Chapter 9. Digital forensics & financial investigations

Unit-responsible partner: BayHfoD

Co-funded by
the European Union

9. Digital forensics & financial investigations

9.1 Introduction

In today's digital world, the boundaries between virtual and real life are often blurred, and this also applies to the dark machinations of human trafficking for the purpose of labour exploitation (shortly: labour exploitation or labour trafficking). The training chapter 'Digital Forensics and Financial Investigations' highlights the crucial role of these two disciplines in detecting and combating labour exploitation. Digital forensics focuses on analysing electronic data to gather digital evidence of criminal activity related to labour exploitation, while financial investigations aim to track money flows and uncover the financial networks behind these crimes. By combining these two approaches, investigators can not only identify perpetrators but also uncover the often complex links between digital traces and financial transactions that enable labour exploitation. In this context, procedures, best practices, methods and possible tools are presented that enable professionals to utilise the dynamic interactions between digital communication and monetary flows to help victims of human trafficking and take legal action against the perpetrators.

The training chapter begins with learning objectives of a training participant (Section 2). These are listed separately for 'digital forensics' and 'financial investigations'. This is followed by definitions of the most important terms for this chapter (Section 3). Section 4, the core of the training chapter, contains the theoretical and informative background to the topics. This is followed by a practical activity for the training chapter, which enables the participant to work with the theoretical information learned in advance

and to process it more deeply (Section 5). The chapter concludes with sources (Section 6).

9.2 Learning objectives

This training chapter equips participants with the necessary knowledge for digital forensics and financial investigations related to human trafficking and labour exploitation. By the end of this chapter, the participant will be able to…

Digital forensics

- understand the principles of digital forensics, including data collection, preservation, and analysis, while ensuring the integrity of the chain of custody
- know how to create forensic backups (image and logical copies)
- know where to search for digital traces and evidence left by traffickers and for what can be derived from different sources of digital evidence
- understand the legal framework surrounding digital evidence and ensure compliance with procedural requirements

Financial investigations

- identify suspicious financial activities that may indicate human trafficking
- apply a step-by-step methodology for conducting financial investigations related to THB
- understand the economic drivers of trafficking

- be aware of challenges in financial investigations, including the use of cryptocurrencies, offshore accounts, and digital obfuscation techniques
- understand the role of public-private partnership (PPP) in financial investigations and international cooperation in combating trafficking

9.3 Definitions

In the following, important keywords of both topics will be shortly outlined.

9.3.1 Keywords related to digital forensics

Digital forensics

Digital forensics involves the identification, preservation, and examination of digital evidence to support criminal investigations. It includes methods for data acquisition, analysis, and documentation to trace digital footprints of criminal activities.

Forensic data backup

The creation of exact copies of digital storage media while maintaining data integrity and traceability (Chain of Custody). It includes physical image backups (RAW, E01) and logical backups (L01, AD1).

Chain of custody

A continuous, chronological documentation of the handling of digital evidence to ensure its authenticity and integrity in legal proceedings.

Anti-Forensics

Measures taken by a user to make the evaluation of digital traces more difficult or even prevent it: Encryption (FDE, container, ...); TOR/private browsing, virtualisation → deleting the virtual machine (VM); programmes for wiping, cleaning, timestamp change etc.; hiding data, e.g., steganography; multiple packing.

eDiscovery

The targeted use of digital forensics to analyse large volumes of data in order to extract relevant information for investigations or legal proceedings. In other words, eDiscovery (electronic discovery) is the analysation of data for specific cases (e.g., for organised crime; economic crime, state security offences). To conduct eDiscovery, specific knowledge about offences and the specific case is required. Additionally, as data is consistently growing, forensic reports require **data excerpts**. What could help to facilitate eDiscovery is the Electronic Discovery Reference Model EDRM, a framework that includes the standards of discovery and recovery of digital data, e.g.:

- Hardware basics
- Basics of digital forensics
- Structure of data carriers and file systems
- Brief introduction to forensic tools
- Basic forensic activities
- Structure and functionality of the Windows operating system
- Forensic artefacts from Windows systems

Forensic boot media

Specialized operating systems (e.g., Linux- or Windows-based systems) used to start digital devices and conduct forensic analyses without altering the original data.

Redundant array of independent disks (RAID)

A system combining multiple hard drives to enhance data security and performance, requiring specialized forensic techniques for data acquisition.

9.3.2 Keywords related to financial investigations

Financial investigations

The examination of financial transactions to uncover illegal activities such as money laundering, terrorist financing, or human trafficking, and to identify perpetrators.

Money laundering (ML)

The process of disguising the illicit origins of funds through a series of financial transactions to make them appear legitimate. (Opposite: Anti-Money Laundering)

Know your customer (KYC)

A regulatory requirement for financial institutions to verify the identity and financial background of their customers to prevent money laundering and terrorist financing.

Suspicious transaction reports (STRs)

Reports that financial institutions must file when a transaction is deemed potentially suspicious or linked to money laundering or terrorist financing.

Blockchain analysis

The investigation of cryptocurrency transactions to identify illegal activities such as money laundering, fraud, or terrorist financing, and to trace networks of offenders.

Cryptocurrencies and obfuscation techniques

Digital currencies (e.g., Bitcoin, Monero) and methods such as mixers, tumblers, or chain-hopping used to obscure financial transactions.

9.4 Theoretical / informative part

9.4.1 Digital forensics

This section gives an overview of digital forensics in Section 9.6.2, providing background information on what it is, how it can be categorized and how a typical digital forensic process looks like. Furthermore, the section describes basic principles a digital scientist or practitioner should consider. Afterwards, Section 9.6.2 deals with basic knowledge about data backups as they build the foundation of a solid and successful digital forensic process. However, a further basic technical introduction to digital forensics (via this first step of the backup) would go too far at this point - especially as e.g., the analysis methods are too diverse to cover here. Accordingly, it is not expedient, particularly since the application is in the context of human trafficking and labour exploitation, to go into further steps. Accordingly, Section 4.1.3 deals with digital forensics in the context of THB.

9.4.2 Overview

Forensics is the application of scientific methods to analyse and prosecute criminal offenses. Digital forensics, specifically, deals with questions like:

- Where are digital traces created?
- How can digital traces be recognised and evaluated?
- How can digital traces be secured and utilised?

Even if digital forensics was already defined in Section 3, it is worth going more into detail. Digital forensics encompasses the (1) search, identification, the (2) description, and (3) examination of digital evidence, including to assess its reliability, validity, and relevance to the specific case. As a last step, (4) digital forensics also involves the reporting of this evidence (Maras, 2014). It includes methods for data acquisition, analysis, and documentation to trace digital footprints of criminal activities, traces on digital devices which can and have to be analysed for the purpose of criminal prosecution.

Normally, there are **specialized units** in law enforcement agencies (LEAs) for digital forensics which is why THB units mainly collaborate with digital forensic units and do not typically work on digital forensics issues alone. Therefore, it is best to establish and take care of the cooperation with this unit. Moreover, it is advisable to know the different professional positions in the agency, e.g., is there a police clerk responsible for IT? Police cybercrime clerk? Technical criminal investigation service? Digital forensic scientist? Who is responsible for what and when can I reach who?

Digital forensics contains the identification, securing and investigation of digital evidence while also (1) considering legal circumstances and framework conditions (to ensure usability in court) and (2) preserving and documenting the chain of custody and data integrity. Key to digital forensics is therefore that every effort and single step is court-proof and usable in court documentation.

Typical tasks of digital forensics scientists encompass: Data backups from computers, data carriers, mobile devices and online storages; preparation and evaluation of computerised evidence; counselling and support during raids.

Furthermore, digital forensics can be divided and categorized into different fields. Figure 11 provides an overview of possible branches of digital forensics. Computer forensics focuses on recovering, analysing, and preserving digital evidence from computers, including hard drives, file systems, operating systems, and application data. Key techniques are disk imaging, file recovery and registry analysis (see e.g., Casey, 2011). The (sometimes separate listed) database forensics is concerned with the examination of databases (including SQL and NoSQL databases) and their metadata and e.g., involves timestamping of a database and live analysis (see e.g., Dubey, Bhatt & Negi, 2023) to uncover data manipulation, unauthorized access or tampering. But database forensics can also count as a subfield of computer forensics because databases are primarily stored on traditional computing systems like servers. Mobile forensics, or sometimes called mobile device forensics, deals with the extraction and analysis of data stored on mobile devices such as smartphones, tablets, and GPS systems (Dubey, Bhatt & Negi, 2023). Network forensics includes network traffic analysis to obtain information, detect intrusion, and get legal evidence. In the subfield firewall forensics, all firewall logs are examined to find valuable evidence. Cloud Forensics investigates evidence stored in cloud environments, addressing challenges related to multi-jurisdictional data storage,

access restrictions, and provider cooperation. Therefore, it requires specialized legal and technical considerations. IoT forensics examines digital traces from Internet of Things (IoT) devices, such as smart home appliances, wearables, industrial sensors, and automotive systems. It often involves a combination of embedded system analysis, network forensics, and traditional device forensics. Memory (RAM) forensics focuses on extracting and analysing volatile memory (RAM) to uncover running processes, encryption keys, malware and live system activity. Malware forensics involves analysing malicious software (malware) to understand its behaviour, identify its origin, and mitigate its impact (e.g., via static and dynamic malware analysis, sandboxing, reserves engineering). Drone Forensics deals with extracting data from unmanned aerial vehicles (UAVs), including flight logs, onboard storage, GPS tracking, and communication systems. Dark web and cryptocurrency forensics focus on illicit activities on the dark web, including human trafficking, drug trade, and cybercrime. Cryptocurrency forensic techniques help trace transactions in Bitcoin or other digital currencies to identify criminal actors.

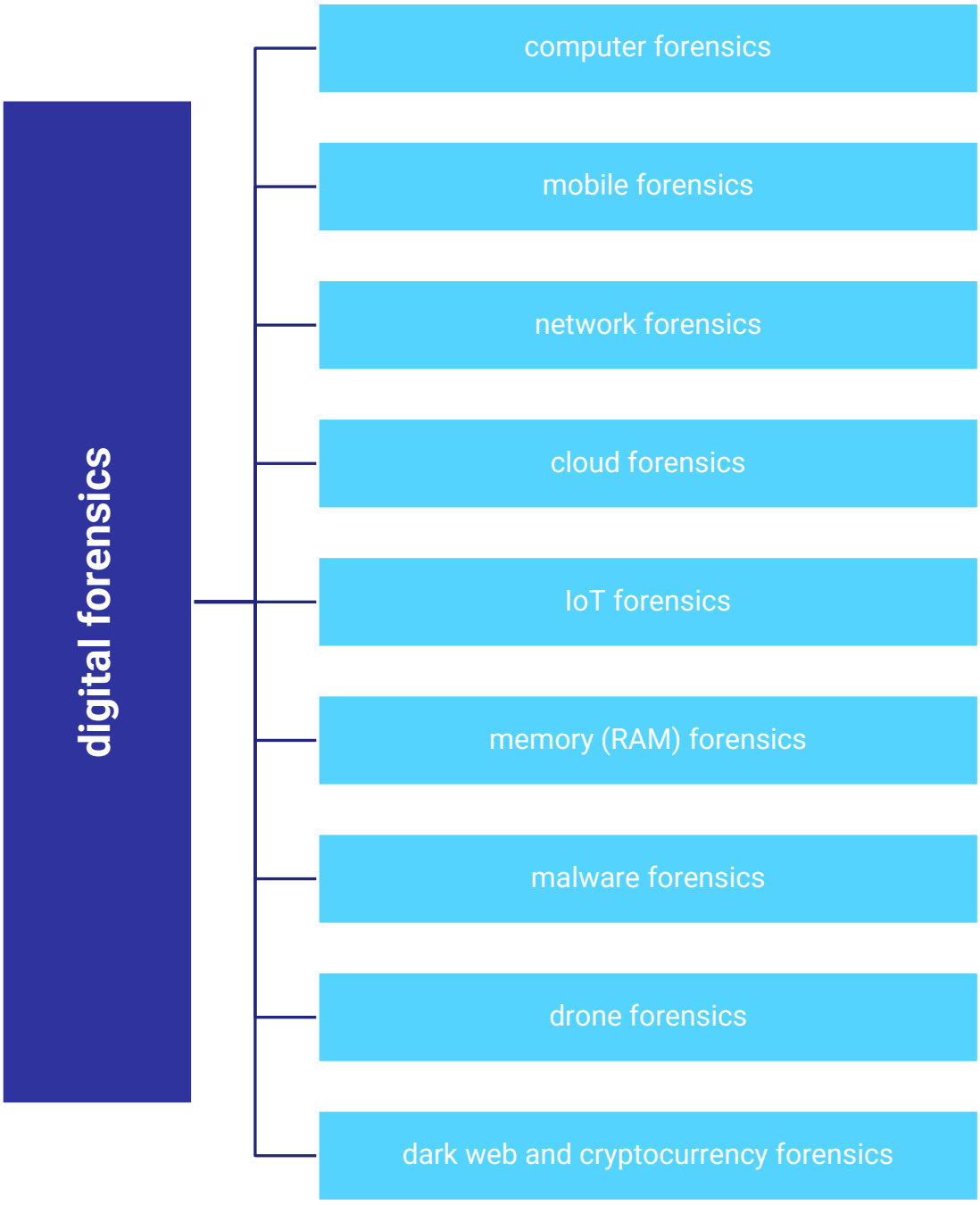

Figure 10. Possible branches of digital forensics

Additionally, the connection between the different branches of digital forensics and the information technology environment is crucial because the type of infrastructure determines where digital evidence is stored, how it can be accessed, and what forensic challenges investigators face:

'Classic' digital forensics vs. online forensics

- Traditional IT → company manages its entire IT infrastructure on-premises, servers, networks, storage, operating systems, and software are physically operated in the company's own facilities. It involves classic computer forensics, network forensics, and database forensics applied to physical machines, local servers, and internal networks. Common sources of evidence are hard drives (HDD, SSD), local databases and system logs. It requires physical access, but full control over the hardware can simplify forensic imaging and analysis.
- IaaS → Infrastructure as a Service; IaaS provides basic IT resources such as virtual servers, storage, and networks over the internet. Companies rent this infrastructure from a cloud provider. The relevant forensic branches are cloud forensics and network forensics. Main data sources are virtual machines, cloud storages, and network traffic logs.
- PaaS → Platform as a Service, PaaS offers a platform where developers can develop, test, and deploy applications. The underlying infrastructure and middleware are managed by the provider. Dominant branches are database forensics and cloud forensics. Data sources are mainly application logs, database snapshots, and API logs.
- SaaS → Software as a Service, SaaS provides fully functional software over the internet. Users access the software via web browsers or apps without needing to

worry about installation, management, or maintenance. No installation required. → Microsoft 365 for example. Cloud forensics and network forensics are the predominant forensic branches here. Important data sources involve audit logs, version history, and user activity records.

Figure 11 shows an overview of the different information technology environments.

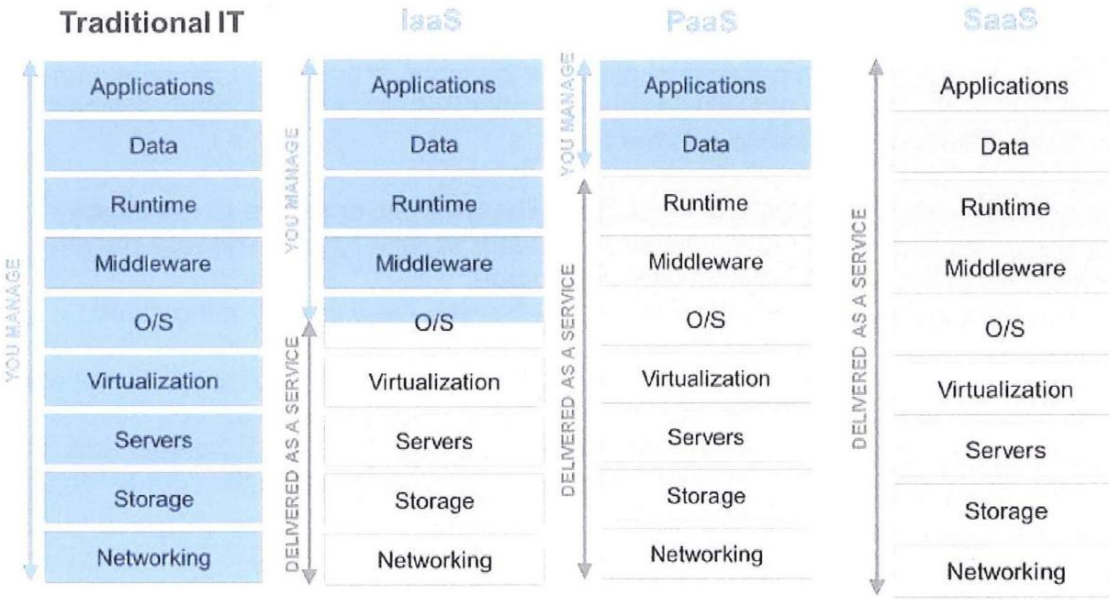

Figure 11. Different information technology environment[96]

Even if there are separate branches and the type of infrastructure has to be considered, the structure of a digital forensic process mainly remains the same. One can shortly summarize the steps as (1) acquisition of digital evidence, (2) its analysis

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

including interpretation, and (3) its presentation (e.g., to case-leading investigators, to court) according to Dubey, Bhatt & Negi (2023). Another influential process model is multidisciplinary digital forensic investigation process model from Lutui (2016) depicted in Figure 12.

Figure 12. Overview of digital forensics process[97]

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

Moreover, for the practitioner another step-by-step guide can help to structure the digital forensic process which contains some more practical elements than the two presented process models before:

Nine practical elements of the digital forensic process

1. **Intake**: receive device as evidence, receive request for examination
2. **Identification**: identify device specifications & capabilities, identify goals of examination, identify legal authority for examination
3. **Preparation**: prepare methods and tools to be used, prepare media and forensic workstation for exam
4. **Isolation**: protect the evidence, prevent remote data destruction, isolate from the network, Bluetooth, Wi-Fi
5. **Processing**: conduct forensic acquisition, perform forensic analysis, scan for malware
6. **Verification**: validate your acquisition, validate your forensic findings
7. **Documenting/Reporting**: keep notes about your findings and process, draft and finalize your forensic reports
8. **Presentation**: prepare exhibits, present your findings
9. **Archiving**: keep a copy of data in a safe place, keep data in common formats for futures

For the digital forensic scientist/practitioner, it is moreover important to bear in mind the whole procedure of a forensic investigation:

Procedure of a forensic investigation

1. Seized evidence handed over to digital forensic scientist
2. Preservation (recorded storage) of data and data carriers (directory, stickers, ...)
3. Creating data backups: physical image backups, logical data backups
4. Secure storage of the original evidence
5. Documentation of chain of custody

In addition, some basic principles of digital forensics should always be applied:

Basic principles of digital forensics

- Creation of data backups, there are different types to differentiate:
    - one-to-one-copies of computerised evidence
    - physical image backups (E01 [encase image file format] or RAW)
    - logical data backups (L01, AD1 or CTR)
- Examine the data backups or copies (post mortem analysis)
- No changes in the secured data
- Precise documentation of who did what and when with the data backups to ensure the chain of custody is fulfilled. The latter requires (1) chronological documentation, and (2) traceability for securing the transfer, the evaluation and the submission of the evidence objects. It follows the principle that (scientifically) recognised methods are applied and a complete documentation is prepared by the digital forensic specialist.

- Creation of one-to-one copies of the computer evidence while considering…
    - to ensure the integrity and authenticity of the evidence
    - to include write protection
    - verification
- Do not change something on purpose! Changes happen fast, e.g., via booting a system or mounting a hard disc.
- **Very important:** Make everything traceable always and everywhere (documentation!)

Besides, it is important to know the legal aspects as lawfulness of the search and seizure must be given. Moreover, as a forensic scientist, one does generally not have to worry about prohibitions of utilisation (= task of the investigating officer and ultimately the public prosecutor). Last, but not least, it is advisable to consult with investigators in the event of chance finds.

9.4.3 Data backup

In digital forensics, data backup is a fundamental step in preserving and analysing digital evidence. Ensuring the integrity and availability of forensic data is critical for investigations, legal proceedings, and cybersecurity incident response. A proper forensic backup allows investigators to work with an exact, unaltered copy of the original data, minimizing the risk of evidence contamination or loss.

This section explores the key aspects of forensic data backup, starting with its core principles (Section 9.6.3.1), including data integrity, authenticity, and chain of custody. It then provides an overview of common forensic backup formats and their structure

(Section 9.6.3.2), followed by an examination of software-based write protection mechanisms to prevent data tempering (Section 9.6.3.3). Different types of data carriers and their role in forensic investigations are also discussed (Section 9.6.3.4), alongside an analysis of specialized forensic backup software and hardware solutions (Section 9.6.3.5). Additionally, the section covers the creation and application of forensic boot media (Section 9.6.3.6), which facilitate data acquisition from live and offline systems. Network-based forensic backup methods, including remote acquisition techniques, are also explored (Section 9.6.3.7). Finally, special considerations for handling complex storage systems, such as RAID arrays and NAS devices, are discussed (Section 9.6.3.8), shortly highlighting the challenges and best practices in preserving such data structures.

By understanding these concepts, forensic specialists and practitioners can ensure reliable, verifiable, and court-admissible data backups, forming the foundation of a sound forensic investigation.

9.4.3.1 Principles of forensic data backup

There are critical principles that must be followed regarding data backups:

- **Creating forensic copies und write-blocking**:
    - Exclusive work on forensic copies, not the original media
    - Creation of forensic copies as bitstream images or logical backups
    - Prevent changes to the original data or media during backup, investigation, and examination
    - Read-only access during backup process (write protection)

- **Ensuring backup integrity**:
    - Ensuring data backups remain suitable for analysing
    - No changes to the backed-up data (second copy if necessary)
    - Usage of wiped backup media (risk of cross-contamination)
    - Verification of image backups (hash comparison between original and copy after backup process or copy processes)
- **Documentation of the chain of custody**: Precise documentation of all interactions with the data backups (maintaining 'chain of custody')

9.4.3.2 Overview and structure of common forensic backup formats

The scope of data backups in digital forensics includes magnetic and SSD hard drives from computers, individual storage devices such as USB drives or flash memory, and optical media. These can be secured using two primary methods: **image backups**, which create comprehensive, sector-by-sector copies, or **logical backups**, which focus on specific files and directories. Both methods are supported by forensic tools such as X-Ways, EnCase, FTK, NUIX Imager, and Magnet Acquire.

Image data backup is a bit-for-bit copy of a storage device, capturing all data, including files, folders, and unallocated, free, and released storage spaces.

The image differs from a clone as the image data backup creates a compressed file (image) of a disk, partition, or system. The image backup which stores data in one large file must be restored before it can be used. In digital forensics, forensic images are taken, for example, of a suspect's hard drive. Imaging is typically used for post-mortem analysis, while **cloning** is for copying systems or creating identical setups (e.g., cloning an old HDD

to SSD without reinstalling the OS). It can sometimes serve forensic needs as well. The cloned disk is immediately bootable and usable. For digital forensics, one could make an exact bitstream copy of a suspect's disk, for instance.

There are several commonly used **forensic image formats**:

- **RAW Format:** A direct bitstream copy of the storage medium. Depending on the backup software, MD5 hashes of the complete image or individual image parts are created.
- **Expert-Witness Format (EWF) (E01)**: Immutable format designed for forensic use. EVF header includes metadata like the number of blocks and sector sizes. Incorporates Cyclic Redundancy Checks (CRC) for verifying individual blocks. Segmented structure with headers, data, and sector tables.
- **EnCase Evidence File Format (Ex01):** developed by Guidance/OpenText and based on the E01 format. More efficient and performant compared to E01 and primarily supported by EnCase and NUIX**.**
- **Advanced Forensic Format (AFF):** Open-source, manufacturer-independent format maintained by an online community. Supports AFF4 and AFF4-L variants. Less commonly used in Germany. Compatible with tools like FTK Imager and Magnet Forensics AXIOM.

Forensics also involve **logical backups**. A logical backup is a copy of the actual data on a storage device or partition, capturing only the files and folders currently present, not unassigned areas or deleted data. Logical backups are typically created on-site or during company searches and from NAS systems.

9.4.3.3 Software write protection

Software write protection refers to tools that prevent the modification of data stored on a data carrier by enforcing read-only access. There is different software that ensure that no data is accidentally altered or deleted during forensic investigations.

- **X-Ways forensics:** Protects entire disks or specific partitions. Effective only after Windows has recognized and accessed the disk.
- **Diskpart:** Used to set or clear write protection on disks or volumes. Effective only after the device is recognized by Windows.
- **FastBloc SE:** Software write-blocking solution enabling forensic imaging on IDE, SATA, SCSI, FireWire, and USB channels without hardware write-blockers.
- **Registry-based protection:** enables write protection for storage devices by modifying system settings to restrict write access.
- **USB ports:** Write protection via diskpart (not reliable) or registry modifications: protection on USB device.

9.4.3.4 Data carriers

Magnetic data carriers, such as hard disk drives, store data magnetically on spinning platters divided into sectors. These sectors typically have a physical size of 512 bytes or 4096 bytes in modern drives, and data is read mechanically using a read/write head.

Flash data carriers, such as SSDs and USB drives, store data electronically in memory cells organised into pages and blocks. Unlike magnetic drives, they have no moving parts. Flash memory uses controllers to emulate the traditional sector-based structure for

compatibility with existing systems. It is shock-resistant, compact in size while offering high storage capacities, and consumes less power. However, it has some drawbacks as well. One significant disadvantage is its limited lifespan. There are primarily two types of flash memory: NAND and NOR. NAND flash memory is cheaper and offers higher storage capacities. It works similarly to a block device, like an HDD, and contains a file system that can be partitioned.

Solid-State Drives (SSDs) use NAND flash memory and are designed to replace traditional hard drives. They provide significant performance improvements, such as faster data read and write speeds. A hybrid storage solution, known as Hybrid Solid State Drives (SSHD), combines a traditional magnetic hard drive with additional flash memory. The frequently accessed data is stored in the flash memory, which speeds up the system's overall performance by caching data for quicker retrieval.

9.4.3.5 Forensic backup software and hardware

Forensic data backup involves a combination of specialized **software** and **hardware** tools. Among the most common software tools are Individual imaging programs such as:

- **FTK Imager:** Portable and installable versions. Supports previewing local drives, network shares, and images. Creates RAW, E01, and SMART format bitstream images. Allows hashing, exporting files, splitting, merging images, and logical backups (AD1 format). Cross-platform compatibility (Windows, Linux, macOS).
- **EnCase Imager:** Proprietary imaging tool with advanced features.
- **Magnet Acquire:** Simple tool for mobile and desktop imaging.

- **NUIX Imager:** Secure imaging for physical drives and cloud environments. Supports unique logical formats (*.nli) with metadata and hash verification.

Additionally, comprehensive forensic suites provide a broader set of tools for digital forensics, such as:

- **X-Ways forensics:** Supports physical and logical drive imaging. Offers various imaging modes (full, minimal, cleaned). It enables file-container creation, format conversion, and sparse compression.
- **EnCase forensics:** Comprehensive suite for imaging and analysis
- **Magnet forensics IEF/AXIOM:** Focuses on digital evidence analysis and imaging

For a specific THB-related overview of digital forensics tools, please be referred to Section 9.6.4.3. Forensic data acquisition also requires specific hardware tools:

- **Write-Blocked Disk Duplicators** are used to create exact, bit-by-bit copies of storage media while preventing any changes to the original media. Examples are Logicube and VOOM Hardcopy. Also, forensic portable devices are solutions designed for quick imaging in field operations and are often used with laptops or external drives.
- **Additional features and tools** include secure image copying facilitated by tools like NUIX Evidence Mover and hash value verification using software such as HashMyFiles, HashCalc, and MD5.exe. These tools integrate seamlessly with forensic software like EnCase and X-Ways to ensure the integrity of E01 image files.

For drive removal from compact systems, resources like iFixit, YouTube tutorials, and official portals (e.g., TeSIT) provide valuable guidance. In cases where drives cannot be physically accessed, using boot media is recommended to facilitate data acquisition.

9.4.3.6 Creation and use of forensic boot media

Forensic boot media is an essential tool in digital forensics, particularly when it is not possible to remove or directly access a storage device from a computer or when a write blocker is not available.

There are two **main types of systems** used for booting:

- 'Basic Input Output System' (BIOS): Traditional interface between computer's hardware and operating system. Supports booting up to four operating systems on one drive. Activates immediately after the computer is powered on. Designed for MBR-based data carriers.
- 'Extensible Firmware Interface' (EFI): Successor to BIOS, with support for up to 128 operating systems on a single disk. Variants include: **UEFI** (Unified Extensible Firmware Interface) for Windows/Linux and **EFI** for macOS. Essential for GPT-based disks. Used for starting the operating system on GPT data carriers. Supported by all current operating systems. Offers enhanced security and functionality:
    - Compatibility Support Module' (CSM): simulates a BIOS for the hardware and the operating system; Compatibility mode/legacy mode
    - Secure Boot: Prevents malware from being loaded before system startup

- Trusted Boot: Signing of kernel/system files from Windows 10 to exclude malicious code to exclude malware

- Boot sequence
  - BIOS: checks the drives specified one after the other for bootable operating systems and transfers boot process
  - UEFI: Includes a built-in boot manager allowing direct drive selection.

Linux-Boot-Media

Linux boot media are equipped with a wide range of free forensic tools for tasks such as data backup, analysis, and recovery. Examples of these tools include: **Backup** (`Guymager`, `dcfldd`, `ddrescue`); **Analysis** (`Sleuthkit`, `Autopsy`) and **Recovery** (`Foremost`, `TestDisk`).

Popular Linux distributions are Knoppix, Helox, CAINE (Computer Aided INvestigative Environment), DeepThought, DEFT¸ Grml, Kali Linux.

Creating Linux Boot Media: Linux systems are stored in FAT32-formatted Casper containers, with user-generated files stored externally. Boot media can be created using tools like **YUMI, Rufus**, or **Linux Live USB-Creator**. Devices like **Zalman** or **IODD** can serve as backup/boot hardware.

Creating image backup: Typically uses **RAW images.** 'dd' is usually available on every Linux system. Syntax: dd if=/dev/sdX of=/media/image.dd. Splitting large images. Progress monitoring with updated `dd` versions or utilities like `Pipe Viewer (pv)`. Verification using hash algorithms (`md5sum` or similar). Merging image parts after splitting.

Alternative Linux backup programmes are Guymager, dcfldd, dc3dd, ddrescue. A logical date backup is created using tar (Tape Archiver), which is now integrated into Windows.

Windows-Based Boot Media

Windows boot media provides alternative or supplementary functionality to Linux boot media.

- Windows Preinstallation Environment (WinPE): A minimalistic, standalone operating system (OS) independent of the system installed on the device. Enables system analysis and imaging without affecting installed OS data.
- Windows Forensic Environment (WinFE): Customized WinPE configured specifically for forensic use. Applications:
    - Forensic data backups using X-Ways Forensics or FTK Imager
    - Triage and preview of evidence
    - Bypassing administrator privileges on target systems
- Windows Image Format (WIM): Stores basic Windows system images (e.g., Pro, Home, Education). Used for booting Windows PE ('boot.wim'). For installation WinPE is started and 'install.wim' is written to the hard disc. Compatible with tools like `7zip` for image inspection. Can also be delivered in compressed ESD (Electronic Software Distribution) format.

Advanced boot media options

- Ventoy: software-based tool for booting ISO images directly from a USB drive. Features include Secure Boot compatibility and GPT partition support. Creates two partitions (FAT for boot manager and exFAT for ISO storage).
- Macintosh Boot Media:
    - **Target Disk Mode (TDM):** Allows Macs to operate as external drives over Thunderbolt or FireWire
    - **Recovery Mode:** Provides access to tools like Disk Utility and Terminal for imaging
    - **FileVault Decryption:** Requires passwords or recovery keys for access
    - **T2 Security Chip Considerations:** Limits external booting and requires device-specific credentials for imaging
- Multi-Boot Media: Tools like YUMI create bootable USBs with multiple OS options (Linux, Windows, macOS). Ensure compatibility with various systems (BIOS/UEFI, macOS System Integrity Protection).

Special considerations for macOS

- **FileVault and T2 Security Chip:** Encryption requires known credentials. T2 chip integrates Secure Boot and external boot restrictions.
- **Fusion Drives:** Hybrid of HDD and SSD, requiring separate imaging of each component and reconstruction.

9.4.3.7 Data backup via network

Network-based data backups provide an effective method for imaging and transferring data between systems.

EnCase and LinEn provide a robust framework for network-based backups, allowing investigators to access and image remote systems securely.

- **Process:**
  - Boot the target computer using a Linux forensic distribution, such as Deft
  - On the backup PC, launch EnCase Imager.
  - Establish a physical connection between the two computers using a crossover cable.
  - Assign static IP addresses to both systems: **Windows**: Configure via the 'Network and Sharing Center' under 'Adapter Settings.' **Linux**: Use system commands to set the IP.
  - Verify the connection by performing a ping test.
  - Copy the LinEn program to an external storage device and mount it on the target system.
  - Navigate to LinEn's location on the target system and execute it. Choose the 'Server' option in LinEn's interface.
  - On the backup PC, use EnCase to initiate the imaging process via the 'Add Evidence' and 'Crossover Preview' options.

- **Advantages:** Prevents automatic write access to connected storage devices. Linux systems can recognize complex hardware configurations, such as RAID controllers

Unix tools and Linux-based forensic boot media offer flexibility and control during network imaging operations.

- **Process:**
    - Connect both systems using either a crossover or standard patch cable. Utilize a network hub or switch if needed.
    - Assign static IP addresses to each computer:

        Windows: Configure through the 'Network and Sharing Center'

        Linux: Set IP using tools like ifconfig (e.g., ifconfig eth0 192.168.100.1).
    - Test connectivity using a ping command to ensure both devices communicate.

The combination of **dd and Netcat** enables straightforward and efficient data transfers over the network.

- **Process:**
    - **Prepare the destination computer:** Start listening for incoming data using Netcat. example: Save data directly to a file or pass it to dd for writing.
    - **Prepare the source computer:** Stream the disk data to the destination: On Linux: Use dd to read data and pipe it to Netcat. On Windows: Use a compatible dd.exe to perform similar tasks.

- Additional considerations**:** Disable firewalls and antivirus software temporarily to avoid interference. Netcat may trigger security alerts as it is often classified as a 'potentially unwanted program.'

Using **SSH** ensures secure data transfers, especially when working with Linux or macOS systems.

- **Process:**
  - Use dd to create a bitstream copy of the source disk.
  - Pipe the output through an SSH connection to the destination system, where it is saved as a forensic image.
- **Additional features**
  - **Progress Tracking**: Use utilities like Pipe Viewer (pv) to monitor data transfer in real-time.
  - **Compression:** Stream data through compression tools such as Gzip to reduce storage requirements.

9.4.3.8 Specialities of data backup

RAID (Redundant Array of Independent Disks) systems are designed to enhance performance and reliability by distributing data across multiple hard drives.

- **Types of RIADs:**
  - **Hardware RAID:** Managed using a dedicated RAID controller card, offering robust performance and reliability

- **Software RAID:** Controlled by the operating system, typically less expensive but reliant on system resources

- **RAID Levels:**
  - **JBOD:** all HDDs are combined into a single large storage; the storage network is a large file system in which the data is stored
  - **RAID0:** all HDDs are combined into a single large storage system; data storage logic (stripe size) ensures that the data is data is stored in chunks on the HDDs
  - **RAID10:** Two or more HDDs are combined to form a single storage area combined (RAID0); storage area is mirrored (RAID1 Mirroring)
  - **RAID5 or RAID6:** at least 3 (RAID5) or at least 4 (RAID6) HDDs are combined into a single storage area; Parity information is distributed across the disks. if one (RAID5) or two (RAID6) HDDs fail their contents can be restored from the remaining data carriers be restored; Depending on the controller/manufacturer, parity information can be rotated 'forward' or 'backward' to the individual hard discs.
  - **Synology Hybrid RAID (SHR):** A variant of RAID using Linux software RAID (MD RAID and LVM2)

- **Best practices for RAID backup**:
  - Precise documentation of RAID configurations (e.g., BIOS settings, RAID controller type, RAID level, stripe size).
  - Backup via RAID controller, e.g., booting with Linux Live CD or WinFE, which recognise the hardware RAID controller.

- Logical data backup, if necessary, e.g., with FTK Imager 'Custom Content Image'.

NAS (Network Attached Storage) systems are compact, self-contained servers that use customized operating systems, usually lightweight, customized versions of Linux. The internal data carrier usually consists of SATA hard drives. The first step is to create classic image backups. When removing drives from the system, it is important to label which drive was in which slot. NAS systems feature a browser-based interface (Web GUI). To access this interface, the NAS must be connected to the investigative network.

9.4.4 Digital forensics in the context of THB and labour exploitation

Human trafficking, including labour exploitation, increasingly relies on digital communication, financial transactions, and online recruitment (Europol, 2020; 2024). As a result, digital forensics plays a crucial role in identifying perpetrators, uncovering victim exploitation patterns, and securing evidence for prosecution. This subsection explores how digital forensic methodologies can be applied to trafficking cases, addressing both, technical and ethical considerations. This section begins with key sources of digital evidence in the field of THB (and wherever possible to gather information, specifically for labour exploitation, Section 9.6.4.1). Afterwards, Section 9.6.4.2 deals with the analysis of THB-typical digital evidence (e.g., what are investigators looking for?). This is followed by Section 9.6.4.3 that shows some possible digital forensics tools for use by law enforcement. Then, main challenges are discussed which are especially relevant for the digital forensics process during THB investigations (Section 9.6.4.4). The section concludes with legal and ethical issues to consider (Section 9.6.4.5). A further overview

of technology used to prevent and combat THB was compiled by UNODC – Module 14: Links between Cybercrime, Trafficking and Smuggling of Migrants.

9.4.4.1 Key sources of digital evidence

Traffickers and exploiters use various digital platforms and technologies, leaving behind critical forensic traces, but law enforcement can use digital evidence to identify human trafficking and the perpetrators and find legal evidence to accuse them of this crime (Cellebrite, 2024). Common sources of evidence include:

Personal digital devices

In the context of labour exploitation investigations, personal digital devices such as mobile phones and computers can serve as critical sources of evidence. These devices often contain communications, contacts, financial transactions, and location data that can reveal exploitative practices.

- **Mobile devices**: Traffickers frequently utilise mobile devices to coordinate illegal activities. Evidence from these devices can include: (1) call logs and contact lists which reveal communication patterns and networks, (2) text messages and chat histories that contain details of recruitment, coordination, and exploitation activities, (3) multimedia files like photos and videos which may document victims, locations, or illicit acts, and (4) location data (GPS information can trace movements and identify key locations).
- **Computers:** Several types of stored or otherwise via the computer accessible data can be of special interest for the investigation of trafficking (overlapping with data from mobile devices possible): (1) communication records like emails and text messages, social media activities or online advertisements or job postings, (2)

financial data like bank transactions and payment records or cryptocurrency records, (3) personal identification data like digital copied of ID documents or location data, (4) records of employment and work conditions like employment contracts, illegal work schedules, timekeeping and attendance systems (e.g. for detecting excessive working hours), (5) travel data like travel booking information from airline or travel agencies or ticket purchases and itineraries, (6) activity histories on the (dark or surface) web, (7) health and medical records which are stored from e.g., visits to the doctor by victims after physical attacks, or (8) data from surveillance cameras or security systems in workplaces or private properties showing the living and working conditions of victims.

Cloud storage

Cloud storage can be used by traffickers due to its convenience, remote access, and ability to store large amounts of data, making it an important source of digital evidence in such cases. The data gathered from cloud storage can be similar to the list that was depicted above for mobile devices and computers. Moreover, special data that can be found more often in clouds storages are digital calendars potentially revealing conducted or planned meetings, travel movements of victims, or other logistical information concerning operations that were shared in the trafficking network. Hence, cloud storages can offer a higher probability to reveal trafficking network structures or the victims that suffer from the organised labour exploitation. Accessing and analysing cloud-stored data requires, though, legal processes and special technical expertise to ensure evidence integrity (if user credentials are not known). Technical ways of (at least partial) access are, for instance, to cooperate with the cloud service provider, to apply cloud data extraction tools, to use cloud service APIs, to get access via confiscated devices (login with user credentials, use device backups and check if the device synchronized data with

the cloud), to conduct metadata analysis with the cloud-stored files, apply network forensics (Section 4.1.1), or to access cloud storage service logs from the cloud service providers for e.g., getting the login history or the file download history.

Communication and recruitment platforms

The internet provides traffickers with access to potential victims through various digital channels, including social media and recruitment websites (UNODC, 2019a). Fraser (2016) elaborated on how the processes between human traffickers and victims is changing with the shift from geographic to online networks. Fraser outlines that traffickers nowadays know how to use online social media and the dark web. The paper also depicts how these networks affect the power imbalance in trafficking and shapes the experiences of victims (Fraser, 2016). Digital evidence from these platforms encompasses (1) profiles and posts which may contain recruitment attempts, deceptive job offers, or advertisements for illicit services, (2) direct messages (facilitating private communication between traffickers and victims) and (3) group memberships indicating involvement in trafficking networks or forums. The analysation of these elements can uncover e.g., recruitment strategies and identify both victims and perpetrators.

- **Social media platforms**: A report from Kunz et al. (2018) summarizes which websites are used for purposes of sexual exploitation. Among these are (1) sites for viewing and commenting like Facebook, Instagram and Snapchat, but also YikYak and Wispher, (2) websites for conversation like Tinder, Blendr, WhatsApp and KIK, but also Yellow and #1 Chat Avenue as fewer common sites, (3) webcam sites including Chatroulette, Omegle and Monkey, and (4) sites for advertising and sales like Cityxguide, skipthegames, bedpage, seekingarrangement.com or sugar-babies.com. For labour exploitation, no such an overview could be found.

Nevertheless, it is known that **mainstream social media platforms** are used for recruitment for exploitative labour along with online job portals and classifieds (see e.g., Europol, 2024).

- **Online recruitment sites**: Even if these portals and potentially classified websites might be legitimate, traffickers can post deceptive job offers, targeting vulnerable populations seeking employment. As a second step, instant messaging applications are used by the traffickers for the exchange of operational details as they provide a safer environment (Europol, 2024).
- **Online advertisements**: The difference to social media platforms, instant messaging applications, and online recruitment sites is, that online advertisements can be seen as *one-way communication*, while the other sources typically aim at *two-way communication* between persons (e.g., potential victim and suspected trafficker). Characteristics of online advertisements for labour trafficking include:
    - **Lack of specificity**: Advertisements often provide vague job descriptions with minimal details about the role, responsibilities, or working conditions. This ambiguity serves to attract a broader range of applicants without revealing potential exploitative situations (Volodko, Cockbain & Kleinberg, 2020).
    - **Unrealistic Promises**: Offers may include unusually high salaries, expedited visa processing, or other benefits that seem too good to be true, aiming to lure individuals seeking better opportunities (see e.g., Fraser, 2016).
    - **Targeted demographics**: Recruitment efforts often focus on specific populations, such as migrants or individuals from economically

disadvantaged backgrounds, who are more susceptible to exploitation (Volodko, Cockbain & Kleinberg, 2020).

  - While there have been efforts to investigate online advertisements for sexual exploitation using modern technological methods such as Natural Language Processing (NLP) (e.g., Perez & Rivas, 2023; Lugo-Graulich et al, 2024), the crime of labour exploitation, as well as other forms of human trafficking, still lacks scientific research in this area.

- **Dark web vs. surface web**: Hosted on encrypted networks requiring specialized software to access, dark web listings and ads offer a higher degree of anonymity. This concealment poses significant challenges for LEAs, as these platforms often implement advanced technical measures to protect user identities. On the opposite, surface web listings and ads are publicly accessible and often found on mainstream platforms like social media networks and classified ad sites. While they may use coded language and imagery to evade detection, their public nature allows for more straightforward monitoring by law enforcement. Traffickers utilise both surface web and dark web platforms to advertise services or exploitative opportunities. Relevant digital evidence on the dark web encompasses e.g., (1) classified ads and listings that may offer illicit services or deceptive employment opportunities, and (2) forum posts and communications in which methods are discussed, information is shared, or transactions are negotiated (e.g., a forum post stating ‘workers available for low-cost labour’), or (3) fake documents which were obtained from darknet marketplaces like fake visas and work permits for undocumented migrants.

Surveillance and tracking

Surveillance and tracking data refer to any data that can reveal the location, movements, or actions of individuals, often gathered through electronic means which is why digital forensics comes into play. Modern environments equipped with surveillance systems and IoT devices can inadvertently capture trafficking activities. Investigation might also allow (if legally confirmed) tracking and monitoring suspects.

Law-enforcement-initiated surveillance (typically require court order)

- **GPS tracking, e.g., vehicle tracking:** can be used by LEAs to monitor movements. Authorities can, for instance, track the movement of a suspect's car that is regularly transporting victims to and from various work locations. Patterns in the vehicle's location data could help authorities to locate trafficking hubs or identify the victim's travel routes or working hours.
- **Surveillance cameras:** CCTV footage from public or private surveillance cameras can be used to track movements of traffickers or victims in certain locations (e.g., in workplaces, near borders).
- **Communication interception (wiretaps):** Wiretapping (e.g., phone calls, emails, messages) can provide insights into trafficking activities. Wiretaps can help authorities listen in on traffickers arranging travel, payments, threatening victims etc.
- **Tracking devices on mobile phones:** cellular triangulation and GPS data from mobile phones can be used to pinpoint victim's or trafficker's location with precision and e.g., to map their locations over time.

- **Drones or aerial surveillance:** Drones equipped with cameras can be used for tracking movements over larger areas (especially in rural or hard-to-reach places where other human surveillance may be difficult).

Trafficker-initiated surveillance (data collected by traffickers)

- **Mobile device tracking by traffickers**: Traffickers may use victims' phones or their own devices to track victims. This can include using GPS tracking apps or even installing spyware (e.g., mSpy, FlexiSPY) to monitor the victim's location and communications.
- **Location data from IoT devices**: IoT devices such smartwatches or even connected vehicles may be used by traffickers to monitor the location of victims. The logs from these devices can be analysed e.g., to find unusual access times, or environmental changes.
- **Online Monitoring**: Traffickers frequently monitor social media accounts of their victims to control their communication or even impersonate them to control their online persona and e.g., prevent them from seeking help. Law enforcement could therefore examine, if the trafficker had user credentials of the victim(s) to login to different social media or other platforms.
- **Video and audio surveillance**: Traffickers may place hidden cameras of audio recording devices in rooms or workplaces to monitor victims continuously, e.g., ensuring they are performing tasks. Law enforcement could focus on detecting such devices and could then evaluated their data to define the scope of labour exploitation and to be able to present reliable evidence in court.

Financial transactions and payment methods

Financial and cryptocurrency transactions (domestic and international): Traffickers often exploit digital forensic systems to launder money and conceal profits. Key digital evidence includes (1) bank statements and transaction histories which highlight unusual patterns indicative of illicit activities, (2) cryptocurrency wallets and transactions used to obscure financial trails, requiring specialized forensic analysis. Financial analysis (see Section 9.2) is crucial in tracing the flow of money, dismantling trafficking operations, and prosecuting offenders (Thomson Reuters, 2025).

- **Traditional banking transactions**
- **Cryptocurrency transactions**
- **Prepaid and digital payment systems**

9.4.4.2 Analysis and correlation of evidence

After the seizure and preservation of the digital evidence (e.g., confiscation of mobile phones, computers, USB drivers, cloud accounts, social media data), the data has to be extracted from these devices or storages, applying different types of forensics that were described in Section 9.1.1 (e.g., cloud forensics; data extraction at hardware level such as chip off or methods like password cracking/decryption). Then, investigators can analyse and correlate the digital evidence. The below presented digital forensic procedures and principles can only be exemplary on the one hand, and, on the other hand, are not entirely unique to THB: many techniques overlap with cybercrime, organised crime, and fraud investigations. However, some aspects make THB unique in this context like the **focus on social media and recruitment ads** (unlike financial crimes, THB cases heavily rely on online deception and communication tracking). Furthermore, a high

amount of **evidence** (which digital forensic teams reconstruct) is **victim-centred** as traffickers keep control over their victim(s) through e.g., threatening messages, blackmailing, or GPS tracking. Moreover, the victims of trafficking often do not possess own computers or laptops, but instead smartphones and cloud accounts. This makes THB investigations more dependent on **mobile and cloud forensics** (see Section 9.1.1).

In cases of THB, digital forensic experts can specifically look for:

- **Communication patterns**: Oftentimes, traffickers use coded language or slang in texts and therefore search for different keywords like 'easy job' , 'cash payment' , 'free travel' in the context of labour exploitation or 'modelling' and 'escort' in the context of sexual exploitation. Oftentimes, those specific keywords related to work, accommodation, and wages are used repetitively. Tong et al. (2017), for instance, found that traffickers in the U.S. and Canada modify their language to evade detection by law enforcement. Moreover, they change the terminology which makes it difficult to develop keyword lists to track trafficking-related ads. This creates a constantly evolving lexicon. For example, instead of explicitly stating 'young girl' , traffickers use obfuscated text, emojis, or slang. (e.g., 'Y❤ng G!rl'). Many ads furthermore lack proper grammatical structures, making traditional NLP techniques less effective. Ads frequently contain symbols, emojis, and non-standard characters. The word order is often inconsistent, resembling social media or text messages rather than structures writing (e.g., '@' instead of 'at' or 'm33t' instead of 'meet'). The complexity of unigram, bigram and trigram is high. The high word variability results from traffickers intentionally modifying words to avoid automated detection (unusual word combinations, rare words, modified word phrases). The ads are typically short (media of 133 words) and lack extensive descriptions. Tong et al. (2017) conclude that traffickers adapt their

language constantly, requiring flexible detection models. Keyword lists alone are insufficient, investigators will need context-aware AI models.

Another way to be able to comprehend and retrace specific communication patterns for digital forensics, one can have a look at the recruitment strategies traffickers apply. These can be categorized into active and passive methods Europol, 2020): **Active recruitment** is like 'hook fishing'' , where criminals post fake job ads on trusted job portals and social media marketplaces. They may even create fake recruitment websites that appear professional, sometimes featuring live chat to make them seem legitimate. UNODC calls this phenomenon also 'hunting strategy' (UNODC, 2020). The active recruitment mostly includes direct messages and chats targeting vulnerable individuals. It can contain patterns of coercion, manipulation and fraudulent job offers. Also not unusual is the sudden deletion of messages or accounts after initial contact (i.e., when the trafficker notices that the to-be-trafficked person is not accessible for the job offer(s)). **Passive recruitment** is more discreet and harder for LEAs to detect. It works like 'net fishing' (or 'fishing strategy', UNODC, 2020), where traffickers monitor job seekers' posts online and reach out to them directly. They promise job opportunities abroad, asking for a fee to secure the job and to cover travel or placement costs. Victims only realize they have been deceived when they arrive in the foreign country (Europol, 2020).

Last, but not least, reliable scientific evidence about investigative techniques for communication patterns is very rare (check out, for instance, the Evidence Gap Map of the International Labour Organization, 2023, for possible updates on scientific elaborations).

- **Geolocation tracking**: Moreover, similar to understanding communication patterns, it can help taking the perspective of the perpetrator: Devices that enable geolocation tracking could have been used for real-time monitoring the victim(s), e.g., via GPS, built-in cameras in smartphones, location-sharing applications (Europol, 2020). The possibility of remote-control lowers perpetrators' inhibition thresholds for exploitation and also complicates the identification efforts by LEAs as Europol stated (2020, p. 3):

  > [While] historically, organised crime groups would have needed to exercise physical control and monopoly over specific city neighbourhoods and would generally consist of a large network of members, newcomers to THB can now efficiently manage an online business without the need for a physical criminal infrastructure and with a reduced workforce. As a result, a mastering of technology can make a criminal group more threatening yet less identifiable by law enforcement agencies.

  More about geolocation tracking can be found in the previous Section 9.1.3.1.

- **Financial analysis**: Financial analysis and digital forensics can go hand in hand, particularly in relation to financial transactions made by traffickers to upload online ads (Europol, 2020). Moreover, victims often have bank transfers to traffickers. A more detailed perspective on finances, financial transactions and financial investigations can be found in Section 9.2.

- **Victim identification**: For victim identification, digital forensic scientists and practitioners may apply facial recognition to find them in e.g., ads or social media posts. Additionally, reverse image search can reveal if victims were advertised on adult sites or black-market platforms.

- **Deep and dark web analysis**: The usage of darknet forums is not unusual for traffickers. Investigators can use TOR forensics and dark web monitoring tools to e.g., find recruitment messages, victim exploitation content, or illicit transactions.

9.4.4.3 Digital forensic approaches and tools

To effectively gather and analyse evidence in cases of THB and labour exploitation, digital forensics heavily rely on:

- Mobile forensics
- Network and cloud forensics
- Financial and cryptocurrency analysis
- Dark web investigations

To proceed chronologically, here are the relevant principles for digital forensics that have to practically be considered, also in the context of THB: In the first phase of identification and preservation, first responders must promptly identify and secure digital devices to prevent data tampering or loss (e.g., isolation from networks; UNODC, 2019b). Then, for the handling of digital evidence, it is important to make detailed records of each device's condition, including operational state (on, off, standby), model, any visible damage. Photographs and written notes aid in maintaining the chain of custody and support the integrity of the evidence (UNODC, 2019b). Data extraction can then be done with specialized forensic tools to retrieve data without altering the original content (see Section 9.6.2 for a general overview). For some devices, this may involve overcoming security features like encryption or passwords. Specifically in the context of human

trafficking/(labour exploitation) LEAs make use of digital forensics tools that facilitate the investigation of this crime.

A whole overview of which digital forensics tools could be used and are used in law enforcement cannot be provided here due to the (1) diversity of what different LEAs throughout Europe make use of (counting for digital forensics as whole and digital forensics for investigation of THB as one branch of it), (2) the interlinked use of different techniques and tools that are dependent on the individual case, and the (3) non-public accessibility how LEAs work in this regard, to only name a few reasons. However, some digital forensic tools and companies offering software solutions for investigating THB cases can superficially be shown:

- **Cellebrite Pathfinder**: a mobile forensic tool that extracts, analyses and decodes data from smartphones, tablets, and cloud sources. It can recover deleted messages, call logs, and GPS locations.

  Potential application in a case of THB/labour exploitation:

  ➔ extracts e.g., WhatsApp, Telegram messages between traffickers and victims

  ➔ recovers deleted conversations where victims were promised fake jobs

  ➔ identifies GPS locations from the victim's phone to ma movement patterns

- **MAGNET FORENSICS**: The company offers several software solutions for public safety, military and intelligence etc.

  MAGNET AXIOM is specifically relevant to THB: The tool specializes in computer and cloud forensics, analysing data from hard drives, social media, emails, and encrypted files.

***Potential application in a case of THB/labour exploitation**:*

- ➔ investigates social media posts and job portal activity where traffickers post fake job ads
- ➔ extracts hidden files (e.g., victim contracts, flight tickets, work permits) from traffickers' computers
- ➔ analyses communication logs between multiple suspects in different countries

MAGNET OUTRIDER can also positively support the digital forensic investigation process as it scans iOS and Android mobile devices and uncovers e.g., illicit apps, contact list, SMS messages, and recently used apps.

Potential application in a case of THB/labour exploitation:

- ➔ reveals hidden online activities and uncovers traffickers using dark web forums or fake social media accounts
- ➔ can detect fake work contracts, job ads, and financial records

MAGNET GRAYKEY, specialized in cracking encrypted mobile devices, can likewise contribute. It bypasses screen locks and extracts file system data.

***Potential application in a case of THB/labour exploitation**:*

- ➔ Unlocks seized traffickers' phones and helps recover WhatsApp, Telegram, Signal, Viber, etc. conversations

Also, other MAGNET software might be helpful (see Pizzuro, 2022).

- MSAB XRY: a mobile forensic tool used by LEAs to extract, analyse, and decode data from mobile phones, tablets, GPS devices, and drones.

Potential application in a case of THB/labour exploitation

➔ extracts mobile communications, potentially revealing THB-relevant digital evidence

➔ analyses social media and job platforms

➔ retrieves deleted files and photos

- **Maltego**: The company offers tools used for mapping relationships between people, companies, social media accounts, and websites (GRAPH), for funning OSINT searches on suspected offenders (SEARCH), monitoring social media in real-time (MONITOR), and conducting social network analysis (EVIDENCE).

  Potential application in a case of THB/labour exploitation:

  ➔ uncovers fake recruitment websites and links them to known traffickers

  ➔ maps connections between different social media profiles used for recruitment

  ➔ identifies crypto-wallet and financial transactions linked to traffickers

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

- **Autopsy**: a free, open-source digital forensic tool offering a platform for hard drive investigations.

  Potential application in a case of THB/labour exploitation:

  ➔ recovers deleted employment contracts or fake visa documents

  ➔ tracks browser history (e.g., visits to fake job websites or encrypted chat platforms)

➔ extracts USB device history to see if external drives were used to store e.g., victim data

- **ADF PRO**: is a digital forensics and triage software designed for rapid analysis of computers, external drives, and mobile devices.

  Potential application in a case of THB/labour exploitation:

  ➔ Rapid seizure of digital evidence at raid sites (e.g., scan suspects' social media, laptops and phones)

  ➔ Facial recognition: quick identification and matching of faces in images and videos (applicable for victim and perpetrator identification)

- **Blockchain analysis tools** (e.g., from Chainalysis, Elliptic, CipherTrace)

  These tools specialize in tracking cryptocurrency transactions, often used by traffickers to receive payments for recruitment fees or victim exploitation.

  Potential application in a case of THB/labour exploitation:

  ➔ traces Bitcoin or crypto transactions made by victims to the exploitative recruiter(s)

  ➔ connects wallet addresses to known human trafficking networks

  ➔ identifies money laundering techniques used to hide illicit profits

For digital forensics processes to combat THB, two more potential approaches are introduced and shortly outlined. To some extent, they may also overlap with already described tools or branches of digital forensics.

The first is the approach to use metadata from images and videos in human trafficking for (digital) forensic investigations. Instead of relying solely on

computationally expensive computer vision techniques, image and video metadata could aid law enforcement in identifying victims and traffickers (Mattmann et al., 2016). Human trafficking often contains textual signs like victim's physical characteristics, location and multimedia elements (i.e., images, videos on different platforms). Mattmann et al. (2016) developed a metadata forensics toolkit for multimedia, encompassing ImageCat (image catalogue) and ImageSpace. ImageCat is an extract, transform, and Load (ETL) system designed to process and catalogue multimedia metadata, particularly in the domain of THB investigations. It can link multiple ads with common metadata (e.g., same camera used for different victims; similarity analysis) and enables search and retrieval of multimedia evidence quickly. Hence, it can help LEAs to identify both, victims and traffickers (Mattmann et al., 2016). Additionally, ImageSpace (built on top of ImageCat) extracts multimedia metadata (i.e., RGB colour space, camera model, geolocation, timestamps). It can search and query large multimedia databases which allows LEAs to search images and videos using text, metadata, or image similarity. Moreover, interactive image browsing and visualisation helps law enforcement to display this evidence in an organised gallery for forensic review and is provides interactive histograms and density plots. ImageSpace also allows for similarity matching between images and videos to cluster related files helping investigators to track e.g., victims across different ads and platforms. Furthermore, it can optimize its search results over time, and it support optical character recognition and text extraction (i.e., extracting phone numbers, emails, addresses) from the images and videos. This specific multimedia approach provides an alternative method to link ads, victims, and traffickers by analysing metadata patterns instead of image or video content alone.

Another approach that is partly incorporated in previously presented tools and resonates in many of the elaborations so far on THB-investigation and digital forensics

is open-source intelligence (OSINT) research. OSINT research refers to collecting and analysing publicly available data to support investigations. It plays a critical role in digital forensics for THB investigations by identifying patterns, tracking digital footprints, and linking suspects to criminal activities. As specifically useful OSINT elements were previously mentioned, this short section about it only serves to outline the importance and the great potential of it. OSINT is essential to identify recruitment and communication patterns as it helps uncover key platforms, language patterns, and recruitment strategies that are used in active (hunting) and passing (fishing) recruitment methods. OSINT, which can be divided in social media intelligence (SOCMINT), geospatial intelligence (GEOINT) and human intelligence (HUMINT), involves i.e., monitoring social media and job listings, analysing forum discussions, dark web activities, and reverse image and video search. It serves to link online ads to trafficking networks by crawling and analysing job ads, tracking cryptocurrency and payments, and domain and website analysis. It can be important for geolocating victims and traffickers by analysing images and videos (and their metadata), or using crowdsourced geolocation (e.g., Google Street View, satellite images). In addition, OSINT can also help to unmask fake identifies and networks by cross-referencing social media (or also dark web) data, by analysing digital footprints and checking for personal data (see e.g., https://epieos.com/ for the reverse lookup if a mail address or phone number is linked with specific accounts like a Google account), or through behavioural analysis (e.g., posting behaviours, language patterns, timing of online activities).

9.4.4.4 Challenges in digital forensics investigations

Investigation trafficking cases presents unique obstacles for digital forensics, such as:

- Encrypted and self-destructing communication
- Data deletion and concealment
- Cros-border data issues
- Victim protection and privacy

To make a more systematic overview of the challenges, one can divide them into matter-related and structural challenges.

Matter-related challenges

Matter-related challenges are challenges which arise from the subject of digital forensics and investigations of trafficking in human beings. Hence, they are immanent to the crime per se. For instance, a differentiation can be drawn between proactive and reactive investigations. **Proactive investigations** are far more complex to start, because the LEA has to identify signs of exploitation that could point out to exploitation. It is challenging to filter these references from the large number of available online adverts, for example (Europol, 2020). Hence, '**reactive investigations** are easier because they have a starting point, such as the testimony of an identified victim and/or the account or website used for recruitment or exploitation purposes' (Europol, 2020, p. 5).

Additionally, the digital evidence per se with which investigators predominantly deal with in cases of THB, poses challenges. As many traffickers use instant messaging apps like WhatsApp, Signal, or Telegram, the incorporated end-to-end encryption (E2EE) make message retrieval difficult. Another point here is that traffickers quite often delete digital evidence (themselves or they use self-deleting functions in e.g., WhatsApp chats). The access to deleted data is limited, and investigators can only try to access backups that were made in the past. Furthermore, traffickers might operate on Tor hidden services

(dark web, VPN use), making tracking difficult. Moreover, traffickers try to blur traces by an extreme diversification of their digital presence - for example by using several SIM cards and mobile phones, various accounts (including fake accounts), etc. This difficulty exemplifies another challenge: The investigator involved in the case often must tame a vast amount of (especially digital) data, look at this data, categorise it as relevant or irrelevant to the crime or crimes to be charged, maintain an overall view and plan further strategic steps. Also related to this challenge is another legal aspect that can become problematic: A case can become incredibly complex in that often not only human trafficking/labour exploitation can be charged, but also e.g., tax evasion; violations of labour law and social security obligations; forced labour; assault; fraud; falsification of documents; or human rights violations. This can also affect digital forensics, for instance, because a more complex case requires more and consistent exchange between the case-leading investigator and the digital forensics specialist.

Structural challenges

Challenges can be seen as structural when they arise from the system (e.g., from the organisation of law enforcement in a country, legislative circumstances). For example, digital technologies applied by traffickers are constantly getting more developed, which is why law enforcement has to adopt itself to these (most recent) technical developments which are applied by the perpetrators (Europol, 2020). In addition, LEAs have to get appropriate human resources for these investigations. This not only applied to human resources of specialized THB investigators and digital forensic scientists and practitioners, but also to other urgently needed personnel for investigating cases of THB like interpreters (for the translation of telecommunications surveillance data, for example). Likewise, the legislative instruments have to be improved to ensure prosecution and conviction (Europol, 2020).

Expanding the legislative possibilities is also particularly relevant as victims are often reluctant to make major confessions and statements as they are already under great psychological stress - threats, blackmail, as well as the inherent risk of public embarrassment via social media (e.g., by publicising their exploitation). Easier access to available data sets for digital forensics is therefore important here in order to drive forward investigations and ultimately support or even enable criminal prosecution (Europol, 2020).

Concerning legal aspects, it should also be mentioned that also efforts to collaborate cross-border can be aggravated, if judicial cooperation and applicable rules are not clearly clarified. This can impede e.g., evidence sharing between countries. Fitting to the lack of standardised international cooperation, there is no centralised global trafficking database yet to track traffickers' online activity globally.

9.4.4.5 Legal and ethical considerations

Due to the sensitive nature of trafficking cases, forensic investigations must adhere to strict ethical and legal standards, some of which were already presented earlier. By integrating these considerations, digital forensics professionals can navigate the complex landscape of THB and labour exploitation investigations ethically, legally, and effectively, ensuring that the pursuit of justice aligns with the protection of individual rights and societal values.

Victim-centred approach

A victim-centred approach prioritizes the rights, needs, and well-being of victims throughout the investigative process. This methodology emphasizes treating victims with respect and sensitivity, ensuring they are informed and supported, and actively

involving them in decisions that affect their lives. By focusing on the victim's experience, investigators can build trust, which is crucial for not only gathering accurate information, but also providing appropriate support services to the victim. This approach not only aids in the recovery of victims but also strengthens the overall integrity of the investigation (International Labour Organization, 2018). 'The safety of victims and their families and loved ones is paramount at all times and is a responsibility of the investigator and prosecutor' (International Labour Organization, 2018, p. 47). This also underlines the necessity to not only focus on the victim as individual, but also on the families/relatives as the possibility of reprisal against family members by traffickers is immanent. (International Labour Organization, 2018).

Moreover, specifically of digital forensics, it is recommended to minimize intrusive digital surveillance by focussing on the traffickers in this regard, not on the victim(s). Victim data confidentiality should be ensured any time to prevent retaliation or public exposure. The investigator should avoid pressuring victims to recount digital interactions multiple times (and use forensic tools instead), he/she should respect victim's consent before accessing personal devices. Aggressive interrogation techniques based on digital findings have to be avoided (e.g., confronting a victim with their chat logs in a way that triggers stress). Another major challenge in prosecuting traffickers can be the reliance on victim testimony which can be traumatizing for the victim, but potentially also unreliable due to i.e., fear. In this regard, digital forensics can strengthen cases and reduce victim reliance in court, which, in turn, can reduce the burden on victims. Digital forensics experts can furthermore prevent victims from retaliation and re-trafficking by scanning their devices, if agreed/desired, for spyware and remove tracking tools afterwards.

Data Protection

During the investigative process: Protecting individuals who expose trafficking activities is vital for encouraging the reporting of crimes. Also, whistle-blower protections ensure that those who come forward do not face retaliation, fostering an environment where information can be shared safely. Additionally, ethical reporting by media and authorities ensures that victims are not re-victimized through exposure and that the information disseminated serves the public interest without causing harm.

UNODC compiled an overview of privacy and data protection in their Module 10 on Privacy and Data protection to be considered for cyber-related matters.

- **Confiscated evidence:** Ensuring the integrity and confidentiality of digital evidence is critical. Proper data protection measures must be in place to prevent unauthorized access, tampering, or loss of evidence. Maintaining a clear chain of custody is essential for the admissibility of evidence in court, as it documents the handling of evidence from collection to presentation. Adherence to legal standards and protocols protects the rights of all parties involved and upholds the credibility of the investigative process.

International cooperation

Human trafficking and labour exploitation are often transnational crimes, necessitating collaboration across borders. International cooperation involves aligning legal frameworks, sharing information, and coordinating efforts among various jurisdictions. This collective approach enhances the ability to track perpetrators, protect victims, and dismantle trafficking networks effectively. The Module 11 – International

Cooperation to Combat Transnational Organized Crime from UNODC can help to get a glimpse of legal possibilities in this regard.

Proportionality and necessity

Investigations should balance the need for information with respect for individual privacy. Collecting digital evidence must be proportionate to the severity of the crime and necessary for the investigation. This principle ensures that investigative measures do not overreach or infringe upon fundamental rights, maintaining ethical standards while pursuing justice.

Integration of AI

The integration of AI in digital forensics offers efficiency but also raises concerns about accuracy and bias. Automated tools must be carefully designed and regularly evaluated to prevent biases that could lead to wrongful accusations or overlook certain victim profiles. Human oversight remains crucial to interpret AI-generated data within the appropriate legal and ethical context. Especially in relevant or even key points in the investigative process, the utilization of AI must not replace human judgement.

Ethical use of OSINT and dark web monitoring

While OSINT and dark web monitoring are valuable in uncovering illicit activities, they must be conducted within legal boundaries. Investigators should avoid unauthorized access or deceptive practices that could compromise the investigation's integrity or violate ethical standards. Respecting privacy and obtaining information lawfully are fundamental to maintaining public trust and upholding the rule of law.

9.5 Financial investigations

Financial investigations are an essential tool in combating financial crimes such as money laundering (ML), terrorist financing (TF), and human trafficking. These investigations focus on analysing financial transactions to detect illicit activities, trace illegal funds, and identify perpetrators and their networks. The basic concepts and objectives of financial investigations revolve around **following the money trail** to uncover and document financial crimes. The primary goals include identifying criminal networks, tracing illicit funds, and gathering evidence that can be used in criminal prosecutions. A well-conducted financial investigation enhances law enforcement efforts by depriving criminals of their financial resources and dismantling the financial infrastructure that supports organised crime.

The relevance of financial analyses in the context of **human trafficking** is particularly significant, as traffickers depend on financial transactions to move, store, and launder their illegal proceeds. By scrutinizing transaction records, bank statements, and digital payment methods, investigators can uncover financial links between traffickers and their associates. This not only aids in prosecuting criminals but also helps identify victims by detecting financial patterns indicative of exploitation. Financial investigations thus play a crucial role in dismantling human trafficking networks by targeting the financial lifelines that sustain them. 'However, widespread acknowledgment, implementation, and harmonization of investigatory strategies and tactics aimed specifically at the finances of THB is still a work in progress' (OSCE, 2019, p. 37).

The following Section 9.7.1 outlines general basics of financial investigation, followed by an introduction about trafficking business structures to highlight the relevance of financial investigation in the topic of THB and labour exploitation (Section

9.7.2). Section 9.7.3 illustrates step-by-step how to conduct a financial investigation in trafficking cases. Section 9.7.4 shows transactional indicators that point to suspicious financial activities in the area of THB and especially labour exploitation. Section 9.7.5 describes challenges in financial investigations, while Section 9.7.6 looks at technical innovations and trends. Section 9.7.7 concludes with some additional recommendations.

9.5.1 Overview

Financial investigations play a crucial role in law enforcement and prosecution, particularly in cases involving ML, terrorist financing, and organised crime (FATF, 2012). The Financial Action Task Force (FATF) Guidance on Financial Investigations outlines the essential principles, tools, and strategies necessary for conducting effective financial inquiries. The primary goal of a financial investigation is to **trace and document the movement of illicit funds**, helping to identify criminal networks, uncover financial structures, and build strong legal cases (FATF, 2012). By examining the financial aspects of criminal activities, investigators can uncover new leads, map out entire criminal networks – including their transnational connections – and gather valuable evidence to prosecute suspects and confiscate illicit assets.

9.5.1.1 Core aspects of financial investigations

A core component of financial investigations is **parallel investigations**, where financial inquiries run alongside criminal investigations. This approach ensures that while law enforcement focuses on crimes such as human trafficking, corruption, or drug trafficking, a simultaneous financial investigation follows the flow of money generated by these activities (FATF, 2012). Parallel investigations help trace illicit assets, identify additional suspects, and support the confiscation of criminal proceeds. To enhance

effectiveness, multi-disciplinary task forces are often established, bringing together financial analysts, forensic accountants, digital forensic experts, and prosecutors. These teams improve intelligence-sharing, reduce duplication of efforts, and ensure a comprehensive approach to financial crime (FATF, 2012).

An essential objective of financial investigations is **asset recovery** and confiscation (see Training chapter 10). Criminals rely on financial gain as a key motivator and depriving them of illicit proceeds weakens their operations. Law enforcement agencies must trace, freeze, and seize illicit assets using advanced financial forensic techniques. Non-conviction-based confiscation is also recommended as an effective legal tool, allowing authorities to seize criminal assets even in cases where a conviction is not possible. Establishing specialized asset recovery units and centralized financial intelligence databases significantly strengthens financial investigations by improving efficiency and coordination.

A successful financial investigation **relies on multiple sources of information**. Law enforcement must have access to financial intelligence reports, including STRs, currency transaction reports, and cross-border cash declarations. Additionally, banking and financial records, company registries, tax filings, customs data, and OSINT provide crucial leads. It is essential that law enforcement officers have the legal authority to access and analyse these records while ensuring compliance with data protection laws.

Investigative techniques

A variety of investigative techniques are employed in financial investigations (listed techniques see FATF, 2012, if no other source indicated).

- **Physical surveillance**: This technique involves monitoring suspects to understand their financial activities, such as movements of bulk cash or interactions with financial intermediaries. It is particularly useful in cases of money laundering and terrorist financing.
- **Trash Runs**: Investigators may lawfully collect and analyse discarded financial records and other documents that might reveal hidden assets or illicit transactions.
- **Compulsory measures**: These include search warrants, subpoenas, and production orders to obtain critical financial records such as bank statements, tax filings, and business ledgers. Properly executed search and seizure procedures ensure that digital and physical evidence is collected legally and maintained under a chain of custody.
- **Intercepting communications**: Law enforcement may conduct wiretaps, email monitoring, and other forms of electronic surveillance to track financial transactions and identify co-conspirators. This method is highly effective but must comply with legal frameworks to avoid privacy violations.
- **Undercover operations**: In some cases, investigators may assume false identities to infiltrate criminal organisations and gather direct evidence of financial misconduct. This technique is resource-intensive and requires extensive training.
- **Controlled deliveries**: This method involves tracking the movement of illicit funds, either in cash or through digital transfers, under law enforcement supervision. It helps to identify key players in money laundering or fraud networks
- **Forensic accounting**: Forensic accounting is a specialized practice that combines accounting, auditing, and investigative skills to examine financial records for signs

of misconduct. Forensic accountants can uncover discrepancies in books, detect fraud, and trace illicit financial activities through detailed financial statements. They apply both quantitative methods, such as data analysis and statistical modelling, and qualitative approaches, including assessing behavioural patterns and organizational culture, to detect anomalies. Benford's Law predicts the frequency distribution of digits in naturally occurring datasets. Forensic accountants utilize this principle to identify irregularities in financial data. Deviations from the expected distribution can signal potential manipulation or fraud. Mark Nigrini, a pioneer in this field, has extensively researched and applied Benford's Law to detect anomalies in accounting data (see e.g., Gorenc, 2019; Siavoshi, 2025).

- **Methods of proving income**: Investigators use direct and indirect methods to establish illegal income sources. The net worth method compares an individual's assets at two points in time to determine unreported income. The bank deposit method analyses unexplained bank account inflows. The expenditure method compares spending patterns to known legal income sources
- **Financial intelligence sharing**: Law enforcement collaborates with Financial Intelligence Units (FIUs), banks, and international counterparts to obtain Suspicious Activity Reports (SARs) and other relevant financial data.
- **Reviewing financial transactions** helps investigators identify suspicious banking patterns, layering techniques, and asset integration methods.
- **Digital forensics** (see Section 9.6.1) plays a key role in tracing online money transfers, analysing cryptocurrency transactions, and intercepting illicit financial communications.

Using synergies of collaboration

FIUs play a critical role in financial investigations by collecting, analysing, and disseminating financial intelligence to law enforcement agencies. FIUs receive AML/CFT disclosures, STRs, and cross-border transaction reports, which can provide early warnings of criminal financial activities. Strong national collaboration between FIUs and investigators ensures that law enforcement has access to timely, actionable intelligence. To enhance efficiency, FIUs and law enforcement agencies should establish secure, real-time data-sharing platforms and develop protocols for analysing financial intelligence.

Since financial crime is often transnational, also international cooperation is vital. Criminals exploit international banking systems and offshore financial centres to conceal illicit funds. Law enforcement agencies must leverage Mutual Legal Assistance Treaties (MLATs), Interpol, Europol, and FATF networks to facilitate cross-border investigations. Establishing joint investigative teams and streamlining legal frameworks for information exchange strengthens the global fight against financial crime (FATF, 2012).

To enhance financial investigations, law enforcement and prosecution agencies should integrate financial forensics into all major crime investigations, leverage financial intelligence systems for real-time analysis, and strengthen international collaboration on asset recovery and intelligence-sharing. By adopting these best practices, financial investigations can serve as a powerful tool in dismantling criminal enterprises and ensuring that crime does not pay.

9.5.1.2 The European Union's efforts

Recognizing the increasing threat of organised crime infiltrating the legitimate economy, the European Union has emphasized the need to enhance financial

investigation capacities. The 2021 EU Strategy to Tackle Organised Crime highlighted the importance of promoting early financial investigations across all EU countries. This approach aims to dismantle the financial infrastructure of criminal organizations, eliminate their profits, and prevent their integration into the legal economy and society (European Commission, n.d.). To support these efforts, the European Multidisciplinary Platform Against Criminal Threats (EMPACT) has prioritized financial investigations in its agenda. EMPACT facilitates collaboration among EU member states to address various criminal threats, including drug trafficking and human trafficking, by integrating financial investigations as a common goal across all priorities.

Additionally, the European Commission provides financial support to the Anti-Money Laundering Operational Network (AMON), a global network of anti-money laundering investigators established in 2012. AMON facilitates the exchange of knowledge among law enforcement units and supports swift operational cooperation in money laundering investigations, reflecting the cross-border nature of such crimes.

Europol has also strengthened its efforts by establishing the European Financial and Economic Crime Centre (EFECC) in 2020. EFECC provides operational support to EU member states in cases involving tax crimes, fraud, corruption, money laundering, asset recovery, euro counterfeiting, and intellectual property crime. This initiative aims to combat highly sophisticated cases of financial crime targeting individuals, companies, and the public sector.

Furthermore, the European Agency for Law Enforcement Training (CEPOL) offers regular training to law enforcement officers to enhance their understanding of money laundering schemes and transnational financial investigation techniques. This training aims to build investigators' capacity to tackle the financial dimensions of organized crime effectively (European Commission, n.d.).

In summary, the European Union's comprehensive approach to financial investigations underscores their critical role in disrupting criminal enterprises, safeguarding the legal economy, and enhancing the effectiveness of law enforcement across member states.

9.5.2 Trafficking as a business

Human trafficking operates as a profit-driven business, much like legitimate businesses, and it is worth looking at this perspective in order to (1) understand key drivers of trafficking and (2) the need to conduct financial investigations. Economic theories of crime suggest that perpetrators make rational choices based on potential profits, risks, and opportunities (see e.g., Belser, 2005). These opportunities arise due to individuals seeking better economic conditions, whether through migration from impoverished rural areas to wealthier urban centres or across international borders. Criminal networks exploit these vulnerabilities by offering false promises of employment, love, or security, leading victims into labour or sexual exploitation or other forms of trafficking (e.g., organ removal). The business model for specifically labour exploitation is simple: victims work under coercion or with unawareness of the exploitative situation, generating high profits while incurring minimal costs for traffickers. Sectors such as agriculture, construction, domestic work, and hospitality provide cover for labour trafficking, while the sexual exploitation remains one of the most lucrative markets for traffickers (see i.e., Aronowitz, Theuermann & Tyurykanova, 2010).

Despite the high profitability, risks for traffickers remain low. Many victims fear law enforcement due to their legal status, social stigma, or threats from their exploiters. In countries where prostitution is illegal, victims are more likely to face arrest than receive

protection. Furthermore, detection and prosecution rates for traffickers remain low, reinforcing the business model's sustainability. Market forces also play a significant role in shaping trafficking operations. It is not solely the demand from consumers that drives human trafficking, but rather the existence of a large supply of vulnerable individuals. Criminal organisations adapt their methods based on legal frameworks, economic conditions, and enforcement mechanisms, much like legitimate businesses responding to market changes (Aronowitz, Theuermann & Tyurykanova, 2010).

Financial investigations into human trafficking must consider these economic drivers. By analysing financial transactions, profit margins, and illicit cash flows, LEAs can identify patterns of exploitation, disrupt networks, and weaken the financial incentives behind trafficking operations. Understanding human trafficking as an economic enterprise is crucial for developing effective countermeasures, including regulatory frameworks, financial oversight, and targeted interventions. The next section outlines the general framework of financial investigations in cases of THB and what specific steps should be taken.

9.5.3 Step-by-step guide to financial investigations related to THB

This section outlines **eleven key steps** for conducting effective financial investigations in cases of human trafficking. These steps are categorized into three areas: *Foundational*, *operational*, and *communal*.

Foundational steps are typically undertaken once during the establishment of the investigative framework and apply broadly across both public and private sectors. Operational steps are more frequently applied due to their relevance to individual

investigations, though their implementation varies between public and private entities. For instance, Steps 7 and 8 primarily concern reporting entities in the private sector. Finally, the communal steps are divided in applicability: both sectors share an interest in Step 10, while financial service providers bear greater responsibility for Step 11.

Figure 14 shows this schematic step-by-step process between LEAs and FIUs. This figure is a copy from OSCE (2020).

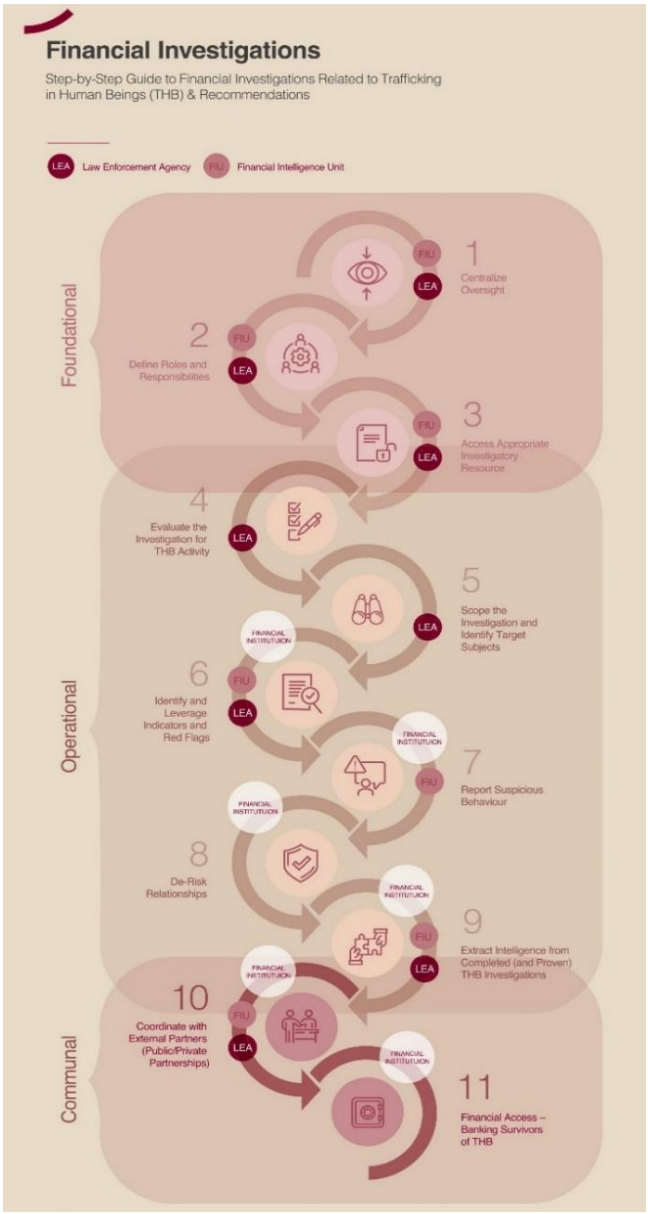

Figure 13. Steps of a financial investigation

Step 1: The first step in a successful financial investigation into human trafficking is **establishing a centralized oversight mechanism**. This ensures a coordinated and comprehensive response to each suspected case, though its structure may vary depending on an institution's size and mandate. Law enforcement agencies often integrate human trafficking investigations into **specialized units**. For example, the New York Police Department (NYPD) and London's Metropolitan Police Service (MPS) have dedicated teams, while Toronto Police Service (TPS) handles trafficking cases within its Sex Crimes Unit, recognizing their distinction from vice-related offenses. Federal agencies such as the FBI and Interpol also centralize expertise, as do FIUs, though the latter often operate with less public visibility.

In the **private sector**, particularly in banks, oversight is less structured due to the high volume of transactions and regulatory demands. However, many institutions maintain **special investigation teams** to address financial crimes, including human trafficking. Centralizing investigative efforts offers several benefits, including reducing duplication, improving efficiency, enhancing expertise, and enabling comprehensive data analysis. However, it also carries risks, such as limiting knowledge to a select group and potential delays in investigations. To mitigate these risks, institutions should promote knowledge-sharing initiatives and allow flexibility in investigative responsibilities to prevent bottlenecks. Ultimately, as long as cases are recorded and appropriately managed, investigations can be conducted by different teams, benefiting both internal and external stakeholders.

Step 2: Once an oversight framework for human trafficking investigations is established, it is crucial to clearly define the roles and responsibilities of those involved. While this is standard practice in many public and private institutions, it is sometimes overlooked. Clearly **outlining responsibilities** helps prevent duplication of efforts,

enhances operational efficiency, and brings additional benefits such as smoother succession planning, more effective triaging of cases, better prioritization of investigations, and consistent communication within and outside the team. **Documenting roles** ensures investigations are conducted more efficiently and in a timely manner. Ultimately, this approach follows the principle of 'divide and conquer' – when everyone understands their role, they can focus on execution. Without clear responsibilities, even well-intended efforts may result in an inconsistent and ineffective investigative process.

Step 3: A successful investigation requires **access to the right resources**, which can vary depending on the nature of the investigation. Financial investigations, particularly those focused on money laundering and human trafficking, demand **specialized tools** different from those used in field operations. Given the complexity of tracing financial flows, investigators must be equipped with adequate resources to efficiently analyse transactions, connect related cases, and adapt to evolving criminal tactics.

Providing investigators with the necessary tools enhances efficiency, improves investigative quality, and increases the likelihood of successful arrests and convictions. Key resources include:

- **Digital case management systems:** A centralized database for storing case notes and evidence enables better case tracking and linking investigations
- **Unrestricted internet access:** Investigators may need access to restricted sites, such as adult content platforms, when tracking human trafficking activity, provided they receive proper training to prevent misuse.
- **OSINT training:** Specialized training in online investigations helps uncover critical information and protect investigators' identities.

- **Access to internal data:** Immediate availability of relevant institutional data, such as transaction records or previous case files, is essential. Overcoming technological, legal, and bureaucratic barriers to data access improves investigative efficiency.
- **Expert legal consultation:** Financial crimes often involve taxation, securities, and real estate, requiring input from specialists. Identifying legal and financial experts early on strengthens investigative outcomes.

While access to resources is vital, institutions must balance efficiency with legal and ethical considerations, ensuring that investigators operate within regulatory boundaries while maximizing their investigative capabilities.

Step 4: One of the key challenges in financial investigations related to THB is the risk of misidentifying crimes — either mistaking another offense for THB or overlooking THB indicators. This can stem from a lack of legal knowledge or the overlapping characteristics of crimes such as human smuggling, or labour violations. Distinguishing these offenses is crucial, particularly for investigators in both public and private sectors. Private institutions should also define which predicate offenses their specialized teams will review, as THB-exclusive units are rare due to resource constraints. Once a foundational understanding of THB-related laws and investigative responsibilities is established, investigators can refine their approach to handling referrals. Public sector agencies typically receive a higher volume of THB-related referrals due to their broader mandates, whereas private sector teams may have fewer cases but greater opportunities for proactive investigation. Proactive strategies include:

- **Reviewing previously closed cases:** Older cases mislabelled as prostitution or smuggling may contain overlooked evidence of THB
- **Conducting historical adverse media searches:** Reviewing news reports on suspected traffickers can reveal financial ties or patterns within an institution's accounts
- **Analysing SARs:** Mining historical SAR data can help identify overlooked THB-related red flags
- **Monitoring high-risk business sectors:** Industries such as massage parlours, strip clubs, and pornography have been linked to THB and warrant closer scrutiny.

Effective financial investigations require both reactive and proactive measures. However, their success depends on the quality of intelligence shared — ensuring that well-documented SARs reach law enforcement and prompt meaningful action.

Step 5: A well-defined investigation scope is crucial to prevent cases from becoming too large to manage and to avoid mistakenly associating innocent individuals with criminal activity. In THB investigations, traffickers frequently exploit their victims' bank accounts for personal gain, making it essential for organisations to have policies that prevent further victimization. **Clearly distinguishing between traffickers and victims is a priority**, followed by **identifying key perpetrators before secondary facilitators**. This risk-based approach optimizes resources and ensures investigative efficiency.

To scope an investigation accurately, it must be as comprehensive as possible from the outset. The 360 Model for example, developed by Peter Warrack, offers a structured method to assess financial activity for potential money laundering and can be applied in both private financial institutions and law enforcement. The model consists of six steps:

1. **Trigger Event** – The investigation begins with an alert, such as a SAR, an automated transaction monitoring flag, adverse media, an internal referral, or a law enforcement request.
2. **Understand the Customer** – Investigators gather contextual background on the subject, including their employment, financial status, and general profile.
3. **Understand the Financial Activity** – The customer's financial behaviour is assessed against their known background to determine if it aligns with expectations.
4. **Eliminate the Norm** – Transactions that appear normal for the customer are filtered out, allowing investigators to focus on truly suspicious activity.
5. **Analyse Remaining Financial Activity** – The investigation zeroes in on the activity that triggered the initial suspicion, analysing patterns and potential links to illicit conduct.
6. **Report and Consider Divesting** – If the investigation confirms suspicion, a SAR is filed with the local FIU, and in law enforcement cases, an arrest warrant may be sought.

This structured approach ensures investigative resources are focused on legitimate threats, minimizing false positives and enhancing overall effectiveness.

Step 6: Understanding what constitutes suspicious financial activity in the context of THB requires both a general knowledge of banking practices and an in-depth awareness of traffickers' methods. While foundational banking knowledge is relatively easy to acquire, recognizing anomalies often demands access to substantial data and hands-on

investigative experience. However, given the extensive documentation available on traffickers' financial behaviours, research can compensate for a lack of direct experience.

At a macro level, **indicators of THB** can be classified into three categories:

1. **Behavioural Indicators** – These involve in-person visual cues that may suggest an individual is trapped in trafficking or that someone is a trafficker.
2. **Know Your Customer (KYC) Indicators** – Red flags based on customer-provided information, such as inconsistencies in identification or addresses.
3. **Transactional Indicators** – Suspicious financial patterns that can emerge at any time after an account is opened, often without face-to-face interaction, particularly with the rise of digital banking.

These indicators can manifest independently or in combination and may be detected by different teams within an organisation — frontline staff identifying behavioural signs, data collection teams spotting KYC red flags, and transaction monitoring teams recognizing financial anomalies. Clear communication and escalation protocols are essential to ensure that potentially suspicious activities are thoroughly investigated. The segmentation of indicators into these three categories aligns with frameworks developed by Thomson Reuters and the Banks Alliance in Europe, Asia, and the United States. Their toolkits provide additional insights, including the relative strength of each indicator and its connection to specific forms of THB, such as labour exploitation.

It is important to recognize that some indicators, like frequent pharmacy purchases, may not be suspicious in isolation. Therefore, analysts must consider multiple factors together to establish reasonable grounds for suspicion. This aligns with guidance from financial intelligence agencies, including:

- **FINTRAC** (Canada, 2016): 'A single transaction taken in isolation may lead to a false assumption of normalcy. Considering all indicators may reveal unknown links that, taken together, could lead to reasonable grounds to suspect THB.'
- **FinCEN** (U.S., 2014): 'No single transactional red flag is a clear indicator of human smuggling or trafficking-related activity. Additional factors, such as a customer's expected financial activity, should also be considered.'

Both FINTRAC and FinCEN emphasize the importance of a structured investigative approach, such as Warrack's 360 Model, to ensure financial red flags are assessed in context rather than in isolation. For a comprehensive list of synthesized indicators, refer to the appendices in the **OSCE's Compendium of Resources and Step-by-Step Guide to Financial Investigations Related to Trafficking in Human Beings (OSCE, 2019)**.

Step 7: SARs play a critical role in financial investigations within both the public and private sectors. Traditionally, a SAR marks the end of a private institution's investigation, typically a financial institution such as a bank, which then submits the report to its FIU. On the public side, a SAR can trigger the start of a law enforcement investigation. However, to maximize their potential, SARs should be viewed as valuable tools throughout the investigative process, not just as a final step or an initiation for public inquiries. They can provide useful intelligence at various stages, either by contributing to ongoing investigations or by offering context for internal investigations within private institutions.

In the **private sector**, it is recommended that technical solutions be used to ease the administrative burden of entering routine data, allowing investigators to focus on the detailed aspects of suspicious activities. Additionally, data from past SARs should be easily accessible to identify patterns, uncover unique offences, and track involved

entities. SARs should also reference previous reports related to the same criminal network to build a cohesive narrative and avoid duplicate filings. It is important for reporting institutions to follow naming conventions established by national FIUs, particularly for high-profile offences like THB. Adhering to these conventions helps ensure compliance with regulatory expectations, enhances the institution's reporting credibility, and assists in identifying financial crime trends. For example, U.S.' FinCEN recommends labelling SARs related to THB as 'Advisory Human Trafficking,' while Canada's FINTRAC suggests using the label 'Project Protect.' Institutions without these coding systems could consider public/private partnerships to implement them.

In the **public sector**, it is advised that FIUs' SAR databases be utilized for all investigations into THB, as this crime typically involves financial gain. Law enforcement agencies should also use tools like production orders and warrants to encourage banks and other reporting entities to file SARs related to open investigations. Despite their importance, SARs have been criticized for an increasing number of low-quality reports. For instance, a 2014 OSCE report highlighted that, in Italy, only 23 out of 37,000 SARs were deemed useful for criminal investigations. A 2019 UK legal reform commission echoed similar concerns, suggesting the need for improvements in SAR reporting to reduce the volume of poor-quality submissions. By implementing some of the recommendations mentioned, such as referencing historical SARs, the quality of future reports can be enhanced.

Step 8: After completing an investigation in a private institution like a bank, a decision must be made on whether to continue the relationship with the customer being investigated. This process, known as **'de-risking'** involves ending the relationship if necessary. It's important to distinguish between the victim and the perpetrator to avoid unjustly punishing the victim, especially in cases like trafficking. If an account belongs to

a victim of trafficking, efforts should be made to maintain the relationship unless multiple violations or complicity are present. De-risking should be approached cautiously, as pushing suspicious activities into illegal markets can make law enforcement investigations more difficult. In some jurisdictions, law enforcement can request that bank accounts be kept open to avoid disrupting investigations. If de-risking becomes necessary, standard messaging should be used to avoid false accusations, and records should be kept of previously de-risked entities for future reference.

Step 9: Identifying actual instances of trafficking in THB based solely on financial transactions is difficult due to the lack of contextual information. Additionally, whether investigators work in a public institution, or a private organisation influences the likelihood of finding conclusive THB cases. Private organisations, such as financial service providers, are not required to prove beyond a reasonable doubt that a predicate offense has occurred before filing a SAR to a FIU. The reporting threshold is often low because financial institutions can only see part of the overall picture. Moreover, FIUs typically do not provide feedback on whether SARs lead to confirmed predicate offenses, making it harder for the private sector to validate THB-related activities.

Since transparency on the outcome of financial investigations into THB is not always possible, proven cases should be used to help with training and future risk mitigation. Financial service providers can identify proven instances of THB by:

- Reviewing daily adverse media updates for connections to internal investigations.
- Subscribing to updates from law enforcement or FIUs on THB enforcement and cross-referencing them with internal cases.

- Setting up a direct referral channel for law enforcement related to THB investigations.

Sharing intelligence from proven THB cases with the broader investigation team, not just the specialized THB unit, is recommended. This aligns with the guidance in Step 1 (Centralize Oversight) and can boost investigator morale, create a sense of purpose, and improve the chances of resource allocation or collaboration between teams.

Step 10: In recent years, the **importance and prevalence of public/private partnerships (PPPs) in combating financial crimes**, particularly human trafficking in business, have **significantly increased**. A global effort to eliminate THB has led to more collaboration between industry competitors to address financial crimes. Anti-financial crime professionals have realized that traffickers move between different institutions and banks, prompting cooperation to tackle these issues. Some of the leading PPPs include the UK's Joint Money Laundering Intelligence Taskforce (JMLIT), Australia's Fintel Alliance, and Canada's Project Protect. The U.S. also has mechanisms like the US: PATRIOT Act 314(a) for information sharing.

Incentives for participating in PPPs include exposure to diverse approaches in financial investigations, quicker development of THB indicators, building stronger relationships with peers and law enforcement, enhanced investigations, shared resources, and a commitment to social good. However, the OSCE recognizes challenges in establishing effective cooperation between FIUs, law enforcement, and entities submitting STRs. One such challenge is the one-sided flow of information from FIUs, which often limits their ability to share intelligence outside their organisation. Feedback on high-quality STRs could improve training, detection methods, and SAR quality.

The lack of feedback from FIUs and the absence of international databases on THB offenders highlight the need for PPPs. Creating a PPP doesn't always require new laws; existing legal frameworks can be used. For instance, Project Protect in Canada successfully operated within their national government's legal framework, focusing on general typologies and indicators while respecting privacy legislation. It's crucial to understand the legal limits and work within them to foster collaboration. Long-term PPP goals can include advocating for changes in legislation based on successful collaborations. Starting or participating in a PPP should follow the establishment of a solid investigative process, but early collaboration is valuable. It can provide insights that shape the investigative process in ways that would be difficult to achieve after the process is already in place. Participating in a PPP will enhance the comprehensiveness of an approach to investigating THB.

Step 11: Investigations into THB, particularly within the banking sector, can negatively impact survivors. This highlights the importance of Step 4 (Evaluate the Investigation for THB Activity), which ensures that activities related to THB are clearly defined at the team or institutional level. Properly executing Step 4 can help reduce unnecessary work later by ensuring that innocent individuals are not wrongly excluded. Since traffickers often manipulate the financial situations of their victims, it is recommended that survivors who have escaped trafficking be given opportunities to rebuild their financial profiles.

A successful example of supporting THB survivors is a program launched by HSBC in the UK in June 2019. This program helps survivors referred by the UK's National Referral Mechanism with challenges like providing proof of address and identification. Additionally, the Lichtenstein Initiative's Blueprint for Mobilizing Finance Against Slavery and Trafficking, created in partnership with the United Nations University and various

governments, has brought together several financial institutions to expand HSBC's efforts across different institutions and jurisdictions. Scotiabank, in collaboration with the Salvation Army's Deborah's Gate anti-human trafficking program, was the first bank to open accounts for survivors under this financial inclusion initiative. It is expected that other participating financial institutions will follow suit and develop similar programs.

As attention and efforts continue to focus on those who facilitate THB, **it is important to not lose sight of the victims**. Public/private partnerships and collaboration with inter-governmental groups can create a comprehensive approach to combating THB, benefiting not only the institutions involved but also the victims, often with minimal costs to execute.

9.5.4 Identifying suspicious financial activity

The OSCE published a **list of transactional financial indicators and so-called red flags which are applicable for human trafficking and especially labour exploitation**. The following list has been taken from the OSCE report and three apparently specific indicators for organ removal as well as seven for sexual exploitation have been removed to make it more appropriate for labour exploitation even if in special cases, the indicators may vary and overlap (OSCE, 2019, p. 61ff).

- Commercial account's use of straw persons
- Non-payment of taxes, workman's compensation and other fees to a tax authority
- Rate of pay for each pay period is identical (no changes for overtime, vacation, sick leave, bonus payments, etc.) in jobs where that would not be expected

- Recurring payments for wages at unreasonably low amounts (such as much lower than min wage scale)
- Significant share of the company's capital in no-term deposits – incommensurate financial turnover
- Loans provided by a shareholder to the related legal person and subsequent transfer back, fictitious loan
- Structuring via commercial entities and transfer of money using contract for loan
- Excessive ride sharing after midnight
- Lack of living expenses such as food, petrol, utilities and rent
- Restaurant purchases and room service, no rooms
- Use of multiple individuals to conduct banking
- High and/or frequent expenditure at airports, ports, other transport hubs or overseas, inconsistent with individual's personal use or stated business activity overseas
- Cash deposits conducted at different cities across the country
- Payments to employment or student recruitment agencies that are not licensed/registered or that have labour violations
- Relatively high expenditures for items inconsistent with stated business purpose
- Transactions that occur outside the time of known business operations
- Cross-border transfers of funds inconsistent with the stated business purpose of the account holder and/or between unexplained patterns of cross-border

transactions between known trafficking routes, or areas where there is a higher risk of trafficking

- Wide use of cash, including for purchasing the assets of the businesses
- Domestic transfers from companies active in sectors sensitive to social fraud, the money is withdrawn in cash immediately afterwards
- Use of institutions not belonging to the financial system (non-traditional)
- Use of cash courier and repeated cash withdrawals
- Purchase of bank drafts payable to a casino immediately after the deposits
- Unexplained/unjustified large profits for a company
- Cash deposits often just under the reporting threshold
- Cash deposits at several branches or ATMs
- Purchase of money orders to pay bills instead of writing personal checks
- Business accounts with apparent deductions in employee wages under various cost types such as housing and food
- Cashed payroll checks where the majority of the funds are either deposited back into the employer's account or kept by the employer
- Remittent or beneficiary with incomplete information
- Purchase of bank drafts payable to a casino immediately after the deposits
- Transfers from different regions to the same persons in countries known to be higher risk for trafficking operations.

- Government assistance checks deposited into the account even though the holder may have substantial amount of money
- Electronic transfers/wires may also be structured
- Co-mingling of cash with legitimate sources of income
- Refining activity (exchanging small denomination bills into larger denomination bills)
- Frequent purchases in multiples of small amounts of Bitcoin or virtual currencies, directly by the client or through exchanges
- Funds transfers involving third parties with alternative names provided in brackets
- Account receives wage payments from legitimate, often nationwide staff agencies but the funds then remain untouched for long periods
- Fast food restaurants: frequent low value purchases in relatively short timelines and inconsistent with expected activity
- Account appears to function as a funnel account

The following case study from Francavilla Lyon & De Cock (2024) exemplifies how financial transaction patterns can serve as indicators of potential labour exploitation within the hospitality sector. This example underscores the critical role of financial analysis in identifying human trafficking risks and detecting covert forms of modern slavery:

Initial situation: A male Chinese citizen opens a private account and states that he works in restaurant X. The analysis of the business relationship shows that the address of this person and the address of Restaurant X are identical. Some of the incoming salary

payments are withdrawn again in cash or transferred to third parties (with no obvious family connection). The salary payments are made irregularly and in varying amounts. During a conversation between the bank and the customer, the latter told the bank that the foreign payments were maintenance payments that he paid to his ex-wife and for their children. According to KYC, however, the client has no children. In addition, according to his employment contract, the client has a permanent position with a fixed salary and does not work on an hourly wage. Expected everyday expenses (food, rent, insurance, etc.) are missing.

The indicators in this scenario are:

- Risk nationality (client)
- Risk sector for labour exploitation
- Pass-through transactions
- Cash transactions
- Absence of expected everyday expenses
- Private address identical to work address
- Contradictory statements from the customer

9.5.5 Challenges in financial investigations

A significant challenge in financial investigations is the evolving nature of **obfuscation techniques** used by criminals to conceal financial trails. Techniques such as **mixing services**, **chain-hopping**, and the use of privacy-focused **cryptocurrencies** pose significant obstacles to investigators. For instance, mixing services, also known as

tumblers, allow users to obscure the origin of their funds by pooling and redistributing them. Chain-hopping involves rapidly converting cryptocurrencies between different platforms, making it harder to track the movement of funds. Additionally, privacy coins such as Monero and Zcash offer enhanced anonymity features, further complicating law enforcement efforts.

To address these challenges, financial investigators increasingly rely on **collaboration with digital forensic experts**. Digital forensics enables investigators to extract and analyse electronic evidence, such as encrypted communications, IP addresses, and transaction metadata. This interdisciplinary approach is crucial in uncovering hidden financial networks and tracing illicit financial flows across borders. Given the transnational nature of financial crimes, cooperation between financial institutions, regulatory bodies, and international organisations is essential for effective financial investigations. 'Innovative ways to move money combined with a growing realization amongst anti-financial crimes professionals that traffickers jump from institution to institution, bank to bank, has led them to collaborate.' (OSCE, 2019, p. 43).

9.5.6 Technological developments and trends

Recent technological developments have significantly influenced financial crime, shaping new methods of illicit activity while also providing enhanced tools for financial investigations. The rise of cryptocurrencies and blockchain technology, for instance, has facilitated various forms of financial crime, including money laundering, fraud, and even human trafficking. The increased use of **digital assets** enables criminals to move funds across borders with greater anonymity, bypassing traditional financial institutions and regulatory controls. While **Bitcoin** remains the most well-known cryptocurrency, there is

a growing shift toward more privacy-focused alternatives such as **Monero** and **Zcash**, which further complicate law enforcement efforts.

One major trend is the use of **obfuscation techniques** designed specifically for digital assets. Criminals increasingly rely on tools like **mixers**, **tumblers**, and **privacy wallets** to obscure transaction trails and evade detection. These methods make it challenging for authorities to track illicit financial flows, particularly in cases related to human trafficking, where traffickers use digital currencies to collect payments and launder proceeds. The decentralized and pseudonymous nature of blockchain-based transactions has created a landscape where financial crime can thrive unless countered by advanced investigative techniques.

At the same time, financial criminals are becoming more **self-sufficient**, moving away from reliance on external sponsors or intermediaries. This trend is evident in the rise of cyber-enabled fraud, ransomware attacks, and online scams, which generate funds for organised crime networks, including those engaged in human trafficking. The increasing use of fraudulent online marketplaces, fake fundraising campaigns, and deceptive e-commerce platforms has further expanded opportunities for financial crime.

Despite these challenges, technological advancements also provide new tools for combating financial crime. **Blockchain analytics** and **AI** are playing a crucial role in financial investigations, helping authorities trace illicit transactions and identify suspicious patterns. AI-powered transaction monitoring systems can analyse vast amounts of data in real time, flagging anomalies that may indicate money laundering or human trafficking-related activities. Additionally, blockchain forensic tools allow investigators to track cryptocurrency movements and uncover hidden connections between criminal entities.

9.5.7 Recommendations

A robust legal framework for prosecuting financial offences is necessary to ensure effective financial investigations. International standards, for example the recommendations set by the **Financial Action Task Force (FATF)**, provide a foundation for AML/CFT measures. These regulations require law enforcement authorities to conduct financial investigations, facilitate cross-border cooperation, and enforce asset confiscation procedures. FATF Recommendation 30, for instance, highlights the importance of designating competent authorities with the power to investigate money laundering and terrorist financing offences.

Due to the war in Ukraine, displaced individuals face an increased risk of human trafficking. In respond to this heightened vulnerability, organisations such as the Organisation for Security and Co-operation in Europe (OSCE) have developed targeted resources to support first line responders. For instance, the OSCE offers *A Compendium of Anti-Trafficking Training Courses for First Line Responders*, which includes specialized training on various aspects of counter-trafficking efforts. Among these, specific courses focus on financial investigations, equipping professionals with the necessary tools to identify and combat illicit financial flows linked to human trafficking. Link to the course overview: https://www.osce.org/cthb/562572.

9.6 Suggested activities for the chapter

Table 14. Activity for digital forensics and financial investigations

Activity Name	Activity for digital forensics
Type of Activity	Group work (e.g., groups of 3-6 people)
Duration	15-35 min
Learning Objectives	Identification of key digital traces and next steps to take
Materials Needed	Case example with sufficient background (e.g., printed 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 (*use auto-translation for the website and select sub-section 'Human Trafficking for Labour Exploitation'*) • Training chapter 8
Guidelines for the facilitator	The participants will be divided into smaller groups. They will get a case study which they will read (3-4 min). Then, they will start to discuss in their group and try to identify what digital evidence would fit best for successful digital forensics. Furthermore, they will discuss which actors would be involved and at which point in the investigative process (10-15 min). • What digital evidence is relevant? What pieces of digital evidence are most useful and why?

	• How can forensic experts extract and analyse these digital traces? • How can it help identify victims, traffickers, and patterns? • What patterns or red flags suggest human trafficking? • What next steps should investigators take? • How can this evidence be used to support victims? Afterwards, each group will present their findings (5-10 min).
Debriefing	The facilitator moderates the presentation after the group work.
Tips for facilitator	If you have more time, you can use different case scenarios, and each group will shortly present the case and then their discussion results (instead of each group working on the same case).
Handouts	e.g., cases studies that should be printed and provided to participants, potentially supplemented by material with imitated extracts from: • WhatsApp chats between the victim and the trafficker with communication in it like 'Don't worry about paperwork, we'll handle it for you.' , 'You will get free housing and transport.' , or 'Meet me at the bus station. Delete these messages.' • Ads from the recruitment platform • Bank transaction records

	• Metadata from a photo sent to the victim with geolocation data • …
Variations for online implement-tation	Online conduction is possible, make break-out sessions for the group task
Activity Name	**Activity for financial investigations**
Type of Activity	Group work (e.g., groups of 3-6 people)
Duration	15-35 min
Learning Objectives	Internalising the steps for financial investigations and reflecting on potential challenges arising in the field of THB
Materials Needed	e.g., cases study that should be printed and provided to participants, potentially supplemented by material with imitated extracts from: • Bank transaction records and bank statements (can also be just a table with the columns: date, description, Debit (EUR), Credit (EUR), and balance (EUR), showing when somebody made transaction (+ to which company/person)

	• Payroll records • Invoices • …
Guidelines for the facilitator	The participants will be divided into smaller groups. They will get a case study which they will read (3-4 min). Then, they will start to discuss in their group and try to identify the steps for financial investigations (e.g., by going through each step learnt previously). Furthermore, they will discuss which actors would be involved and at which point in the investigative process (10-15 min). • What financial investigation techniques should be used? • How can law enforcement collaborate with FIUs here? • What legal tools should be applied? • Which challenges can be identified? Afterwards, each group will present their findings.
Debriefing	The facilitator moderates the presentation after the group work.
Tips for facilitator	If you have more time, you can use different case scenarios, and each group will shortly present the case and then their discussion results (instead of each group working on the same case).

Handouts	*A case study should be printed and provided to participants* • 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
Variations for online implement-tation	Online conduction is possible, make break-out sessions for the group task

9.7 References

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.