Inhaltsverzeichnis

1 Jura

1.1 Grundrechte der Betroffenen und Zugriff auf Netzwerkspeicher

Fragen: Welche Ermächtigungsgrundlagen gibt es, um im Rahmen einer Durchsuchung auf Netzwerkspeicher zuzugreifen? Wie funktioniert das technisch?
Kurzantwort: Offene Maßnahme: Durchsicht nach § 110 bei Durchsuchung nach § 102 bzw. Sicherstellung nach §§ 94ff. Oder Verborgen: bei Online-Durchsuchung nach § 100b / Durch Experten mit spezieller Software für Cloud Forensik wie Kumood (ermöglicht durch Trojaner), genaueres in der Übung

Welche Grundrechtlichen Probleme gibt es, die bei einer Untersuchung zu beachten sind:

- **Artikel 1 I, 2 I**: Schutz der Privatsphäre
- **GG Artikel 10**: Schutz der Telekommunikation (Fernmeldegeheimnis)
- **GG Artikel 12**: Recht auf freie Wahl der Arbeit: Im Bezug auf Homeoffice und dafür notwendige Geräte wichtig
- **GG Artikel 13**: Unverletzlichkeit der Wohnung
- **GG Artikel 14**: Eigentumsrecht an Gegenständen

Rechtliche Problematik bei Cloud (Netzwerkspeicher) Untersuchung:

- Verletzung von Artikel 12 beim Dienstleistungsanbieter
- Verletzung der Privatsphäre beim Kunden
- Cloudspeicher kann im Ausland sein ⇒ Überschreitung der Staatsgrenzen

Eingriffe in Grundrechte benötigen immer eine parlamentarische Ermächtigungsgrundlage (z.b. Gesetze) und genaue Beschreibungen wie diese statt zu finden haben (z.b. inklusive Straftatenkatalog, Vorgehensweise, Einschränkungen). Zudem müssen diese auch immer von einem Richter bestätigt werden.

Offene Ermittlung Ermächtigungsgrundlage ist die StPO. Mittels §§ 94 ff StPO darf die Polizei (meist im Auftrag der Staatsanwaltschaft immer durch Bestätigung des Gerichtes) den physischen Rechner beschlagnahmen. Voraussetzung dafür ist ein begründeter Verdacht. Unbeteiligte (z.b. Provider der Cloud) dürfen dabei nicht durchsucht werden.

Mittels §110 StPO ist dann die Durchsicht von Papieren und Speichermedien geregelt, welche bei einer Durchsuchung gefunden werden. Dabei ist auch explizit (Absatz 3) die Durchsicht räumlich getrennter wie Cloud-Speicher (wenn ein Verlust dieser Daten zu befürchten ist) definiert.
Ablauf: § 102 definiert Durchsuchung die nach § 105 gerichtlich legitimiert sein muss. Nach § 110 können dann die Daten gesichtet werden und mittels § 94 sichergestellt werden. Abschließend müssen beschlagnahmte Gegenstände in angemessener Zeit wieder zurückgegeben werden. Gegenstände die für das Leben notwendig sind dürfen nicht beschlagnahmt werden.
Probleme mit §110 Absatz 3:

1. Gerät ist zugangsgesichert: Umgehen mit Kooperation oder Erzwingen von biometrischen Daten oder Passwort zufällig finden oder Sicherheitslücken ausnutzen
2. Daten im Ausland: In der Regel wird dafür eine Rechthilfeersuchen bei den Ländern angefragt und dann entweder geholfen oder nicht, ansonsten wird Souveränität des Staates verletzt. Lösung: Kooperation, Finden von Passwörtern
3. Wer durchsucht?: Sachverständige oder Software, für die eig. nicht (da nicht Staatsanwalt und Polizei) direkt die Grundrechtseingriffe genehmigt sind
4. Zufallsfunde: Dürfen nur verwendet werden, insofern die gefundenen Inhalte auch eine Durchsuchung rechtfertigen würden (z.b. bei Mord)

Verdeckte Ermittlung Beispielsweise möglich durch Telekommunikationsüberwachung TKÜ. Da es aber meistens verschlüsselt (TKÜ somit nicht zielführend) ist, wird meist eine Quellen-TKÜ oder Online-Durchsuchung benötigt. Für die letzten beiden wird (fast immer) ein Tojaner auf dem System benötigt. Die Online Durchsuchung ermöglicht dann auch die Analyse von Netzwerkspeichern.

1.2 Einsatz polizeilicher Ermittlungswerkzeuge

Fragen: Wie funktioniert eine Telekommunikationsüberwachung technisch? Welche Unterschiede bestehen zur so genannten Quellen-Telekommunikationsüberwachung?
Kurzantwort: Mittels Tojaner, Spähsoftware / Unterschied verschlüsselt und unverschlüsselt

Technische Möglichkeiten Dabei geht es zu großen Teilen um verdeckten Einsatz technischer Mittel, also Trojaner. Dabei gibt es zwei Bauarten:

1. **Verdeckte Existenz** sind Trojaner, deren Existenz den Benutzer ungekannt ist
2. **Verdeckter Zweck** sind Programme, die (zusätzlich) unbekannte Zwecke erfüllen

Zudem gibt es noch unterschiedlichste Ermittlungsziele, welche den Zugriff auf Daten betreffen:

1. Datenverkehr (ggf. verschlüsselt) überwachen: **Telekommunikationsüberwachung TKÜ**
2. Datenverkehr + Inhalte (entschlüsselt) überwachen: **Quellen-TKÜ**
3. Gesamtsystem überwachen: **Online-Durchsuchung**

Bei einer TKÜ wird der reine Datenverkehr abgefangen, gedoppelt und den Ermittlern zugeschickt. Das betrifft nicht nur Inhalte sondern auch Umstände (z.b. Mit wem wird Kommuniziert?). Da immer mehr verschlüsselt wird (Messangern sei Dank), wurde das Gesetzt nachgeschärft, sodass nun auch die Kommunikation in unverschlüsselter Form abgefangen werden kann, was Quellen-TKÜ genannt wird. Im Allgemeinen wird dazu ein Tojaner auf dem Gerät des Betroffenen verwendet. Denkbar ist aber auch ein Abfangen der Daten, z.b. beim Provider.
Anmerkung: Die rechtliche Eingriffshürden für (Quellen)-TKÜ ist generell geringer, aber die technische Hürde ist in beiden Fällen vergleichbar. Seit 2017 dürfen nicht nur besondere Stellen (z.b. BKA privilegiert durch BKA-Gesetze), sondern auch die Polizei zum Zwecke der Strafverfolgung Q-TKÜ und Onlinedurchsuchung nutzen (§100a und b wurden geändert)

Fragen: Staatliche Spähsoftware: Wozu wird staatliche Spähsoftware eingesetzt? Woher stammen die Erkenntnisse über staatliche Spähsoftware?
Kurzantwort: Exfiltration / Wenig Infos, meist von unabhängigen Forschenden (CCC, Freiling), welche bekannte Vorfälle staatlicher Spähsoftware untersuchen (z.b. Image aus Strafverfahren, Links an Journalisten überprüfen)

Exkurs Staatliche Spähsoftware Über staatliche Spähsoftware ist im Allgemeinen wenig bekannt, besonders über solche, die aktuell praktisch verwendet werden. Grund: Behörden wollen sich nicht in die Karten schauen lassen.
Trotzdem werden darüber, z.b. durch den CCC oder Forschende, Informationen bekannt. Z.B. hat Herr Freiling BckR2D2-I/II 2011 analysiert. Mit einem forensischen Image eines Datenträgers aus einem Strafverfahren konnte das Programm anhand gelöschter Dateien rekonstruiert werden. Damit konnten dann auch die überwachten Anwendungen und Interaktionsmöglichkeiten nachvollzogen werden.
Einblick Infektionsweg: Ein Möglichkeit ist über Dateien mit Namen „exe.blablabla.jpg“. Durch Hinzufügen eines bestimmten Unicorn Zeichens (RLO-Zeichen) wird der Dateiname rückwärts interpretiert. Beim Anklicken wird ein Programm gestartet.
Einblick Verschleierungstechnik: Dabei wird ein Programm von einer **nicht** standardisierten virtuellen Maschine (Packer) ausgeführt. Es können auch mehrere solcher Maschinen ineinander gestackt werden.
Million Dollar Dissident: Menschenrechtler bekommt Link. Dieser downloaded Exploit Kit für Iphone. Dieses nutzt Exploitchain (Browser- und zwei Kernelexploits) um das Handy zu Jailbreaken und Software zu installieren. Wert der drei Zero Days: ca. 1 Mio. Die vom BKA verwendete Software Pegasus basiert auf vergleichbaren Techniken.
Ziel: (Fast) jeder (staatliche) Trojaner möchte **Exfiltration** durchführen, also relevante Daten nach außen kommunizieren. Die verschickten Dateien sind dabei standardmäßig verschlüsselt.

Zusammenfassendes Vorgehen

1. Gerät wird ausfindig gemacht
2. Target wird infiziert (z.b. per SmS)
3. Zugriff auf Installationsserver zum Downloaden
4. Installation unter Verwendung von Exploits
5. Beginn der Exfiltration und ggf. weiterer Aktivitäten (z.b. Software updaten)

Möglichkeiten um bei Quellen-TKÜ Verschlüsselung ohne Tojaner zu umgehen

- **Offene Maßnahmen**:
  - Cold-Boot und Hot-Plug (Datenträger)
  - offene Online-Durchsuchung (Datenträger)
- **Ohne Infiltration**:
  - Herstellerkooperation mit Backdoor (Kommunikation)
  - Keylogger (Datenträger)
  - Live-Durchsuchung z.b. mit Trojaner (Datenträger)
  - Seitenkanäle/Metadaten (Kommunikation)

1.3 Ermächtigungsgrundlage für verdeckte Zugriffe

Zu den Aufgaben der Polizei gehört Repression und Prävention:

- **Strafverfolgung** (Repression):
  - Retrospektive, Anlass ist konkrete Straftat
  - Strafprozessrecht, Bundesrecht
- **Gefahrenabwehr** (Prävention):
  - prospektiv, Anlass ist konkrete Gefahr
  - Grundlegende Polizeiaufgabe die im Polizeirecht geregelt ist
  - Polizeirecht ist meist Landesrecht
  - Ausnahme: BKA-Gesetze sind Bundesrecht

Im folgenden werden die Gesetze zur Ermächtigung (Ermächtigungsgrundlagen - Diese sind immer dann relevant, wenn es sich um Eingriffe in die Grundrechte handelt) behandelt:

Fragen: Welche Norm erlaubt das Abhören von Datenverkehr durch die Strafverfolgungsbehörden?

Kurzantwort: § 100a
Fragen: Was ist der Unterschied zwischen § 100a und § 100b StPO?
Kurzantwort: Datenverkehr vs. Gesamtsystem
Fragen: Was versteht man im Kontext von § 100a StPO unter der kleinen Online-Durchsuchung?
Kurzantwort: Die Quellen-TKÜ, da diese fast immer wie auch die Online-Durchsuchung einen Tojaner auf dem System benötigt
Fragen: Unter welchen Bedingungen ist eine Quellen-Telekommunikationsüberwachung heute erlaubt? Welche Ermächtigungsgrundlagen gibt es?
Kurzantwort: Immer dann, wenn auch eine TKÜ erlaubt ist und es sich zusätzlich um verschlüsselte Kommunikation handelt / § 100a StPO

§ 100a StPO Telekommunikationsüberwachung TKÜ

> (1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn
> 1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
> 2. die Tat auch im Einzelfall schwer wiegt und
> 3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.
>
> Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

- Richterliche Genehmigung notwendig
- Nur bei bestimmten **schwere Straftaten** (Im Straftatenkatalog aufgeführt) anwendbar
- Ist auf drei Monate befristet (verlängerbar)
- **Technisch muss dabei sichergestellt werden**:
  - Nur die Kommunikation, der Inhalt und die Umstände dürfen aufgezeichnet werden, insofern diese Daten auch im öffentlichen Netz hätten überwacht werden können
  - Veränderungen sind nur erlaubt, wenn sie unerlässlich für die Datenerhebung sind
  - Veränderungen müssen rückgängig gemacht werden
  - Eingesetzte Mittel und abgefangene Daten müssen nach Stand der Technik gegen unbefugte Nutzung geschützt werden
  - Es muss alles dokumentiert werden

Fragen: Was ist eine Online-Durchsuchung? Welche Ermächtigungsgrundlagen gibt es dafür?
Kurzantwort: Überwachung und Analyse eines Gesamtsystems z.b. Handy / § 100b StPO

§ 100b StPO Online Durchsuchung

> Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn
> 1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
> 2. die Tat auch im Einzelfall besonders schwer wiegt und
> 3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

- Benötigt richterliche Genehmigung durch spezielle Kammer
- Auf einen Monat begrenzt (verlängerbar)
- Erheblicher Aufwand zur Durchführung notwendig

- Eigener Straftatenkatalog definiert wann es eingesetzt werden darf (z.b. **besonders schwere Fälle** von Waffenhandel / Geldwäsche, Kinderpornographie)

§100c und d StPO Großer Lauschangriff
- Dabei wird der Wohnraum akustisch überwacht
- Reglementierung ähnlich zu §100b

Weitere Aspekte von §100
- 100e Vorgehensweise bei 100a bis 100c: z.b. Befristung auf 3 Monate
- 100f kleiner Lauschangriff: Akustische Überwachung außerhalb von Wohnraum
- 100g Erhebung von Verkehrsdaten: z.b. Metadaten des Providers
- 100j Bestandsdatenauskunft: z.b. Name, Adresse aber ach Pins und Passwörter

Weitere Durchsuchungen geregelt in §§102 - 110
- Durchsuchung von Personen und Räumen
- Regelungen wie diese Ablaufen
- Umgang mit beschlagnahmten Gegenständen
- §100 ermöglicht dann Durchsicht von Papieren und Speichermedien
- Benötigen richterliche Genehmigungen, sind örtlich begrenzt, Betroffener darf dabei sein

Wann sind verdeckte technische Zugriffe angebracht? Der Einsatz eines Mittels ist verhältnismäßg, wenn:
- es legitim ist (Gesetzlich fundiert),
- zur Erfüllung des Zweckes geeignet ist
- das mildeste Mittel im Sinne des Grundrechtseingriffs ist

1.4 Nachrichtendienste

Fragen: Welche Ermächtigungsgrundlagen zum Abhören von Telekommunikation bestehen für die Nachrichtendienste? Was versteht man in diesem Zusammenhang unter „strategischer TKÜ“? Wie wird diese durchgeführt?
Kurzantwort: Die G10-Gesetze erlauben TKÜ und strategische TKÜ / Datenströme bei Providern abhören / Am Knotenpunkt doppeln, filtern, auf 20% begrenzen und anschließend mit Suchbegriffen analysieren

Nachrichtendienste (Verfassungsschutz, BND, MAD) dürfen wie die Polizei TKÜ betreiben. Grund: Erkenntnisgewinn zur Wahrung der Sicherheit der BRD. Dafür stehen eigene rechtliche Grundlagen zur Verfügung, z.b. die Bundesnachrichtengesetze oder die G10 Gesetze. Diese sind besonders durch Snowden und den NSA-Untersuchungsausschuss wieder relevant geworden.

Ermächtigungsgrundlage Basiert auf den G10-Gesetzen. §1 G10 ermöglicht Nachrichtendiensten Artikel 10 zu verletzen und damit Überwachung/Aufzeichnung von Telekommunikation und Umgehung des Brief-/Postgeheimnisses. Zudem sind nach §2 G10 geschäftsmäßige Telekommunikationsdienstleister (Provider) verpflichtet, Überwachung und Aufzeichnung der Datenverkehre zu ermöglichen.

Ermächtigung bei TKÜ im Einzelfall

- Beispiel: Einen Spion überwachen
- Ablauf vergleichbar mit Polizei
- § 3 G10 listet Voraussetzungen: Strafkatalog gegeben, Verdacht gegen konkrete Person muss vorliegen

Definition 1.1 Strategische Telekommunikationsüberwachung

Bei der strategischen TKÜ handelt es sich um eine Methode der Verdachts- bzw. Verdächtigengewinnung, die unabhängig vom Einzelfall ist und großflächig an Leistungsbündel durchgeführt wird anhand von Suchbegriffen und Filterungen (Anmerkung: Polizei darf das nicht)

Ermächtigung für strategische TKÜ

- Bei gebündelter internationaler Kommunikation zur Prävention
- § 5 G10 listet Voraussetzungen: Sammlung nur zu konkreten Zwecken, aber ohne Konkreten Anlass. Beispiele können sein: Terroristischer Anschlag, internationaler Waffenhandel/Geldwäsche
- Beschränkung durch §10: Nur 20% der Übertragungskapazität, Angabe von Suchbegriffen, Befristung auf 3 Monate
- Wird durch spezielle Kommission (G10-Kommission), welche von der Politik berufen wird, kontrolliert
- Darf nicht gezielt gegen Einzelpersonen verwendet werden

Routineverkehre Ausland-Ausland-Verkehr, bzw. Verkehr mit ohne nach Artikel 10 geschützten Personen (z.b. keine Deutsche). Es war lange strittig ob diese auch unter Artikel 10 fallen. Grund: Einschränkungen nach BND-Gesetz lockerer.

Urteil des Verfassungsgerichtes

- Schutz von Artikel 10 gilt für alle
- Aber: Strategische TKÜ im Grundsatz mit Verfassung, daher möglich
- Einschränkung: Nur mit Verhältnismäßigkeit, Volumeneinschränkung(20%), Bestimmung geographischer Gebiete, Trennung zw. Routineverkehr und nicht Routineverkehr
- Weitere Resultate:
  - Weitergabe (z.b. an ein Strafverfahren) nur Erlaubt, wenn diese auch rechtlich gezielt erhoben werden dürften
  - Rechtstaatliche Umgang (relevant fürs Ausland) muss gewährleistet werden
  - Suchbegriffe müssen plausibilisiert werden
- Gesetz wurde angepasst

Praxis der strategischen TKÜ

- Abhören von Datenverkehr an großen Knotenpunkten oder via Satellit
- Ablauf: Gremium muss Genehmigung erteilen ⇒ Anfrage des BND an Provider ⇒ Dieser doppelt dann den Übertragungsweg, Datenverkehr wird in vollem Umfang kopiert und ausgeleitet ⇒ Übergabepunkt findet in Räumlichkeiten des Providers statt
- Dabei wird anhand formaler Kriterien Vorgefiltert und in Routineverkehr und G10-geschütze Verkehre aufgeteilt
- Anschließend filter BND nach vorgegebenen Suchbegriffen/Kriterien, Treffer werden manuell analysiert

Datenfilterungssystem DAFIS

- Große Menge an Suchbegriffen und Selektoren
- Zur Wahrung der G10-geschützen Daten
- Mehrstufiges Vorgehen: Generelle G10-Relevanz (Vorwahl, .de), G10-Positivliste (Bekannte Zuordnungen, z.b. ausländischer Nummern zu Deutschen), Verstoß gegen deutsche Interessen

Probleme:

- Unklar wie Vorfilterung und Aufteilung durch den Provider korrekt realisiert werden kann. Keine Methode via Metadaten bisher bekannt (aber auch wichtig, da bekannte Verfahren umgangen werden könnten)
- Beschränkung auf 20%, was ist das? Kapazität oder Fluss? Bei Kapazität könnte es zu 100% Datenüberwachung führen
- Wie wird Routineverkehr und nicht Routineverkehr korrekt getrennt?
- Wo wird abgehört, wie effektiv sind die Filter?

2 Technik

2.1 Ermittlungen im Netz

Fragen: Welche prinzipiellen Möglichkeiten der Rückverfolgung gibt es, wenn als einzige Angabe eine IP-Adresse vorliegt?
Kurzantwort: Traceroute, IP-Geolocations-Dienste, Ping Triangulation

Der Ausgangspunkt ist ein Computersystem C, dass den Behörden physisch vorliegt. Dieses hat Verbindungen zu anderen Rechner L haben (z.b. L hat C gehackt, der L ist illegales Forum). Die Frage ist nun, wie man die Spuren von C sichern kann (Live-Analyse), wie man L identifizieren und lokalisieren kann und bei L Spuren sichert (übers Netz). Probleme dabei sind Verschlüsselung, flüchtige Spuren, Anonymisierungstechniken, etc.

Das Lokalisierungsproblem Dabei gibt es im allgemeinen drei Probleme:

1. **User Geolocation**: Wo ist der Benutzer?
2. **IP Geolocation**: Wo ist der Rechner?
3. **IP Adress Extraction**: Welche IP hat der Rechner, an dem ein gewisser Benutzer sitzt?

Die Lösung von Problem 1 ist das, was in der Praxis meistens benötigt wird. Kennt man die IP, so gibt es Tool die Problem 2 einfach lösen und damit (oft) Problem 1 lösen. Kann man also Problem 3 lösen, kann man alle drei Probleme lösen.

Klassische Lokalisierungstechniken Relevante Technologien sind Protokolle wie TCP/IP (Verhalten von Protokollen können Infos liefern) oder DNS (Offizielle Register). Andere Informationsquellen sind externe Dienstleister, auch Open Source Intelligence genannt (z.b. Historische Daten, Webarchive, IP-Geolocation).
IP-Adress-Extraction mit DNS Das Domain Name System ist eine verteilte Datenbank die Domains mit IP-Adressen macht. Damit kann sowohl die IP zu einer Domain als auch die Domains (plural) zu einer IP ermittelt werden. Mit Diensten wie `viewdns.info` ist dies zusätzlich mit dazugehörigen historischen Daten möglich.
Traceroute Terminalprogramm das die Protokollinformationen nutzt um die Route einer Domain/IP-Abfrage nachzuvollziehen. Dabei werden unter anderem die Internet-Knotenpunkte (und damit geographische Kenndaten) mit ausgegeben.
IP-Geolocation Das sind meistens kommerzielle Dienste (`geoiptool.com`), welche IP-Adressen approximativ orten. Dafür werden zahlreiche öffentliche Daten oder Providerinformationen genutzt. Interessant dabei sind auch Regionale Internet Register. Diese entstehen, indem zum einen auf globaler Ebene (Europa, Afrika, etc. zugeteilt durch offizielle Organisation) aber auch auf Lokaler Ebene (Verwaltet von Providern) gewissen Regionen IP-Adressbereiche zugeordnet werden.

IP-Verschleierungstechniken Grundlegend gibt es drei Klassen von Verschleierungstechniken:
- Remote Sessions
- Proxies / VPN
- Long Distance Dialup

Bei der **Remote Session** ist der eigene Computer mit einem anderen verbunden, über den die ganzen anfragen laufen. Dies ist besonders dann praktisch, wenn man remote auf einen Rechner im Ausland zugreift, da die Behörden Schwierigkeiten beim Überschreiten von Ländergrenzen haben. **Proxies / VPN** sind dann professionellere Umsetzungen von remote Sessions (z.b. mehrere remote Sessions gleichzeitig verwalten). Das **Long Distance Dialup** nutzt als Zwischenknoten ein Modem, welches den Datenverkehr mit dem Telefonnetz verbindet.

Fortgeschrittene Lokalisierungstechniken Eine aktive Methode ist via **Ping Triangulation**, was auf der Berechnung der Round Trip Time RTT basiert: Man hat Probe P, Target T und mehrere geographisch gut verteilte Landmarks L_i. Man berechnet von P zu allen L_i und zu T eine RTT. T liegt dann geographisch nahe zu dem L_i, dessen RTT am nähesten an der von T ist. Verbessert werden kann dies durch mehrere gut verteilte Proben P_i und liefert in Europa/USA eine Genauigkeit von ca. 100km (Im Jahre 2004).

Bei passiven Lokalisierungtechniken versucht man den Client dazu zu bringen, auf einen Server zuzugreifen und dabei die IP zu übermitteln. Dies funktioniert über gewisse Java-Exploits.
Rückverfolgungstechnik von Proxykaskaden: Beide Seiten abhören und auf der einen Seite periodische Verzögerungen in der Übertragung erzwingen. Diese bleiben (approximativ) in der Proxykaskade erhalten, auch wenn sich die Daten ändern und kann beim Eintreffen gemessen und verglichen werden. Dadurch kann trotz Proxykaskade Kommunikation nachgewiesen werden.
Fazit: Lokalisierung von Ahnunglosen ist einfach, aber die Lokalisierung von (z.b. durch Proxy) geschützen ist schwierig.

Sicherung von Spuren über das Netz Interessant sind dabei nicht nur die aktuellen, sondern auch die vergangenen Daten.
Wie sieht / sah eine Webseite heute / früher aus?: Man kann durch bestimme Suchmodifikatoren die Suche von Google spezifizieren. Dadurch kann z.b. mit *cache* :< *adresse* >, der Cache von Google zu einer Seite geladen werden. Dadurch können die Daten einer Seite zu einem vorherigen Zeitpunkt (wenn Google halt das letzte mal darauf zugegriffen hat, Datum wird angegeben) abgefragt werden.
Eine Alternative ist das Internet Archive (Way Back Machine). Das ist ein Webcrawler, der regelmäßig Schnappschüsse vom Internet macht und speichert.
Wie kriegt man Daten von Server?

1. Gefundener Rechner hat Laufwerk über das Netz eingebunden
2. Falls nicht geschützt: Daten des Ziellaufwerks über das Netz holen und sichern
3. Ansonsten: Zugangscode aus Hauptspeicher extrahieren und dann sichern

Problem: Die Cloud Anbieter haben meist eine eigene Schnittstelle, mit der man kommuniziert. Somit können nur die Funktionen der API zum Zugriff auf Daten verwendet werden und ein vollständiges Abbild (1:1 Sicherung) ist nicht möglich. Mehr dazu in der Übung.

2.2 Live Analyse

Es geht um Flüchtige Spuren, Live Analyse, Flüchtige Spuren im engeren Sinne (Netzwerk) und als Hauptteil flüchtige spuren im weiteren Sinne (Hauptspeicher). Bei letzterem sind dann auch die Qualitätskriterien, die Sicherung und Analyse relevant.

2.2.1 Flüchtige Spuren

Fragen: Was besagt die Flüchtigkeitshierarchie? Welche Auswirkungen hat sie auf die Behandlung von digitalen Spuren?
Kurzantwort: Es gibt digitale Spuren mit unterschiedlichem Grad der Flüchtigkeit / Spuren sollten immer in der Reihenfolge abnehmender Flüchtigkeit gesichert werden

Spuren müssen im allgemeinen identifiziert, gesichert und falls nicht möglich dokumentiert werden. Besonders bei nicht persistenten Spuren, also flüchtigen Spuren stellt dies ein Problem dar.

Definition 2.1 Flüchtigkeit

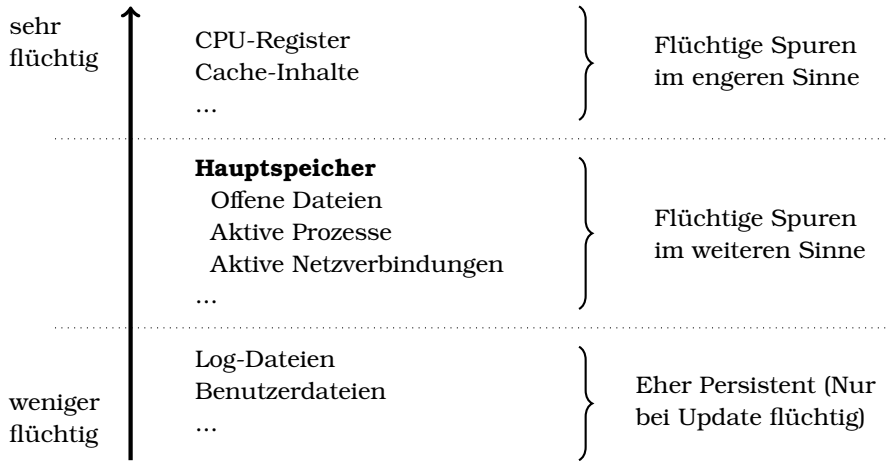
> Flüchtige Daten sind Informationen, die beim geordneten Herunterfahren oder Ausschalten des IT-Systems verloren gehen könnten

In einem Computer gibt es nun digitale Spuren mit unterschiedlichem Grad der Flüchtigkeit. Zum Beispiel sind CPU-Register flüchtiger als Dateien auf einer Festplatte. Dieser Zusammenhang wird auch **Flüchtigkeitshierarchie** genannt. Eine dazugehörige Kategorisierung kann wie folgt aussehen:

- **Flüchtige Spuren im engeren Sinne**: bleiben im laufenden Betrieb und trotz dauerhafter Stromzufuhr nur temporär erhalten(Register-, Pufferinhalte, etc.)
- **Flüchtige Spuren im weiteren Sinne**: bleiben nur mit einer entsprechenden Stromzufuhr dauerhaft gespeichert (RAM)

- **Nicht-flüchtige / Persistente Spuren**: bleiben über einen vergleichsweise großen Zeitraum ohne Stromzufuhr erhalten (Daten auf Festplatten, CDs, etc.)

Beispiele:



Allgemeine Regel

Spuren sichern in der Reihenfolge abnehmender Flüchtigkeit!

2.2.2 Live-Analyse

Die Live-Analyse betrachtet ein lebendiges System (laufender Rechner) und die Tot-Analyse persistente Daten (z.b. ein Image).

Gründe für Live-Analyse

1. Sicherung von (flüchtigen) Spuren die sonst verloren gehen:
   - Hauptspeicherinhalte wie kryptographische Schlüssel
   - Spuren speicherresistenter Schadsoftware (Hinterlassen teilweise wenig/keine persistenten Daten, hauptsächlich im Hauptspeicher vorhanden)
2. Beschleunigung der Tot-Analyse
   - Sichtung eines Systems ohne komplette Kopie anzufertigen (Bei immer größeren Datenmengen problematisch)
   - Ermöglicht selektive Sicherung von Daten

Zwei Varianten der Live-Analyse

1. Nutzung der Hardware des untersuchten Systems
   - Rechner wird vor Ort mit Live-CD gebootet
   - Analyse mittels Software der CD
   - Datensicherung über das Netz oder externe Datenträger
2. Nutzung der Hardware und Software des Systems
   - Zugriff auf den laufenden Rechner
   - Nutzung der Betriebssystemfunktionen des Rechners
   - Problem: Angaben des System kann nicht vertraut werden, angezeigte Daten könnten durch Kernel-Manipulation (Linuxsysteme) nicht dem Standard entsprechen und falsch interpretiert werden, vorhandene Maleware läuft weiterhin, etc.

Welche der beiden Varianten eingesetzt wird muss nach Risikobewertung geschehen. Dabei muss bedacht werden, dass Aktivitäten das System verändern können, andere Systeme gefährden könnte und den Angaben des Systems nicht unbedingt zu vertrauen ist. Daher sollten alle Aktivitäten verstanden und dokumentiert werden.

Weitere Herausforderungen

- Smoking-Gun Szenario bei flüchtigen Spuren: ggf. nur ein Versuch, ggf. schließt die Sicherung einer Spur die Sicherung anderer aus (gute Entscheidungen und Dokumentation notwendig)
- Maleware, Kernelmodifikationen, etc. ggf. im laufenden Betrieb nicht erkennbar
- Keine Ideallösung, keine Wiederholungsmöglichkeit und kein Zaubertool vorhanden ⇒ Wissen und Erfahrung nötig
- Vorsicht vor Spuren des eigenen Handelns

2.2.3 Sicherung flüchtiger Spuren im engeren Sinne

Flüchtige Netzwerkdaten können durch **Sniffing** (Mitlesen der Daten im Netz) sichergestellt werden. Der Netzwerverkehr ist schwer zu manipulieren und kann daher helfen Untersuchungsergebnisse zu evaluieren. Erschwert wird das durch verschlüsselte Daten, wodurch nur noch Metadaten extrahiert werden können

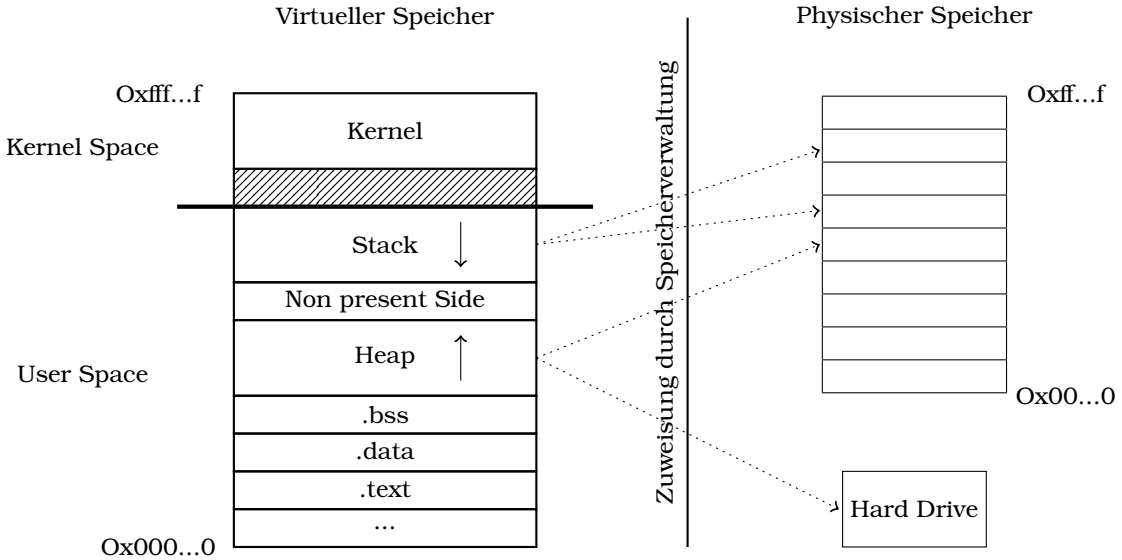
Zwei Arten

1. LAN-Sniffing (durch Mirroring am Switch/Router Daten doppeln)
2. WLAN-Sniffing (innerhalb der Reichweite des WLAN möglich)

Analyse der Daten durch Progamme (z.b. Wireshark). Polizei kann das (§100a) als TKÜ durchführen. Man selbst kann sich (§202b, Hackerparagraph) durch Abfangen der Daten strafbar machen.
Registerinhalte: Es gibt Möglichkeiten kryptographische Schlüssel (fast) nur in Registern zu halten (TRESOR-Paper). Aus forensischer Sicht ist es aber (fast) unmöglich Registerinhalte praktisch auszulesen

2.2.4 Sicherung flüchtiger Spuren im weiteren Sinne (Hauptspeicher)

Fragen: Gibt es eine optimale Methode der Hauptspeichersicherung? Wie definiert man in diesem Zusammenhang optimal?
Kurzantwort: In der Praxis nicht / Maximale Güte nach den Kriterien Atomarität, Korrektheit und Integrität

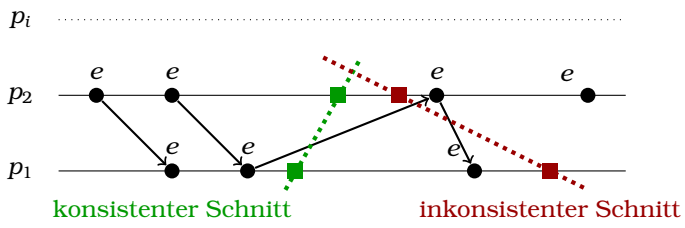


Die Darstellung ist vereinfacht. Beispielsweise kann der Virtuelle Speicher auch in mehrere Seiten aufgeteilt sein. Das relevante ist zu erkennen, das der Hauptspeicher meist „dreckig und chaotisch“ ist. Daher ist es oft notwendig über die einzelnen Abstraktionsschichten (z.b. virtuelle Speicherverwaltung) zu gehen und damit die Programme und Daten zu rekonstruieren.

Qualitätskriterien bei Hauptspeichersicherung Die Kriterien sind Atomarität, Korrektheit und Integrität und werden im folgenden genauer analysiert:

Atomarität (der eingesetzten Werkzeuge)

- Sicherung soll nicht durch laufende Aktivität (z.b. des BS) beeinflusst werden
- **Memory Smearing**: Das Bild des Hauptspeichers dauert Zeit, wobei das System aber weiterläuft. Dadurch wird kontinuierlich der Hauptspeicher verändert. Bei Atomarität versucht man dem Effekt entgegen zu wirken
- **Problem mit Nebenläufigkeit**: Es laufen mehrere sich gegenseitig beeinflussende Prozesse (bzw. Speicherbereiche im RAM), die sich in einem Prozess Zeit Diagramm darstellen lassen (e_i Ereignisse, bzw. read/write im RAM, durch Kausalitätsrelation verbunden):



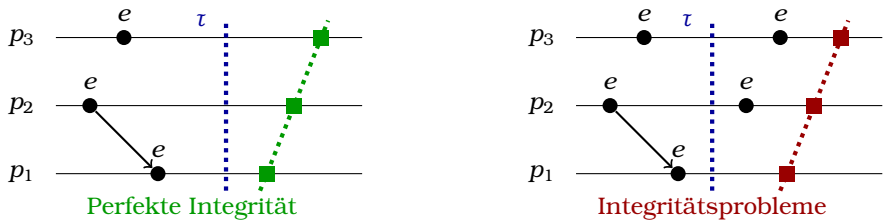
- Ein Schnitt ist eine Ereignismenge (teilt Diagramm in Past und Future). Bei einem konsistenten Schnitt ist zu jeder Wirkung auch die Ursache enthalten (Darf keine kausalen Inkonsistenzen enthalten)
- Ein Hauptspeicherabbild kann durch einen solchen Schnitt beschrieben werden
- Ein konsistenter Schnitt ist schließlich atomar

Korrektheit (der eingesetzten Werkzeuge)

- Gesicherte Daten stimmen mit Hauptspeicherdaten überein
- Auch leere und nicht verwendete Adressen müssen übernommen werden (Es dürfen keine Bereiche ausgelassen werden)

Integrität (der Vorhergehensweise)

- Grad der Veränderung der Ergebnisse durch die Sicherungsmethode (oder eigenes Handeln)
- Perfekt: Konsistenter Schnitt zu exakt einem Zeitpunkt τ ohne Zeitverzögerung
- Software braucht aber Zeit: Die Veränderungen an noch nicht gesicherten Einträgen während die Software läuft beeinträchtigt Integrität:



- Aber auch: Speicherungssoftware im Hauptspeicher kann Integrität verändern
- Funfakt: Integrität ⇒ Atomarität und Korrektheit (Rückrichtung gilt nicht!)

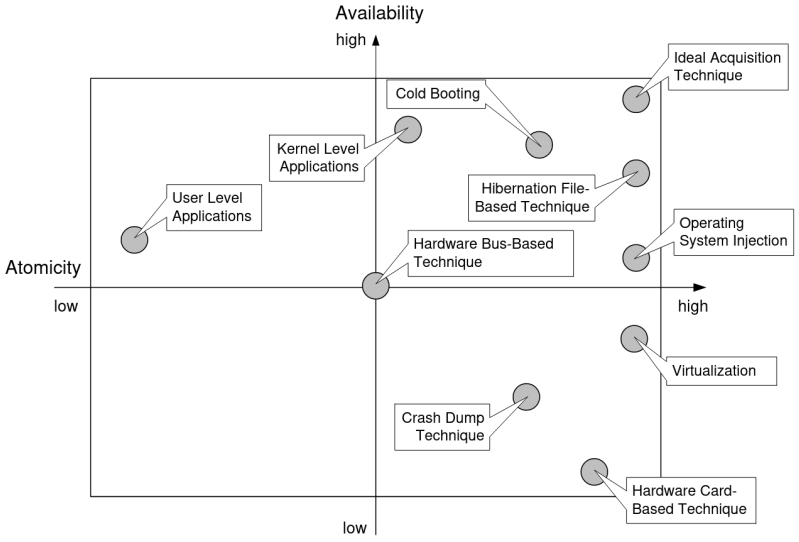
2.2.5 Sicherung von Hauptspeichern

Fragen: Welche Möglichkeiten gibt es, Kopien des Hauptspeichers anzufertigen? Welche Vor- und Nachteile haben diese Methoden? Welche Gefahren bestehen bei der forensischen Hauptspeichersicherung?
Kurzantwort: Siehe Klassen von Sicherungsansätzen / goto 0 / Rechner stürzt ab, Sicherungsmethode beeinflusst Hauptspeicherinhalte

Klassen von Sicherungsansätzen

- **Virtuelle Maschine**: Kann man anhalten und dann Datei mit Hauptspeicher auslesen (Vorteil: Sehr gutes Abbild eines Hauptspeichers, Problem: Abhängig von Konstruktion der VM (nicht unbedingt vollständig, Prozesse und Daten die nicht aktiv gebraucht werden ggf. nicht enthalten), Nicht unbedingt immer verfügbar)
- **Software**: Root-Rechte notwendig, USB-Stick mit Tool, ließt RAM sequentiell aus (Problem: Liegt selbst im Arbeitsspeicher, Benötigt Zeit zur Sicherung in der der Rechner weiterläuft (Problem mit Integrität, Atomarität))

- **Cold-Boot**: RAM-Inhalte verflüchtigen sich beim Ausschalten erst nach Sekunden/Minuten. Z.b. kann man den RAM physisch entwenden, in nen anderen Rechner stecken und dann per Software auslesen (Problem: RAM ist pseudozufällig um Speicher-Interferenzen zu vermeiden, Schnelligkeit und Kühlung notwendig da sich Daten langsam verflüchtigen)
- **Windows-Crash-Dump**: Tool von Windows (muss aktiviert werden), Bluescreen provozieren (Vorteil: Verlässlich, da von BS vorgesehen Problem: Nur (für Windows wichtige) Teile werden gesichert)
- **Hardware basierte Verfahren**: FireWire ist eine Datenübertragungsschnittstelle wie USB (war mal für externe Festplatten relevant, heute eher Thunderbold). Wenn man spezielle Hardware (Zugriffsgerät auf DMA) an den Rechner anschließt, kann dies genutzt werden um den Hauptspeicher auszulesen (Vorteil: Auslesen aller Daten mit minimalen Eingriffen ins System, d.h. RAM-Riegel müssen nicht rausgezogen werden, Software muss nicht in RAM geladen werden, System kann weiterlaufen. Bei Linux teilweise noch relevant Nachteile: Hard-/Software technische Schutzmechanismen (bei Windows und MAC heute üblich), hardwareabhängig, veraltete Vorgehensweise)



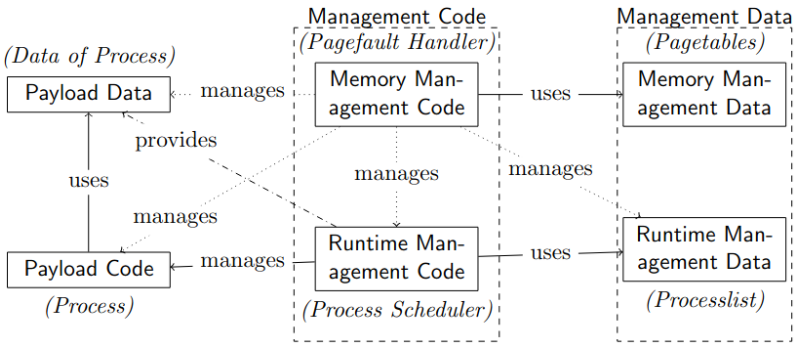
Genauerer Einblick in Speicherakquise via Software Lempereur et al. haben virtuelle Maschinen im Idle-Mode laufen lassen und diese regelmäßig angehalten, den Hauptspeicher gesichert und die Veränderung dokumentiert. Ergebnis: Es gibt permanent ein Grundrauschen im RAM. Aber es sind nur ca. 0.5% der Bits betroffen. Unterschied zw. mehreren Maschinen ist nicht signifikant.
Campbell 2013 hat die Veränderung von RAM-Sicherungssoftware auf den Hauptspeicher analysiert. Dafür hat man zwei identische Maschinen laufen lassen und bei einer mit verschiedener Software den RAM gesichert und anschließend die Hauptspeicher und die Ergebnisse verglichen. Ergebnis: Unterschiedliche Tools haben unterschiedliche Auswirkungen auf den RAM und liefern unterschiedlich Gute Ergebnisse.
Vömel/Stüttgen haben das ganze im Bezug auf die vorherigen Kenngrößen analysiert. Mit einer speziellen Technik (Analysesoftware mit Hypercalls instrumentalisieren) konnten sie das Ganze für mehrere Programme sehr feingranular überwachen. Ergebnis: Güte Der Atomarität nimmt mit RAM-Größe ab. Güte der Integrität bei größeren RAM ($> 1024MB$) tendenziell besser.
Eine andere Möglichkeit zur Evaluation von Integrität und Atomarität haben Gruhn und Freiling 2016 gemacht: Den RAM periodisch mit vorhersagbarem Muster (z.b. Zahlensequenz) beschreiben. Somit kennt man das Verhalten des RAMs und kann anhand der Ergebnisse der Sicherungsmethoden deren Güte approximieren.
Sicherung unterhalb Ring 0: Softwarebasierte Verfahren können bei Rechnern mit Maleware forensisch unbrauchbar werden. Eine Methode dies zum Umgehen ist von Userlevel auf Kernellevel zu gehen. Bei Kernellevel Rootkit kann man dann versuchen ins hypervisor level zu gehen (gibt noch tiefere level). Der Vorteil: Man hat von den tieferen Level auch immer Zugriff auf den Speicher der vorherigen Level. Sinn: Sicherungssoftware wird nicht mehr von Maleware kompromitiert.

2.2.6 Analyse bei Hauptspeichern

Fragen: Inwiefern kann man die Untersuchung von Hauptspeichersicherungen vergleichen mit der Untersuchung von Festplattensicherungen?
Kurzantwort: Man hat in beidem Fällen Tot-Analyse. Zudem sind die Datenkategorien vergleichbar.
Fragen: Was ist der Unterschied zwischen strukturierten und einfachen Hauptspeicheranalysen? Welche Vorteile haben strukturierte Analysen? Wie funktionieren die Werkzeuge für strukturierte Analysen wie Volatility?
Kurzantwort: Einfach: Carving auf unstrukturierter und chaotischer Datenmenge gemacht. Strukturiert: Versucht den Speicher zu strukturieren und zu interpretieren um Programm-, Daten- oder Systemstrukturen zu rekonstruieren / Diese Ergebnisse können analysiert werden und geben mehr Kontextbezug und können helfen Daten Programme und Netzwerkstrukturen besser zu verstehen / Jedes BS(-Version) verwaltet und handhabt den RAM unterschiedlich. Dazu sind aufwändige Analysen der dazugehörigen Strukturen notwendig. Kennt man die Strukturen, kann man diese mit Carving ausfindig machen und extrahieren.

Datenkategorien nach Carrier kann man verwenden um über alle Filesysteme zu reden und die gleichen Tools zur Analyse verwenden (The Sleuthkit):
- File System Category (Konfigurationsdaten des Dateisystems, z.b. Größe eines Datenblocks)
- Content data
- Metadata
- File Name Category (eig. Metadaten, aber relevant)
- Applications data (Programmdaten)

Eine solche Kategorisierung für Hauptspeicher ist noch nicht so ausgereift. Vorgestellt wird eine mögliche Realisierung. Relevant dabei ist besonders die Unterteilung in **Anwendungsdaten** und **Management Daten**:



Vergleich mit Carrier: Inhaltsdaten entspricht den Payload Daten und Code. Hauptspeicherkonfigurationsdateien (z.b. von virtueller Speicherverwaltung) entspricht File System Category. Die Metadaten entsprechen den Management Daten. Somit ist dies eine Verallgemeinerung des Modells von Carrier.
Interessant: Analysemethoden von Festplatten können für Hauptspeicher ggf. übernommen werden, wenn man die Modelle verallgemeinert. Aber RAM ist komplexer und hat mehr spezielle Daten, somit kann nicht jedes Werkzeug davon auch für Festplatten verwendet werden. Sinn: Gibt es eine Kategorisierung kann man dementsprechend Analysewerkzeuge bauen, bzw. bekannte Werkzeuge von der Festplattentechnik übernehmen (Aktueller Stand der Forschung)

Einfache Analysen Standardmäßiges Carving. Damit wird eine rein textbasierte und Schlüsselwortorientierte Analyse bezeichnet. Beispielsweise kann man aus den gespeicherten Rohdaten mittels dem Terminalbefehl *string* lesbare Bereiche extrahieren, die man dann mit *grep* auf Schlagwörter untersuchen kann. (Alternativ: Hexdump Analyse)
Probleme: Kontext und Zusammenhang für die gefundenen Textstellen nicht gegeben. Extrahierte Datenmenge ist oftmals zu groß, somit kann man zu viele irrelevante Treffer haben.

Strukturierte Analysen Dabei wird zuerst versucht die gesicherten Rohdaten zu strukturieren und zu interpretieren. Dabei wird insbesonders versucht Systemstrukturen zu rekonstruieren. Vorteile: Man hat mehr Semantik für die Erkenntnisse, mehr Kontext, man kann mehr Erkenntnisse gewinnen, man findet kryptographische Schlüssel einfacher, versteht Programm und Netzwerkstrukturen besser. Probleme: Detailierte BS-Kentnisse nötigt, welche aber oft schlecht dokumentiert sind und sich oft verändern. D.h. Aufwändige Analyse dieser Strukturen notwendig, Memory Smearing und generell schlechte Atomarität erschweren Strukturierung, Generell stark abhängig von Qualität der Sicherung.
Vergleich mit Live Analyse: Ähnlich wie bei der Live Analyse kann eine Vielzahl potenzieller Beweisartefakte (Prozessinformationen, Schlüssel, ...) gewonnen werden. Unterschied: Durchgeführte Untersuchungen können wiederholt und besser nachvollzogen werden.
Volatility: Standardwerkzeug (Open Source) zur strukturierten Hauptspeicheranalyse. Unterstützt viele BS-Versionen, welche vorher manuell ausgewählt werden müssen (Somit kennt Volatility viele Strukturinformationen). Interessante Funktionen: Ausgabe von Metadaten, viele Scans für Carving, Prozessliste und Prozessbäume anzeigen, Prozessscans, Kernelmodulscans, Netzwerkanalyse, etc. (Funktionen können sich für einzelne BS unterscheiden)

2.3 Browser- und Anwendungsanalyse

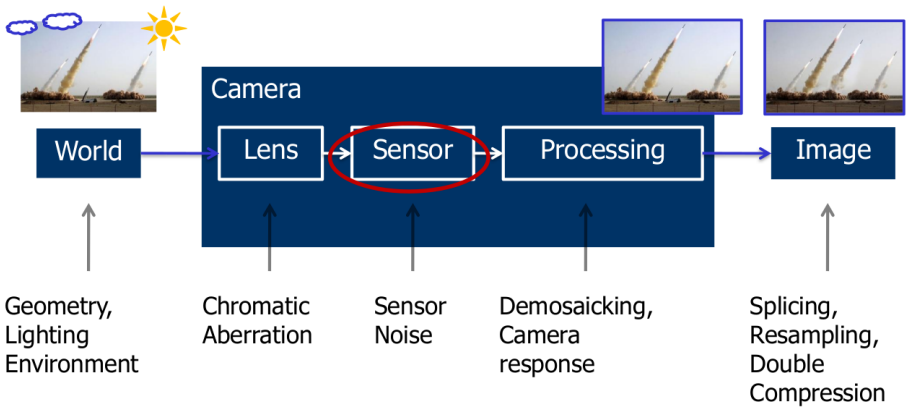
Fragen: Wie kann man prinzipiell das Ein-/Ausgabeverhalten von Anwendungen analysieren? Nennen Sie die Vor- und Nachteile der Ereignismethode und der Zustandsmethode.
Kurzantwort: ...
Fragen: Beschreiben Sie Quellen für digitale Spuren, die auf der lokalen Festplatte des Browsers beim Aufruf einer Webseite anfallen können?
Kurzantwort: ...

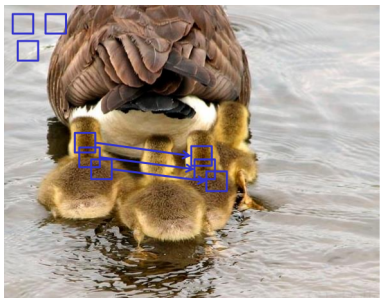
TODO

2.4 Multimedia Forensik

Fragen: Wodurch unterscheiden sich Browser-Spuren von den Spuren, die Digitalkameras in Bilder hinterlassen? Warum haben Kameras einen individuellen camera fingerprint? Gibt es ähnliche Spuren auch in Audiodaten?
Kurzantwort: Browserspruchen entstehen durch digitale Effekte (Algorithmen), wohingegen Kameraspuren durch physische Effekte entstehen (Produktionsungenauigkeiten) / Sensorunterschiede führen zu PRNU, welche einen Fingerprint ergeben / Produktionsunterschiede haben (fast) alle Geräte, also ja. Inwieweit das zu zielführenden Forensischen Analysen führt ist eine andere Frage

Dabei geht es um Spuren in Multimedia Dateien. Die Hauptfragen dabei sind, ob eine Foto einer Kamera zugeordnet werden kann (Ursprungsgeräterkennung) und ob ein Foto verändert wurden (Authentizitätsprüfung). Es wurden ein paar Beispiele vorgestellt.





Copy-Move Bildmanipulation Das ist eine Methode um resultierende Bilder zu verändern. Dabei werden Teilbereiche eines Bildes kopiert und zusätzlich an anderer Stelle eingefügt (Alles im selben Bild).
Ansatz um sowas zu identifizieren: Bild in Blöcke unterteilen, dann für die Blöcke Merkmale (Z.b. Durchschnittsfarbe) berechnen und dann Blöcke mit ähnlichen Merkmalen einander zuordnen. Findet man dann mehrere Paare mit ähnlicher Zuordnung, so kann das ein Hinweis auf Manipulation sein.

Resampling Artefakte nutzen Vor dem Einfügen muss ein Objekt oft skaliert oder rotiert werden. Dies wird technisch durch Interpolation realisiert und hinterlässt Artefakte. Man kann nun eine p-map (probability map, Hell unwarhscheinlich, Dunkel wahrscheinlich) für ein Bild berechnen, welche angibt, wie wahrscheinlich ein Pixel von seinen Nachbarn interpoliert wird. Diese p-map kann man sich dann betrachten um Manipulation festzustellen.

Fertigungsunterschiede bei Sensoren Die Sensorzellen einer Kamera haben durch minimale Produktionsunterschiede leicht unterschiedliche Lichtempfindlichkeiten. Dieser Störeffekt wird Photo Response Non Uniformity PRNU bezeichnet (Könnte man durch Kalibrierung minimieren, ist aber meist zu teuer).
Für eine einzelnes Bild irrelevant, da dies von andere Rauschquellen überdeckt wird. Nimmt man aber mehrere Bilder und mittelt diese, so fällt der variable Rauschanteil weg und anhand des konstanten PRNU kann ein fingerprint für eine Kamera erstellt werden.
Damit hat man eine Möglichkeit um ein Bild einer Kamera zuzuordnen: Fingerprint von Kamera Extrahieren, PRNU von Bild extrahieren und beides vergleichen. Bei hoher Korrelation kann es sich um die erzeugende Kamera handeln.
Pros: Resistent gegen JPEG-Kodierung, Aufhellung, Abdunkelung. Cons: Probleme bei Bildbearbeitung (Beschneidung, Skalierung, Rotation)

Analyse des Lichteinfalls Physik basierte Verfahren versuchen die Konsistenz einer Szene zu analysieren. Bei Licht bedeutet dies, ob der Lichteinfall identisch, die Schatten konsistent oder die Farben plausibel sind.
Um zu prüfen ob Lichtquellen identisch sind, unterteilt man das Bild in unterschiedliche Objekte und vergleicht die dazugehörigen Helligkeitsverläufe. Korrelieren diese nicht, so kann das ein Hinweis auf Manipulation sein.

2.5 Standards in der digitalen Forensik

Fragen: Welche Vor- und Nachteile bietet einem Sachverständigen die öffentliche Bestellung und Vereidigung?
Kurzantwort: Vorteile: Vernehmung von Zeugen, Akteneinsicht, Priorisierte Wahl Nachteile: Haftbar für Fehler, Prüfung notwendig, befristet
Fragen: Was ist der Unterschied zwischen best practices und internationalen Standards? Sind best practices immer methodisch begründet?
Kurzantwort: Best Practices sind Erfolgsmodelle, Standards institutionell festgelegte Prozesse / Nein

IT-Sachverständige in Deutschland Sachverstände sind eins von 4 rechtlich zugelassenen Beweismittel vor Gericht. Jeder kann sich als freier Sachverständiger bezeichnen (nicht geschützter Begriff). Der Begriff **öffentlich bestellten und vereidigten** Sachverständiger hingegen ist geschützt. Die Industrien- und Handelskammer definieren dazu (deutschlandweit sehr einheitlich) die notwendigen Regeln (Hier: Ordnung der Handelskammer Nürnberg, 2016):

- **Öffentliche Bestellung**:
  - besonders sachkundige und persönlich geeignete Leute benötigt

  - Bestellung limitiert auf 5 Jahre
  - Tätigkeitsausübung (mit dem Titel) deutschlandweit möglich

- **Bestellvoraussetzungen**:
  - Ausreichende Lebens- und Berufserfahrung
  - Überdurchschnittliche Fachkenntnisse und praktische Erfahrung, Fähigkeit Gutachten zu erstellen (bei IT: abgeschlossenes Studium, Berufserfahrung in IT, mind. 5 vorherige Gutachten, z.b. als freier Sachverständiger. Dann kann man IHK Prüfung ablegen)
  - Kentnisse des deutschen Rechts und Fähigkeit zur verständlichen Erläuterung eines Sachverhaltes
  - ...

- **Zuständigkeit und Verfahren für Bestimmung**:
  - Industrie- und Handelskammer mit IT-Gremium aus fachkundigen Dritten
  - Sachverständige erhalten dann Urkunde und Stempel, die aber Eigentum der Industrie- und Handelskammer bleiben

- **Pflichten**:
  - Unabhängig, weisungsfrei, gewissenhaft und unparteiisch sein
  - Berücksichtigung des aktuellen Standes der Technik und Wissenschaft
  - Gutachten in eigener Sachen dürfen nicht erstellt werden (keine persönliche Bereicherung)
  - Bei Anfrage ist man verpflichtet Gutachten zu erstellen (außer mit wichtigem Grund!)

- **Regeln für Gutachten**:
  - Systematisch, nachvollziehbar, übersichtlich, grundsätzlich, logischer Aufbau, ...

- **Rechte des öbuv Sachverständige**:
  - Vernehmung von Zeugen
  - Akteneinsicht
  - Werden vor Gericht priorisiert gewählt (Gesetzlich sogar gefordert???)

- **Unterschied zu Ermittlern**: Sachverständiger ist
  - Nicht Parteiisch, also absolut neutral
  - Werkzeug des Richters
  - Eigenständig und haftbar für Fehler (Gute Haftpflichtversicherung notwendig)
  - Kann vom Richter abgelehnt werden (z.b. wg. Befangenheit)

BSI-Leitfaden Veralteter grundlegender Leitfaden für forensische Gutachten. Nice to Know.

Internationale Standards Diese werden durch unterschiedlichste Vertreter definiert:

> **Diverse Steakholder**
> - Standardisierungsgremien wie ISO, NIST
> - Politik, Justiz und Strafverfolgungsbehörden
> - Arbeits- und Forschungsgruppen (z.b. Scientific Working Group und Digital Evidence)
> - Aber auch Paper und Bücher

Problem: Zugrundeliegende Rechtssysteme oft unterschiedlich

> **Best Practices und internationale Standards**
> - **Best Practices**: sind nicht methodisch fundiert, sondern sind die Standards (oder Methoden, Techniken), welche sich in Praxis als gut herauskristallisiert haben (Erfolgsrezepte)
> - **(Internationale) Standards**: Werden durch Authoritäten und/oder durch allgemeinen Konsens und/oder auf Basis von Vergleichen festgelegt

2.6 Challenges

Frage: Welche Arten von Forensic Challenges gibt es? Wie verhalten diese sich zu Capture-the-Flag-Veranstaltungen, wie sie sich im Hacking-Bereich etabliert haben?
Kurzantwort: Maleware, Netzwerke, Images analysieren / Weniger weit entwickelt, kleinere Community, Erstellung von Challenges noch nicht ausgereift, Bewertungskriterien schwierig gut umzusetzen

Challenges sind wichtig um praktische Erfahrungen zu sammeln und auch zur Weiterbildung. Des weiteren wird dadurch die reale Welt mit entschlossenen Gegenspielern und Limitierenden Resourcen wie Zeit oder Rechenpower sinnvoll simuliert.

Kategorien von Herausforderungen

- Man hat meistens Teamarbeit
- Online (für ein paar Stunden) oder Offline (Wochen/Monate)
- Angriff (Exploits ausnutzen) oder Verteidigung (Exploits patchen)
- Im Professionellen oder Bildungssetting möglich

Schwierigkeiten beim Erstellen der Aufgaben

- Hoher Aufwand zum Erstellen und Vorbereiten (oft nicht Wiederverwendbar)
- Die Aufgaben dürfen weder zu schwierig (frustrierend) oder einfach (langweilig) sein
- Bewertungssystem muss fair und betrugs-sicher sein
- Teure Infrastruktur: Rechenleistung für Realzeitanwendungen und Hohe Bandbreite

Capture the Flag Der DEFCON CTF ist die bekannteste Veranstaltung, welche mit der DEFCON Konverenz mit eingeht. Früher musste eine Menge an Aufgaben bezüglich Sicherheitsfragen gelöst werden (z.b. Exploits in Programmen finden). Heute Standard CTF mit Attack und Defence.

Klassisches CTF Setup

- Alle haben gleiches System in gemeinsamen Netzwerk
- Ziel: Andere Systeme exploiten und eigenes System patchen
- Jury Node: Platziert automatisch Flaggen in den Diensten der Nodes und überprüft regelmäßig deren Status. Daraus wird Bewertung gebildet.
- Offensive Punkte: Flaggen anderer finden
- Defensive Punkte: Eigene Flaggen behalten und sichern

Das UCSB iCTF ist die größte CTF Competition im Bildungsbereich. 2008 schockten diese mit einem neuen Aufbau: Security Treasure Hunt. Es mussten mehrere Instanzen in einem Netzwerk gebrochen werden um am Ende eine Bombe zu entschärfen. Es gab keinen Einfluss auf andere Teams, aber einen Tipp Geber, von dem man eine begrenzte Menge an Hinweisen bekam.
2009 gab es wieder neue Challenge: Botnet Attack Scenario. Es wurden 1024 User simuliert, welche eine wiederholende Suchroutine mit Bankseite und weiteren Websiten hatten. Das Ziel der Teams war es diese User auf eine eigene Seite zu lenken, mit einem drive-by-Download ein eigenes Skript auf deren Rechnern zum laufen zu bringen und am Ende Geld zu transferieren. Die Größe des so entstandenen Botnetzes und die Menge des Geldes hat dann Punkte gegeben.

Entstandene Erkenntnisse

- Bewertungssystem muss einfach sein
- Teams bereiten sich meist gezielt auf Szenarien vor
- Unterschiedliche Designs benötigen somit mehr Vorbereitung

Forensische Challenges
Arten forensischer Challenges

- Maleware analysieren
- Netzwerke analysieren
- Host/File System Forensik (Image analysieren)

Die Analyse von Images ist das relevante. Diese werden meist **per Hand** erstellt (Pro: Komplette Kontrolle, keine Privatssphäre zu beachten, wenig Beschränkungen Con: Aufwändig). Eine Alternative waren **Honeypots**. Dabei wurden verwundbare Rechner ans Internet gehängt und von

echten Angreifer kompromittiert. Damit konnte man anschließend echte Fälle analysiern (Pro: Realbezug, wenig Privatssphäreprobleme Con: Keine Kontrolle über Güte des Falles). Ähnlich dazu sind auch Festplatten und Images aus **zweiter Hand**. Dazu werden gebrauchte Festplatten gekauft und anschließend analysiert (Pro: Einfach zu bekommen Con: Nicht unbedingt interessant, Probleme mit Privatssphäre).
Challenge Generation Tools: Mit einem Skript wird automatisch ein Image für die forensische Analyse verändert. Das Skript simuliert dabei das Verhalten des Benutzers und kann sogar in Teilen randomisiert sein. Dadurch kann effizient ein Image mit benötigtem Kontextbezug hergestellt werden, bei welchem man adäquat bewerten kann, da man volle Kontrolle hat und alles Kennt. Problem: Stand der Forschung. Nicht so vielfältig einsetzbar wie erhofft. Images fühlen sich künstlich an.
Forensische Challenges zu Konferenzen: Dafür wird meistens ein Fall herausgegeben und als Ziel Fragen, z.b. von der Staatsanwaltschaft beantwortet. Dabei gibt es zwei Arten:
1. **Long-Term**: Wochen/Monate für unterschiedliche Skill-Level. Preisvergabe bei Konferenz
2. **Short-Term**: Challenge während der Konferenz

Beispielchallenges: Windows/Linux Memory Forensics, Smartphone/Playstation/Android Analysis, IoT device analysis (Mehrere Geräte gleichzeitig).
Eine Alternative dazu bilden forensische **Rodeos**. Diese sind ähnlich zu CTF und dabei müssen z.b. auf einem Image Flags in Form von rhinographischem Material gefunden werden.

> **Abschließender Vergleich**
>
> - Klassische CTF sind viel weiter entwickelt, haben eine größere Community und mehr Varianz als forensische Challenges
> - Zwar ist Attack/Defense Szenario auch für Forensik möglich, aber bisher wenig erforscht
> - Bewertungskriterien für forensische Challenges sind im allgemeinen schwieriger zu realisieren als bei CTF
> - Erstellung von Challenges noch nicht ausgereift

3 Übungen

Frage: Wodurch unterschied sich die Datenträgeranalyse im Rahmen des Planspiels von den Datenträgeranalysen, die Sie bisher durchgeführt haben?
Kurzantwort: ...
Frage: Welche Herausforderungen gibt es bei der Zusammenarbeit zwischen Juristen und IT-Experten? Gibt es Erfahrungen aus dem Planspiel, von denen Sie berichten möchten?
Kurzantwort: ...
Frage: Welche Ansätze haben Sie bei der Analyse des Cloud-Speicherdienstes in der Übung zu Cloud-Forensik verfolgt? Welche waren erfolgreich? Auf welche Schwierigkeiten sind Sie gestoßen?
Kurzantwort: ...
Frage: Wie sähe ein ideales Werkzeug aus, um Cloud-Daten forensisch zu sichern? Ist ein solches Werkzeug realisierbar?
Kurzantwort: ...

4 Weitere Klausurfragen aus vorherigen Semestern

Jura

- Die Polizei kann offene und verdeckte Hauptspeicheraquise machen. Welche Ermächtigungsgrundlagen gibts dafür? (Offen: §102 Durchsuchen, §94 beschlagenehmen, §110 Elektronisches Medium sichten. Verdeckt: § 100b Online-Durchsuchung)
- Was darf man bei Quellen-TKÜ? (§ 100a beschrieben)
- In der Praxis werden 2 Ansätze diskutiert, benennen sie Vor- und Nachteile:
  1. Man schleust einen Trojaner in das System ein und fängt die Kommunikation aus der Anwendung ab, bevor sie verschlüsselt wird (Vorteil: Zugriff auf komplette unverschlüsselte Kommunikation / Nachteil: Hürde vergleichbar mit Online-Durchsuchung, Abgrenzung dazu auch schwierig)
  2. Man holt sich aus der Anwendung den Schlüssel, schickt diesen an die Polizei und sie entschlüsseln damit den Inhalt der Messengernachrichten, die über die Leitung gehen (Vorteil: Man fängt tatsächlich nur laufende Kommunikation ab / Nachteil: Schlüssel darf nach § 100a eig. nicht exfiltriert werden)
- Wie würden sie die Schwere des Eingriffs durch TKÜ bzw. Online-Durchsuchung abwiegen? Immerhin sind in beiden Fällen Trojaner auf dem Rechner (Diskussion)
- § 100a und § 100b im StPO. Es werden ja für beide Trojaner genutzt. Wieso macht man die nicht beide in einen Paragraf und nutzt den gleichen Trojaner? (100b greift tiefer in Privatssphäre und Grundrechte ein, hat anderen Straftatenkatalog, nur sehr schwere Fälle, somit ist Unterscheidung wichtig)
- Juristen sehen ja den großen Lauschangriff schlimmer an als Online-Durchsuchung? Wie würden sie das persönlich sehen? (Diskussion, Online-Durchsuchung kann selbiges Erzeugen, indem man Mikro und Kamera aktiviert)
- Unterschied QTKÜ und Online-Durchsuchung benennen. Was sind jeweils die technischen/juristischen Schwierigkeiten?
- Was sind die Einschränkungen bei den Maßnahmen? (Richterbeschluss, Straftatenkatalog, ...)
- Wie wird sichergestellt, dass die Polizei keine Spuren fälscht? (Alles muss dokumentiert werden!)
- Für welche Maßnahmen (100a, 100b) sind die Hürden höher? (unterschiedliche Stratatenkataloge, schwere Straftaten bei 100a, besonders schwere bei 100b)
- Bei Hausdurchsuchungen werden häufig Dinge beschlagnahmt, was bedeutet das? (§102 ff StPO regelt Hausdurchsuchung. Unterscheidung einfache Sicherstellung (freiwillige Herausgabe) und Beschlagnahmung (nach §94 ff StPO))
- Wie ist denn der Zugriff auf Cloud-Dienste gesetzlich geregelt?
- Wie unterscheiden sich Sicherstellung und Beschlagnahme? Wie läuft die Mitnahme zur Durchsicht ab, da gibt es doch Regelungen zur Zeit für die Rückgabe? (Rückgabe muss angemessen zügig von statten gehen)
- Bei der Durchsicht beschlagnahmter Objekte werden Benutzerdaten z.b. für ein E-Mail Konto gefunden. Dürfen diese verwendet werden? (Die Durchsicht darf sich auch auf elektronische Daten beziehen, die von dem mitgenommenen aus erreichbar sind, sofern man diese nicht schnell genug anderweitig sicherstellen kann. Anscheinend aber nur, wenn der Provider in D sitzt)

Technik

- Was sind flüchtige Spuren? Was besagt die Flüchtigkeitshierarchie? Was ist die Standard Reihenfolge zur Sicherung flüchtiger spuren? Was versteht man unter Flüchtigkeit im engeren und weiteren Sinne und persistenten Daten?
- Was ist Live- und Totanalyse? Bei klassischer Forensik gibt es Standard Vorgehen, gibt es die auch bei Live-Analyse? (Nein, jeder Fall ist individuell und benötigt gute Entscheidungen)
- Was sind Kriterien zur Bewertung von Hauptspeichersicherung? Wie sind diese definiert? Wie hängen Atomarität und Integrität zusammen? (Integrität $\Rightarrow$ Atomarität)
- Ist es Integritätsverletzung, wenn der Rechner oder die Sicherungssoftware den Arbeitsspeicher seit beginn der Sicherung verändern?
- Welche Möglichkeiten gibt es zur Arbeitsspeichersicherung? Wie funktionieren diese? Welche Vor- und Nachteile haben diese? Wie verhält sich das bezüglich Atomarität/Availability? (Grafik erläutern)
- Übergang Jura: Wie kann man verdeckt den Hauptspeicher sichern? Ermächtigungsgrundlage?

- Wie untersucht man Hauptspeichersicherungen? (strukturiert/unstrukturiert) Welche Vor- und Nachteile haben diese Vorgehensweisen?
- Wäre das schlimm, wenn jetzt das Abbild nicht atomar wäre? (Bei der strukturellen Auswertung könnte das Analyseprogramm deshalb fehlschlagen) Können sie mir ein Beispiel für einen inkonsistenten Zustand im Abbild geben, der durch schlechte Atomarität entsteht?
- Wie kann man Festplattensicherungen mit Hauptspeichersicherungen vergleichen? (Vorgehen bei Tot-Analyse ähnlich, Strukturen bei RAM auch vorhanden aber unterschiedlich, komplizierter, dreckiger und stark BS-abhängig)
- Was ist ihre Meinung zu einem perfekten Hauptspeicher-Sicherungstool? (Diskussion)
- Welche Datenkategorien gibt es für den Arbeitsspeicher? Vergleichen Sie diese mit den Carrier-Datenkategorien.
- Wofür sind denn eigentlich die Volatility-Profile da?
- Bei welchem BS hat die Polizei bei Live-Analyse eher Probleme, Linux-Systeme oder Windows? (Linux, da Kernelmodifikation leichter möglich, System kann dann nicht vertraut werden)

Übungen
- Was war ihre größte Schwierigkeit?
- Planspiel: Was war denn anders als bei den Analysen, die Sie in Forensik 1 durchgeführt haben?
- Planspiel: Können Sie etwas zur Zusammenarbeit mit den Juristen sagen?
- Planspiel und Technik: Warum braucht man dann denn einen Sachverständigen für die Auswertung? Was kann der denn dann überhaupt sagen? (Z.b. Manipulation erkennen, forensische Software verwenden,etc.)