Kapitel 9. Digitale Forensik und Finanzermittlungen

Unit-responsible partner: BayHfoD

Co-funded by
the European Union

9. Digitale Forensik und Finanzermittlungen

9.1 Einführung

In der heutigen digitalen Welt sind die Grenzen zwischen virtuellem und realem Leben oft verschwommen, und dies gilt auch für die dunklen Machenschaften des Menschenhandels zum Zweck der Arbeitsausbeutung (kurz: Arbeitsausbeutung oder Arbeitszwangshandel). Das Trainingskapitel „Digitale Forensik und Finanzermittlungen“ hebt die entscheidende Rolle dieser beiden Disziplinen bei der Erkennung und Bekämpfung von Arbeitsausbeutung hervor. Die digitale Forensik konzentriert sich auf die Analyse elektronischer Daten, um digitale Beweise für kriminelle Aktivitäten im Zusammenhang mit Arbeitsausbeutung zu sammeln, während Finanzermittlungen darauf abzielen, Geldflüsse nachzuverfolgen und die finanziellen Netzwerke hinter diesen Verbrechen aufzudecken. Durch die Kombination dieser beiden Ansätze können Ermittler nicht nur Täter identifizieren, sondern auch die oft komplexen Verbindungen zwischen digitalen Spuren und finanziellen Transaktionen aufdecken, die Arbeitsausbeutung ermöglichen. In diesem Zusammenhang werden Verfahren, bewährte Praktiken, Methoden und mögliche Werkzeuge vorgestellt, die Fachkräften ermöglichen, die dynamischen Wechselwirkungen zwischen digitaler Kommunikation und Geldflüssen zu nutzen, um Opfern von Menschenhandel zu helfen und rechtliche Schritte gegen die Täter einzuleiten.

Das Trainingskapitel beginnt mit den Lernzielen eines Teilnehmers (Abschnitt 2). Diese sind getrennt für „digitale Forensik“ und „Finanzermittlungen“ aufgeführt. Es folgen Definitionen der wichtigsten Begriffe für dieses Kapitel (Abschnitt 3). Abschnitt 4, der Kern des Trainingskapitels, enthält den theoretischen und informativen Hintergrund zu

den Themen. Darauf folgt eine praktische Übung für das Trainingskapitel, die es dem Teilnehmer ermöglicht, mit den zuvor erlernten theoretischen Informationen zu arbeiten und diese vertiefend zu bearbeiten (Abschnitt 5). Das Kapitel schließt mit Quellenangaben (Abschnitt 6).

9.2 Lernziele

Dieses Schulungskapitel vermittelt den Teilnehmern die erforderlichen Kenntnisse für die digitale Forensik und Finanzermittlungen im Zusammenhang mit Menschenhandel und Arbeitsausbeutung. Am Ende dieses Kapitels werden die Teilnehmer in der Lage sein:

Digitale Forensik

- die Grundsätze der digitalen Forensik zu verstehen, einschließlich der Datenerfassung, -sicherung und -analyse, unter Gewährleistung der Integrität der Beweiskette
- zu wissen, wie man forensische Backups (Image- und logische Kopien) erstellt
- zu wissen, wo man nach digitalen Spuren und Beweisen von Menschenhändlern suchen muss und was sich aus verschiedenen Quellen digitaler Beweise ableiten lässt
- die rechtlichen Rahmenbedingungen für digitale Beweise zu verstehen und die Einhaltung der Verfahrensvorschriften sicherzustellen

Finanzermittlungen

- verdächtige Finanzaktivitäten zu identifizieren, die auf Menschenhandel hindeuten können

- eine schrittweise Methodik für die Durchführung von Finanzermittlungen im Zusammenhang mit Menschenhandel anzuwenden
- die wirtschaftlichen Triebkräfte des Menschenhandels zu verstehen
- sich der Herausforderungen bei Finanzermittlungen bewusst zu sein, einschließlich der Verwendung von Kryptowährungen, Offshore-Konten und digitalen Verschleierungstechniken
- die Rolle von öffentlich-privaten Partnerschaften (ÖPP) bei Finanzermittlungen und der internationalen Zusammenarbeit bei der Bekämpfung des Menschenhandels zu verstehen

9.3 Definitionen

Im Folgenden werden wichtige Stichworte zu beiden Themen kurz umrissen.

9.3.1 Schlüsselwörter im Zusammenhang mit digitaler Forensik

Digitale Forensik

Die digitale Forensik umfasst die Identifizierung, Sicherung und Untersuchung digitaler Beweismittel zur Unterstützung strafrechtlicher Ermittlungen. Dazu gehören Methoden zur Datenerfassung, -analyse und -dokumentation, um digitale Spuren krimineller Aktivitäten aufzuspüren.

Forensische Datensicherung

Die Erstellung exakter Kopien digitaler Speichermedien unter Wahrung der Datenintegrität und Rückverfolgbarkeit (Chain of Custody). Dazu gehören physische Image-Backups (RAW, E01) und logische Backups (L01, AD1).

Beweiskette

Eine lückenlose, chronologische Dokumentation der Handhabung digitaler Beweismittel, um deren Authentizität und Integrität in Gerichtsverfahren sicherzustellen.

Anti-Forensik

Maßnahmen, die ein Nutzer ergreift, um die Auswertung digitaler Spuren zu erschweren oder sogar zu verhindern: Verschlüsselung (FDE, Container, ...); TOR/privates Surfen, Virtualisierung → Löschen der virtuellen Maschine (VM); Programme zum Löschen, Bereinigen, Ändern von Zeitstempeln usw.; Verstecken von Daten, z.B. Steganografie; mehrfaches Packen.

eDiscovery

Der gezielte Einsatz digitaler Forensik zur Analyse großer Datenmengen, um relevante Informationen für Ermittlungen oder Gerichtsverfahren zu extrahieren. Mit anderen Worten: eDiscovery (electronic discovery) ist die Analyse von Daten für bestimmte Fälle (z.B. für organisierte Kriminalität, Wirtschaftskriminalität, Staatssicherheitsdelikte). Um eDiscovery durchzuführen, sind spezifische Kenntnisse über Straftaten und den konkreten Fall erforderlich. Da die Datenmengen ständig wachsen, erfordern forensische Berichte außerdem Datenauszüge. Eine Erleichterung für eDiscovery könnte das Electronic Discovery Reference Model EDRM sein, ein Rahmenwerk, das die Standards für die Ermittlung und Wiederherstellung digitaler Daten umfasst, z.B.:

- Grundlagen der Hardware
- Grundlagen der digitalen Forensik
- Aufbau von Datenträgern und Dateisystemen
- Kurze Einführung in forensische Tools
- Grundlegende forensische Aktivitäten
- Aufbau und Funktionsweise des Windows-Betriebssystems
- Forensische Artefakte aus Windows-Systemen

Forensische Bootmedien

Spezielle Betriebssysteme (z.B. Linux- oder Windows-basierte Systeme), die zum Starten digitaler Geräte und zur Durchführung forensischer Analysen verwendet werden, ohne die Originaldaten zu verändern.

Redundant array of independent disks (RAID)

Ein System, das mehrere Festplatten kombiniert, um die Datensicherheit und Leistung zu verbessern und für das spezielle forensische Techniken zur Datenerfassung erforderlich sind.

9.3.2 Schlüsselwörter im Zusammenhang mit Finanzermittlungen

Finanzermittlungen

Die Überprüfung von Finanztransaktionen, um illegale Aktivitäten wie Geldwäsche, Terrorismusfinanzierung oder Menschenhandel aufzudecken und die Täter zu identifizieren.

Geldwäsche (Money laundering, ML)

Der Prozess der Verschleierung der illegalen Herkunft von Geldern durch eine Reihe von Finanztransaktionen, um sie als legitim erscheinen zu lassen. (Gegenteil: Bekämpfung der Geldwäsche)

Know your customer (KYC)

Eine regulatorische Anforderung an Finanzinstitute, die Identität und den finanziellen Hintergrund ihrer Kunden zu überprüfen, um Geldwäsche und Terrorismusfinanzierung zu verhindern.

Verdachtsmeldungen (Suspicious transaction reports, STRs)

Meldungen, die Finanzinstitute einreichen müssen, wenn eine Transaktion als potenziell verdächtig oder mit Geldwäsche oder Terrorismusfinanzierung in Verbindung stehend eingestuft wird.

Blockchain Analyse

Die Untersuchung von Kryptowährungstransaktionen, um illegale Aktivitäten wie Geldwäsche, Betrug oder Terrorismusfinanzierung aufzudecken und Netzwerke von Straftätern aufzuspüren.

Kryptowährungen und Verschleierungstechniken

Digitale Währungen (z.B. Bitcoin, Monero) und Methoden wie Mixer, Tumbler oder Chain-Hopping, die zur Verschleierung von Finanztransaktionen eingesetzt werden.

9.4 Theoretischer / informativer Teil

9.4.1 Digitale Forensik

Dieser Abschnitt gibt einen Überblick über die digitale Forensik in Abschnitt 9.6.2 und liefert Hintergrundinformationen darüber, was sie ist, wie sie kategorisiert werden kann und wie ein typischer digitaler forensischer Prozess aussieht. Darüber hinaus beschreibt der Abschnitt grundlegende Prinzipien, die ein Digitalwissenschaftler oder -praktiker berücksichtigen sollte. Anschließend befasst sich Abschnitt 9.6.2 mit Grundkenntnissen über Datensicherungen, da diese die Grundlage für einen soliden und erfolgreichen digitalen forensischen Prozess bilden. Eine weitere grundlegende technische Einführung in die digitale Forensik (über diesen ersten Schritt der Sicherung hinaus) würde an dieser Stelle jedoch zu weit führen – zumal beispielsweise die Analysemethoden zu vielfältig sind, um sie hier zu behandeln. Dementsprechend ist es nicht sinnvoll, insbesondere da die Anwendung im Zusammenhang mit Menschenhandel und Arbeitsausbeutung steht, auf weitere Schritte einzugehen. Dementsprechend befasst sich Abschnitt 4.1.3 mit der digitalen Forensik im Zusammenhang mit THB.

9.4.2 Überblick

Forensik ist die Anwendung wissenschaftlicher Methoden zur Analyse und Verfolgung von Straftaten. Die digitale Forensik befasst sich insbesondere mit Fragen wie:

- Wo entstehen digitale Spuren?
- Wie können digitale Spuren erkannt und ausgewertet werden?
- Wie können digitale Spuren gesichert und genutzt werden?

Auch wenn die digitale Forensik bereits in Abschnitt 3 definiert wurde, lohnt es sich, näher darauf einzugehen. Die digitale Forensik umfasst die (1) Suche, Identifizierung, (2) Beschreibung und (3) Untersuchung digitaler Beweismittel, einschließlich der Beurteilung ihrer Zuverlässigkeit, Gültigkeit und Relevanz für den konkreten Fall. Als letzter Schritt umfasst die digitale Forensik auch die (4) Berichterstattung über diese Beweismittel (Maras, 2014). Sie umfasst Methoden zur Datenerfassung, -analyse und -dokumentation, um digitale Spuren krimineller Aktivitäten aufzuspüren, Spuren auf digitalen Geräten, die zum Zwecke der Strafverfolgung analysiert werden können und müssen.

Normalerweise gibt es in Strafverfolgungsbehörden (LEAs) spezialisierte Einheiten für digitale Forensik, weshalb THB-Einheiten hauptsächlich mit digitalen Forensik-Einheiten zusammenarbeiten und sich in der Regel nicht allein mit Fragen der digitalen Forensik befassen. Daher ist es am besten, die Zusammenarbeit mit dieser Einheit aufzubauen und zu pflegen. Darüber hinaus ist es ratsam, die verschiedenen beruflichen Positionen in der Behörde zu kennen, z.B. gibt es einen Polizeibeamten, der für IT zuständig ist? Einen Polizeibeamten für Cyberkriminalität? Einen technischen Kriminaldienst? Einen digitalen Forensiker? Wer ist für was zuständig und wann kann ich wen erreichen?

Die digitale Forensik umfasst die Identifizierung, Sicherung und Untersuchung digitaler Beweismittel unter Berücksichtigung (1) der rechtlichen Rahmenbedingungen (um die Verwertbarkeit vor Gericht sicherzustellen) und (2) der Aufrechterhaltung und Dokumentation der Beweiskette und Datenintegrität. Entscheidend für die digitale

Forensik ist daher, dass alle Maßnahmen und einzelnen Schritte gerichtsverwertbar sind und in der Gerichtsdokumentation verwendet werden können.

Typische Aufgaben von Digitalforensikern umfassen: Datensicherung von Computern, Datenträgern, Mobilgeräten und Online-Speichern; Aufbereitung und Auswertung computergestützter Beweismittel; Beratung und Unterstützung bei Durchsuchungen.

Darüber hinaus lässt sich die digitale Forensik in verschiedene Bereiche unterteilen und kategorisieren. Abbildung 11 bietet einen Überblick über mögliche Zweige der digitalen Forensik. Die Computerforensik konzentriert sich auf die Wiederherstellung, Analyse und Sicherung digitaler Beweismittel von Computern, einschließlich Festplatten, Dateisystemen, Betriebssystemen und Anwendungsdaten. Wichtige Techniken sind Festplattenabbilder, Dateiwiederherstellung und Registry-Analyse (siehe z.B. Casey, 2011). Die (manchmal separat aufgeführte) Datenbankforensik befasst sich mit der Untersuchung von Datenbanken (einschließlich SQL- und NoSQL-Datenbanken) und deren Metadaten und umfasst beispielsweise die Zeitstempelung einer Datenbank und die Live-Analyse (siehe z.B. Dubey, Bhatt & Negi, 2023), um Datenmanipulation, unbefugten Zugriff oder Manipulation aufzudecken. Die Datenbankforensik kann aber auch als Teilgebiet der Computerforensik angesehen werden, da Datenbanken hauptsächlich auf traditionellen Computersystemen wie Servern gespeichert werden. Die Mobile Forensik, auch als Mobile Device Forensik bezeichnet, beschäftigt sich mit der Extraktion und Analyse von Daten, die auf mobilen Geräten wie Smartphones, Tablets und GPS-Systemen gespeichert sind (Dubey, Bhatt & Negi, 2023). Die Netzwerkforensik umfasst die Analyse des Netzwerkverkehrs, um Informationen zu gewinnen, Eindringlinge zu erkennen und rechtliche Beweise zu sichern. Im Teilbereich der Firewall-Forensik werden alle Firewall-Protokolle untersucht, um wertvolle Beweise zu finden. Die Cloud-

Forensik untersucht Beweismittel, die in Cloud-Umgebungen gespeichert sind, und behandelt dabei Herausforderungen im Zusammenhang mit der Speicherung in mehreren Rechtsgebieten, Zugriffsrestriktionen und der Zusammenarbeit mit Anbietern. Daher erfordert sie spezielle rechtliche und technische Überlegungen. Die IoT-Forensik untersucht digitale Spuren von Internet-of-Things-(IoT)-Geräten, wie intelligente Haushaltsgeräte, Wearables, Industriesensoren und Fahrzeugsysteme. Sie umfasst oft eine Kombination aus eingebetteter Systemanalyse, Netzwerkforensik und traditioneller Geräteforensik. Die Speicher-(RAM)-Forensik konzentriert sich auf die Extraktion und Analyse des flüchtigen Speichers (RAM), um laufende Prozesse, Verschlüsselungsschlüssel, Schadsoftware und die Aktivität des laufenden Systems aufzudecken. Die Malware-Forensik befasst sich mit der Analyse von Schadsoftware (Malware), um deren Verhalten zu verstehen, den Ursprung zu identifizieren und die Auswirkungen zu mindern (z.B. durch statische und dynamische Malware-Analyse, Sandboxing, Reverse Engineering). Die Drohnen-Forensik beschäftigt sich mit der Extraktion von Daten aus unbemannten Luftfahrzeugen (UAVs), einschließlich Flugprotokollen, Onboard-Speicher, GPS-Tracking und Kommunikationssystemen. Die Dark-Web- und Kryptowährungs-Forensik konzentriert sich auf illegale Aktivitäten im Dark Web, einschließlich Menschenhandel, Drogenhandel und Cyberkriminalität. Kryptowährungs-Forensik-Techniken helfen dabei, Transaktionen in Bitcoin oder anderen digitalen Währungen nachzuverfolgen, um kriminelle Akteure zu identifizieren.

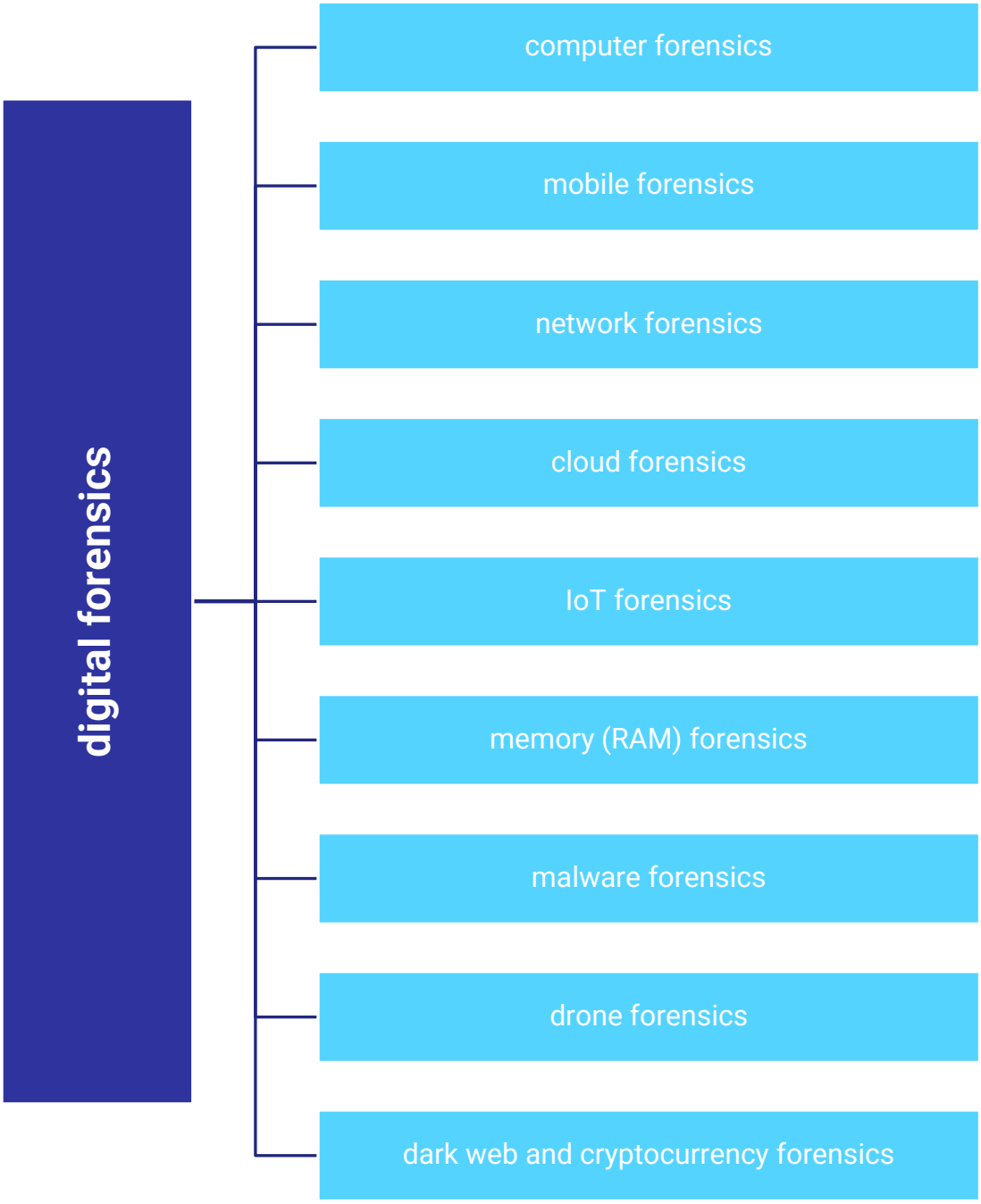

Abbildung 1. Mögliche Bereiche der digitalen Forensik

Zudem ist die Verbindung zwischen den verschiedenen Bereichen der digitalen Forensik und der IT-Umgebung von entscheidender Bedeutung, da die Art der Infrastruktur bestimmt, wo digitale Beweismittel gespeichert werden, wie auf sie zugegriffen werden kann und vor welchen forensischen Herausforderungen die Ermittler stehen:

„Klassische“ digitale Forensik vs. Online-Forensik

- **Traditionelle IT:** Das Unternehmen verwaltet seine gesamte IT-Infrastruktur vor Ort, Server, Netzwerke, Speicher, Betriebssysteme und Software werden physisch in den eigenen Räumlichkeiten betrieben. Dazu gehören klassische Computerforensik, Netzwerkforensik und Datenbankforensik, die auf physische Maschinen, lokale Server und interne Netzwerke angewendet werden. Häufige Beweisquellen sind Festplatten (HDD, SSD), lokale Datenbanken und Systemprotokolle. Dies erfordert physischen Zugriff, aber die vollständige Kontrolle über die Hardware kann die forensische Bildgebung und Analyse vereinfachen.
- **IaaS:** Infrastructure as a Service; IaaS stellt grundlegende IT-Ressourcen wie virtuelle Server, Speicher und Netzwerke über das Internet bereit. Unternehmen mieten diese Infrastruktur von einem Cloud-Anbieter. Die relevanten forensischen Bereiche sind Cloud-Forensik und Netzwerkforensik. Die wichtigsten Datenquellen sind virtuelle Maschinen, Cloud-Speicher und Netzwerkverkehrsprotokolle.
- **PaaS:** Platform as a Service, PaaS bietet eine Plattform, auf der Entwickler Anwendungen entwickeln, testen und bereitstellen können. Die zugrunde liegende Infrastruktur und Middleware werden vom Anbieter verwaltet. Dominante Bereiche sind Datenbankforensik und Cloudforensik. Datenquellen sind hauptsächlich Anwendungsprotokolle, Datenbank-Snapshots und API-Protokolle.

- **SaaS:** Software as a Service, SaaS stellt über das Internet voll funktionsfähige Software bereit. Benutzer greifen über Webbrowser oder Apps auf die Software zu, ohne sich um Installation, Verwaltung oder Wartung kümmern zu müssen. Keine Installation erforderlich. Beispiel: Microsoft 365. Cloud-Forensik und Netzwerk-Forensik sind hier die vorherrschenden forensischen Bereiche. Wichtige Datenquellen sind Audit-Protokolle, Versionshistorie und Aufzeichnungen der Benutzeraktivitäten.

Abbildung 11 zeigt einen Überblick über die verschiedenen IT-Umgebungen.

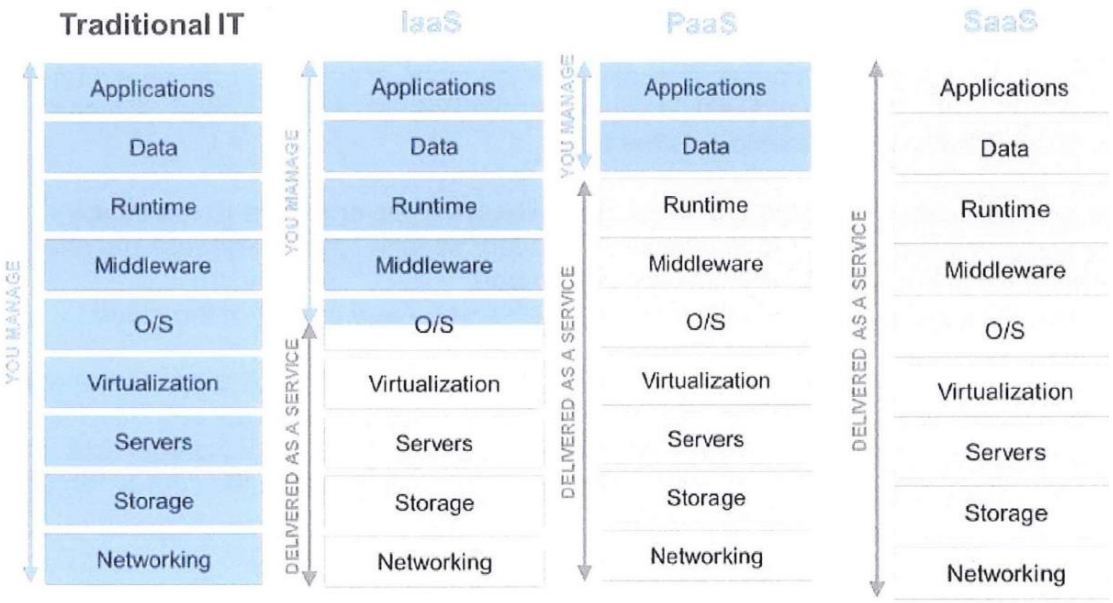

Abbildung 2. Unterschiedliche IT-Umgebungent[1]

[1] Source: Bavarian Police. No distribution without permit allowed.

Auch wenn es separate Zweige gibt und die Art der Infrastruktur berücksichtigt werden muss, bleibt die Struktur eines digitalen forensischen Prozesses im Wesentlichen dieselbe. Die Schritte lassen sich laut Dubey, Bhatt & Negi (2023) kurz wie folgt zusammenfassen: (1) Erfassung digitaler Beweise, (2) deren Analyse einschließlich Interpretation und (3) deren Präsentation (z.B. vor den ermittelnden Beamten, vor Gericht). Ein weiteres einflussreiches Prozessmodell ist das multidisziplinäre digitale forensische Untersuchungsprozessmodell von Lutui (2016), das in Abbildung 12 dargestellt ist.

Abbildung 3. Überblick über den Prozess der digitalen Forensik[2]

[2] Source: Original depiction of Lutui (2016), p. 601

Darüber hinaus kann für den Praktiker eine weitere Schritt-für-Schritt-Anleitung hilfreich sein, um den digitalen forensischen Prozess zu strukturieren, die einige praktischere Elemente enthält als die beiden zuvor vorgestellten Prozessmodelle:

Neun praktische Elemente des digitalen forensischen Prozesses

1. **Aufnahme:** Gerät als Beweismittel entgegennehmen, Antrag auf Untersuchung entgegennehmen

2. **Identifizierung:** Gerätespezifikationen und -funktionen identifizieren, Ziele der Untersuchung identifizieren, rechtliche Befugnis für die Untersuchung identifizieren

3. **Vorbereitung:** Zu verwendende Methoden und Werkzeuge vorbereiten, Medien und forensische Workstation für die Untersuchung vorbereiten

4. **Isolierung:** Beweismittel schützen, Fernlöschung von Daten verhindern, vom Netzwerk, Bluetooth und WLAN isolieren

5. **Verarbeitung:** Durchführung der forensischen Erfassung, Durchführung der forensischen Analyse, Suche nach Malware

6. **Überprüfung:** Validierung der Erfassung, Validierung der forensischen Ergebnisse

7. **Dokumentation/Berichterstattung:** Notizen zu den Ergebnissen und dem Prozess erstellen, forensische Berichte entwerfen und fertigstellen

8. **Präsentation:** Beweisstücke vorbereiten, Ergebnisse präsentieren

9. **Archivierung:** Kopie der Daten an einem sicheren Ort aufbewahren, Daten in gängigen Formaten für die Zukunft aufbewahren

Für den digitalen Forensiker/Praktiker ist es darüber hinaus wichtig, den gesamten Ablauf einer forensischen Untersuchung im Blick zu behalten:

Ablauf einer forensischen Untersuchung

1. Beschlagnahmte Beweismittel werden an einen digitalen Forensiker übergeben

2. Aufbewahrung (gespeicherte Archivierung) von Daten und Datenträgern (Verzeichnis, Aufkleber, ...)

3. Erstellung von Datensicherungen: physische Image-Backups, logische Datensicherungen

4. Sichere Aufbewahrung der Originalbeweismittel

5. Dokumentation der Beweiskette

Darüber hinaus sollten stets einige Grundprinzipien der digitalen Forensik angewendet werden:

Grundprinzipien der digitalen Forensik

- Erstellung von Datensicherungen, wobei zwischen verschiedenen Arten zu unterscheiden ist:
    - Eins-zu-eins-Kopien von computergestützten Beweismitteln

- physische Image-Backups (E01 [Encase-Image-Dateiformat] oder RAW)
- logische Datensicherungen (L01, AD1 oder CTR)

- Untersuchung der Datensicherungen oder Kopien (Post-Mortem-Analyse)
- Keine Änderungen an den gesicherten Daten
- Genaue Dokumentation, wer wann was mit den Datensicherungen gemacht hat, um die Beweiskette zu gewährleisten. Letzteres erfordert (1) eine chronologische Dokumentation und (2) die Rückverfolgbarkeit zur Sicherung der Übergabe, der Auswertung und der Vorlage der Beweisstücke. Es gilt der Grundsatz, dass (wissenschaftlich) anerkannte Methoden angewendet werden und eine vollständige Dokumentation durch den Spezialisten für digitale Forensik erstellt wird.
- Erstellung von Eins-zu-Eins-Kopien der Computerbeweise unter Berücksichtigung von…
  - Sicherstellung der Integrität und Authentizität der Beweise
  - Einbeziehung des Schreibschutzes
  - Verifizierung
- Ändern Sie nichts absichtlich! Änderungen geschehen schnell, z.B. durch das Booten eines Systems oder das Einbinden einer Festplatte.
- **Sehr wichtig:** Machen Sie alles immer und überall nachvollziehbar (Dokumentation!).

Außerdem ist es wichtig, die rechtlichen Aspekte zu kennen, da die Rechtmäßigkeit der Durchsuchung und Beschlagnahme gegeben sein muss. Darüber hinaus muss man sich als Forensiker in der Regel keine Gedanken über Verwertungsverbote machen (=

Aufgabe des Ermittlungsbeamten und letztlich des Staatsanwalts). Nicht zuletzt ist es ratsam, sich bei Zufallsfunden mit den Ermittlern abzustimmen.

9.4.3 Datensicherung

In der digitalen Forensik ist die Datensicherung ein grundlegender Schritt zur Aufbewahrung und Analyse digitaler Beweismittel. Die Gewährleistung der Integrität und Verfügbarkeit forensischer Daten ist für Ermittlungen, Gerichtsverfahren und die Reaktion auf Cybersicherheitsvorfälle von entscheidender Bedeutung. Eine ordnungsgemäße forensische Sicherung ermöglicht es den Ermittlern, mit einer exakten, unveränderten Kopie der Originaldaten zu arbeiten, wodurch das Risiko einer Verfälschung oder eines Verlusts von Beweismitteln minimiert wird.

In diesem Abschnitt werden die wichtigsten Aspekte der forensischen Datensicherung behandelt, beginnend mit den Grundprinzipien (Abschnitt 9.6.3.1), darunter Datenintegrität, Authentizität und Beweiskette. Anschließend wird ein Überblick über gängige forensische Sicherungsformate und deren Struktur gegeben (Abschnitt 9.6.3.2), gefolgt von einer Untersuchung softwarebasierter Schreibschutzmechanismen zur Verhinderung von Datenmanipulationen (Abschnitt 9.6.3.3). Außerdem werden verschiedene Arten von Datenträgern und ihre Rolle bei forensischen Untersuchungen behandelt (Abschnitt 9.6.3.4) sowie spezielle forensische Backup-Software- und Hardware-Lösungen analysiert (Abschnitt 9.6.3.5). Darüber hinaus befasst sich dieser Abschnitt mit der Erstellung und Anwendung forensischer Boot-Medien (Abschnitt 9.6.3.6), die die Datenerfassung aus Live- und Offline-Systemen erleichtern. Netzwerkbasierte forensische Sicherungsmethoden, einschließlich Fernabfragetechniken, werden ebenfalls untersucht (Abschnitt 9.6.3.7). Abschließend werden besondere Überlegungen zum Umgang mit komplexen Speichersystemen wie

RAID-Arrays und NAS-Geräten erörtert (Abschnitt 9.6.3.8), wobei kurz auf die Herausforderungen und bewährten Verfahren bei der Erhaltung solcher Datenstrukturen eingegangen wird.

Durch das Verständnis dieser Konzepte können Forensiker und Praktiker zuverlässige, überprüfbare und vor Gericht zulässige Datensicherungen gewährleisten, die die Grundlage für eine solide forensische Untersuchung bilden.

9.4.3.1 Grundsätze der forensischen Datensicherung

Bei der Datensicherung sind folgende wichtige Grundsätze zu beachten:

- **Erstellung forensischer Kopien und Schreibschutz:**
    - Ausschließliche Arbeit an forensischen Kopien, nicht an den Originalmedien
    - Erstellung forensischer Kopien als Bitstream-Images oder logische Backups
    - Verhinderung von Änderungen an den Originaldaten oder -medien während der Sicherung, Untersuchung und Prüfung
    - Schreibgeschützter Zugriff während des Sicherungsvorgangs (Schreibschutz)
- **Sicherstellung der Integrität der Sicherung:**
    - Sicherstellung, dass Datensicherungen für die Analyse geeignet bleiben
    - Keine Änderungen an den gesicherten Daten (ggf. zweite Kopie)
    - Verwendung gelöschter Sicherungsmedien (Risiko der Kreuzkontamination)

- Überprüfung von Image-Backups (Hash-Vergleich zwischen Original und Kopie nach dem Sicherungsprozess oder Kopiervorgängen)

- **Dokumentation der Beweiskette:** Genaue Dokumentation aller Interaktionen mit den Datensicherungen (Aufrechterhaltung der „Beweiskette")

9.4.3.2 Übersicht und Struktur gängiger forensischer Backup-Formate

Der Umfang der Datensicherung in der digitalen Forensik umfasst magnetische und SSD-Festplatten von Computern, einzelne Speichergeräte wie USB-Sticks oder Flash-Speicher sowie optische Medien. Diese können mit zwei primären Methoden gesichert werden: **Image-Backups**, die umfassende Kopien Sektor für Sektor erstellen, oder **logische Backups**, die sich auf bestimmte Dateien und Verzeichnisse konzentrieren. Beide Methoden werden von forensischen Tools wie X-Ways, EnCase, FTK, NUIX Imager und Magnet Acquire unterstützt.

Eine **Image-Datensicherung** ist eine bitweise Kopie eines Speichergeräts, die alle Daten erfasst, einschließlich Dateien, Ordner und nicht zugewiesene, freie und freigegebene Speicherplätze.

Das Image unterscheidet sich von einem Klon, da bei der Image-Datensicherung eine komprimierte Datei (Image) einer Festplatte, Partition oder eines Systems erstellt wird. Die Image-Sicherung, bei der Daten in einer großen Datei gespeichert werden, muss wiederhergestellt werden, bevor sie verwendet werden kann. In der digitalen Forensik werden forensische Images beispielsweise von der Festplatte eines Verdächtigen erstellt. Imaging wird in der Regel für Post-Mortem-Analysen verwendet, während Klonen zum Kopieren von Systemen oder zum Erstellen identischer Setups dient (z.B. das Klonen einer alten Festplatte auf eine SSD ohne Neuinstallation des Betriebssystems). Manchmal kann es auch forensischen Zwecken dienen. Die geklonte Festplatte ist sofort

bootfähig und einsatzbereit. Für die digitale Forensik könnte man beispielsweise eine exakte Bitstream-Kopie der Festplatte eines Verdächtigen erstellen.

Es gibt mehrere häufig verwendete **forensische Image-Formate**:

- **RAW-Format:** Eine direkte Bitstream-Kopie des Speichermediums. Je nach Backup-Software werden MD5-Hashes des gesamten Images oder einzelner Image-Teile erstellt.
- **Expert-Witness-Format (EWF) (E01):** Unveränderliches Format für forensische Zwecke. Der EVF-Header enthält Metadaten wie die Anzahl der Blöcke und die Sektorgrößen. Enthält zyklische Redundanzprüfungen (CRC) zur Überprüfung einzelner Blöcke. Segmentierte Struktur mit Headern, Daten und Sektortabellen.
- **EnCase Evidence File Format (Ex01):** Entwickelt von Guidance/OpenText und basierend auf dem E01-Format. Effizienter und leistungsfähiger als E01 und wird in erster Linie von EnCase und NUIX unterstützt.
- **Advanced Forensic Format (AFF):** Open-Source-Format, herstellerunabhängig und von einer Online-Community gepflegt. Unterstützt die Varianten AFF4 und AFF4-L. In Deutschland weniger verbreitet. Kompatibel mit Tools wie FTK Imager und Magnet Forensics AXIOM.

Die Forensik umfasst auch **logische Backups**. Ein logisches Backup ist eine Kopie der tatsächlichen Daten auf einem Speichergerät oder einer Partition, wobei nur die aktuell vorhandenen Dateien und Ordner erfasst werden, nicht jedoch nicht zugewiesene Bereiche oder gelöschte Daten. Logische Backups werden in der Regel vor Ort oder bei Unternehmensdurchsuchungen sowie von NAS-Systemen erstellt.

9.4.3.3 Software-Schreibschutz

Software-Schreibschutz bezieht sich auf Tools, die die Änderung von auf einem Datenträger gespeicherten Daten verhindern, indem sie den Zugriff auf den Lesemodus beschränken. Es gibt verschiedene Softwareprogramme, die sicherstellen, dass während forensischer Untersuchungen keine Daten versehentlich verändert oder gelöscht werden.

- **X-Ways Forensics:** Schützt ganze Festplatten oder bestimmte Partitionen. Wirksam erst, nachdem Windows die Festplatte erkannt und darauf zugegriffen hat.

- **Diskpart:** Dient zum Setzen oder Aufheben des Schreibschutzes auf Festplatten oder Volumes. Wirksam erst, nachdem das Gerät von Windows erkannt wurde.

- **FastBloc SE:** Software-Lösung zum Schreibschutz, die forensische Imaging-Verfahren auf IDE-, SATA-, SCSI-, FireWire- und USB-Kanälen ohne Hardware-Schreibschutz ermöglicht.

- **Registry-basierter Schutz:** Aktiviert den Schreibschutz für Speichergeräte, indem die Systemeinstellungen geändert werden, um den Schreibzugriff zu beschränken.

- **USB-Anschlüsse:** Schreibschutz über Diskpart (nicht zuverlässig) oder Registry-Änderungen: Schutz auf USB-Geräten.

9.4.3.4 Datenträger

Magnetische Datenträger wie Festplatten speichern Daten magnetisch auf rotierenden Platten, die in Sektoren unterteilt sind. Diese Sektoren haben in modernen

Laufwerken in der Regel eine physische Größe von 512 Byte oder 4096 Byte, und die Daten werden mechanisch mit einem Lese-/Schreibkopf gelesen.

Flash-Datenträger wie SSDs und USB-Laufwerke speichern Daten elektronisch in Speicherzellen, die in Seiten und Blöcke organisiert sind. Im Gegensatz zu magnetischen Laufwerken haben sie keine beweglichen Teile. Flash-Speicher verwenden Controller, um die traditionelle sektorbasierte Struktur zu emulieren und so die Kompatibilität mit bestehenden Systemen zu gewährleisten. Sie sind stoßfest, kompakt, bieten hohe Speicherkapazitäten und verbrauchen weniger Strom. Allerdings haben sie auch einige Nachteile. Ein wesentlicher Nachteil ist ihre begrenzte Lebensdauer. Es gibt hauptsächlich zwei Arten von Flash-Speichern: NAND und NOR. NAND-Flash-Speicher sind kostengünstiger und bieten höhere Speicherkapazitäten. Sie funktionieren ähnlich wie ein Blockgerät, z.B. eine HDD, und enthalten ein Dateisystem, das partitioniert werden kann.

Solid-State-Laufwerke (SSDs) verwenden NAND-Flash-Speicher und sind als Ersatz für herkömmliche Festplatten konzipiert. Sie bieten erhebliche Leistungsverbesserungen, wie z.B. schnellere Lese- und Schreibgeschwindigkeiten. Eine hybride Speicherlösung, bekannt als Hybrid Solid State Drives (SSHD), kombiniert eine herkömmliche magnetische Festplatte mit zusätzlichem Flash-Speicher. Die häufig abgerufenen Daten werden im Flash-Speicher gespeichert, was die Gesamtleistung des Systems beschleunigt, indem Daten für einen schnelleren Abruf zwischengespeichert werden.

9.4.3.5 Forensische Backup-Software und -Hardware

Die forensische Datensicherung umfasst eine Kombination aus speziellen **Software- und Hardware-Tools**. Zu den gängigsten Software-Tools gehören individuelle Imaging-Programme wie:

- **FTK Imager:** Portable und installierbare Versionen. Unterstützt die Vorschau von lokalen Laufwerken, Netzwerkfreigaben und Images. Erstellt Bitstream-Images im RAW-, E01- und SMART-Format. Ermöglicht Hashing, Exportieren von Dateien, Teilen, Zusammenführen von Images und logische Backups (AD1-Format). Plattformübergreifende Kompatibilität (Windows, Linux, macOS).
- **EnCase Imager:** Proprietäres Imaging-Tool mit erweiterten Funktionen.
- **Magnet Acquire:** Einfaches Tool für mobiles und Desktop-Imaging.
- **NUIX Imager:** Sicheres Imaging für physische Laufwerke und Cloud-Umgebungen. Unterstützt einzigartige logische Formate (*.nli) mit Metadaten und Hash-Verifizierung.

Darüber hinaus bieten umfassende Forensik-Suiten eine breitere Palette an Tools für die digitale Forensik, wie zum Beispiel:

- **X-Ways Forensics:** Unterstützt die Imaging-Erstellung für physische und logische Laufwerke. Bietet verschiedene Imaging-Modi (vollständig, minimal, bereinigt). Ermöglicht die Erstellung von Dateicontainern, Formatkonvertierungen und Sparse-Komprimierung.
- **EnCase Forensics:** Umfassende Suite für Imaging und Analyse
- **Magnet Forensics IEF/AXIOM:** Konzentriert sich auf die Analyse und das Imaging digitaler Beweismittel

Eine spezifische Übersicht über digitale Forensik-Tools im Zusammenhang mit THB finden Sie in Abschnitt 9.6.4.3. Die forensische Datenerfassung erfordert auch spezielle Hardware-Tools:

- **Schreibgeschützte Festplattenduplikatoren** werden verwendet, um exakte, bitweise Kopien von Speichermedien zu erstellen und gleichzeitig Änderungen am Originalmedium zu verhindern. Beispiele hierfür sind Logicube und VOOM Hardcopy. Außerdem gibt es forensische tragbare Geräte, die für die schnelle Erstellung von Images im Außeneinsatz konzipiert sind und häufig mit Laptops oder externen Laufwerken verwendet werden.
- Zu den **zusätzlichen Funktionen und Tools** gehören das sichere Kopieren von Images mit Tools wie NUIX Evidence Mover und die Hashwert-Überprüfung mit Software wie HashMyFiles, HashCalc und MD5.exe. Diese Tools lassen sich nahtlos in forensische Software wie EnCase und X-Ways integrieren, um die Integrität von E01-Image-Dateien sicherzustellen.

Für die Entfernung von Laufwerken aus kompakten Systemen bieten Ressourcen wie iFixit, YouTube-Tutorials und offizielle Portale (z.B. TeSIT) wertvolle Anleitungen. In Fällen, in denen kein physischer Zugriff auf Laufwerke möglich ist, wird die Verwendung von Boot-Medien empfohlen, um die Datenerfassung zu erleichtern.

9.4.3.6 Erstellung und Verwendung forensischer Bootmedien

Forensische Bootmedien sind ein unverzichtbares Werkzeug in der digitalen Forensik, insbesondere wenn es nicht möglich ist, ein Speichergerät aus einem Computer zu entfernen oder direkt darauf zuzugreifen, oder wenn kein Schreibschutz verfügbar ist.

Es gibt **zwei Haupttypen** von Systemen, die zum Booten verwendet werden:

- „Basic Input Output System“ (BIOS): Traditionelle Schnittstelle zwischen der Hardware und dem Betriebssystem eines Computers. Unterstützt das Booten von bis zu vier Betriebssystemen auf einem Laufwerk. Wird unmittelbar nach dem Einschalten des Computers aktiviert. Entwickelt für MBR-basierte Datenträger.
- • „Extensible Firmware Interface“ (EFI): Nachfolger des BIOS, unterstützt bis zu 128 Betriebssysteme auf einer einzigen Festplatte. Varianten sind: **UEFI** (Unified Extensible Firmware Interface) für Windows/Linux und **EFI** für macOS. Unverzichtbar für GPT-basierte Festplatten. Wird zum Starten des Betriebssystems auf GPT-Datenträgern verwendet. Wird von allen aktuellen Betriebssystemen unterstützt. Bietet verbesserte Sicherheit und Funktionalität:
    - „Compatibility Support Module“ (CSM): Simuliert ein BIOS für die Hardware und das Betriebssystem; Kompatibilitätsmodus/Legacy-Modus.
    - Secure Boot: Verhindert das Laden von Malware vor dem Systemstart.
    - Trusted Boot: Signierung von Kernel-/Systemdateien ab Windows 10, um bösartigen Code auszuschließen und Malware zu verhindern.
- Boot Reihenfolge
    - BIOS: Überprüft die angegebenen Laufwerke nacheinander auf bootfähige Betriebssysteme und überträgt den Boot-Prozess.
    - UEFI: Enthält einen integrierten Boot-Manager, der eine direkte Laufwerksauswahl ermöglicht.

Linux-Boot-Media

Linux-Bootmedien sind mit einer Vielzahl kostenloser forensischer Tools für Aufgaben wie Datensicherung, Analyse und Wiederherstellung ausgestattet. Beispiele für diese Tools sind: **Backup** (`Guymager`, `dcfldd`, `ddrescue`); **Analysis** (`Sleuthkit`, `Autopsy`) und **Recovery** (`Foremost`, `TestDisk`).

Beliebte Linux-Distributionen sind Knoppix, Helox, CAINE (Computer Aided INvestigative Environment), DeepThought, DEFT, Grml und Kali Linux.

Erstellen von Linux-Bootmedien: Linux-Systeme werden in FAT32-formatierten Casper-Containern gespeichert, wobei vom Benutzer erstellte Dateien extern gespeichert werden. Bootmedien können mit Tools wie YUMI, Rufus oder Linux Live USB-Creator erstellt werden. Geräte wie Zalman oder IODD können als Backup-/Boot-Hardware dienen.

Erstellen von Image-Backups: In der Regel werden **RAW-Images** verwendet. „dd" ist normalerweise auf jedem Linux-System verfügbar. Syntax: dd if=/dev/sdX of=/media/image.dd. Aufteilen großer Images. Fortschrittsüberwachung mit aktualisierten dd-Versionen oder Dienstprogrammen wie Pipe Viewer (pv). Überprüfung mit Hash-Algorithmen (`md5sum` oder ähnliches). Zusammenführen von Image-Teilen nach dem Aufteilen.

Alternative Linux-Backup-Programme sind Guymager, dcfldd, dc3dd, ddrescue. Ein logisches Datums-Backup wird mit tar (Tape Archiver) erstellt, das jetzt in Windows integriert ist.

Windows-Based Boot Media

Windows-Bootmedien bieten alternative oder ergänzende Funktionen zu Linux-Bootmedien.

- Windows Preinstallation Environment (WinPE): Ein minimalistisches, eigenständiges Betriebssystem (OS), das unabhängig vom auf dem Gerät installierten System ist. Ermöglicht die Systemanalyse und -abbildung, ohne die Daten des installierten Betriebssystems zu beeinträchtigen.

- Windows Forensic Environment (WinFE): Speziell für forensische Zwecke konfiguriertes, angepasstes WinPE. Anwendungen:

    - Forensische Datensicherungen mit X-Ways Forensics oder FTK Imager

    - Triage und Vorschau von Beweismitteln

    - Umgehung von Administratorrechten auf Zielsystemen

- Windows Image Format (WIM): Speichert grundlegende Windows-System-Images (z.B. Pro, Home, Education). Wird zum Booten von Windows PE („boot.wim“) verwendet. Zur Installation wird WinPE gestartet und „install.wim” auf die Festplatte geschrieben. Kompatibel mit Tools wie `7zip` zur Image-Prüfung. Kann auch im komprimierten ESD-Format (Electronic Software Distribution) geliefert werden.

Erweiterte Startmedienoptionen

- Ventoy: Softwarebasiertes Tool zum direkten Starten von ISO-Images von einem USB-Laufwerk. Zu den Funktionen gehören Secure Boot-Kompatibilität und GPT-Partitionsunterstützung. Erstellt zwei Partitionen (FAT für den Boot-Manager und exFAT für die ISO-Speicherung).

- Macintosh-Startmedium:

    - **Zielfestplattenmodus (TDM):** Ermöglicht den Betrieb von Macs als externe Laufwerke über Thunderbolt oder FireWire.

    - **Wiederherstellungsmodus:** Bietet Zugriff auf Tools wie Festplatten-Dienstprogramm und Terminal für die Imageerstellung.

    - **FileVault-Entschlüsselung:** Erfordert Passwörter oder Wiederherstellungsschlüssel für den Zugriff.

    - **T2-Sicherheitschip:** Schränkt das externe Booten ein und erfordert gerätespezifische Anmeldedaten für die Imageerstellung.

- Multi-Boot-Medien: Tools wie YUMI erstellen bootfähige USB-Sticks mit mehreren Betriebssystemoptionen (Linux, Windows, macOS). Stellen Sie die Kompatibilität mit verschiedenen Systemen sicher (BIOS/UEFI, macOS System Integrity Protection).

Besondere Überlegungen für macOS

- **FileVault und T2-Sicherheitschip:** Die Verschlüsselung erfordert bekannte Anmeldedaten. Der T2-Chip integriert Secure Boot und externe Startbeschränkungen.

- **Fusion Drives:** Hybrid aus HDD und SSD, erfordert separate Image-Erstellung für jede Komponente und Rekonstruktion.

9.4.3.7 Datensicherung über das Netzwerk

Netzwerkbasierte Datensicherungen bieten eine effektive Methode zum Erstellen von Images und zum Übertragen von Daten zwischen Systemen.

EnCase und LinEn bieten ein robustes Framework für netzwerkbasierte Sicherungen, mit dem Ermittler sicher auf Remote-Systeme zugreifen und Images davon erstellen können

- **Vorgehensweise:**
    - Starten Sie den Zielcomputer mit einer Linux-Forensik-Distribution wie Deft.
    - Starten Sie EnCase Imager auf dem Backup-PC.
    - Stellen Sie mit einem Crossover-Kabel eine physische Verbindung zwischen den beiden Computern her.
    - Weisen Sie beiden Systemen statische IP-Adressen zu: Windows: Konfigurieren Sie diese über das „Netzwerk- und Freigabecenter“ unter „Adaptereinstellungen“. Linux: Verwenden Sie Systembefehle, um die IP festzulegen.
    - Überprüfen Sie die Verbindung mit einem Ping-Test.

- Kopieren Sie das LinEn-Programm auf ein externes Speichergerät und mounten Sie es auf dem Zielsystem.
- Navigieren Sie zum Speicherort von LinEn auf dem Zielsystem und führen Sie es aus. Wählen Sie in der Benutzeroberfläche von LinEn die Option „Server“.
- Starten Sie auf dem Backup-PC mit EnCase den Imaging-Prozess über die Optionen „Add Evidence“ (Beweismittel hinzufügen) und „Crossover Preview“ (Crossover-Vorschau).

- **Vorteile:** Verhindert den automatischen Schreibzugriff auf angeschlossene Speichergeräte. Linux-Systeme können komplexe Hardwarekonfigurationen wie RAID-Controller erkennen.

Unix tools und Linux-basierte forensische Boot-Medien bieten Flexibilität und Kontrolle bei Netzwerk-Imaging-Vorgängen.

- **Vorgehensweise:**
  - Verbinden Sie beide Systeme entweder über ein Crossover- oder ein Standard-Patchkabel. Verwenden Sie bei Bedarf einen Netzwerk-Hub oder -Switch.
  - Weisen Sie jedem Computer statische IP-Adressen zu:

    Windows: Konfigurieren Sie diese über das „Netzwerk- und Freigabecenter“.

    Linux: Legen Sie die IP-Adresse mit Tools wie ifconfig fest (z.B. ifconfig eth0 192.168.100.1).

- Testen Sie die Konnektivität mit einem Ping-Befehl, um sicherzustellen, dass beide Geräte kommunizieren.

Die Kombination aus **dd und Netcat** ermöglicht eine einfache und effiziente Datenübertragung über das Netzwerk.

- **Vorgehensweise:**
  - **Zielcomputer vorbereiten:** Starten Sie Netcat, um auf eingehende Daten zu warten. Beispiel: Speichern Sie Daten direkt in einer Datei oder leiten Sie sie zum Schreiben an dd weiter.
  - **Quellcomputer vorbereiten:** Streamen Sie die Festplattendaten an das Ziel: Unter Linux: Verwenden Sie dd, um Daten zu lesen und an Netcat weiterzuleiten. Unter Windows: Verwenden Sie eine kompatible dd.exe, um ähnliche Aufgaben auszuführen.
- Zusätzliche Überlegungen: Deaktivieren Sie vorübergehend Firewalls und Antivirensoftware, um Störungen zu vermeiden. Netcat kann Sicherheitswarnungen auslösen, da es oft als „potenziell unerwünschtes Programm" eingestuft wird.

Die Verwendung von **SSH** gewährleistet eine sichere Datenübertragung, insbesondere bei der Arbeit mit Linux- oder macOS-Systemen.

- **Vorgehensweise:**
  - Erstellen Sie mit dd eine Bitstream-Kopie der Quellfestplatte.

- Leiten Sie die Ausgabe über eine SSH-Verbindung an das Zielsystem weiter, wo sie als forensisches Image gespeichert wird.

- **Zusätzliche Funktionen**
  - **Fortschrittsverfolgung:** Verwenden Sie Dienstprogramme wie Pipe Viewer (pv), um die Datenübertragung in Echtzeit zu überwachen.
  - **Komprimierung:** Streamen Sie Daten über Komprimierungstools wie Gzip, um den Speicherbedarf zu reduzieren.

9.4.3.8 Besonderheiten der Datensicherung

RAID (Redundant Array of Independent Disks) Systeme wurden entwickelt, um die Leistung und Zuverlässigkeit durch die Verteilung von Daten auf mehrere Festplatten zu verbessern.

- **Arten von RIADs:**
  - **Hardware RAID:** Wird über eine spezielle RAID-Controllerkarte verwaltet und bietet robuste Leistung und Zuverlässigkeit.
  - **Software RAID:** Wird vom Betriebssystem gesteuert, ist in der Regel kostengünstiger, aber abhängig von den Systemressourcen.
- **RAID Levels:**
  - **JBOD:** Alle Festplatten werden zu einem einzigen großen Speicher kombiniert; das Speichernetzwerk ist ein großes Dateisystem, in dem die Daten gespeichert werden.

- **RAID0:** Alle Festplatten werden zu einem einzigen großen Speichersystem kombiniert; die Datenspeicherlogik (Stripe-Größe) sorgt dafür, dass die Daten in Blöcken auf den Festplatten gespeichert werden.
- **RAID10:** Zwei oder mehr Festplatten werden zu einem einzigen Speicherbereich kombiniert (RAID0); der Speicherbereich wird gespiegelt (RAID1-Spiegelung).
- **RAID5 oder RAID6:** Mindestens 3 (RAID5) oder mindestens 4 (RAID6) Festplatten werden zu einem einzigen Speicherbereich zusammengefasst; Paritätsinformationen werden auf die Festplatten verteilt. Wenn eine (RAID5) oder zwei (RAID6) Festplatten ausfallen, kann ihr Inhalt von den verbleibenden Datenträgern wiederhergestellt werden. Je nach Controller/Hersteller können Paritätsinformationen „vorwärts“ oder „rückwärts“ zu den einzelnen Festplatten rotiert werden.
- **Synology Hybrid RAID (SHR):** Eine Variante von RAID, die Linux-Software-RAID (MD RAID und LVM2) verwendet.

- **Bewährte Verfahren für RAID-Backups:**
  - Genaue Dokumentation der RAID-Konfigurationen (z.B. BIOS-Einstellungen, RAID-Controllertyp, RAID-Level, Stripe-Größe).
  - Backup über RAID-Controller, z.B. Booten mit Linux Live CD oder WinFE, die den Hardware-RAID-Controller erkennen.
  - Logische Datensicherung, falls erforderlich, z.B. mit FTK Imager „Custom Content Image”.

NAS-Systeme (Network Attached Storage) sind kompakte, in sich geschlossene Server, die mit angepassten Betriebssystemen arbeiten, in der Regel leichtgewichtige,

angepasste Versionen von Linux. Der interne Datenträger besteht in der Regel aus SATA-Festplatten. Der erste Schritt besteht darin, klassische Image-Backups zu erstellen. Beim Entfernen von Laufwerken aus dem System ist es wichtig zu kennzeichnen, welches Laufwerk sich in welchem Steckplatz befand. NAS-Systeme verfügen über eine browserbasierte Schnittstelle (Web-GUI). Um auf diese Schnittstelle zugreifen zu können, muss das NAS mit dem Ermittlungsnetzwerk verbunden sein.

9.4.4 Digitale Forensik im Zusammenhang mit Menschenhandel und Arbeitsausbeutung

Menschenhandel, einschließlich Arbeitsausbeutung, stützt sich zunehmend auf digitale Kommunikation, Finanztransaktionen und Online-Rekrutierung (Europol, 2020; 2024). Daher spielt die digitale Forensik eine entscheidende Rolle bei der Identifizierung der Täter, der Aufdeckung von Ausbeutungsmustern der Opfer und der Sicherung von Beweismitteln für die Strafverfolgung. In diesem Unterabschnitt wird untersucht, wie digitale forensische Methoden auf Fälle von Menschenhandel angewendet werden können, wobei sowohl technische als auch ethische Überlegungen berücksichtigt werden. Dieser Abschnitt beginnt mit den wichtigsten Quellen für digitale Beweismittel im Bereich des Menschenhandels (und, soweit möglich, für die Sammlung von Informationen speziell zur Arbeitsausbeutung, Abschnitt 9.6.4.1). Anschließend befasst sich Abschnitt 9.6.4.2 mit der Analyse von für Menschenhandel typischen digitalen Beweisen (z.B. wonach suchen die Ermittler?). Es folgt Abschnitt 9.6.4.3, in dem einige mögliche digitale forensische Tools für den Einsatz durch Strafverfolgungsbehörden vorgestellt werden. Anschließend werden die wichtigsten Herausforderungen erörtert, die für den digitalen Forensikprozess bei THB-Ermittlungen besonders relevant sind (Abschnitt 9.6.4.4). Der Abschnitt schließt mit rechtlichen und ethischen Fragen, die zu

berücksichtigen sind (Abschnitt 9.6.4.5). Ein weiterer Überblick über Technologien zur Prävention und Bekämpfung von THB wurde von UNODC zusammengestellt – Module 14: Links between Cybercrime, Trafficking and Smuggling of Migrants.

9.4.4.1 Wichtige Quellen für digitale Beweise

Menschenhändler und Ausbeuter nutzen verschiedene digitale Plattformen und Technologien und hinterlassen dabei wichtige forensische Spuren. Die Strafverfolgungsbehörden können jedoch digitale Beweise nutzen, um Menschenhandel und die Täter zu identifizieren und rechtliche Beweise zu finden, um sie dieses Verbrechens anzuklagen (Cellebrite, 2024). Zu den gängigen Beweisquellen gehören:

Persönliche digitale Geräte

Im Rahmen von Ermittlungen wegen Arbeitsausbeutung können persönliche digitale Geräte wie Mobiltelefone und Computer als wichtige Beweisquellen dienen. Diese Geräte enthalten häufig Kommunikationsdaten, Kontakte, Finanztransaktionen und Standortdaten, die auf ausbeuterische Praktiken hinweisen können.

- **Mobile Geräte:** Menschenhändler nutzen häufig mobile Geräte, um illegale Aktivitäten zu koordinieren. Zu den Beweisen, die diese Geräte liefern können, gehören: (1) Anrufprotokolle und Kontaktlisten, die Kommunikationsmuster und Netzwerke offenlegen, (2) Textnachrichten und Chat-Verläufe, die Details zu Rekrutierungs-, Koordinierungs- und Ausbeutungsaktivitäten enthalten, (3) Multimedia-Dateien wie Fotos und Videos, die Opfer, Orte oder illegale Handlungen dokumentieren können, und (4) Standortdaten (GPS-Informationen können Bewegungen nachverfolgen und wichtige Orte identifizieren).

- **Computers:** Verschiedene Arten von gespeicherten oder anderweitig über den Computer zugänglichen Daten können für die Untersuchung von Menschenhandel von besonderem Interesse sein (Überschneidungen mit Daten von Mobilgeräten möglich): (1) Kommunikationsaufzeichnungen wie E-Mails und Textnachrichten, Aktivitäten in sozialen Medien oder Online-Anzeigen oder Stellenanzeigen, (2) Finanzdaten wie Banktransaktionen und Zahlungsaufzeichnungen oder Kryptowährungsaufzeichnungen, (3) personenbezogene Identifikationsdaten wie digitale Kopien von Ausweisdokumenten oder Standortdaten, (4) Aufzeichnungen über Beschäftigungsverhältnisse und Arbeitsbedingungen wie Arbeitsverträge, illegale Arbeitszeiten, Zeiterfassungs- und Anwesenheitssysteme (z.B. zur Erkennung übermäßiger Arbeitszeiten), (5) Reisedaten wie Reisebuchungsinformationen von Fluggesellschaften oder Reisebüros oder Ticketkäufe und Reiserouten, (6) Aktivitätsverläufe im (Dark oder Surface) Web, (7) Gesundheits- und Krankenakten, die z.B. bei Arztbesuchen von Opfern nach körperlichen Angriffen gespeichert werden, oder (8) Daten von Überwachungskameras oder Sicherheitssystemen an Arbeitsplätzen oder auf Privatgrundstücken, die die Lebens- und Arbeitsbedingungen der Opfer zeigen.

Cloud Speicher

Cloud-Speicher kann aufgrund seiner Bequemlichkeit, seines Fernzugriffs und seiner Fähigkeit, große Datenmengen zu speichern, von Menschenhändlern genutzt werden, was ihn in solchen Fällen zu einer wichtigen Quelle für digitale Beweise macht. Die aus Cloud-Speichern gesammelten Daten können denen ähneln, die oben für mobile Geräte und Computer beschrieben wurden. Darüber hinaus finden sich in Cloud-Speichern häufig spezielle Daten wie digitale Kalender, die Aufschluss über durchgeführte oder geplante Treffen, Reisen der Opfer oder andere logistische Informationen zu Operationen geben,

die innerhalb des Menschenhandelsnetzwerks ausgetauscht wurden. Daher bieten Cloud-Speicher eine höhere Wahrscheinlichkeit, die Strukturen von Menschenhandelsnetzwerken oder die Opfer organisierter Arbeitsausbeutung aufzudecken. Der Zugriff auf und die Analyse von in Cloud-Speichern gespeicherten Daten erfordern jedoch rechtliche Verfahren und spezielles technisches Fachwissen, um die Integrität der Beweise zu gewährleisten (wenn die Anmeldedaten der Benutzer nicht bekannt sind). Technische Möglichkeiten für einen (zumindest teilweisen) Zugriff sind beispielsweise die Zusammenarbeit mit dem Cloud-Dienstanbieter, die Verwendung von Tools zur Extraktion von Cloud-Daten, die Nutzung von Cloud-Dienst-APIs, der Zugriff über beschlagnahmte Geräte (Anmeldung mit Benutzeranmeldedaten, Verwendung von Geräte-Backups und Überprüfung, ob das Gerät Daten mit der Cloud synchronisiert hat), die Durchführung einer Metadatenanalyse mit den in der Cloud gespeicherten Dateien, die Anwendung von Netzwerkforensik (Abschnitt 4.1.1) oder Zugriff auf die Protokolle der Cloud-Speicherdienste der Cloud-Dienstleister, um beispielsweise den Anmeldeverlauf oder den Dateidownloadverlauf abzurufen.

Kommunikations- und Rekrutierungsplattformen

Das Internet bietet Menschenhändlern über verschiedene digitale Kanäle, darunter soziale Medien und Rekrutierungswebsites, Zugang zu potenziellen Opfern (UNODC, 2019a). Fraser (2016) hat ausführlich dargelegt, wie sich die Prozesse zwischen Menschenhändlern und Opfern mit der Verlagerung von geografischen zu Online-Netzwerken verändern. Fraser skizziert, dass Menschenhändler heutzutage wissen, wie sie soziale Medien und das Dark Web nutzen können. Der Artikel beschreibt auch, wie diese Netzwerke das Machtungleichgewicht im Menschenhandel beeinflussen und die Erfahrungen der Opfer prägen (Fraser, 2016). Digitale Beweise aus diesen Plattformen umfassen (1) Profile und Beiträge, die Rekrutierungsversuche, irreführende

Stellenangebote oder Werbung für illegale Dienstleistungen enthalten können, (2) Direktnachrichten (die die private Kommunikation zwischen Menschenhändlern und Opfern erleichtern) und (3) Gruppenmitgliedschaften, die auf eine Beteiligung an Menschenhandelsnetzwerken oder -foren hindeuten. Die Analyse dieser Elemente kann beispielsweise Rekrutierungsstrategien aufdecken und sowohl Opfer als auch Täter identifizieren.

- **Social-Media-Plattformen:** Ein Bericht von Kunz et al. (2018) fasst zusammen, welche Websites für Zwecke der sexuellen Ausbeutung genutzt werden. Dazu gehören (1) Websites zum Ansehen und Kommentieren wie Facebook, Instagram und Snapchat, aber auch YikYak und Wispher, (2) Websites für Unterhaltungen wie Tinder, Blendr, WhatsApp und KIK, aber auch Yellow und #1 Chat Avenue als weniger verbreitete Websites, (3) Webcam-Seiten wie Chatroulette, Omegle und Monkey und (4) Seiten für Werbung und Verkauf wie Cityxguide, skipthegames, bedpage, seekingarrangement.com oder sugar-babies.com. Für die Arbeitsausbeutung konnte kein solcher Überblick gefunden werden. Es ist jedoch bekannt, dass neben Online-Jobportalen und Kleinanzeigen auch gängige Social-Media-Plattformen für die Anwerbung von Arbeitskräften zu Ausbeutungszwecken genutzt werden (siehe z.B. Europol, 2024).
- **Online-Rekrutierungsseiten:** Auch wenn diese Portale und möglicherweise Kleinanzeigen-Websites legitim sind, können Menschenhändler dort irreführende Stellenangebote veröffentlichen, die sich an schutzbedürftige Bevölkerungsgruppen richten, die auf der Suche nach Arbeit sind. In einem zweiten Schritt nutzen die Menschenhändler Instant-Messaging-Anwendungen für den Austausch operativer Details, da diese eine sicherere Umgebung bieten (Europol, 2024).

- **Online-Anzeigen:** Der Unterschied zu Social-Media-Plattformen, Instant-Messaging-Anwendungen und Online-Stellenbörsen besteht darin, dass Online-Anzeigen als einseitige Kommunikation betrachtet werden können, während die anderen Quellen in der Regel auf eine wechselseitige Kommunikation zwischen Personen abzielen (z.B. potenzielle Opfer und mutmaßliche Menschenhändler). Zu den Merkmalen von Online-Anzeigen für Arbeitsausbeutung gehören:
    - **Mangelnde Spezifität:** Stellenanzeigen enthalten oft vage Stellenbeschreibungen mit minimalen Details zu Aufgaben, Verantwortlichkeiten oder Arbeitsbedingungen. Diese Unklarheit dient dazu, ein breiteres Spektrum von Bewerbern anzusprechen, ohne potenzielle Ausbeutungssituationen offenzulegen (Volodko, Cockbain & Kleinberg, 2020).
    - **Unrealistische Versprechungen:** Die Angebote können ungewöhnlich hohe Gehälter, eine beschleunigte Bearbeitung von Visa oder andere Vorteile enthalten, die zu gut erscheinen, um wahr zu sein, und darauf abzielen, Personen anzulocken, die nach besseren Möglichkeiten suchen (siehe z.B. Fraser, 2016).
    - **Zielgruppen:** Die Rekrutierungsbemühungen konzentrieren sich oft auf bestimmte Bevölkerungsgruppen, wie Migranten oder Personen aus wirtschaftlich benachteiligten Verhältnissen, die anfälliger für Ausbeutung sind (Volodko, Cockbain & Kleinberg, 2020).
    - Zwar gibt es Bestrebungen, Online-Anzeigen für sexuelle Ausbeutung mit modernen technologischen Methoden wie Natural Language Processing (NLP) zu untersuchen (z.B. Perez & Rivas, 2023; Lugo-Graulich et al., 2024), doch mangelt es nach wie vor an wissenschaftlicher Forschung zu diesem

Thema im Bereich der Arbeitsausbeutung und anderer Formen des Menschenhandels.

- **Dark Web vs. Surface Web:** Dark-Web-Angebote und -Anzeigen werden auf verschlüsselten Netzwerken gehostet, für deren Zugriff spezielle Software erforderlich ist, und bieten ein höheres Maß an Anonymität. Diese Verschleierung stellt Strafverfolgungsbehörden vor erhebliche Herausforderungen, da diese Plattformen häufig fortschrittliche technische Maßnahmen zum Schutz der Identität der Nutzer einsetzen. Im Gegensatz dazu sind Einträge und Anzeigen im Surface Web öffentlich zugänglich und oft auf Mainstream-Plattformen wie sozialen Netzwerken und Kleinanzeigen-Websites zu finden. Zwar verwenden sie möglicherweise verschlüsselte Sprache und Bilder, um einer Entdeckung zu entgehen, doch aufgrund ihres öffentlichen Charakters lassen sie sich von den Strafverfolgungsbehörden leichter überwachen. Menschenhändler nutzen sowohl Surface-Web- als auch Dark-Web-Plattformen, um für ihre Dienste oder Ausbeutungsmöglichkeiten zu werben. Relevante digitale Beweise im Dark Web umfassen z.B. (1) Kleinanzeigen und Angebote, die illegale Dienstleistungen oder betrügerische Beschäftigungsmöglichkeiten anbieten, und (2) Forenbeiträge und Mitteilungen, in denen Methoden diskutiert, Informationen ausgetauscht oder Transaktionen ausgehandelt werden (z.B. ein Forenbeitrag mit dem Titel „Arbeitskräfte für billige Arbeit verfügbar") oder (3) gefälschte Dokumente, die auf Darknet-Marktplätzen erworben wurden, wie gefälschte Visa und Arbeitsgenehmigungen für Migranten ohne Papiere.

Überwachung und Ortung

Überwachungs- und Ortungsdaten beziehen sich auf alle Daten, die den Standort, die Bewegungen oder Handlungen von Personen offenlegen können und häufig mit elektronischen Mitteln erfasst werden, weshalb hier die digitale Forensik ins Spiel kommt. Moderne Umgebungen, die mit Überwachungssystemen und IoT-Geräten ausgestattet sind, können unbeabsichtigt Menschenhandelsaktivitäten erfassen. Die Ermittlungen können auch (sofern rechtlich bestätigt) die Ortung und Überwachung von Verdächtigen ermöglichen.

Von Strafverfolgungsbehörden initiierte Überwachung (erfordert in der Regel einen Gerichtsbeschluss)

- **GPS-Ortung, z.B. Fahrzeugortung:** Kann von Strafverfolgungsbehörden zur Überwachung von Bewegungen eingesetzt werden. Behörden können beispielsweise die Bewegungen des Autos eines Verdächtigen verfolgen, der regelmäßig Opfer zu verschiedenen Arbeitsorten transportiert. Muster in den Standortdaten des Fahrzeugs könnten den Behörden helfen, Umschlagplätze für Menschenhandel zu lokalisieren oder die Reiserouten oder Arbeitszeiten der Opfer zu ermitteln.
- **Überwachungskameras:** CCTV-Aufnahmen von öffentlichen oder privaten Überwachungskameras können verwendet werden, um die Bewegungen von Menschenhändlern oder Opfern an bestimmten Orten (z.B. an Arbeitsplätzen, in der Nähe von Grenzen) zu verfolgen.
- **Kommunikationsüberwachung (Abhören):** Das Abhören (z.B. von Telefonaten, E-Mails, Nachrichten) kann Einblicke in Menschenhandelsaktivitäten geben. Abhörmaßnahmen können den Behörden helfen, Menschenhändler zu belauschen, die Reisen organisieren, Zahlungen vereinbaren, Opfer bedrohen usw.

- **Ortungsgeräte auf Mobiltelefonen:** Mithilfe von Mobilfunk-Triangulation und GPS-Daten von Mobiltelefonen kann der Standort von Opfern oder Menschenhändlern präzise bestimmt und beispielsweise im Zeitverlauf kartiert werden.
- **Drohnen oder Luftüberwachung:** Mit Kameras ausgestattete Drohnen können zur Verfolgung von Bewegungen über größere Gebiete hinweg eingesetzt werden (insbesondere in ländlichen oder schwer erreichbaren Gebieten, in denen eine Überwachung durch Menschen schwierig sein kann).

Von Menschenhändlern initiierte Überwachung (von Menschenhändlern gesammelte Daten)

- **Ortung mobiler Geräte durch Menschenhändler:** Menschenhändler können die Telefone der Opfer oder ihre eigenen Geräte verwenden, um Opfer zu orten. Dazu kann die Verwendung von GPS-Ortungs-Apps oder sogar die Installation von Spyware (z.B. mSpy, FlexiSPY) gehören, um den Standort und die Kommunikation des Opfers zu überwachen.
- **Standortdaten von IoT-Geräten:** IoT-Geräte wie Smartwatches oder sogar vernetzte Fahrzeuge können von Menschenhändlern verwendet werden, um den Standort der Opfer zu überwachen. Die Protokolle dieser Geräte können beispielsweise analysiert werden, um ungewöhnliche Zugriffszeiten oder Veränderungen in der Umgebung festzustellen.
- **Online-Überwachung:** Menschenhändler überwachen häufig die Social-Media-Konten ihrer Opfer, um deren Kommunikation zu kontrollieren oder sich sogar als diese auszugeben, um deren Online-Persönlichkeit zu kontrollieren und sie beispielsweise daran zu hindern, Hilfe zu suchen. Die Strafverfolgungsbehörden könnten daher untersuchen, ob der Menschenhändler über die Zugangsdaten des

Opfers/der Opfer verfügte, um sich bei verschiedenen sozialen Medien oder anderen Plattformen anzumelden.

- **Video- und Audioüberwachung:** Menschenhändler können versteckte Kameras oder Audioaufzeichnungsgeräte in Räumen oder an Arbeitsplätzen anbringen, um ihre Opfer kontinuierlich zu überwachen, z.B. um sicherzustellen, dass sie ihre Aufgaben erfüllen. Die Strafverfolgungsbehörden könnten sich auf die Aufspürung solcher Geräte konzentrieren und dann deren Daten auswerten, um das Ausmaß der Arbeitsausbeutung zu ermitteln und vor Gericht zuverlässige Beweise vorlegen zu können.

Finanzielle Transaktionen und Zahlungsmethoden

Finanzielle und Kryptowährungstransaktionen (national und international): Täter nutzen häufig digitale forensische Systeme, um Geld zu waschen und Gewinne zu verschleiern. Wichtige digitale Beweismittel umfassen (1) Kontoauszüge und Transaktionsverläufe, die ungewöhnliche Muster aufzeigen, die auf illegale Aktivitäten hinweisen, sowie (2) Kryptowährungs-Wallets und Transaktionen, die verwendet werden, um finanzielle Spuren zu verwischen und eine spezialisierte forensische Analyse erfordern. Die Finanzanalyse (siehe Abschnitt 9.2) ist entscheidend, um Geldflüsse nachzuverfolgen, Menschenhandelsnetzwerke zu zerschlagen und Täter strafrechtlich zu verfolgen (Thomson Reuters, 2025).

- **Traditionelle Banktransaktionen**
- **Kryptowährungstransaktionen**
- **Prepaid- und digitale Zahlungssysteme**

9.4.4.2 Analyse und Verknüpfung von Beweismitteln

Nach der Sicherstellung und Bewahrung der digitalen Beweismittel (z.B. Beschlagnahme von Mobiltelefonen, Computern, USB-Sticks, Cloud-Konten, Social-Media-Daten) müssen die Daten aus diesen Geräten oder Speichern extrahiert werden. Dabei kommen verschiedene Arten der Forensik zum Einsatz, die in Abschnitt 9.1.1 beschrieben sind (z.B. Cloud-Forensik; Datenextraktion auf Hardware-Ebene wie Chip-Off oder Methoden wie Passwortknacken/Entschlüsselung). Anschließend können die Ermittler die digitalen Beweismittel analysieren und miteinander in Beziehung setzen. Die im Folgenden dargestellten digitalen forensischen Verfahren und Prinzipien sind einerseits nur beispielhaft und andererseits nicht ausschließlich auf den Menschenhandel (THB) beschränkt: Viele Techniken überschneiden sich mit Ermittlungen zu Cyberkriminalität, organisierter Kriminalität und Betrugsdelikten. Dennoch gibt es einige Aspekte, die THB in diesem Zusammenhang einzigartig machen, wie der Fokus auf soziale Medien und Rekrutierungsanzeigen (im Gegensatz zu Finanzdelikten basieren THB-Fälle stark auf Online-Betrug und der Verfolgung von Kommunikation). Darüber hinaus ist ein großer Teil der Beweismittel, die digitale Forensik-Teams rekonstruieren, opferzentriert, da Täter ihre Opfer z.B. durch Drohungen, Erpressung oder GPS-Tracking kontrollieren. Zudem verfügen die Opfer von Menschenhandel häufig nicht über eigene Computer oder Laptops, sondern hauptsächlich über Smartphones und Cloud-Konten. Dies macht THB-Ermittlungen stärker abhängig von mobiler Forensik und Cloud-Forensik (siehe Abschnitt 9.1.1).

In Fällen von Menschenhandel (THB) können digitale Forensik-Experten gezielt nach folgenden Aspekten suchen:

- **Kommunikationsmuster:** Oft verwenden Menschenhändler in Textnachrichten eine codierte Sprache oder Slang und suchen daher nach verschiedenen Schlüsselwörtern wie „leichter Job“, „Barzahlung“, „kostenlose Reise“ im Kontext von Arbeitsausbeutung oder „Model“ und „Escort“ im Kontext sexueller Ausbeutung. Häufig werden diese spezifischen Schlüsselwörter, die sich auf Arbeit, Unterkunft und Löhne beziehen, wiederholt verwendet. Tong et al. (2017) fanden beispielsweise heraus, dass Menschenhändler in den USA und Kanada ihre Sprache verändern, um der Entdeckung durch die Strafverfolgungsbehörden zu entgehen. Außerdem ändern sie die Terminologie, was es schwierig macht, Schlüsselwortlisten zur Verfolgung von Anzeigen im Zusammenhang mit Menschenhandel zu erstellen. Dies führt zu einem sich ständig weiterentwickelnden Lexikon. So verwenden Menschenhändler anstelle der expliziten Formulierung (z.B., ‘Y❤ng G!rl’). Viele Anzeigen weisen zudem keine korrekten grammatikalischen Strukturen auf, was traditionelle NLP-Techniken weniger effektiv macht. Anzeigen enthalten häufig Symbole, Emojis und nicht standardisierte Zeichen. Die Wortstellung ist oft inkonsistent und ähnelt eher der von sozialen Medien oder Textnachrichten als der formellen Schriftsprache (z.B. „@“ statt „at“ oder „m33t“ statt „meet“). Die Komplexität von Unigrammen, Bigrammen und Trigrammen ist hoch. Die hohe Variabilität der Wörter resultiert daraus, dass Menschenhändler Wörter absichtlich verändern, um eine automatische Erkennung zu vermeiden (ungewöhnliche Wortkombinationen, seltene Wörter, modifizierte Wortphrasen). Die Anzeigen sind typischerweise kurz (im Mittel 133 Wörter) und enthalten keine ausführlichen Beschreibungen. Tong et al. (2017) kommen zu dem Schluss, dass Menschenhändler ihre Sprache ständig anpassen, was flexible Erkennungsmodelle erfordert. Allein

Schlüsselwortlisten sind unzureichend; Ermittler benötigen kontextbewusste KI-Modelle.

Eine weitere Möglichkeit, spezifische Kommunikationsmuster für die digitale Forensik zu verstehen und nachzuvollziehen, besteht darin, sich die Rekrutierungsstrategien anzusehen, die von Menschenhändlern angewendet werden. Diese lassen sich in aktive und passive Methoden unterteilen (Europol, 2020): **Aktive Rekrutierung** ist vergleichbar mit „Angel-Haken-Fischen“, bei der Kriminellen gefälschte Stellenanzeigen auf vertrauenswürdigen Jobportalen und in sozialen Medien veröffentlichen. Sie erstellen manchmal sogar gefälschte Rekrutierungswebseiten, die professionell wirken und gelegentlich einen Live-Chat anbieten, um legitim zu erscheinen. Die UNODC bezeichnet dieses Phänomen auch als „Jagdstrategie“ (UNODC, 2020). Die aktive Rekrutierung umfasst meist direkte Nachrichten und Chats, die sich an verletzliche Personen richten. Dabei können Muster von Zwang, Manipulation und betrügerischen Jobangeboten auftreten. Auch das plötzliche Löschen von Nachrichten oder Accounts nach dem Erstkontakt (z.B., wenn der Menschenhändler bemerkt, dass die potenziell zu handelnde Person für das Jobangebot nicht erreichbar ist). **Passive Rekrutierung** ist diskreter und für Strafverfolgungsbehörden schwerer zu erkennen. Sie funktioniert wie „Netz-Fischen“ (oder „Angelstrategie“, UNODC, 2020), bei dem Menschenhändler die Online-Beiträge von Arbeitssuchenden beobachten und sie direkt kontaktieren. Sie versprechen Arbeitsmöglichkeiten im Ausland und verlangen eine Gebühr, um den Job zu sichern und Reise- oder Vermittlungskosten zu decken. Die Opfer erkennen erst, dass sie getäuscht wurden, wenn sie im Ausland angekommen sind (Europol, 2020).
Zuletzt, aber nicht weniger wichtig, sind verlässliche wissenschaftliche Belege zu Ermittlungstechniken für Kommunikationsmuster sehr selten (siehe zum Beispiel

die Evidence Gap Map der Internationalen Arbeitsorganisation, 2023, für mögliche Aktualisierungen zu wissenschaftlichen Ausarbeitungen).

- **Geolokalisierungstracking:** Ähnlich wie beim Verständnis von Kommunikationsmustern kann es auch hilfreich sein, die Perspektive der Täter einzunehmen: Geräte, die Geolokalisierungstracking ermöglichen, könnten für die Echtzeitüberwachung der Opfer verwendet worden sein, z.B. über GPS, eingebaute Kameras in Smartphones oder Standortfreigabe-Apps (Europol, 2020). Die Möglichkeit der Fernsteuerung senkt die Hemmschwelle der Täter für Ausbeutung und erschwert zudem die Identifizierungsbemühungen der Strafverfolgungsbehörden, wie Europol (2020, S. 3) feststellte:

  > [Während] organisierte kriminelle Gruppen historisch gesehen physische Kontrolle und ein Monopol über bestimmte Stadtviertel ausüben mussten und in der Regel aus einem großen Netzwerk von Mitgliedern bestanden, können Neueinsteiger im Menschenhandel heute ein Online-Geschäft effizient führen, ohne eine physische kriminelle Infrastruktur und mit reduziertem Personal. Dadurch kann die Beherrschung von Technologie eine kriminelle Gruppe bedrohlicher machen, aber gleichzeitig für Strafverfolgungsbehörden schwerer identifizierbar.

  Mehr zum Thema Geolokalisierungstracking ist in Abschnitt 9.1.3.1 zu finden.

- **Finanzanalyse:** Finanzanalyse und digitale Forensik können insbesondere im Zusammenhang mit von Menschenhändlern getätigten Finanztransaktionen zur Veröffentlichung von Online-Anzeigen Hand in Hand gehen (Europol, 2020). Zudem erhalten Opfer häufig Banküberweisungen von Menschenhändlern. Eine detailliertere Betrachtung von Finanzen, Finanztransaktionen und Finanzermittlungen findet sich in Abschnitt 9.2.

- **Opferidentifikation:** Zur Identifikation von Opfern können digitale Forensiker und Praktiker Gesichtserkennung einsetzen, um sie beispielsweise in Anzeigen oder Beiträgen in sozialen Medien zu finden. Zusätzlich kann eine umgekehrte Bildersuche aufdecken, ob Opfer auf Erwachsenen-Websites oder Schwarzmarkt-Plattformen beworben wurden.
- **Analyse von Deep und Dark Web:** Die Nutzung von Darknet-Foren ist für Menschenhändler nicht ungewöhnlich. Ermittler können TOR-Forensik und Dark-Web-Monitoring-Tools verwenden, um beispielsweise Rekrutierungsnachrichten, Inhalte zur Ausbeutung von Opfern oder illegale Transaktionen zu finden.

9.4.4.3 Digitale forensische Ansätze und Tools

Um Beweise in Fällen von Menschenhandel und Arbeitsausbeutung effektiv zu sammeln und zu analysieren, stützt sich die digitale Forensik stark auf:

- Mobile Forensik
- Netzwerk- und Cloud-Forensik
- Finanz- und Kryptowährunsanalyse
- Dark-Web-Ermittlungen

Um chronologisch vorzugehen, sind hier die relevanten Grundsätze für die digitale Forensik aufgeführt, die auch im Zusammenhang mit THB praktisch zu berücksichtigen sind: In der ersten Phase der Identifizierung und Sicherung müssen Ersthelfer digitale Geräte unverzüglich identifizieren und sichern, um Datenmanipulationen oder -verluste zu verhindern (z.B. durch Isolierung von Netzwerken; UNODC, 2019b). Für den Umgang mit digitalen Beweismitteln ist es dann wichtig, detaillierte Aufzeichnungen über den Zustand

jedes Geräts zu machen, einschließlich des Betriebszustands (ein, aus, Standby), des Modells und aller sichtbaren Schäden. Fotos und schriftliche Notizen helfen dabei, die Beweiskette aufrechtzuerhalten und die Integrität der Beweismittel zu gewährleisten (UNODC, 2019b). Die Datenextraktion kann dann mit speziellen forensischen Tools durchgeführt werden, um Daten abzurufen, ohne den ursprünglichen Inhalt zu verändern (siehe Abschnitt 9.6.2 für einen allgemeinen Überblick). Bei einigen Geräten kann dies die Überwindung von Sicherheitsfunktionen wie Verschlüsselung oder Passwörtern erfordern. Insbesondere im Zusammenhang mit Menschenhandel/ Arbeitsausbeutung nutzen Strafverfolgungsbehörden digitale Forensik-Tools, die die Untersuchung dieser Straftaten erleichtern.

Eine vollständige Übersicht darüber, welche digitalen Forensik-Tools in der Strafverfolgung eingesetzt werden könnten und tatsächlich eingesetzt werden, kann hier nicht gegeben werden, da (1) die verschiedenen Strafverfolgungsbehörden in Europa sehr unterschiedliche Tools verwenden (sowohl für die digitale Forensik insgesamt als auch für die digitale Forensik zur Ermittlung von Menschenhandel als einen Teilbereich davon), (2) die vernetzte Nutzung verschiedener Techniken und Tools, die vom Einzelfall abhängen, und (3) die nicht öffentliche Zugänglichkeit der Arbeitsweise der Strafverfolgungsbehörden in diesem Bereich, um nur einige Gründe zu nennen. Einige digitale Forensik-Tools und Unternehmen, die Softwarelösungen für die Ermittlung von THB-Fällen anbieten, können jedoch oberflächlich dargestellt werden:

- **Cellebrite Pathfinder**: Ein mobiles forensisches Tool, das Daten aus Smartphones, Tablets und Cloud-Quellen extrahiert, analysiert und entschlüsselt. Es kann gelöschte Nachrichten, Anrufprotokolle und GPS-Standorte wiederherstellen.

  Anwendung in einem Fall von Menschenhandel/ Arbeitsausbeutung:

- ➔ Extrahiert z.B. WhatsApp- und Telegram-Nachrichten zwischen Menschenhändlern und Opfern
- ➔ Stellt gelöschte Unterhaltungen wieder her, in denen Opfern falsche Jobs versprochen wurden
- ➔ Identifiziert GPS-Standorte aus dem Telefon des Opfers, um Bewegungsmuster zu ermitteln

- **MAGNET FORENSICS**: Das Unternehmen bietet verschiedene Softwarelösungen für die öffentliche Sicherheit, das Militär, Nachrichtendienste usw. an.

  MAGNET AXIOM ist speziell für THB relevant: Das Tool ist auf Computer- und Cloud-Forensik spezialisiert und analysiert Daten von Festplatten, sozialen Medien, E-Mails und verschlüsselten Dateien.

Mögliche Anwendung in einem Fall von THB/ Arbeitsausbeutung:

- ➔ Untersuchung von Social-Media-Beiträgen und Aktivitäten auf Jobportalen, auf denen Menschenhändler gefälschte Stellenanzeigen veröffentlichen
- ➔ Extrahieren versteckter Dateien (z.B. Opferverträge, Flugtickets, Arbeitsgenehmigungen) aus den Computern der Menschenhändler
- ➔ Analyse der Kommunikationsprotokolle zwischen mehreren Verdächtigen in verschiedenen Ländern

MAGNET OUTRIDER kann auch den digitalen forensischen Ermittlungsprozess positiv unterstützen, da es iOS- und Android-Mobilgeräte scannt und beispielsweise illegale Apps, Kontaktlisten, SMS-Nachrichten und kürzlich verwendete Apps aufdeckt.

Mögliche Anwendung in einem Fall von Menschenhandel/ Arbeitsausbeutung:

- ➔ deckt versteckte Online-Aktivitäten auf und entlarvt Menschenhändler, die Dark-Web-Foren oder gefälschte Social-Media-Konten nutzen
- ➔ kann gefälschte Arbeitsverträge, Stellenanzeigen und Finanzunterlagen aufspüren

MAGNET GRAYKEY, das auf das Knacken verschlüsselter Mobilgeräte spezialisiert ist, kann ebenfalls einen Beitrag leisten. Es umgeht Bildschirmsperren und extrahiert Dateisystemdaten.

Mögliche Anwendung in einem Fall von Menschenhandel/Arbeitsausbeutung:

- ➔ Entsperrt beschlagnahmte Telefone von Menschenhändlern und hilft bei der Wiederherstellung von WhatsApp-, Telegram-, Signal-, Viber- und anderen Unterhaltungen

Auch andere MAGNET-Software könnte hilfreich sein (siehe Pizzuro, 2022).

- MSAB XRY: Ein mobiles forensisches Tool, das von Strafverfolgungsbehörden verwendet wird, um Daten aus Mobiltelefonen, Tablets, GPS-Geräten und Drohnen zu extrahieren, zu analysieren und zu entschlüsseln.

  Mögliche Anwendung in einem Fall von Menschenhandel/Arbeitsausbeutung:

  - ➔ Extrahiert mobile Kommunikation und deckt möglicherweise digitale Beweise im Zusammenhang mit Menschenhandel auf
  - ➔ Analysiert soziale Medien und Jobplattformen
  - ➔ Stellt gelöschte Dateien und Fotos wieder her

- **Maltego**: Das Unternehmen bietet Tools zur Darstellung von Beziehungen zwischen Personen, Unternehmen, Social-Media-Konten und Websites (GRAPH),

zur Durchführung von OSINT-Recherchen zu mutmaßlichen Straftätern (SEARCH), zur Echtzeitüberwachung von Social Media (MONITOR) und zur Durchführung von Analysen sozialer Netzwerke (EVIDENCE).

Mögliche Anwendung in einem Fall von Menschenhandel/Arbeitsausbeutung:

➔ deckt gefälschte Rekrutierungswebsites auf und verknüpft sie mit bekannten Menschenhändlern

➔ bildet Verbindungen zwischen verschiedenen Social-Media-Profilen ab, die für die Rekrutierung genutzt werden

➔ identifiziert Krypto-Wallets und Finanztransaktionen, die mit Menschenhändlern in Verbindung stehen

https://www.maltego.com/blog/shining-a-light-empowering-ngos-during-national-human-trafficking-prevention-month/

- **Autopsy**: ein kostenloses Open-Source-Tool für die digitale Forensik, das eine Plattform für die Untersuchung von Festplatten bietet.

  Mögliche Anwendung in einem Fall von Menschenhandel/Arbeitsausbeutung:

  ➔ stellt gelöschte Arbeitsverträge oder gefälschte Visumdokumente wieder her

  ➔ verfolgt den Browserverlauf (z.B. Besuche auf gefälschten Job-Websites oder verschlüsselten Chat-Plattformen)

  ➔ extrahiert den Verlauf von USB-Geräten, um festzustellen, ob externe Laufwerke zur Speicherung von z.B. Opferdaten verwendet wurden

  ADF PRO: ist eine Software für digitale Forensik und Triage, die für die schnelle Analyse von Computern, externen Laufwerken und Mobilgeräten entwickelt wurde.

  Mögliche Anwendung in einem Fall von Menschenhandel/Arbeitsausbeutung:

➔ Schnelle Beschlagnahmung digitaler Beweismittel an Räumungsorten (z.B. Scannen der sozialen Medien, Laptops und Telefone von Verdächtigen)

➔ Gesichtserkennung: schnelle Identifizierung und Abgleich von Gesichtern in Bildern und Videos (anwendbar für die Identifizierung von Opfern und Tätern)

- **Blockchain-Analyse-Tools** (z.B. von Chainalysis, Elliptic, CipherTrace)

  Diese Tools sind auf die Verfolgung von Kryptowährungstransaktionen spezialisiert, die häufig von Menschenhändlern verwendet werden, um Zahlungen für Vermittlungsgebühren oder die Ausbeutung von Opfern zu erhalten.

  Mögliche Anwendung in einem Fall von Menschenhandel/ Arbeitsausbeutung:

  ➔ Verfolgung von Bitcoin- oder Kryptotransaktionen, die von Opfern an ausbeuterische Anwerber getätigt wurden

  ➔ Verbindung von Wallet-Adressen mit bekannten Menschenhandelsnetzwerken

  ➔ Identifizierung von Geldwäschetechniken, die zur Verschleierung illegaler Gewinne eingesetzt werden

Für digitale forensische Verfahren zur Bekämpfung von THB werden zwei weitere mögliche Ansätze vorgestellt und kurz beschrieben. In gewissem Maße können sie sich auch mit bereits beschriebenen Tools oder Bereichen der digitalen Forensik überschneiden.

Der erste Ansatz besteht darin, Metadaten aus Bildern und Videos im Bereich des Menschenhandels für (digitale) forensische Untersuchungen zu nutzen. Anstatt sich ausschließlich auf rechenintensive Computer-Vision-Techniken zu verlassen, könnten Bild- und Videometadaten den Strafverfolgungsbehörden bei der Identifizierung von Opfern und Menschenhändlern helfen (Mattmann et al., 2016). Menschenhandel enthält

oft textuelle Hinweise wie die körperlichen Merkmale der Opfer, den Ort und Multimedia-Elemente (d. h. Bilder, Videos auf verschiedenen Plattformen). Mattmann et al. (2016) entwickelten ein Metadaten-Forensik-Toolkit für Multimedia, das ImageCat (Bildkatalog) und ImageSpace umfasst. ImageCat ist ein ETL-System (Extract, Transform, Load), das für die Verarbeitung und Katalogisierung von Multimedia-Metadaten, insbesondere im Bereich der Ermittlungen zu Menschenhandel, entwickelt wurde. Es kann mehrere Anzeigen mit gemeinsamen Metadaten verknüpfen (z.B. gleiche Kamera für verschiedene Opfer; Ähnlichkeitsanalyse) und ermöglicht die schnelle Suche und den Abruf von Multimedia-Beweismaterial. Somit kann es Strafverfolgungsbehörden dabei helfen, sowohl Opfer als auch Menschenhändler zu identifizieren (Mattmann et al., 2016). Darüber hinaus extrahiert ImageSpace (auf Basis von ImageCat) Multimedia-Metadaten (d.h. RGB-Farbraum, Kameramodell, Geolokalisierung, Zeitstempel). Es kann große Multimedia-Datenbanken durchsuchen und abfragen, wodurch Strafverfolgungsbehörden Bilder und Videos anhand von Text, Metadaten oder Bildähnlichkeit suchen können. Darüber hinaus hilft die interaktive Bilddurchsicht und -visualisierung den Strafverfolgungsbehörden, diese Beweise in einer übersichtlichen Galerie für die forensische Überprüfung anzuzeigen, und bietet interaktive Histogramme und Dichteplots. ImageSpace ermöglicht auch den Abgleich von Ähnlichkeiten zwischen Bildern und Videos, um verwandte Dateien zu clustern, was Ermittlern hilft, z.B. Opfer über verschiedene Anzeigen und Plattformen hinweg zu verfolgen. Darüber hinaus kann es seine Suchergebnisse im Laufe der Zeit optimieren und unterstützt die optische Zeichenerkennung und Textextraktion (d. h. das Extrahieren von Telefonnummern, E-Mails, Adressen) aus den Bildern und Videos. Dieser spezifische Multimedia-Ansatz bietet eine alternative Methode, um Anzeigen, Opfer und Menschenhändler miteinander zu verknüpfen, indem Metadatenmuster anstelle von Bild- oder Videoinhalten allein analysiert werden.

Ein weiterer Ansatz, der teilweise in zuvor vorgestellten Tools enthalten ist und in vielen der bisherigen Ausführungen zur THB-Ermittlung und digitalen Forensik wiederzufinden ist, ist die Open-Source-Intelligence-Recherche (OSINT). OSINT-Recherche bezieht sich auf das Sammeln und Analysieren öffentlich zugänglicher Daten zur Unterstützung von Ermittlungen. Sie spielt eine entscheidende Rolle in der digitalen Forensik für THB-Ermittlungen, indem sie Muster identifiziert, digitale Spuren verfolgt und Verdächtige mit kriminellen Aktivitäten in Verbindung bringt. Da bereits zuvor besonders nützliche OSINT-Elemente erwähnt wurden, dient dieser kurze Abschnitt lediglich dazu, die Bedeutung und das große Potenzial dieser Methode zu skizzieren. OSINT ist für die Identifizierung von Rekrutierungs- und Kommunikationsmustern von entscheidender Bedeutung, da sie dabei hilft, wichtige Plattformen, Sprachmuster und Rekrutierungsstrategien aufzudecken, die bei aktiven (Jagd) und passiven (Fischen) Rekrutierungsmethoden zum Einsatz kommen. OSINT, das in Social Media Intelligence (SOCMINT), Geospatial Intelligence (GEOINT) und Human Intelligence (HUMINT) unterteilt werden kann, umfasst beispielsweise die Überwachung von sozialen Medien und Stellenanzeigen, die Analyse von Forumsdiskussionen, Aktivitäten im Dark Web sowie die umgekehrte Bild- und Videosuche. Es dient dazu, Online-Anzeigen mit Menschenhandelsnetzwerken in Verbindung zu bringen, indem Stellenanzeigen gecrawlt und analysiert, Kryptowährungen und Zahlungen verfolgt sowie Domains und Websites analysiert werden. Es kann wichtig sein, um Opfer und Menschenhändler zu geolokalisieren, indem Bilder und Videos (und deren Metadaten) analysiert werden oder Crowdsourced Geolocation (z.B. Google Street View, Satellitenbilder) verwendet wird. Darüber hinaus kann OSINT auch dabei helfen, gefälschte Identitäten und Netzwerke aufzudecken, indem Daten aus sozialen Medien (oder auch dem Dark Web) abgeglichen, digitale Spuren analysiert und personenbezogene Daten überprüft werden (siehe z.B. https://epieos.com/ für die umgekehrte Suche, wenn eine E-Mail-Adresse oder

Telefonnummer mit bestimmten Konten wie einem Google-Konto verknüpft ist) oder durch Verhaltensanalysen (z.B. Posting-Verhalten, Sprachmuster, Zeitpunkt von Online-Aktivitäten).

9.4.4.4 Herausforderungen bei digitalen forensischen Untersuchungen

Die Untersuchung von Fällen von Menschenhandel stellt die digitale Forensik vor besondere Herausforderungen, darunter:

- Verschlüsselte und selbstzerstörende Kommunikation
- Löschung und Verschleierung von Daten
- Grenzüberschreitende Datenproblematik
- Opfer- und Datenschutz

Um einen systematischeren Überblick über die Herausforderungen zu erhalten, kann man sie in sachbezogene und strukturelle Herausforderungen unterteilen.

Sachbezogene Herausforderungen

Materielle Herausforderungen sind Herausforderungen, die sich aus dem Thema der digitalen Forensik und der Ermittlungen im Bereich des Menschenhandels ergeben. Sie sind daher dem Verbrechen an sich immanent. So kann beispielsweise zwischen proaktiven und reaktiven Ermittlungen unterschieden werden. **Proaktive Ermittlungen** sind weitaus komplexer, da die Strafverfolgungsbehörden Anzeichen für Ausbeutung identifizieren müssen, die auf Ausbeutung hindeuten könnten. Es ist schwierig, diese Hinweise aus der Vielzahl der verfügbaren Online-Anzeigen herauszufiltern (Europol, 2020). Daher sind **„reaktive Ermittlungen** einfacher, da sie einen Ausgangspunkt haben,

wie beispielsweise die Aussage eines identifizierten Opfers und/oder das Konto oder die Website, die für Rekrutierungs- oder Ausbeutungszwecke genutzt werden“ (Europol, 2020, S. 5).

Darüber hinaus stellen die digitalen Beweise, mit denen Ermittler in Fällen von Menschenhandel überwiegend zu tun haben, eine Herausforderung dar. Da viele Menschenhändler Instant-Messaging-Apps wie WhatsApp, Signal oder Telegram verwenden, erschwert die integrierte End-to-End-Verschlüsselung (E2EE) das Abrufen von Nachrichten. Ein weiterer Punkt ist, dass Menschenhändler digitale Beweise häufig löschen (entweder selbst oder mithilfe von Selbstlöschfunktionen, z.B. in WhatsApp-Chats). Der Zugriff auf gelöschte Daten ist eingeschränkt, und Ermittler können nur versuchen, auf in der Vergangenheit erstellte Backups zuzugreifen. Darüber hinaus können Menschenhändler über versteckte Dienste von Tor (Dark Web, VPN-Nutzung) operieren, was die Verfolgung erschwert. Außerdem versuchen Menschenhändler, ihre Spuren durch eine extreme Diversifizierung ihrer digitalen Präsenz zu verwischen – beispielsweise durch die Verwendung mehrerer SIM-Karten und Mobiltelefone, verschiedener Konten (einschließlich gefälschter Konten) usw. Diese Schwierigkeit veranschaulicht eine weitere Herausforderung: Der mit dem Fall befasste Ermittler muss oft eine riesige Menge an (vor allem digitalen) Daten bewältigen, diese Daten sichten, sie als relevant oder irrelevant für die zu verfolgende Straftat oder Straftaten kategorisieren, den Überblick behalten und weitere strategische Schritte planen. Im Zusammenhang mit dieser Herausforderung gibt es noch einen weiteren rechtlichen Aspekt, der problematisch werden kann: Ein Fall kann unglaublich komplex werden, da oft nicht nur Menschenhandel/Arbeitsausbeutung angeklagt werden kann, sondern auch z.B. Steuerhinterziehung, Verstöße gegen das Arbeitsrecht und Sozialversicherungsvorschriften, Zwangsarbeit, Körperverletzung, Betrug, Urkundenfälschung oder Menschenrechtsverletzungen. Dies kann sich auch auf die

digitale Forensik auswirken, da ein komplexerer Fall einen intensiveren und konsistenteren Austausch zwischen dem leitenden Ermittler und dem Spezialisten für digitale Forensik erfordert.

Strukturelle Herausforderungen

Herausforderungen können als strukturell angesehen werden, wenn sie aus dem System selbst resultieren (z.B. aus der Organisation der Strafverfolgung in einem Land oder aus den rechtlichen Rahmenbedingungen). So werden beispielsweise die von Menschenhändlern eingesetzten digitalen Technologien ständig weiterentwickelt, weshalb sich die Strafverfolgungsbehörden an diese (neuesten) technischen Entwicklungen anpassen müssen, die von den Tätern genutzt werden (Europol, 2020). Darüber hinaus müssen die Strafverfolgungsbehörden für diese Ermittlungen mit geeigneten personellen Ressourcen ausgestattet werden. Dies gilt nicht nur für spezialisierte Ermittler im Bereich Menschenhandel und digitale Forensiker und Praktiker, sondern auch für anderes dringend benötigtes Personal für die Untersuchung von Fällen von Menschenhandel, wie z.B. Dolmetscher (für die Übersetzung von Telekommunikationsüberwachungsdaten). Ebenso müssen die Rechtsinstrumente verbessert werden, um die Strafverfolgung und Verurteilung sicherzustellen (Europol, 2020).

Die Erweiterung der gesetzlichen Möglichkeiten ist auch deshalb besonders relevant, weil Opfer oft zögern, wichtige Geständnisse und Aussagen zu machen, da sie bereits unter großem psychischen Stress stehen – durch Drohungen, Erpressung sowie das inhärente Risiko einer öffentlichen Blamage über soziale Medien (z.B. durch die Veröffentlichung ihrer Ausbeutung). Ein leichterer Zugang zu verfügbaren Datensätzen für die digitale Forensik ist daher wichtig, um Ermittlungen voranzutreiben und

letztendlich die strafrechtliche Verfolgung zu unterstützen oder sogar zu ermöglichen (Europol, 2020).

In Bezug auf rechtliche Aspekte sollte auch erwähnt werden, dass grenzüberschreitende Zusammenarbeit erschwert werden kann, wenn die justizielle Zusammenarbeit und die geltenden Vorschriften nicht klar geregelt sind. Dies kann beispielsweise den Austausch von Beweismitteln zwischen Ländern behindern. Entsprechend der mangelnden standardisierten internationalen Zusammenarbeit gibt es noch keine zentralisierte globale Datenbank zur Verfolgung der Online-Aktivitäten von Menschenhändlern.

9.4.4.5 Rechtliche und ethische Erwägungen

Aufgrund der Sensibilität von Fällen von Menschenhandel müssen forensische Untersuchungen strengen ethischen und rechtlichen Standards entsprechen, von denen einige bereits zuvor vorgestellt wurden. Durch die Berücksichtigung dieser Aspekte können Fachleute für digitale Forensik die komplexe Landschaft der Ermittlungen im Bereich Menschenhandel und Arbeitsausbeutung ethisch, rechtlich und effektiv navigieren und so sicherstellen, dass die Verfolgung der Gerechtigkeit mit dem Schutz der Rechte des Einzelnen und der gesellschaftlichen Werte im Einklang steht.

Opferzentrierter Ansatz

Ein opferzentrierter Ansatz stellt die Rechte, Bedürfnisse und das Wohlergehen der Opfer während des gesamten Ermittlungsprozesses in den Vordergrund. Diese Methodik betont, dass Opfer mit Respekt und Einfühlungsvermögen behandelt, informiert und unterstützt werden und aktiv in Entscheidungen einbezogen werden müssen, die ihr Leben betreffen. Indem sie sich auf die Erfahrungen der Opfer konzentrieren, können

Ermittler Vertrauen aufbauen, was nicht nur für die Sammlung genauer Informationen, sondern auch für die Bereitstellung angemessener Unterstützungsleistungen für die Opfer von entscheidender Bedeutung ist. Dieser Ansatz trägt nicht nur zur Genesung der Opfer bei, sondern stärkt auch die allgemeine Integrität der Ermittlungen (Internationale Arbeitsorganisation, 2018). „Die Sicherheit der Opfer und ihrer Familien und Angehörigen hat jederzeit oberste Priorität und liegt in der Verantwortung der Ermittler und Staatsanwälte“ (Internationale Arbeitsorganisation, 2018, S. 47). Dies unterstreicht auch die Notwendigkeit, sich nicht nur auf das Opfer als Einzelperson zu konzentrieren, sondern auch auf die Familien/Angehörigen, da die Möglichkeit von Vergeltungsmaßnahmen gegen Familienmitglieder durch Menschenhändler immer gegeben ist (Internationale Arbeitsorganisation, 2018).

Darüber hinaus wird speziell im Bereich der digitalen Forensik empfohlen, die invasive digitale Überwachung zu minimieren, indem man sich in dieser Hinsicht auf die Menschenhändler konzentriert und nicht auf die Opfer. Die Vertraulichkeit der Daten der Opfer sollte jederzeit gewährleistet sein, um Vergeltungsmaßnahmen oder eine öffentliche Bloßstellung zu verhindern. Der Ermittler sollte es vermeiden, die Opfer unter Druck zu setzen, digitale Interaktionen mehrfach zu schildern (und stattdessen forensische Tools verwenden), und er sollte die Zustimmung des Opfers einholen, bevor er auf persönliche Geräte zugreift. Aggressive Verhörtechniken auf der Grundlage digitaler Erkenntnisse sind zu vermeiden (z.B. die Konfrontation eines Opfers mit seinen Chat-Protokollen in einer Weise, die Stress auslöst). Eine weitere große Herausforderung bei der Strafverfolgung von Menschenhändlern kann die Abhängigkeit von Opferaussagen sein, die für das Opfer traumatisierend sein können, aber aufgrund von z.B. Angst auch potenziell unzuverlässig sind. In dieser Hinsicht kann die digitale Forensik Fälle stärken und die Abhängigkeit der Opfer vor Gericht verringern, was wiederum die

Belastung für die Opfer reduzieren kann. Experten für digitale Forensik können darüber hinaus verhindern, dass Opfer Vergeltungsmaßnahmen ausgesetzt werden oder erneut Opfer von Menschenhandel werden, indem sie ihre Geräte, sofern vereinbart/gewünscht, auf Spyware scannen und anschließend Tracking-Tools entfernen.

Datenschutz

- **Während des Ermittlungsverfahrens:** Der Schutz von Personen, die Menschenhandelsaktivitäten aufdecken, ist für die Förderung der Anzeige von Straftaten von entscheidender Bedeutung. Außerdem gewährleistet der Schutz von Hinweisgebern, dass diejenigen, die sich melden, keinen Vergeltungsmaßnahmen ausgesetzt sind, wodurch ein Umfeld geschaffen wird, in dem Informationen sicher weitergegeben werden können. Darüber hinaus stellt eine ethische Berichterstattung durch Medien und Behörden sicher, dass Opfer nicht durch die Veröffentlichung erneut zu Opfern werden und dass die verbreiteten Informationen dem öffentlichen Interesse dienen, ohne Schaden anzurichten.

  Das UNODC hat in seinem Modul 10 zum Thema Datenschutz und Datensicherheit einen Überblick über Datenschutz und Datensicherheit zusammengestellt, der bei cyberbezogenen Angelegenheiten berücksichtigt werden sollte.

- **Beschlagnahmte Beweismittel:** Die Gewährleistung der Integrität und Vertraulichkeit digitaler Beweismittel ist von entscheidender Bedeutung. Es müssen angemessene Datenschutzmaßnahmen getroffen werden, um unbefugten Zugriff, Manipulation oder Verlust von Beweismitteln zu verhindern. Die Aufrechterhaltung einer lückenlosen Beweiskette ist für die Zulässigkeit von Beweismitteln vor Gericht unerlässlich, da sie die Handhabung der Beweismittel

von der Erhebung bis zur Vorlage dokumentiert. Die Einhaltung gesetzlicher Standards und Protokolle schützt die Rechte aller Beteiligten und wahrt die Glaubwürdigkeit des Ermittlungsverfahrens.

Internationale Zusammenarbeit

Menschenhandel und Arbeitsausbeutung sind oft grenzüberschreitende Straftaten, die eine Zusammenarbeit über Grenzen hinweg erfordern. Die internationale Zusammenarbeit umfasst die Angleichung der Rechtsrahmen, den Informationsaustausch und die Koordinierung der Bemühungen verschiedener Gerichtsbarkeiten. Dieser kollektive Ansatz verbessert die Möglichkeiten, Täter aufzuspüren, Opfer zu schützen und Menschenhandelsnetzwerke wirksam zu zerschlagen. Das Modul 11 – Internationale Zusammenarbeit zur Bekämpfung der grenzüberschreitenden organisierten Kriminalität der UNODC kann einen Einblick in die rechtlichen Möglichkeiten in dieser Hinsicht geben.

Verhältnismäßigkeit und Notwendigkeit

Bei Ermittlungen sollte ein Gleichgewicht zwischen dem Informationsbedarf und der Achtung der Privatsphäre des Einzelnen hergestellt werden. Die Sammlung digitaler Beweise muss in einem angemessenen Verhältnis zur Schwere der Straftat stehen und für die Ermittlungen notwendig sein. Dieser Grundsatz stellt sicher, dass Ermittlungsmaßnahmen nicht über das erforderliche Maß hinausgehen oder Grundrechte verletzen, sodass bei der Strafverfolgung ethische Standards gewahrt bleiben.

Integration von KI

Die Integration von KI in die digitale Forensik bietet Effizienz, wirft aber auch Bedenken hinsichtlich Genauigkeit und Voreingenommenheit auf. Automatisierte Tools müssen sorgfältig entwickelt und regelmäßig evaluiert werden, um Verzerrungen zu vermeiden, die zu falschen Anschuldigungen führen oder bestimmte Opferprofile übersehen könnten. Die menschliche Aufsicht bleibt entscheidend, um KI-generierte Daten im entsprechenden rechtlichen und ethischen Kontext zu interpretieren. Insbesondere an relevanten oder sogar entscheidenden Punkten im Ermittlungsprozess darf der Einsatz von KI das menschliche Urteilsvermögen nicht ersetzen.

Ethische Nutzung von OSINT und Dark-Web-Überwachung

OSINT und Dark-Web-Überwachung sind zwar wertvoll für die Aufdeckung illegaler Aktivitäten, müssen jedoch innerhalb der gesetzlichen Grenzen durchgeführt werden. Ermittler sollten unbefugten Zugriff oder betrügerische Praktiken vermeiden, die die Integrität der Ermittlungen beeinträchtigen oder gegen ethische Standards verstoßen könnten. Die Achtung der Privatsphäre und die rechtmäßige Beschaffung von Informationen sind von grundlegender Bedeutung für die Aufrechterhaltung des öffentlichen Vertrauens und die Wahrung der Rechtsstaatlichkeit.

9.5 Finanzermittlungen

Finanzermittlungen sind ein unverzichtbares Instrument zur Bekämpfung von Finanzkriminalität wie Geldwäsche (ML), Terrorismusfinanzierung (TF) und Menschenhandel. Diese Ermittlungen konzentrieren sich auf die Analyse von Finanztransaktionen, um illegale Aktivitäten aufzudecken, illegale Gelder aufzuspüren und Täter und ihre Netzwerke zu identifizieren. Die grundlegenden Konzepte und Ziele von Finanzermittlungen drehen sich darum, den **Geldfluss zu verfolgen**, um

Finanzkriminalität aufzudecken und zu dokumentieren. Zu den vorrangigen Zielen gehören die Identifizierung krimineller Netzwerke, die Rückverfolgung illegaler Gelder und die Sammlung von Beweismaterial, das in Strafverfahren verwendet werden kann. Eine gut durchgeführte Finanzermittlung unterstützt die Strafverfolgung, indem sie Kriminellen ihre finanziellen Ressourcen entzieht und die finanzielle Infrastruktur, die das organisierte Verbrechen stützt, zerschlägt.

Die Relevanz von Finanzanalysen im Zusammenhang mit **Menschenhandel** ist besonders groß, da Menschenhändler auf Finanztransaktionen angewiesen sind, um ihre illegalen Erlöse zu bewegen, zu lagern und zu waschen. Durch die genaue Prüfung von Transaktionsaufzeichnungen, Kontoauszügen und digitalen Zahlungsmethoden können Ermittler finanzielle Verbindungen zwischen Menschenhändlern und ihren Komplizen aufdecken. Dies hilft nicht nur bei der Strafverfolgung von Kriminellen, sondern auch bei der Identifizierung von Opfern, indem finanzielle Muster aufgedeckt werden, die auf Ausbeutung hindeuten. Finanzermittlungen spielen daher eine entscheidende Rolle bei der Zerschlagung von Menschenhandelsnetzwerken, indem sie auf die finanziellen Lebensadern abzielen, die diese Netzwerke am Leben erhalten. „Die breite Anerkennung, Umsetzung und Harmonisierung von Ermittlungsstrategien und -taktiken, die speziell auf die Finanzen des Menschenhandels abzielen, ist jedoch noch in Arbeit“ (OSZE, 2019, S. 37).

Der folgende Abschnitt 9.7.1 beschreibt allgemeine Grundlagen der Finanzermittlung, gefolgt von einer Einführung in die Strukturen des Menschenhandels, um die Relevanz der Finanzermittlung im Zusammenhang mit Menschenhandel und Arbeitsausbeutung hervorzuheben (Abschnitt 9.7.2). Abschnitt 9.7.3 erläutert Schritt für Schritt, wie eine Finanzermittlung in Fällen von Menschenhandel durchgeführt wird. Abschnitt 9.7.4 zeigt Transaktionsindikatoren auf, die auf verdächtige Finanzaktivitäten im Bereich des

Menschenhandels und insbesondere der Arbeitsausbeutung hinweisen. Abschnitt 9.7.5 beschreibt die Herausforderungen bei Finanzermittlungen, während Abschnitt 9.7.6 sich mit technischen Innovationen und Trends befasst. Abschnitt 9.7.7 schließt mit einigen zusätzlichen Empfehlungen.

9.5.1 Überblick

Finanzermittlungen spielen eine entscheidende Rolle bei der Strafverfolgung und Strafverfolgung, insbesondere in Fällen von Geldwäsche, Terrorismusfinanzierung und organisierter Kriminalität (FATF, 2012). Die Leitlinien der Financial Action Task Force (FATF) Guidance on Financial Investigations umreißen die wesentlichen Grundsätze, Instrumente und Strategien, die für die Durchführung wirksamer Finanzermittlungen erforderlich sind. Das Hauptziel einer Finanzermittlung besteht darin, die **Bewegungen illegaler Gelder nachzuverfolgen und zu dokumentieren**, um kriminelle Netzwerke zu identifizieren, Finanzstrukturen aufzudecken und stichhaltige Rechtsfälle aufzubauen (FATF, 2012). Durch die Untersuchung der finanziellen Aspekte krimineller Aktivitäten können Ermittler neue Hinweise aufdecken, ganze kriminelle Netzwerke – einschließlich ihrer transnationalen Verbindungen – aufzeichnen und wertvolle Beweise sammeln, um Verdächtige strafrechtlich zu verfolgen und illegale Vermögenswerte zu beschlagnahmen.

9.5.1.1 Kernaspekte von Finanzermittlungen

Ein zentraler Bestandteil von Finanzermittlungen sind **parallele Ermittlungen**, bei denen Finanzermittlungen parallel zu strafrechtlichen Ermittlungen durchgeführt werden. Dieser Ansatz stellt sicher, dass sich die Strafverfolgungsbehörden auf Straftaten wie Menschenhandel, Korruption oder Drogenhandel konzentrieren, während gleichzeitig

Finanzermittlungen den Geldflüssen dieser Aktivitäten nachgehen (FATF, 2012). Parallele Ermittlungen helfen dabei, illegale Vermögenswerte aufzuspüren, weitere Verdächtige zu identifizieren und die Einziehung von Erträgen aus Straftaten zu unterstützen. Um die Effektivität zu steigern, werden häufig multidisziplinäre Task Forces eingerichtet, in denen Finanzanalysten, forensische Buchprüfer, Experten für digitale Forensik und Staatsanwälte zusammenarbeiten. Diese Teams verbessern den Informationsaustausch, reduzieren Doppelarbeit und gewährleisten einen umfassenden Ansatz zur Bekämpfung der Finanzkriminalität (FATF, 2012).

Ein wesentliches Ziel von Finanzermittlungen ist die **Wiedererlangung und Einziehung von Vermögenswerten** (siehe Schulungskapitel 10). Kriminelle sind in erster Linie auf finanziellen Gewinn aus und die Einziehung ihrer illegalen Erträge schwächt ihre Aktivitäten. Strafverfolgungsbehörden müssen illegale Vermögenswerte mithilfe fortschrittlicher finanzforensischer Techniken aufspüren, einfrieren und beschlagnahmen. Die Einziehung ohne Verurteilung wird ebenfalls als wirksames Rechtsinstrument empfohlen, da sie es den Behörden ermöglicht, kriminelle Vermögenswerte auch in Fällen zu beschlagnahmen, in denen eine Verurteilung nicht möglich ist. Die Einrichtung spezialisierter Einheiten für die Vermögensrückgewinnung und zentralisierter Finanzinformationsdatenbanken stärkt die Finanzermittlungen erheblich, indem sie die Effizienz und Koordination verbessert.

Eine erfolgreiche Finanzermittlung **stützt sich auf mehrere Informationsquellen**. Die Strafverfolgungsbehörden müssen Zugang zu Finanzinformationsberichten haben, darunter STRs, Währungstransaktionsberichte und grenzüberschreitende Bargeldanmeldungen. Darüber hinaus liefern Bank- und Finanzunterlagen, Unternehmensregister, Steuererklärungen, Zolldaten und OSINT wichtige Hinweise. Es ist

von entscheidender Bedeutung, dass Strafverfolgungsbeamte die rechtliche Befugnis haben, auf diese Unterlagen zuzugreifen und sie zu analysieren, wobei die Einhaltung der Datenschutzgesetze gewährleistet sein muss.

Ermittlungsmethoden

Bei Finanzermittlungen kommen verschiedene Ermittlungsmethoden zum Einsatz (eine Liste der Methoden finden Sie in FATF, 2012, sofern keine andere Quelle angegeben ist).

- **Physische Überwachung:** Bei dieser Methode werden Verdächtige überwacht, um ihre finanziellen Aktivitäten zu verstehen, z.B. Bargeldbewegungen oder Interaktionen mit Finanzintermediären. Sie ist besonders nützlich in Fällen von Geldwäsche und Terrorismusfinanzierung.
- **Müllsammeln:** Ermittler können rechtmäßig weggeworfene Finanzunterlagen und andere Dokumente sammeln und analysieren, die versteckte Vermögenswerte oder illegale Transaktionen aufdecken könnten.
- **Zwangsmaßnahmen:** Dazu gehören Durchsuchungsbefehle, Vorladungen und Vorlageverfügungen, um wichtige Finanzunterlagen wie Kontoauszüge, Steuererklärungen und Geschäftsbücher zu beschaffen. Ordnungsgemäß durchgeführte Durchsuchungs- und Beschlagnahmungsverfahren stellen sicher, dass digitale und physische Beweismittel rechtmäßig gesammelt und unter einer Kontrollkette aufbewahrt werden.
- **Überwachung der Kommunikation:** Strafverfolgungsbehörden können Abhörmaßnahmen, E-Mail-Überwachung und andere Formen der elektronischen Überwachung durchführen, um Finanztransaktionen zu verfolgen und Mitverschwörer zu identifizieren. Diese Methode ist sehr effektiv, muss jedoch den

gesetzlichen Rahmenbedingungen entsprechen, um Verletzungen der Privatsphäre zu vermeiden.

- **Verdeckte Ermittlungen:** In einigen Fällen können Ermittler falsche Identitäten annehmen, um kriminelle Organisationen zu infiltrieren und direkte Beweise für finanzielles Fehlverhalten zu sammeln. Diese Technik ist ressourcenintensiv und erfordert eine umfassende Ausbildung.
- **Kontrollierte Lieferungen:** Bei dieser Methode wird die Bewegung illegaler Gelder, entweder in bar oder durch digitale Überweisungen, unter Aufsicht der Strafverfolgungsbehörden verfolgt. Dies hilft dabei, wichtige Akteure in Geldwäsche- oder Betrugsnetzwerken zu identifizieren.
- **Forensische Buchführung:** Die forensische Buchführung ist ein Spezialgebiet, das Buchhaltungs-, Prüfungs- und Ermittlungsfähigkeiten kombiniert, um Finanzunterlagen auf Anzeichen von Fehlverhalten zu untersuchen. Forensische Buchhalter können Unstimmigkeiten in Büchern aufdecken, Betrugsfälle aufdecken und illegale Finanzaktivitäten anhand detaillierter Finanzberichte nachverfolgen. Sie wenden sowohl quantitative Methoden wie Datenanalyse und statistische Modellierung als auch qualitative Ansätze wie die Bewertung von Verhaltensmustern und der Unternehmenskultur an, um Anomalien aufzudecken. Das Benfordsche Gesetz sagt die Häufigkeitsverteilung von Ziffern in natürlich vorkommenden Datensätzen voraus. Forensische Buchhalter nutzen dieses Prinzip, um Unregelmäßigkeiten in Finanzdaten zu identifizieren. Abweichungen von der erwarteten Verteilung können auf mögliche Manipulationen oder Betrug hinweisen. Mark Nigrini, ein Pionier auf diesem Gebiet, hat das Benfordsche Gesetz umfassend erforscht und angewendet, um Anomalien in Buchhaltungsdaten aufzudecken (siehe z.B. Gorenc, 2019; Siavoshi, 2025).

- **Methoden zum Nachweis von Einkünften:** Ermittler verwenden direkte und indirekte Methoden, um illegale Einkommensquellen aufzudecken. Bei der Vermögensmethode werden die Vermögenswerte einer Person zu zwei Zeitpunkten verglichen, um nicht gemeldete Einkünfte zu ermitteln. Bei der Bankguthabenmethode werden unerklärliche Zuflüsse auf Bankkonten analysiert. Bei der Ausgabenmethode werden Ausgabengewohnheiten mit bekannten legalen Einkommensquellen verglichen.
- **Austausch von Finanzinformationen:** Die Strafverfolgungsbehörden arbeiten mit Finanzermittlungsstellen (FIUs), Banken und internationalen Partnern zusammen, um Verdachtsmeldungen (SARs) und andere relevante Finanzdaten zu erhalten.
- **Die Überprüfung von Finanztransaktionen** hilft den Ermittlern, verdächtige Bankmuster, Layering-Techniken und Methoden zur Vermögensintegration zu identifizieren.
- **Die digitale Forensik** (siehe Abschnitt 9.6.1) spielt eine wichtige Rolle bei der Rückverfolgung von Online-Geldtransfers, der Analyse von Kryptowährungstransaktionen und der Überwachung illegaler Finanzkommunikation.

Nutzung von Synergien durch Zusammenarbeit

FIUs spielen eine entscheidende Rolle bei Finanzermittlungen, indem sie Finanzinformationen sammeln, analysieren und an Strafverfolgungsbehörden weitergeben. FIUs erhalten AML/CFT-Meldungen, STRs und Berichte über grenzüberschreitende Transaktionen, die frühzeitig vor kriminellen Finanzaktivitäten warnen können. Eine enge nationale Zusammenarbeit zwischen FIUs und Ermittlern stellt sicher, dass die Strafverfolgungsbehörden Zugang zu zeitnahen, verwertbaren

Informationen haben. Um die Effizienz zu steigern, sollten FIUs und Strafverfolgungsbehörden sichere Plattformen für den Datenaustausch in Echtzeit einrichten und Protokolle für die Analyse von Finanzinformationen entwickeln.

Da Finanzkriminalität oft grenzüberschreitend ist, ist auch die internationale Zusammenarbeit von entscheidender Bedeutung. Kriminelle nutzen internationale Bankensysteme und Offshore-Finanzzentren, um illegale Gelder zu verschleiern. Strafverfolgungsbehörden müssen Rechtshilfeabkommen (MLATs), Interpol, Europol und FATF-Netzwerke nutzen, um grenzüberschreitende Ermittlungen zu erleichtern. Die Einrichtung gemeinsamer Ermittlungsgruppen und die Straffung der rechtlichen Rahmenbedingungen für den Informationsaustausch stärken den weltweiten Kampf gegen Finanzkriminalität (FATF, 2012).

Um Finanzermittlungen zu verbessern, sollten Strafverfolgungsbehörden und Staatsanwaltschaften Finanzforensik in alle Ermittlungen zu schweren Straftaten integrieren, Finanzinformationssysteme für Echtzeitanalysen nutzen und die internationale Zusammenarbeit bei der Vermögensrückgewinnung und dem Informationsaustausch verstärken. Durch die Anwendung dieser bewährten Verfahren können Finanzermittlungen als wirksames Instrument zum Zerschlagen krimineller Unternehmen und zur Sicherstellung dienen, dass sich Verbrechen nicht lohnen.

9.5.1.2 Die Bemühungen der Europäischen Union

Angesichts der zunehmenden Gefahr, dass die organisierte Kriminalität in die legale Wirtschaft eindringt, hat die Europäische Union die Notwendigkeit betont, die Kapazitäten für Finanzermittlungen zu verbessern. In der EU-Strategie zur Bekämpfung der organisierten Kriminalität von 2021 wurde hervorgehoben, wie wichtig es ist, frühzeitige

Finanzermittlungen in allen EU-Ländern zu fördern. Dieser Ansatz zielt darauf ab, die finanzielle Infrastruktur krimineller Organisationen zu zerschlagen, ihre Gewinne zu beseitigen und ihre Integration in die legale Wirtschaft und Gesellschaft zu verhindern (Europäische Kommission, o. J.). Um diese Bemühungen zu unterstützen, hat die Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen (EMPACT) Finanzermittlungen in ihrer Agenda priorisiert. EMPACT erleichtert die Zusammenarbeit zwischen den EU-Mitgliedstaaten bei der Bekämpfung verschiedener krimineller Bedrohungen, darunter Drogenhandel und Menschenhandel, indem Finanzermittlungen als gemeinsames Ziel in alle Prioritäten integriert werden.

Darüber hinaus leistet die Europäische Kommission finanzielle Unterstützung für das Anti-Money Laundering Operational Network (AMON), ein 2012 gegründetes globales Netzwerk von Ermittlern zur Bekämpfung der Geldwäsche. AMON erleichtert den Wissensaustausch zwischen Strafverfolgungsbehörden und unterstützt eine rasche operative Zusammenarbeit bei Ermittlungen im Bereich der Geldwäsche, was dem grenzüberschreitenden Charakter dieser Straftaten Rechnung trägt.

Europol hat seine Bemühungen ebenfalls verstärkt und 2020 das Europäische Zentrum für Finanz- und Wirtschaftskriminalität (EFECC) eingerichtet. Das EFECC leistet den EU-Mitgliedstaaten operative Unterstützung in Fällen von Steuerkriminalität, Betrug, Korruption, Geldwäsche, Vermögensrückgewinnung, Euro-Fälschung und Verbrechen im Bereich des geistigen Eigentums. Diese Initiative zielt darauf ab, hochkomplexe Fälle von Finanzkriminalität zu bekämpfen, die sich gegen Einzelpersonen, Unternehmen und den öffentlichen Sektor richten.

Darüber hinaus bietet die Europäische Agentur für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) regelmäßig Schulungen für Strafverfolgungsbeamte

an, um deren Verständnis für Geldwäschepraktiken und grenzüberschreitende Finanzermittlungstechniken zu verbessern. Diese Schulungen zielen darauf ab, die Fähigkeiten der Ermittler zu stärken, damit sie die finanziellen Aspekte der organisierten Kriminalität wirksam bekämpfen können (Europäische Kommission, o. J.).

Zusammenfassend lässt sich sagen, dass der umfassende Ansatz der Europäischen Union bei Finanzermittlungen deren entscheidende Rolle bei der Zerschlagung krimineller Unternehmen, dem Schutz der legalen Wirtschaft und der Verbesserung der Wirksamkeit der Strafverfolgung in allen Mitgliedstaaten unterstreicht.

9.5.2 Menschenhandel als Geschäft

Menschenhandel funktioniert wie ein gewinnorientiertes Geschäft, ähnlich wie legitime Unternehmen, und es lohnt sich, diese Perspektive zu betrachten, um (1) die Hauptursachen des Menschenhandels zu verstehen und (2) die Notwendigkeit finanzieller Ermittlungen zu erkennen. Wirtschaftstheorien zur Kriminalität legen nahe, dass Täter rationale Entscheidungen auf der Grundlage potenzieller Gewinne, Risiken und Chancen treffen (siehe z.B. Belser, 2005). Diese Chancen ergeben sich, weil Menschen nach besseren wirtschaftlichen Bedingungen suchen, sei es durch Migration aus verarmten ländlichen Gebieten in wohlhabendere städtische Zentren oder über internationale Grenzen hinweg. Kriminelle Netzwerke nutzen diese Schwachstellen aus, indem sie falsche Versprechungen in Bezug auf Arbeit, Liebe oder Sicherheit machen und die Opfer so zu Arbeits- oder sexueller Ausbeutung oder anderen Formen des Menschenhandels (z.B. Organentnahme) verleiten. Das Geschäftsmodell speziell für die Arbeitsausbeutung ist einfach: Die Opfer arbeiten unter Zwang oder ohne sich der ausbeuterischen Situation bewusst zu sein, wodurch hohe Gewinne bei minimalen

Kosten für die Menschenhändler erzielt werden. Sektoren wie Landwirtschaft, Bauwesen, Hausarbeit und Gastgewerbe bieten Deckung für den Menschenhandel zum Zwecke der Arbeitsausbeutung, während die sexuelle Ausbeutung nach wie vor einer der lukrativsten Märkte für Menschenhändler ist (siehe z.B. Aronowitz, Theuermann & Tyurykanova, 2010).

Trotz der hohen Rentabilität bleiben die Risiken für Menschenhändler gering. Viele Opfer fürchten sich aufgrund ihres rechtlichen Status, sozialer Stigmatisierung oder Drohungen ihrer Ausbeuter vor Strafverfolgungsbehörden. In Ländern, in denen Prostitution illegal ist, müssen Opfer eher mit einer Verhaftung rechnen als mit Schutz. Darüber hinaus sind die Aufklärungs- und Strafverfolgungsquoten für Menschenhändler nach wie vor gering, was die Nachhaltigkeit dieses Geschäftsmodells noch verstärkt. Auch die Marktkräfte spielen eine wichtige Rolle bei der Gestaltung der Menschenhandelsaktivitäten. Es ist nicht allein die Nachfrage der Konsumenten, die den Menschenhandel antreibt, sondern vielmehr das große Angebot an schutzbedürftigen Personen. Kriminelle Organisationen passen ihre Methoden an die rechtlichen Rahmenbedingungen, die wirtschaftlichen Bedingungen und die Strafverfolgungsmechanismen an, ähnlich wie legitime Unternehmen, die auf Marktveränderungen reagieren (Aronowitz, Theuermann & Tyurykanova, 2010).

Bei finanziellen Ermittlungen im Bereich Menschenhandel müssen diese wirtschaftlichen Faktoren berücksichtigt werden. Durch die Analyse von Finanztransaktionen, Gewinnspannen und illegalen Geldflüssen können Strafverfolgungsbehörden Muster der Ausbeutung erkennen, Netzwerke zerschlagen und die finanziellen Anreize hinter Menschenhandelsoperationen schwächen. Das Verständnis von Menschenhandel als wirtschaftliches Unterfangen ist entscheidend für die Entwicklung wirksamer Gegenmaßnahmen, darunter regulatorische

Rahmenbedingungen, Finanzaufsicht und gezielte Interventionen. Im nächsten Abschnitt werden der allgemeine Rahmen für finanzielle Ermittlungen in Fällen von Menschenhandel und die zu ergreifenden konkreten Maßnahmen dargelegt.

9.5.3 Schritt-für-Schritt-Anleitung für Finanzermittlungen im Zusammenhang mit THB

Dieser Abschnitt beschreibt **elf wichtige Schritte für die Durchführung wirksamer Finanzermittlungen in Fällen von Menschenhandel**. Diese Schritte sind in drei Bereiche unterteilt: *grundlegende, operative* und *gemeinschaftliche* Schritte.

Grundlegende Schritte werden in der Regel einmalig bei der Einrichtung des Ermittlungsrahmens durchgeführt und gelten allgemein sowohl für den öffentlichen als auch für den privaten Sektor. Operative Schritte werden aufgrund ihrer Relevanz für einzelne Ermittlungen häufiger angewendet, ihre Umsetzung variiert jedoch zwischen öffentlichen und privaten Einrichtungen. So betreffen beispielsweise die Schritte 7 und 8 in erster Linie meldepflichtige Stellen im privaten Sektor. Die gemeinschaftlichen Schritte unterscheiden sich schließlich in ihrer Anwendbarkeit: Beide Sektoren haben ein gemeinsames Interesse an Schritt 10, während Finanzdienstleister eine größere Verantwortung für Schritt 11 tragen.

Abbildung 13 zeigt diesen schematischen schrittweisen Prozess zwischen Strafverfolgungsbehörden und FIUs. Diese Abbildung ist eine Kopie aus OSZE (2020).

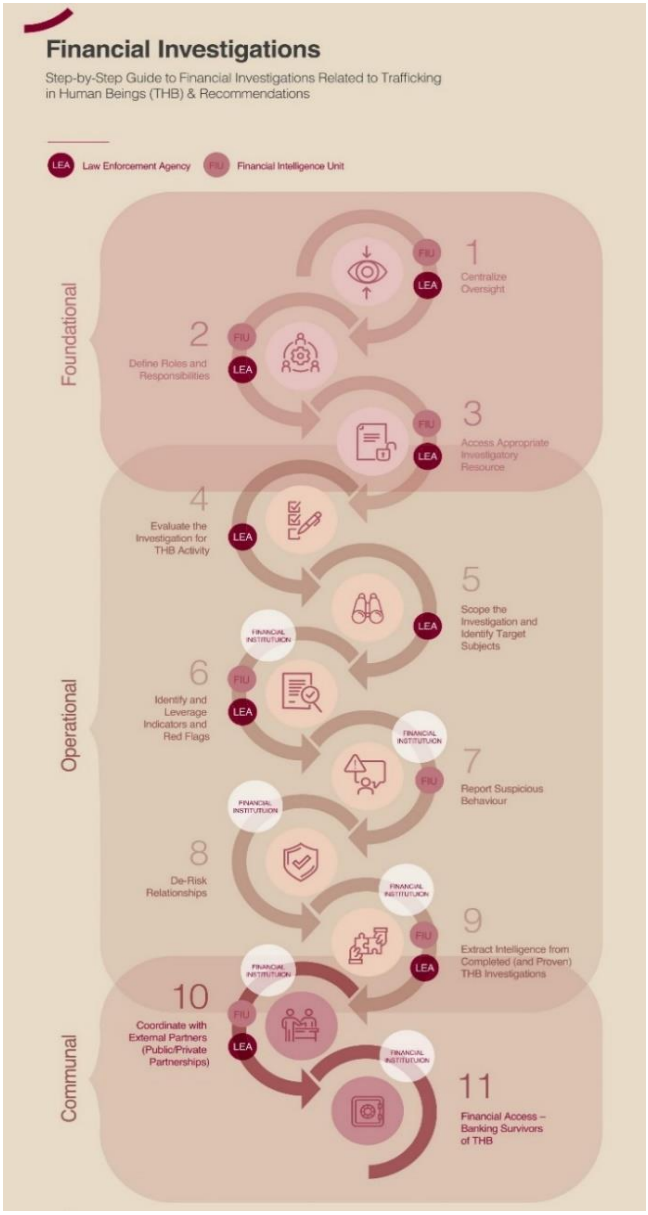

Abbildung 4. Schritte einer Finanzermittlung

Schritt 1: Der erste Schritt für eine erfolgreiche finanzielle Untersuchung von Menschenhandel ist die **Einrichtung eines zentralisierten Überwachungsmechanismus**. Dieser gewährleistet eine koordinierte und umfassende Reaktion auf jeden Verdachtsfall, wobei seine Struktur je nach Größe und Auftrag der jeweiligen Institution variieren kann. Strafverfolgungsbehörden integrieren Ermittlungen im Bereich Menschenhandel häufig in **spezialisierte Einheiten**. So verfügen beispielsweise das New York Police Department (NYPD) und der London Metropolitan Police Service (MPS) über spezielle Teams, während die Toronto Police Service (TPS) Fälle von Menschenhandel innerhalb ihrer Abteilung für Sexualdelikte behandelt, da sie diese von anderen Straftaten unterscheidet. Bundesbehörden wie das FBI und Interpol zentralisieren ebenso wie FIUs ihr Fachwissen, wobei letztere oft weniger öffentlich sichtbar sind.

Im **privaten Sektor**, insbesondere bei Banken, ist die Aufsicht aufgrund des hohen Transaktionsvolumens und der regulatorischen Anforderungen weniger strukturiert. Viele Institutionen unterhalten jedoch **spezielle Ermittlungsteams**, die sich mit Finanzkriminalität, einschließlich Menschenhandel, befassen. Die Zentralisierung der Ermittlungsbemühungen bietet mehrere Vorteile, darunter die Verringerung von Doppelarbeit, die Verbesserung der Effizienz, die Erweiterung des Fachwissens und die Ermöglichung einer umfassenden Datenanalyse. Allerdings birgt sie auch Risiken, wie die Beschränkung des Wissens auf eine ausgewählte Gruppe und mögliche Verzögerungen bei den Ermittlungen. Um diese Risiken zu mindern, sollten die Institutionen Initiativen zum Wissensaustausch fördern und Flexibilität bei den Ermittlungsaufgaben zulassen, um Engpässe zu vermeiden. Letztendlich können die Ermittlungen, solange die Fälle erfasst und angemessen verwaltet werden, von verschiedenen Teams durchgeführt werden, was sowohl internen als auch externen Interessengruppen zugute kommt.

Schritt 2: Sobald ein Überwachungsrahmen für Ermittlungen im Bereich Menschenhandel eingerichtet ist, ist es von entscheidender Bedeutung, die Rollen und Verantwortlichkeiten der Beteiligten klar zu definieren. Dies ist zwar in vielen öffentlichen und privaten Einrichtungen gängige Praxis, wird jedoch manchmal übersehen. Eine **klare Abgrenzung der Verantwortlichkeiten** trägt dazu bei, Doppelarbeit zu vermeiden, die operative Effizienz zu steigern und zusätzliche Vorteile zu erzielen, wie z.B. eine reibungslosere Nachfolgeplanung, eine effektivere Falltriage, eine bessere Priorisierung von Ermittlungen und eine konsistente Kommunikation innerhalb und außerhalb des Teams. Die **Dokumentation der Rollen** stellt sicher, dass Ermittlungen effizienter und zeitnah durchgeführt werden. Letztendlich folgt dieser Ansatz dem Prinzip „Teile und herrsche“ – wenn jeder seine Rolle versteht, kann er sich auf die Ausführung konzentrieren. Ohne klare Zuständigkeiten können selbst gut gemeinte Bemühungen zu einem inkonsistenten und ineffektiven Ermittlungsprozess führen.

Schritt 3: Eine erfolgreiche Ermittlung erfordert den **Zugang zu den richtigen Ressourcen**, die je nach Art der Ermittlung variieren können. Finanzermittlungen, insbesondere solche, die sich auf Geldwäsche und Menschenhandel konzentrieren, erfordern spezielle Instrumente, die sich von denen unterscheiden, die bei Einsätzen vor Ort zum Einsatz kommen. Angesichts der Komplexität der Rückverfolgung von Finanzströmen müssen Ermittler mit angemessenen Ressourcen ausgestattet sein, um Transaktionen effizient analysieren, verwandte Fälle miteinander in Verbindung bringen und sich an neue kriminelle Taktiken anpassen zu können.

Die Bereitstellung der erforderlichen Werkzeuge für Ermittler erhöht die Effizienz, verbessert die Qualität der Ermittlungen und erhöht die Wahrscheinlichkeit erfolgreicher Festnahmen und Verurteilungen. Zu den wichtigsten Ressourcen gehören:

- **Digitale Fallverwaltungssysteme:** Eine zentralisierte Datenbank zur Speicherung von Fallnotizen und Beweismitteln ermöglicht eine bessere Fallverfolgung und die Verknüpfung von Ermittlungen.
- **Uneingeschränkter Internetzugang:** Ermittler benötigen möglicherweise Zugang zu eingeschränkten Websites, wie z.B. Plattformen mit nicht jugendfreien Inhalten, wenn sie Menschenhandelsaktivitäten verfolgen, vorausgesetzt, sie erhalten eine angemessene Schulung, um Missbrauch zu verhindern.
- **OSINT-Schulung:** Eine spezielle Schulung für Online-Ermittlungen hilft dabei, wichtige Informationen aufzudecken und die Identität der Ermittler zu schützen.
- **Zugriff auf interne Daten:** Die sofortige Verfügbarkeit relevanter institutioneller Daten, wie Transaktionsaufzeichnungen oder frühere Fallakten, ist von entscheidender Bedeutung. Die Überwindung technologischer, rechtlicher und bürokratischer Hindernisse beim Datenzugriff verbessert die Effizienz der Ermittlungen.
- **Fachkundige Rechtsberatung:** Finanzdelikte betreffen häufig die Bereiche Steuern, Wertpapiere und Immobilien, sodass die Hinzuziehung von Spezialisten erforderlich ist. Die frühzeitige Einbindung von Rechts- und Finanzexperten stärkt die Ermittlungsergebnisse.

Der Zugang zu Ressourcen ist zwar von entscheidender Bedeutung, doch müssen Institutionen ein Gleichgewicht zwischen Effizienz und rechtlichen und ethischen Erwägungen finden und sicherstellen, dass Ermittler innerhalb der gesetzlichen Grenzen arbeiten und gleichzeitig ihre Ermittlungsfähigkeiten maximieren.

Schritt 4: Eine der größten Herausforderungen bei Finanzermittlungen im Zusammenhang mit THB ist das Risiko einer falschen Identifizierung von Straftaten – entweder indem eine andere Straftat mit THB verwechselt oder THB-Indikatoren übersehen werden. Dies kann auf mangelnde Rechtskenntnisse oder die sich überschneidenden Merkmale von Straftaten wie Menschenschmuggel oder Arbeitsrechtsverletzungen zurückzuführen sein. Die Unterscheidung dieser Straftaten ist von entscheidender Bedeutung, insbesondere für Ermittler im öffentlichen und privaten Sektor. Private Institutionen sollten auch festlegen, welche Vortaten ihre spezialisierten Teams überprüfen werden, da aufgrund begrenzter Ressourcen nur selten Einheiten existieren, die sich ausschließlich mit THB befassen. Sobald ein grundlegendes Verständnis der THB-bezogenen Gesetze und Ermittlungsaufgaben vorhanden ist, können Ermittler ihren Ansatz für die Bearbeitung von Hinweisen verfeinern. Behörden des öffentlichen Sektors erhalten aufgrund ihres breiteren Aufgabenbereichs in der Regel eine größere Anzahl von THB-bezogenen Hinweisen, während Teams des privaten Sektors möglicherweise weniger Fälle haben, aber mehr Möglichkeiten für proaktive Ermittlungen. Zu den proaktiven Strategien gehören:

- **Überprüfung zuvor abgeschlossener Fälle:** Ältere Fälle, die fälschlicherweise als Prostitution oder Schmuggel eingestuft wurden, können übersehene Hinweise auf Menschenhandel enthalten
- **Durchführung historischer Recherchen in negativen Medien:** Die Überprüfung von Nachrichtenberichten über verdächtige Menschenhändler kann finanzielle Verbindungen oder Muster innerhalb der Konten einer Institution aufdecken
- **Analyse von Verdachtsmeldungen (SARs):** Die Auswertung historischer SAR-Daten kann helfen, übersehene Warnsignale im Zusammenhang mit Menschenhandel zu identifizieren

- **Überwachung von Hochrisiko-Geschäftsbereichen:** Branchen wie Massagesalons, Stripclubs und Pornografie stehen im Zusammenhang mit Menschenhandel und erfordern eine genauere Beobachtung

Effektive finanzielle Ermittlungen erfordern sowohl reaktive als auch proaktive Maßnahmen. Ihr Erfolg hängt jedoch von der Qualität der geteilten Informationen ab – es muss sichergestellt werden, dass gut dokumentierte Verdachtsmeldungen (SARs) die Strafverfolgungsbehörden erreichen und zu sinnvollen Maßnahmen führen.

Schritt 5: Ein klar definierter Untersuchungsumfang ist entscheidend, um zu verhindern, dass Fälle zu groß werden, um sie zu bewältigen, und um zu vermeiden, dass unschuldige Personen fälschlicherweise mit kriminellen Aktivitäten in Verbindung gebracht werden. Bei THB-Ermittlungen nutzen Menschenhändler häufig die Bankkonten ihrer Opfer zu ihrem persönlichen Vorteil, weshalb es für Organisationen unerlässlich ist, Richtlinien zu haben, die eine weitere Viktimisierung verhindern. Die **klare Unterscheidung zwischen Menschenhändlern und Opfern hat Priorität, gefolgt von der Identifizierung der Haupttäter vor den sekundären Mittätern**. Dieser risikobasierte Ansatz optimiert die Ressourcen und gewährleistet die Effizienz der Ermittlungen.

Um den Umfang einer Untersuchung genau zu bestimmen, muss sie von Anfang an so umfassend wie möglich sein. Das von Peter Warrack entwickelte 360-Modell beispielsweise bietet eine strukturierte Methode zur Bewertung finanzieller Aktivitäten auf potenzielle Geldwäsche und kann sowohl in privaten Finanzinstituten als auch bei Strafverfolgungsbehörden angewendet werden. Das Modell besteht aus sechs Schritten:

1. **Auslösendes Ereignis** – Die Untersuchung beginnt mit einer Warnmeldung, z.B. einer SAR, einer automatisierten Transaktionsüberwachungsmarkierung,

negativen Medienberichten, einer internen Weiterleitung oder einer Anfrage einer Strafverfolgungsbehörde.

2. **Den Kunden verstehen** – Die Ermittler sammeln Hintergrundinformationen über die Person, darunter Angaben zu ihrer Beschäftigung, ihrer finanziellen Situation und ihrem allgemeinen Profil.
3. **Finanzielle Aktivitäten verstehen** – Das Finanzverhalten des Kunden wird anhand seines bekannten Hintergrunds bewertet, um festzustellen, ob es den Erwartungen entspricht.
4. **Die Norm eliminieren** – Transaktionen, die für den Kunden normal erscheinen, werden herausgefiltert, sodass sich die Ermittler auf wirklich verdächtige Aktivitäten konzentrieren können.
5. **Analyse der verbleibenden finanziellen Aktivitäten** – Die Untersuchung konzentriert sich auf die Aktivitäten, die den ursprünglichen Verdacht ausgelöst haben, und analysiert Muster und mögliche Verbindungen zu illegalen Handlungen.
6. **Meldung und Erwägung einer Veräußerung** – Wenn die Untersuchung den Verdacht bestätigt, wird eine SAR bei der lokalen FIU eingereicht, und in Fällen, die die Strafverfolgung betreffen, kann ein Haftbefehl beantragt werden.

Dieser strukturierte Ansatz stellt sicher, dass die Ermittlungsressourcen auf legitime Bedrohungen konzentriert werden, wodurch Fehlalarme minimiert und die Gesamteffektivität erhöht werden.

Schritt 6: Um zu verstehen, was im Zusammenhang mit Menschenhandel verdächtige Finanzaktivitäten sind, braucht man sowohl allgemeine Kenntnisse über

Bankgeschäfte als auch ein tiefes Verständnis der Methoden von Menschenhändlern. Während grundlegende Bankkenntnisse relativ leicht zu erwerben sind, erfordert das Erkennen von Unregelmäßigkeiten oft den Zugang zu umfangreichen Daten und praktische Ermittlungserfahrung. Angesichts der umfangreichen Dokumentation über das Finanzverhalten von Menschenhändlern kann jedoch Forschung einen Mangel an direkter Erfahrung ausgleichen.

Auf Makroebene lassen sich Indikatoren für Menschenhandel in drei Kategorien einteilen:

1. **Verhaltensindikatoren** – Dazu gehören persönliche visuelle Hinweise, die darauf hindeuten können, dass eine Person Opfer von Menschenhandel ist oder dass jemand Menschenhändler ist.
2. **Know-Your-Customer-Indikatoren (KYC)** – Warnsignale, die auf von Kunden bereitgestellten Informationen basieren, wie z.B. Unstimmigkeiten bei der Identifizierung oder bei Adressen.
3. **Transaktionsindikatoren** – Verdächtige Finanzmuster, die jederzeit nach der Eröffnung eines Kontos auftreten können, oft ohne persönliche Interaktion, insbesondere mit dem Aufkommen des digitalen Bankwesens.

Diese Indikatoren können einzeln oder in Kombination auftreten und von verschiedenen Teams innerhalb einer Organisation erkannt werden – von Mitarbeitern mit Kundenkontakt, die Verhaltensauffälligkeiten feststellen, von Datenerfassungsteams, die KYC-Warnsignale erkennen, und von Transaktionsüberwachungsteams, die finanzielle Anomalien feststellen. Eine klare Kommunikation und Eskalationsprotokolle sind unerlässlich, um sicherzustellen, dass potenziell verdächtige Aktivitäten gründlich untersucht werden. Die Einteilung der Indikatoren in diese drei Kategorien entspricht den

von Thomson Reuters und der Banks Alliance in Europa, Asien und den Vereinigten Staaten entwickelten Rahmenwerken. Ihre Toolkits bieten zusätzliche Einblicke, darunter die relative Aussagekraft jedes Indikators und dessen Zusammenhang mit bestimmten Formen von THB, wie z.B. Arbeitsausbeutung.

Es ist wichtig zu erkennen, dass einige Indikatoren, wie z.B. häufige Apothekenkäufe, für sich genommen möglicherweise nicht verdächtig sind. Daher müssen Analysten mehrere Faktoren zusammen betrachten, um einen begründeten Verdacht zu begründen. Dies steht im Einklang mit den Leitlinien von Finanzermittlungsbehörden, darunter:

- **FINTRAC** (Kanada, 2016): „Eine einzelne Transaktion, die isoliert betrachtet wird, kann zu einer falschen Annahme der Normalität führen. Die Berücksichtigung aller Indikatoren kann unbekannte Zusammenhänge aufdecken, die zusammengenommen zu einem begründeten Verdacht auf Menschenhandel führen können."
- **FinCEN** (USA, 2014): „Keine einzelne Transaktion ist ein eindeutiger Indikator für Menschenschmuggel oder Menschenhandel. Zusätzliche Faktoren, wie die zu erwartende finanzielle Aktivität eines Kunden, sollten ebenfalls berücksichtigt werden."

Sowohl FINTRAC als auch FinCEN betonen die Bedeutung eines strukturierten Untersuchungsansatzes, wie beispielsweise des 360-Modells von Warrack, um sicherzustellen, dass finanzielle Warnsignale im Kontext und nicht isoliert bewertet werden. Eine umfassende Liste der zusammengefassten Indikatoren finden Sie in den Anhängen des Kompendiums der Ressourcen und der Schritt-für-Schritt-Anleitung für Finanzermittlungen im Zusammenhang mit Menschenhandel der OSZE (OSZE, 2019).

Schritt 7: **SARs** spielen eine entscheidende Rolle bei Finanzermittlungen sowohl im öffentlichen als auch im privaten Sektor. Traditionell markiert ein SAR das Ende der Ermittlungen einer privaten Institution, in der Regel eines Finanzinstituts wie einer Bank, die den Bericht dann an ihre FIU weiterleitet. Auf öffentlicher Seite kann ein SAR den Beginn einer strafrechtlichen Ermittlung auslösen. Um ihr Potenzial voll auszuschöpfen, sollten SARs jedoch als wertvolle Instrumente während des gesamten Ermittlungsprozesses betrachtet werden und nicht nur als letzter Schritt oder Auslöser für öffentliche Ermittlungen. Sie können in verschiedenen Phasen nützliche Informationen liefern, indem sie entweder zu laufenden Ermittlungen beitragen oder einen Kontext für interne Ermittlungen innerhalb privater Institutionen bieten.

Im **privaten Sektor** wird empfohlen, technische Lösungen einzusetzen, um den Verwaltungsaufwand für die Eingabe von Routinedaten zu verringern, damit sich die Ermittler auf die detaillierten Aspekte verdächtiger Aktivitäten konzentrieren können. Darüber hinaus sollten Daten aus früheren Verdachtsmeldungen leicht zugänglich sein, um Muster zu erkennen, einzigartige Straftaten aufzudecken und beteiligte Unternehmen zu verfolgen. SARs sollten auch auf frühere Meldungen zum selben kriminellen Netzwerk verweisen, um ein zusammenhängendes Bild zu erstellen und doppelte Meldungen zu vermeiden. Für meldende Institutionen ist es wichtig, die von den nationalen FIUs festgelegten Namenskonventionen zu befolgen, insbesondere bei hochkarätigen Straftaten wie THB. Die Einhaltung dieser Konventionen trägt dazu bei, die Einhaltung der regulatorischen Anforderungen sicherzustellen, die Glaubwürdigkeit der Meldungen der Institution zu erhöhen und Trends bei Finanzkriminalität zu erkennen. Beispielsweise empfiehlt die US-Behörde FinCEN, SARs im Zusammenhang mit Menschenhandel als „Advisory Human Trafficking" zu kennzeichnen, während die kanadische FINTRAC die Verwendung der Bezeichnung „Project Protect" vorschlägt. Institutionen, die nicht über

solche Kodierungssysteme verfügen, könnten öffentlich-private Partnerschaften in Betracht ziehen, um diese zu implementieren.

Im **öffentlichen Sektor** wird empfohlen, die SAR-Datenbanken der FIUs für alle Ermittlungen im Bereich des Menschenhandels zu nutzen, da diese Straftat in der Regel mit finanziellen Vorteilen verbunden ist. Strafverfolgungsbehörden sollten auch Instrumente wie Produktionsanordnungen und Durchsuchungsbefehle einsetzen, um Banken und andere meldepflichtige Stellen zu ermutigen, SARs im Zusammenhang mit laufenden Ermittlungen einzureichen. Trotz ihrer Bedeutung werden SARs wegen einer zunehmenden Anzahl von Meldungen geringer Qualität kritisiert. So wurde beispielsweise in einem Bericht der OSZE aus dem Jahr 2014 hervorgehoben, dass in Italien nur 23 von 37.000 SARs als nützlich für strafrechtliche Ermittlungen angesehen wurden. Eine britische Rechtsreformkommission äußerte 2019 ähnliche Bedenken und wies auf die Notwendigkeit hin, die SAR-Berichterstattung zu verbessern, um die Zahl der Meldungen von schlechter Qualität zu reduzieren. Durch die Umsetzung einiger der genannten Empfehlungen, wie z.B. die Bezugnahme auf historische SARs, kann die Qualität künftiger Berichte verbessert werden.

Schritt 8: Nach Abschluss einer Untersuchung in einer privaten Einrichtung wie einer Bank muss entschieden werden, ob die Beziehung zu dem untersuchten Kunden fortgesetzt werden soll. Dieser als „**De-Risking**“ bezeichnete Prozess beinhaltet gegebenenfalls die Beendigung der Beziehung. Es ist wichtig, zwischen Opfer und Täter zu unterscheiden, um eine ungerechtfertigte Bestrafung des Opfers zu vermeiden, insbesondere in Fällen wie Menschenhandel. Wenn ein Konto einem Opfer von Menschenhandel gehört, sollten Anstrengungen unternommen werden, um die Geschäftsbeziehung aufrechtzuerhalten, es sei denn, es liegen mehrere Verstöße oder

Mittäterschaft vor. De-Risking sollte mit Vorsicht angegangen werden, da die Verdrängung verdächtiger Aktivitäten in illegale Märkte die Ermittlungen der Strafverfolgungsbehörden erschweren kann. In einigen Rechtsordnungen können Strafverfolgungsbehörden verlangen, dass Bankkonten offen gehalten werden, um Ermittlungen nicht zu behindern. Wenn eine Risikominderung erforderlich wird, sollten Standardnachrichten verwendet werden, um falsche Anschuldigungen zu vermeiden, und es sollten Aufzeichnungen über zuvor risikominderte Unternehmen für zukünftige Referenzzwecke aufbewahrt werden.

Schritt 9: Die Identifizierung tatsächlicher Fälle von Menschenhandel, die ausschließlich auf Finanztransaktionen basieren, ist aufgrund fehlender Kontextinformationen schwierig. Darüber hinaus hat es Einfluss auf die Wahrscheinlichkeit, schlüssige Fälle von Menschenhandel aufzudecken, ob die Ermittler in einer öffentlichen Einrichtung oder einer privaten Organisation tätig sind. Private Organisationen, wie beispielsweise Finanzdienstleister, sind nicht verpflichtet, vor der Einreichung einer Verdachtsmeldung bei einer FIU zweifelsfrei nachzuweisen, dass eine Vortat begangen wurde. Die Meldeschwelle ist oft niedrig, da Finanzinstitute nur einen Teil des Gesamtbildes sehen können. Darüber hinaus geben FIUs in der Regel kein Feedback darüber, ob Verdachtsmeldungen zu bestätigten Vortaten führen, was es für den privaten Sektor schwieriger macht, THB-bezogene Aktivitäten zu validieren.

Da Transparenz über die Ergebnisse von Finanzermittlungen zu THB nicht immer möglich ist, sollten nachgewiesene Fälle für Schulungen und die zukünftige Risikominderung herangezogen werden. Finanzdienstleister können nachgewiesene Fälle von THB identifizieren, indem sie:

- Überprüfung der täglichen negativen Medienberichte auf Verbindungen zu internen Ermittlungen.
- Abonnement von Updates von Strafverfolgungsbehörden oder FIUs zu THB-Durchsetzungsmaßnahmen und Abgleich mit internen Fällen.
- Einrichtung eines direkten Überweisungskanals für Strafverfolgungsbehörden im Zusammenhang mit THB-Ermittlungen.

Es wird empfohlen, Informationen aus nachgewiesenen THB-Fällen nicht nur mit der spezialisierten THB-Einheit, sondern mit dem gesamten Ermittlungsteam zu teilen. Dies steht im Einklang mit den Leitlinien in Schritt 1 (Zentralisierung der Aufsicht) und kann die Moral der Ermittler stärken, ein Gefühl der Sinnhaftigkeit schaffen und die Chancen für die Zuweisung von Ressourcen oder die Zusammenarbeit zwischen den Teams verbessern.

Schritt 10: In den letzten Jahren haben **öffentliche/private Partnerschaften (PPPs) bei der Bekämpfung von Finanzkriminalität**, insbesondere Menschenhandel in der Wirtschaft, **erheblich an Bedeutung und Verbreitung gewonnen**. Globale Bemühungen zur Bekämpfung des Menschenhandels haben zu einer verstärkten Zusammenarbeit zwischen Wettbewerbern der Branche geführt, um Finanzkriminalität zu bekämpfen. Fachleute für die Bekämpfung von Finanzkriminalität haben erkannt, dass Menschenhändler zwischen verschiedenen Institutionen und Banken wechseln, was zu einer Zusammenarbeit bei der Bekämpfung dieser Probleme geführt hat. Zu den führenden ÖPP gehören die Joint Money Laundering Intelligence Taskforce (JMLIT) im Vereinigten Königreich, die Fintel Alliance in Australien und das Project Protect in Kanada. Auch die USA verfügen über Mechanismen wie den US: PATRIOT Act 314(a) für den Informationsaustausch.

Zu den Anreizen für die Teilnahme an PPPs gehören der Zugang zu verschiedenen Ansätzen bei Finanzermittlungen, die schnellere Entwicklung von THB-Indikatoren, der Aufbau engerer Beziehungen zu Kollegen und Strafverfolgungsbehörden, verbesserte Ermittlungen, gemeinsame Nutzung von Ressourcen und das Engagement für das soziale Wohl. Die OSZE erkennt jedoch die Herausforderungen bei der Einrichtung einer wirksamen Zusammenarbeit zwischen FIUs, Strafverfolgungsbehörden und Stellen, die STRs einreichen, an. Eine dieser Herausforderungen ist der einseitige Informationsfluss von FIUs, der oft ihre Fähigkeit einschränkt, Informationen außerhalb ihrer Organisation weiterzugeben. Feedback zu hochwertigen Verdachtsmeldungen könnte die Ausbildung, die Ermittlungsmethoden und die Qualität der Verdachtsmeldungen verbessern.

Das Fehlen von Rückmeldungen seitens der FIUs und das Fehlen internationaler Datenbanken zu THB-Straftätern unterstreichen die Notwendigkeit von PPPs. Die Schaffung einer PPP erfordert nicht immer neue Gesetze; bestehende rechtliche Rahmenbedingungen können genutzt werden. So wurde beispielsweise das Projekt „Project Protect" in Kanada erfolgreich innerhalb des rechtlichen Rahmens der nationalen Regierung durchgeführt, wobei der Schwerpunkt auf allgemeinen Typologien und Indikatoren lag und gleichzeitig die Datenschutzgesetze eingehalten wurden. Es ist von entscheidender Bedeutung, die rechtlichen Grenzen zu kennen und innerhalb dieser Grenzen zu arbeiten, um die Zusammenarbeit zu fördern. Zu den langfristigen Zielen von PPPs kann die Förderung von Gesetzesänderungen auf der Grundlage erfolgreicher Kooperationen gehören. Die Gründung oder Teilnahme an einer PPP sollte nach der Einrichtung eines soliden Ermittlungsprozesses erfolgen, aber eine frühzeitige Zusammenarbeit ist wertvoll. Sie kann Erkenntnisse liefern, die den Ermittlungsprozess in einer Weise prägen, die nach dessen Einführung nur schwer zu erreichen wäre. Die

Teilnahme an einer PPP verbessert die Vollständigkeit des Ansatzes zur Ermittlung von Menschenhandel.

Schritt 11: Ermittlungen zu THB, insbesondere im Bankensektor, können sich negativ auf Überlebende auswirken. Dies unterstreicht die Bedeutung von Schritt 4 (Bewertung der Ermittlungen zu THB-Aktivitäten), der sicherstellt, dass Aktivitäten im Zusammenhang mit THB auf Team- oder institutioneller Ebene klar definiert sind. Die ordnungsgemäße Durchführung von Schritt 4 kann dazu beitragen, unnötige Arbeit später zu reduzieren, indem sichergestellt wird, dass unschuldige Personen nicht zu Unrecht ausgeschlossen werden. Da Menschenhändler häufig die finanzielle Situation ihrer Opfer manipulieren, wird empfohlen, Überlebenden, die dem Menschenhandel entkommen sind, die Möglichkeit zu geben, ihr finanzielles Profil wieder aufzubauen.

Ein erfolgreiches Beispiel für die Unterstützung von Überlebenden von Menschenhandel ist ein Programm, das HSBC im Juni 2019 in Großbritannien ins Leben gerufen hat. Dieses Programm hilft Überlebenden, die vom britischen National Referral Mechanism (Nationales Verweisungsmechanismus) überwiesen werden, bei Herausforderungen wie der Vorlage von Adress- und Identitätsnachweisen. Darüber hinaus hat die Blueprint for Mobilizing Finance Against Slavery and Trafficking (Blaupause zur Mobilisierung von Finanzmitteln gegen Sklaverei und Menschenhandel) der Lichtenstein Initiative, die in Zusammenarbeit mit der Universität der Vereinten Nationen und verschiedenen Regierungen erstellt wurde, mehrere Finanzinstitute zusammengebracht, um die Bemühungen der HSBC auf verschiedene Institutionen und Gerichtsbarkeiten auszuweiten. Die Scotiabank war in Zusammenarbeit mit dem Anti-Menschenhandelsprogramm „Deborah's Gate“ der Heilsarmee die erste Bank, die im Rahmen dieser Initiative zur finanziellen Inklusion Konten für Überlebende eröffnete. Es

wird erwartet, dass andere teilnehmende Finanzinstitute diesem Beispiel folgen und ähnliche Programme entwickeln werden.

Da die Aufmerksamkeit und die Bemühungen weiterhin auf diejenigen gerichtet sind, die Menschenhandel ermöglichen, ist es wichtig, **die Opfer nicht aus den Augen zu verlieren**. Öffentlich-private Partnerschaften und die Zusammenarbeit mit zwischenstaatlichen Gruppen können einen umfassenden Ansatz zur Bekämpfung des Menschenhandels schaffen, von dem nicht nur die beteiligten Institutionen, sondern auch die Opfer profitieren, oft mit minimalen Kosten für die Umsetzung.

9.5.4 Identifizierung verdächtiger Finanzaktivitäten

Die OSZE hat eine **Liste mit finanziellen Transaktionsindikatoren und sogenannten „Red Flags" veröffentlicht, die für Menschenhandel und insbesondere für Arbeitsausbeutung gelten**. Die folgende Liste wurde dem OSZE-Bericht entnommen, wobei drei offensichtlich spezifische Indikatoren für Organentnahme sowie sieben für sexuelle Ausbeutung entfernt wurden, um sie besser auf Arbeitsausbeutung abzustimmen, auch wenn die Indikatoren in besonderen Fällen variieren und sich überschneiden können (OSZE, 2019, S. 61ff).

- Nutzung von Strohmännern für Geschäftskonten
- Nichtzahlung von Steuern, Arbeitnehmerentschädigungen und anderen Gebühren an eine Steuerbehörde
- Der Lohnsatz für jeden Zahlungszeitraum ist identisch (keine Änderungen für Überstunden, Urlaub, Krankheitsurlaub, Bonuszahlungen usw.) in Berufen, in denen dies nicht zu erwarten wäre

- Wiederkehrende Zahlungen für Löhne in unangemessen niedriger Höhe (z.B. weit unter dem Mindestlohn)
- Erheblicher Anteil des Unternehmenskapitals in Festgeldanlagen – unverhältnismäßiger Finanzumsatz
- Von einem Anteilseigner an die verbundene juristische Person gewährte Darlehen und anschließende Rückübertragung, fiktives Darlehen
- Strukturierung über gewerbliche Unternehmen und Geldtransfer unter Verwendung eines Darlehensvertrags
- Übermäßige Mitfahrgelegenheiten nach Mitternacht
- Fehlende Lebenshaltungskosten wie Lebensmittel, Benzin, Nebenkosten und Miete
- Restaurantbesuche und Zimmerservice, keine Zimmer
- Einsatz mehrerer Personen zur Durchführung von Bankgeschäften
- Hohe und/oder häufige Ausgaben an Flughäfen, Häfen, anderen Verkehrsknotenpunkten oder im Ausland, die nicht mit dem persönlichen Gebrauch oder der angegebenen Geschäftstätigkeit im Ausland vereinbar sind
- Bareinzahlungen in verschiedenen Städten des Landes
- Zahlungen an Arbeitsvermittlungs- oder Studentenvermittlungsagenturen, die nicht lizenziert/registriert sind oder gegen Arbeitsgesetze verstoßen
- Relativ hohe Ausgaben für Gegenstände, die nicht mit dem angegebenen Geschäftszweck vereinbar sind
- Transaktionen, die außerhalb der bekannten Geschäftszeiten stattfinden

- Grenzüberschreitende Geldtransfers, die nicht mit dem angegebenen Geschäftszweck des Kontoinhabers vereinbar sind, und/oder zwischen ungeklärten Mustern grenzüberschreitender Transaktionen zwischen bekannten Handelsrouten oder Gebieten, in denen ein höheres Risiko für Menschenhandel besteht
- Umfassende Verwendung von Bargeld, auch für den Kauf von Unternehmensvermögen
- Inländische Überweisungen von Unternehmen, die in Bereichen tätig sind, die für Sozialbetrug anfällig sind, wobei das Geld unmittelbar danach in bar abgehoben wird
- Nutzung von Institutionen, die nicht zum Finanzsystem gehören (nicht traditionell)
- Nutzung von Bargeldkurieren und wiederholte Bargeldabhebungen
- Kauf von Bankschecks, die unmittelbar nach der Einzahlung an ein Casino zahlbar sind
- Unerklärliche/ungerechtfertigte hohe Gewinne für ein Unternehmen
- Bareinzahlungen, die oft knapp unter der Meldepflichtgrenze liegen
- Bareinzahlungen in mehreren Filialen oder an mehreren Geldautomaten
- Kauf von Zahlungsanweisungen zur Begleichung von Rechnungen anstelle der Ausstellung persönlicher Schecks
- Geschäftskonten mit offensichtlichen Abzügen von Arbeitnehmerlöhnen unter verschiedenen Kostenarten wie Unterkunft und Verpflegung
- Einlösbare Gehaltsschecks, bei denen der Großteil der Gelder entweder wieder auf das Konto des Arbeitgebers eingezahlt oder vom Arbeitgeber einbehalten wird

- Überweisender oder Begünstigter mit unvollständigen Angaben
- Kauf von Bankschecks, die unmittelbar nach der Einzahlung an ein Casino zahlbar sind
- Überweisungen aus verschiedenen Regionen an dieselben Personen in Ländern, die als besonders anfällig für Menschenhandel gelten.
- Einzahlung von staatlichen Beihilfen auf das Konto, obwohl der Kontoinhaber möglicherweise über beträchtliche Geldbeträge verfügt
- Elektronische Überweisungen/Überweisungen können ebenfalls strukturiert sein
- Vermischung von Bargeld mit legitimen Einkommensquellen
- Veredelungsaktivitäten (Umtausch von Banknoten mit kleinem Nennwert in Banknoten mit größerem Nennwert)
- Häufige Käufe in Vielfachen kleiner Beträge von Bitcoin oder virtuellen Währungen, direkt durch den Kunden oder über Börsen
- Geldtransfers unter Beteiligung Dritter mit alternativen Namen in Klammern
- Das Konto erhält Lohnzahlungen von legitimen, oft landesweit tätigen Personalagenturen, aber die Gelder bleiben dann über lange Zeiträume unberührt
- Fast-Food-Restaurants: häufige Käufe von geringem Wert in relativ kurzer Zeit und nicht im Einklang mit der zu erwartenden Aktivität
- Das Konto scheint als Trichterkonto zu fungieren

Die folgende Fallstudie von Francavilla Lyon & De Cock (2024) veranschaulicht, wie Finanztransaktionsmuster als Indikatoren für potenzielle Arbeitsausbeutung im Gastgewerbe dienen können. Dieses Beispiel unterstreicht die entscheidende Rolle der

Finanzanalyse bei der Identifizierung von Risiken des Menschenhandels und der Aufdeckung verdeckter Formen moderner Sklaverei:

Ausgangssituation: Ein chinesischer Staatsbürger eröffnet ein Privatkonto und gibt an, dass er im Restaurant X arbeitet. Die Analyse der Geschäftsbeziehung zeigt, dass die Adresse dieser Person und die Adresse des Restaurants X identisch sind. Ein Teil der eingehenden Gehaltszahlungen wird wieder in bar abgehoben oder an Dritte (ohne offensichtliche familiäre Verbindung) überwiesen. Die Gehaltszahlungen erfolgen unregelmäßig und in unterschiedlicher Höhe. Während eines Gesprächs zwischen der Bank und dem Kunden teilte dieser der Bank mit, dass es sich bei den Auslandsüberweisungen um Unterhaltszahlungen an seine Ex-Frau und für deren Kinder handele. Laut KYC hat der Kunde jedoch keine Kinder. Außerdem hat der Kunde laut seinem Arbeitsvertrag eine Festanstellung mit festem Gehalt und arbeitet nicht auf Stundenlohnbasis. Erwartete alltägliche Ausgaben (Lebensmittel, Miete, Versicherungen usw.) fehlen.

Die Indikatoren in diesem Szenario sind:

- Risikoländer (Kunde)
- Risikosektor für Arbeitsausbeutung
- Durchlaufende Transaktionen
- Bargeldtransaktionen
- Fehlen der zu erwartenden täglichen Ausgaben
- Private Adresse identisch mit Arbeitsadresse
- Widersprüchliche Angaben des Kunden

9.5.5 Herausforderungen bei Finanzermittlungen

Eine große Herausforderung bei Finanzermittlungen ist die sich ständig weiterentwickelnde Natur der **Verschleierungstechniken**, die Kriminelle einsetzen, um finanzielle Spuren zu verwischen. Techniken wie **Mixing-Dienste, Chain-Hopping** und die Verwendung von datenschutzorientierten **Kryptowährungen** stellen Ermittler vor erhebliche Hindernisse. Mixing-Dienste, auch als Tumblers bekannt, ermöglichen es Nutzern beispielsweise, die Herkunft ihrer Gelder zu verschleiern, indem sie diese bündeln und neu verteilen. Chain-Hopping beinhaltet die schnelle Umwandlung von Kryptowährungen zwischen verschiedenen Plattformen, wodurch es schwieriger wird, die Bewegung von Geldern zu verfolgen. Darüber hinaus bieten Privacy Coins wie Monero und Zcash verbesserte Anonymitätsfunktionen, was die Strafverfolgung weiter erschwert.

Um diesen Herausforderungen zu begegnen, stützen sich Finanzermittler zunehmend auf die **Zusammenarbeit mit Experten für digitale Forensik**. Die digitale Forensik ermöglicht es Ermittlern, elektronische Beweise wie verschlüsselte Kommunikation, IP-Adressen und Transaktionsmetadaten zu extrahieren und zu analysieren. Dieser interdisziplinäre Ansatz ist entscheidend, um versteckte Finanznetzwerke aufzudecken und illegale Finanzströme über Grenzen hinweg zu verfolgen. Angesichts des transnationalen Charakters von Finanzkriminalität ist die Zusammenarbeit zwischen Finanzinstituten, Aufsichtsbehörden und internationalen Organisationen für eine effektive Finanzermittlung unerlässlich. „Innovative Methoden des Geldtransfers in Verbindung mit der wachsenden Erkenntnis unter Fachleuten für Finanzkriminalität, dass Menschenhändler von Institution zu Institution und von Bank zu Bank wechseln, hat sie zur Zusammenarbeit veranlasst.“ (OSZE, 2019, S. 43).

9.5.6 Technologische Entwicklungen und Trends

Die jüngsten technologischen Entwicklungen haben die Finanzkriminalität erheblich beeinflusst, indem sie neue Methoden für illegale Aktivitäten hervorgebracht und gleichzeitig verbesserte Instrumente für Finanzermittlungen bereitgestellt haben. Der Aufstieg von Kryptowährungen und Blockchain-Technologie hat beispielsweise verschiedene Formen der Finanzkriminalität begünstigt, darunter Geldwäsche, Betrug und sogar Menschenhandel. Die zunehmende Nutzung **digitaler Vermögenswerte** ermöglicht es Kriminellen, Gelder grenzüberschreitend mit größerer Anonymität zu bewegen und dabei traditionelle Finanzinstitute und behördliche Kontrollen zu umgehen. Während **Bitcoin** nach wie vor die bekannteste Kryptowährung ist, gibt es eine zunehmende Verlagerung hin zu Alternativen mit stärkerem Fokus auf Datenschutz wie **Monero und Zcash**, was die Strafverfolgung weiter erschwert.

Ein wichtiger Trend ist der Einsatz von **Verschleierungstechniken**, die speziell für digitale Vermögenswerte entwickelt wurden. Kriminelle setzen zunehmend auf Tools wie **Mixer, Tumbler und Privacy Wallets**, um Transaktionsspuren zu verschleiern und einer Aufdeckung zu entgehen. Diese Methoden erschweren es den Behörden, illegale Finanzströme zu verfolgen, insbesondere in Fällen von Menschenhandel, in denen die Täter digitale Währungen nutzen, um Zahlungen einzuziehen und Erlöse zu waschen. Die Dezentralität und Pseudonymität von Blockchain-basierten Transaktionen hat ein Umfeld geschaffen, in dem Finanzkriminalität florieren kann, sofern sie nicht durch fortschrittliche Ermittlungsmethoden bekämpft wird.

Gleichzeitig werden Finanzkriminelle immer **selbstständiger** und machen sich zunehmend unabhängig von externen Sponsoren oder Vermittlern. Dieser Trend zeigt sich deutlich in der Zunahme von Cyberbetrug, Ransomware-Angriffen und Online-Betrug,

durch die Gelder für organisierte kriminelle Netzwerke, darunter auch solche, die sich mit Menschenhandel befassen, generiert werden. Die zunehmende Nutzung betrügerischer Online-Marktplätze, gefälschter Spendenkampagnen und irreführender E-Commerce-Plattformen hat die Möglichkeiten für Finanzkriminalität weiter erweitert.

Trotz dieser Herausforderungen bieten technologische Fortschritte auch neue Instrumente zur Bekämpfung von Finanzkriminalität. **Blockchain-Analysen und KI** spielen eine entscheidende Rolle bei Finanzermittlungen und helfen den Behörden dabei, illegale Transaktionen aufzuspüren und verdächtige Muster zu identifizieren. KI-gestützte Transaktionsüberwachungssysteme können riesige Datenmengen in Echtzeit analysieren und Anomalien markieren, die auf Geldwäsche oder Aktivitäten im Zusammenhang mit Menschenhandel hindeuten könnten. Darüber hinaus ermöglichen Blockchain-Forensik-Tools den Ermittlern, Bewegungen von Kryptowährungen zu verfolgen und versteckte Verbindungen zwischen kriminellen Organisationen aufzudecken.

9.5.7 Empfehlungen

Ein solider Rechtsrahmen für die Verfolgung von Finanzdelikten ist notwendig, um wirksame Finanzermittlungen zu gewährleisten. Internationale Standards, beispielsweise die Empfehlungen der **Financial Action Task Force (FATF)**, bilden die Grundlage für Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Diese Vorschriften verlangen von den Strafverfolgungsbehörden, Finanzermittlungen durchzuführen, die grenzüberschreitende Zusammenarbeit zu erleichtern und Verfahren zur Einziehung von Vermögenswerten durchzusetzen. In der FATF-Empfehlung 30 wird beispielsweise betont, wie wichtig es ist, zuständige Behörden zu benennen, die befugt

sind, Straftaten im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung zu untersuchen.

Aufgrund des Krieges in der Ukraine sind Vertriebene einem erhöhten Risiko von Menschenhandel ausgesetzt. Als Reaktion auf diese erhöhte Gefährdung haben Organisationen wie die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) gezielte Ressourcen zur Unterstützung von Ersthelfern entwickelt. So bietet die OSZE beispielsweise ein Kompendium mit Schulungskursen zur Bekämpfung des Menschenhandels für Ersthelfer an, das spezielle Schulungen zu verschiedenen Aspekten der Bekämpfung des Menschenhandels umfasst. Darunter befinden sich auch spezielle Kurse mit Schwerpunkt auf Finanzermittlungen, in denen Fachleute mit den notwendigen Instrumenten ausgestattet werden, um illegale Finanzströme im Zusammenhang mit Menschenhandel zu identifizieren und zu bekämpfen. Link zur Kursübersicht: https://www.osce.org/cthb/562572.

9.6 Vorgeschlagene Aktivität des Kapitels

Tabelle 1. Aktivitäten im Bereich digitale Forensik und Finanzermittlungen

Activity Name	Aktivität für digitale Forensik
Art der Aktivität	Gruppenarbeit (z.B. Gruppen von 3 bis 6 Personen)
Dauer	15-35 min
Lernziele	Identifizierung wichtiger digitaler Spuren und nächste Schritte
Benötigte Materialien	Fallbeispiel mit ausreichendem Hintergrund (z.B. gedruckte Version) • Thomas, Day & Jackson (2019) on pp. 31-38 and pp. 38 – 42 at https://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Crates (2022) on pp. 9-14 at https://www.antislaverycommissioner.co.uk/media/h4ggz4c2/iasc-construction-report-april-2022.pdf

	• U.S. Department of Labour Blog (2022) at https://blog.dol.gov/2022/01/11/fighting-human-trafficking-the-legacy-of-the-el-monte-sweatshop • Lam & Skivankova (2009) on p. 5 at https://www.antislavery.org/wp-content/uploads/2017/01/trafficking_and_compensation2009.pdf • KOK German NGO Network against Trafficking in Human Beings (n.d.) at https://www.kok-gegen-menschenhandel.de/menschenhandel/was-ist-menschenhandel/fallbeispiele (*Unterabschnitt „Menschenhandel zum Zwecke der Arbeitsausbeutung“)* • Schulungskapitel 8
Leitfaden für die Moderation	Die Teilnehmer werden in kleinere Gruppen aufgeteilt. Sie erhalten eine Fallstudie, die sie lesen werden (3-4 Min.). Anschließend beginnen sie in ihrer Gruppe zu diskutieren und versuchen herauszufinden, welche digitalen Beweise für eine erfolgreiche digitale Forensik am besten geeignet sind. Darüber hinaus diskutieren sie, welche Akteure zu welchem Zeitpunkt des Ermittlungsprozesses beteiligt wären (10-15 Min.). • Welche digitalen Beweise sind relevant? Welche digitalen Beweise sind am nützlichsten und warum?

	• Wie können Forensiker diese digitalen Spuren extrahieren und analysieren? • Wie kann dies dazu beitragen, Opfer, Menschenhändler und Muster zu identifizieren? • Welche Muster oder Warnsignale deuten auf Menschenhandel hin? • Welche nächsten Schritte sollten die Ermittler unternehmen? • Wie können diese Beweise zur Unterstützung der Opfer genutzt werden? Anschließend präsentiert jede Gruppe ihre Ergebnisse (5–10 Min.).
Nach-besprechung	Der Moderator moderiert die Präsentation nach der Gruppenarbeit.
Tipps für die Moderation	Wenn Sie mehr Zeit haben, können Sie verschiedene Fallbeispiele verwenden, und jede Gruppe stellt kurz den Fall und anschließend ihre Diskussionsergebnisse vor (anstatt dass jede Gruppe denselben Fall bearbeitet).
Handouts	*z.B. Fallstudien, die ausgedruckt und den Teilnehmern zur Verfügung gestellt werden sollten, eventuell ergänzt durch Material mit nachgeahmten Auszügen aus:*

	• WhatsApp-Chats zwischen dem Opfer und dem Menschenhändler mit Aussagen wie „Mach dir keine Sorgen um den Papierkram, wir kümmern uns darum“, „Du bekommst kostenlose Unterkunft und Transport“ oder „Triff mich am Busbahnhof. Lösche diese Nachrichten.“ • Anzeigen von der Rekrutierungsplattform • Banküberweisungsbelege • Metadaten aus einem an das Opfer gesendeten Foto mit Geolokalisierungsdaten • …
Varianten für die Online-Implementierung	Online-Durchführung ist möglich, Breakout-Sessions für die Gruppenaufgabe einrichten
Activity Name	**Aktivität für Finanzermittlungen**
Art der Aktivität	Gruppenarbeit (z.B. Gruppen von 3 bis 6 Personen)
Dauer	15-35 min

Lernziele	Die Schritte für Finanzermittlungen verinnerlichen und über mögliche Herausforderungen im Bereich THB nachdenken
Benötigte Materialien	z.B. Fallstudien, die ausgedruckt und den Teilnehmern ausgehändigt werden sollten, eventuell ergänzt durch Material mit nachgeahmten Auszügen aus: Banktransaktionsaufzeichnungen und Kontoauszüge (kann auch nur eine Tabelle mit den Spalten Datum, Beschreibung, Soll (EUR), Haben (EUR) und Saldo (EUR) sein, aus der hervorgeht, wann jemand eine Transaktion durchgeführt hat (+ an welches Unternehmen/welche Person) • Lohnabrechnungen • Rechnungen • …
Leitfaden für die Moderation	Die Teilnehmer werden in kleinere Gruppen aufgeteilt. Sie erhalten eine Fallstudie, die sie lesen werden (3-4 Min.). Anschließend beginnen sie in ihrer Gruppe zu diskutieren und versuchen, die Schritte für Finanzermittlungen zu identifizieren (z.B. indem sie jeden zuvor gelernten Schritt durchgehen). Darüber hinaus diskutieren sie, welche Akteure an welchem Punkt des Ermittlungsprozesses beteiligt wären (10-15 Min.). Welche Finanzermittlungstechniken sollten eingesetzt werden?

	• Wie können Strafverfolgungsbehörden hier mit FIUs zusammenarbeiten? Welche rechtlichen Instrumente sollten angewendet werden? • Welche Herausforderungen lassen sich identifizieren? Anschließend präsentiert jede Gruppe ihre Ergebnisse.
Nach-besprechung	Der Moderator moderiert die Präsentation nach der Gruppenarbeit.
Tipps für die Moderation	Wenn Sie mehr Zeit haben, können Sie verschiedene Fallbeispiele verwenden, und jede Gruppe stellt kurz den Fall und anschließend ihre Diskussionsergebnisse vor (anstatt dass jede Gruppe denselben Fall bearbeitet).
Handouts	*Eine Fallstudie sollte ausgedruckt und den Teilnehmern zur Verfügung gestellt werden.* • Thomas, Day & Jackson (2019) on pp. 31-38 and pp. 38 – 42 at https://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Case Study of Top Glove (Malaysia), details available at https://sevenpillarsinstitute.org/labor-exploitation-case-study-of-top-glove/#:~:text=This%20case%20study%20examines%20the%20allegations%20of%20forced,serves%20as%20the%20home

	%20of%20this%20multinational%20corporation. And Malaysia: Hidden cameras reveal poor working & living conditions at Top Glove factory, fuelling forced labour concerns in glove industry; incl. company comments - Business & Human Rights Resource Centre
Varianten für die Online-Implementierung	Online-Durchführung ist möglich, Breakout-Sessions für die Gruppenaufgabe einrichten

9.7 Referenzen

Aronowitz, Alexis & Theuermann, Gerda & Tyurykanova, Elena. (2010). OSCE. *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime*. https://www.osce.org/files/f/documents/c/f/69028.pdf

Belser, P. (2005). *Forced labour and human trafficking: Estimating the profits*. Geneva: International Labour Office. https://ecommons.cornell.edu/bitstream/1813/99623/1/Forced_labor_no__17_Forced_labour_and_human.pdf

Cellebrite. (2024, November 15). *How Law Enforcement Can Turn the Tide Against Human Trafficking with Digital Evidence*. https://cellebrite.com/en/how-law-enforcement-can-turn-the-tide-against-human-trafficking-with-digital-evidence/

Dubey, H., Bhatt, S., & Negi, L. (2023). *Digital forensics techniques and trends: a review* The International Arab Journal of Information Technology, *20*(4), 644-654.

European Commission. (n.d.). *Financial investigations*. https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/financial-investigations_en

Europol. (2020). *The challenges of countering human trafficking in the digital era*. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

Europol. (2024, July). *Tackling threats, addressing challenges. Europol's response to migrant smuggling and trafficking in human beings in 2023 and onwards*. European Migrant Smuggling Centre (EMSC).

https://www.europol.europa.eu/cms/sites/default/files/documents/Tackling_threats__addressing_challenges_-_Europol%E2%80%99s_response_to_migrant_smuggling_and_trafficking_in_human_beings_in_2023_and_onwards.pdf

Francavilla, F., Lyon, S., & De Cock, M. (2024). *Profits and poverty: The economics of forced labour*. ILO. https://www.ilo.org/sites/default/files/2024-10/Profits%20and%20poverty%20-%20The%20economics%20of%20forced%20labour_WEB_20241017.pdf

Fraser, C. (2016). An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading. *International Journal of Development Issues*, *15*(2), 98-112.

Gorenc, M. (2019). Benford's Law As a Useful Tool to Determine Fraud in Financial Statements. *Management, 14*(1). 19-31. 10.26493/1854-4231.14.19-31.

International Labour Organization. (2018). *Investigating Human Trafficking Cases Using a Victim-centred Approach*. International Organization for Migration. https://publications.iom.int/system/files/pdf/investigating_human_trafficking.pdf

International Labour Organization. (2023, July 30). H*uman Trafficking Evidence Gap Map*. https://rtaproject.org/human-trafficking-egm/#:~:text=The%20Evidence%20Gap%20Maps%20are%20a%20visual%20tool,the%20areas%20where%20evidence%20is%20limited%20or%20non-existent.

Kunz, R., Baughman, M., Yarnell, R., & Williamson, C. (2018). *Social media and sex trafficking process: From connection and recruitment, to sales*. Ohio: University of Toledo. https://www.utoledo.edu/hhs/htsji/pdfs/smr.pdf

Lugo-Graulich, K., Meyer, L. F., Souza, K., Tapp, S. N., Maryfield, B., & Bostwick, L. (2024). Improving sex trafficking victim identification: Indicators of trafficking in Online Escort Ads. *Journal of Human Trafficking*, 1-22.

Maras, M.-H. (2014). *Computer Forensics: Cybercriminals, Laws and* Evidence (2nd edition). Jones and Bartlett.

Mattmann, C., Yan G. H., Manjunatha, H., Gowda N, T., Zhou, A. J., Luo, J., & McGibbney, L. J. (2016). *Multimedia metadata-based forensics in human trafficking web data*. In: Murdock, V., Clarke, C. L. A., Kamps, J. & J. Karlgren. *Search an Exploration of X-rated Information*. p. 10-13.

OSCE. (2019, November 7). *Following the Money: Compendium of Resources and Step-by-Step Guide to Financial Investigations Related to Trafficking in Human Beings*. https://www.osce.org/files/f/documents/f/5/438323_0.pdf

Perez, A. R., & Rivas, P. (2023). Combatting human trafficking in the cyberspace: A natural language processing-based methodology to analyze the language in online advertisements. *arXiv preprint arXiv:2311.13118*.

Pizzuro, J. (2022, March 11). *Leveraging Magnet Forensics Software for Human Trafficking Investigations.* MAGNET FORENSICS. https://www.magnetforensics.com/blog/leveraging-magnet-forensics-software-for-human-trafficking-investigations/

Siavoshi, M. (2025, February 25). *Unraveling the Mystery of Benford's Law: Applications in Fraud Detection*. Statology. https://www.statology.org/unraveling-the-mystery-of-benfords-law-applications-in-fraud-detection/

Thomson Reuters. (2025, January 2). *Technology and human trafficking: Fighting the good fight.* https://legal.thomsonreuters.com/blog/technology-and-human-trafficking/#:~:text=How%20technology%20can%20fight%20human%20trafficking%201%20Prevention,in%20several%20ways%20that%20incorporate%20digital%20technology.%20

UNODC. (2019a, May). *Technology facilitating trafficking in persons*. https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html

UNODC. (2019b, March). *Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics. Handling of digital evidence*. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

UNODC. (2020). *Global report on trafficking in persons 2020*. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

Volodko, A., Cockbain, E., & Kleinberg, B. (2020). 'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers. *Trends in Organized Crime*, *23*, 7-35.

www.eradicating2project.eu

Co-funded by the European Union