH:Mozilla Firef
6/18/2009	23:35:39	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe	UEME_RUNPATH:C:/Program
6/18/2009	23:35:39	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed	FIREFOX.EXE-E60C0AA7.pf - [
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/	[DELETED] ???/00000003/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/	[DELETED] ???/{83da6326-97a
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/	[DELETED] ???/0000000E/

T · · Systems ·

MALWARE ANALYSIS

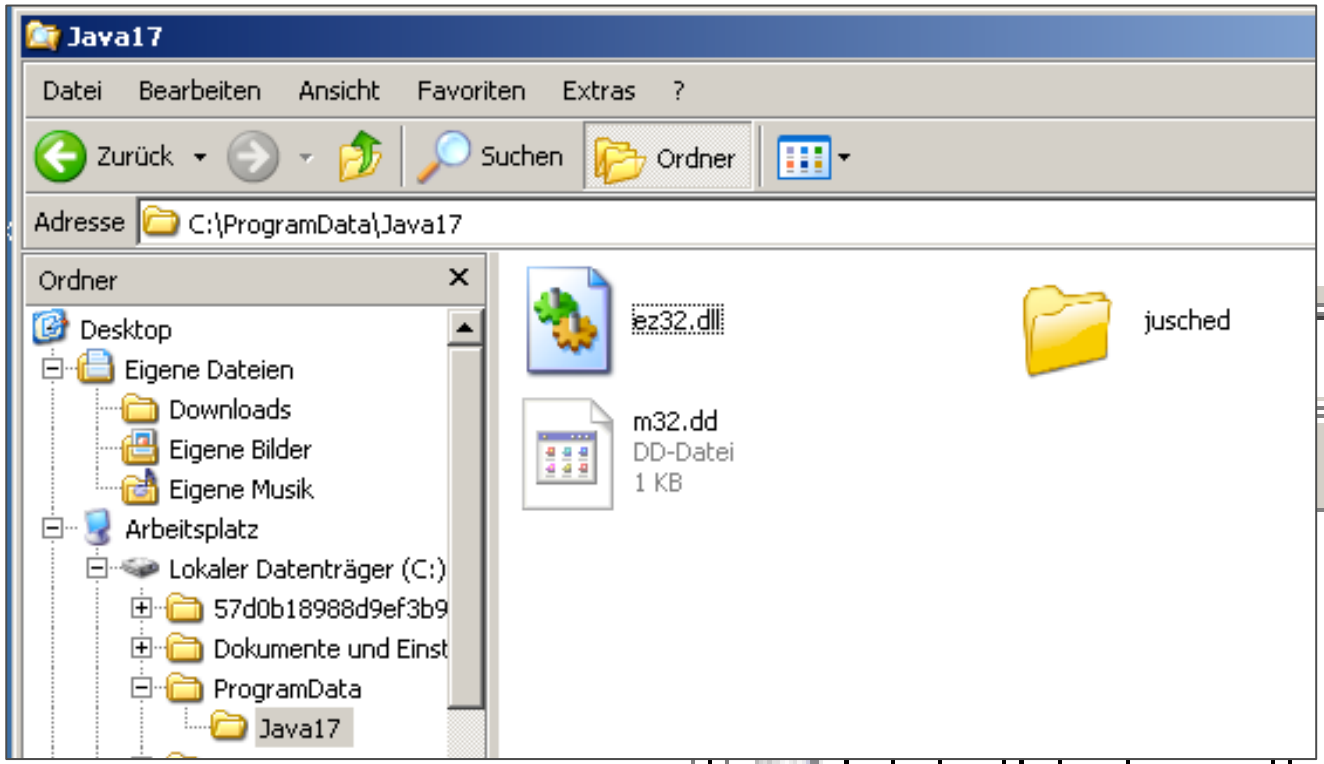
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

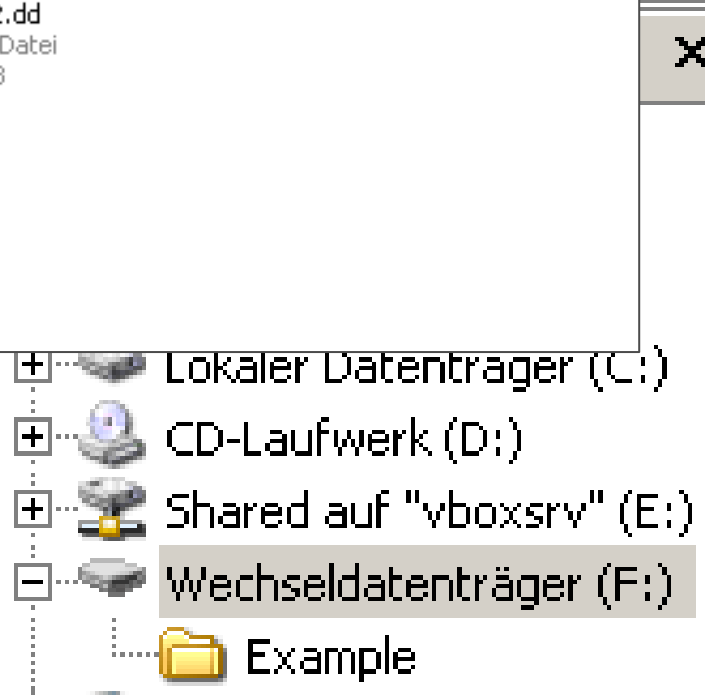
- Dynamic Analysis (Ausführen)
- Static Analysis (Reverse Engineering)
- Hybrid Analysis (Ausführen und Reverse Engineering)

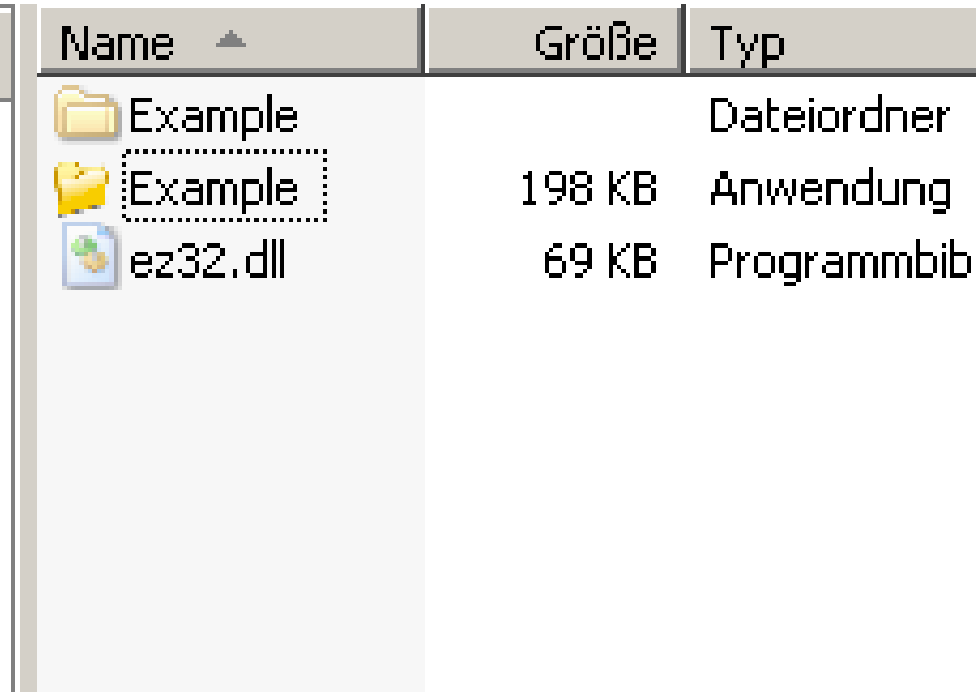
T · · Systems ·

MALWARE DYNAMIC ANALYSIS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



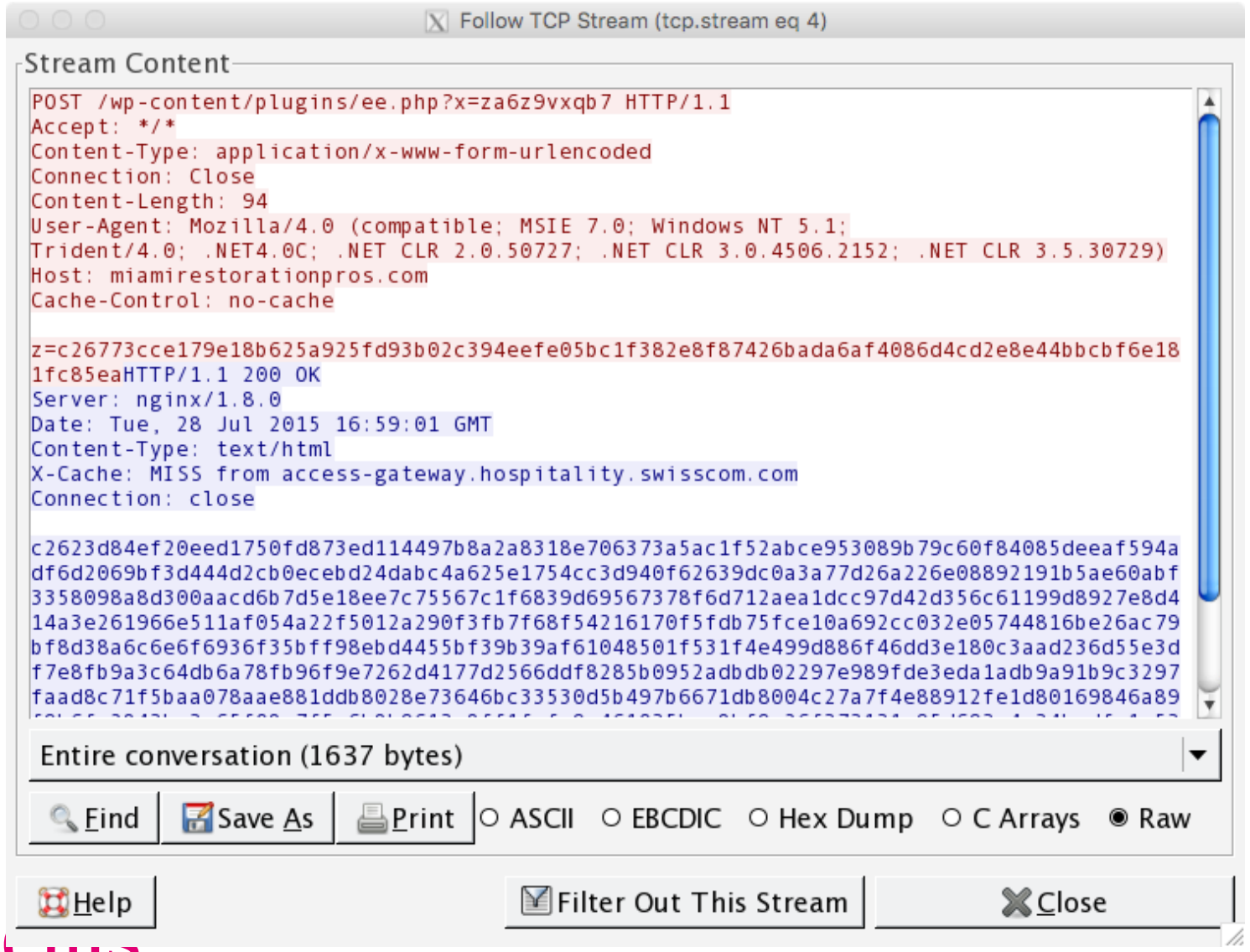




T · · Systems ·

MALWARE DYNAMIC ANALYSIS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



T · · Systems

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

DOKUMENTATION

T · · Systems ·

FORENSISCHE UNTERSUCHUNGSABSCHNITTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Prozessbegleitende Dokumentation

- Schon während des gesamten Prozesses ist eine engmaschige Dokumentation sinnvoll, um das Vorgehen bei der Analyse im Nachhinein nachvollziehbar zu machen
- Protokollierung von Daten und Prozess:
  - Genutzte Software (Name und Version)
  - Softwarekonfiguration (einzelne Einstellungen oder Kommandozeilenparameter)
  - Begründung zur Entscheidung für die Software
  - Protokollierung der gewonnenen Daten und durchgeführten Prozesse
  - Werkzeugeinsatz (Warum?, Wie?)
  - Interpretation der Ergebnisse (Fakten)

T · · Systems ·

FORENSISCHE UNTERSUCHUNGSABSCHNITTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

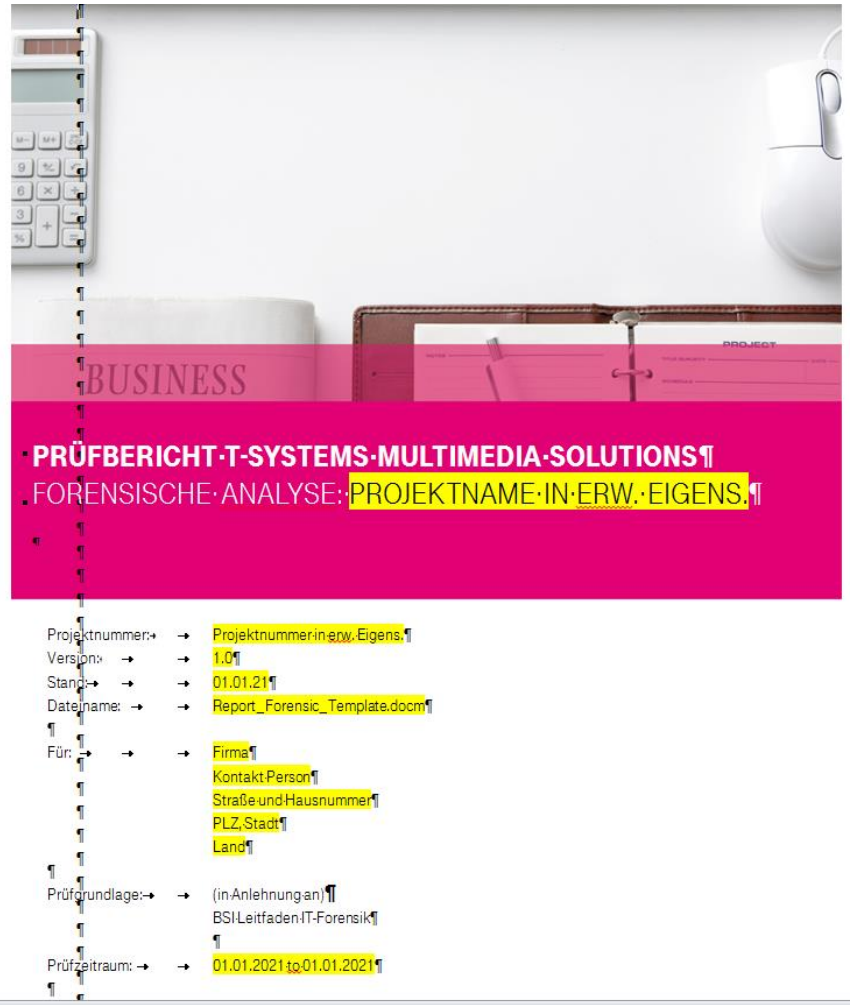
Abschließende Dokumentation

- Ziel: aus den einzelnen Daten und Erkenntnissen ein Gesamtbild erstellen
- Inhalte:
  - Wie wurde die Untersuchung durchgeführt?
  - Lückenlose Beschreibung des Untersuchungsverlaufes sowie der eingesetzten Werkzeuge und Methoden
  - Welche Informationen wurden gewonnen?
    - Ermittlung der Identität des Täters / der Täter,
    - Ermittlung des Zeitraums der Tat (Erstellung „Timeline“),
    - Ermittlung des Umfanges der Tat,
    - Ermittlung der Ursache und Durchführung
  - Rekonstruktion des Vorfalls anhand der Ergebnisse und Fakten
- Lessons learned

T · · Systems ·

ABSCHLUSSBERICHT

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

FORENSISCHE METHODEN

T · · Systems ·

FORENSISCHE METHODEN

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Untersuchungen des Betriebssystem
  - Im Betriebssystem wird ein Großteil der forensisch relevanten Daten verwaltet.
  - Beispiele:
    - Flüchtige Daten im Arbeitsspeicher
    - Nichtflüchtige Daten im Massenspeicher
    - Verwaltung des Netzwerkes
    - Logging Daten (Sitzungsdaten, geöffnete Dateien, laufende Prozesse)
    - Registry Einträge
- Untersuchung des Dateisystems
  - Das Dateisystem der Datenträger ist einer der bedeutsamsten Orte, um nichtflüchtige Daten zu gewinnen
  - Untersuchung der Partitionen und Sektoren
  - Partition Gap (Nicht belegter Platz zwischen 2 Partitionen)
  - RAM- Auslagerung (Swap)
  - Suspend-to-disc (Spezielle Datei in den mobile Geräte ihren Arbeitsspeicher verschlüsselt ablegen.)

T · · Systems ·

FORENSISCHE METHODEN

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Auswertung vorhandene Angriffserkennung
  - Automatisierte Maßnahmen zur Erkennung von Unregelmäßigkeiten (IDS, on-access-Virenscanner, SIEM, Logfunktionalitäten)
  - Diese Werkzeuge müssen in der Phase der strategischen Vorbereitung, also bevor ein Vorfall eintritt, aktiviert werden
- Untersuchung von IT-Anwendungen IT-Anwendung
  - Untersuchung von Anwendungslogs und Verlaufslogs (z.B. Browser)
- Skalierung von Beweismöglichkeiten
  - Alle Methoden und Hilfsmittel die nur im konkreten Verdachtsfall durchgeführt werden. (z.B. Mitschneiden des Netzwerkverkehrs)
- Datenbearbeitung und Auswertung
  - Analyse von Ausgangsdaten um Daten zu extrahieren oder rekonstruieren
  - Anschauliche Darstellung von Sachverhalten aus forensischer Sicht

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

FORENSISCHER ARBEITSPLATZ

T · · Systems ·

FORENSISCHER ARBEITSPLATZ

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

GRUNDAUSSTATTUNG

Hardware-Schreibschutzadapter

- IDE
- SATA
- USB 3.0
- FireWire

ESD-Arbeitsmatte

Digitale Kamera

Werkzeug

T · · Systems ·

FORENSISCHER ARBEITSPLATZ

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

COMPUTERAUSSTATTUNG

Auswertecomputer / Forensische Workstation

- für die Untersuchung der Asservate
- keine Netzwerkverbindung zur Außenwelt
- Reduzierung von Zugriffsmöglichkeiten und Rechten
- Rücksetzbar auf vorher definierten Stand

Office-Rechner

- Erstellen des Untersuchungsberichts/Gutachtens
- empfohlen, das System vollständig zu verschlüsseln

Internetcomputer

- Internetrecherchen, Downloads und sonstigen Internetnutzungen

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

VIELEN DANK

T · · Systems ·

KONTAKT

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

DR. ANTJE WINKLER
T-Systems Multimedia Solutions GmbH

Riesaer Straße 5
D-01129 Dresden

Telefon: +49 351 2820 – 2093

E-Mail: antje.winkler@t-systems.com
Internet: www.t-systems-mms.com

T · · Systems ·