# Poglavje 9. Digitalna forenzika in finančne preiskave

Odgovorni partner: BayHfoD

Co-funded by
the European Union

# 9. Chapter 9. Digitalna forenzika & finančne preiskave

## 9.1 Uvod

V današnjem digitalnem svetu so meje med virtualnim in resničnim življenjem pogosto zabrisane, kar velja tudi za prikrite mehanizme trgovine z ljudmi z namenom delovnega izkoriščanja (v nadaljevanju: delovno izkoriščanje oziroma trgovina z ljudmi z namenom delovnega izkoriščanja). Poglavje usposabljanja »Digitalna forenzika in finančne preiskave« poudarja ključno vlogo teh dveh disciplin pri odkrivanju in preprečevanju delovnega izkoriščanja. Digitalna forenzika se osredotoča na analizo elektronskih podatkov z namenom pridobivanja digitalnih dokazov o kaznivih dejanjih, povezanih z delovnim izkoriščanjem, finančne preiskave pa sledijo denarnim tokovom in razkrivajo finančna omrežja, ki stojijo za temi kaznivimi dejanji. S kombiniranjem obeh pristopov lahko preiskovalci ne le identificirajo storilce, temveč tudi razkrijejo pogosto kompleksne povezave med digitalnimi sledmi in finančnimi transakcijami, ki omogočajo delovno izkoriščanje. V tem okviru so predstavljeni postopki, dobre prakse, metode in možna orodja, ki strokovnjakom omogočajo, da izkoristijo dinamične interakcije med digitalno komunikacijo in denarnimi tokovi za pomoč žrtvam trgovine z ljudmi ter za izvajanje pravnih ukrepov zoper storilce.

Poglavje usposabljanja se začne z učnimi cilji udeleženca usposabljanja (poglavje 2). Ti so posebej navedeni za »digitalno forenziko« in »finančne preiskave«. Sledijo definicije najpomembnejših pojmov za to poglavje (poglavje 3). Poglavje 4, ki predstavlja jedro usposabljanja, vsebuje teoretično in informativno ozadje obravnavanih tem. Nato sledi

praktična aktivnost, ki udeležencu omogoča, da uporablja predhodno osvojene teoretične informacije in jih poglobi (poglavje 5). Poglavje se zaključi z viri (poglavje 6).

## 9.2 Učni cilji

- To poglavje usposabljanja udeležence opremi s potrebnim znanjem za izvajanje digitalne forenzike in finančnih preiskav, povezanih s trgovino z ljudmi in delovnim izkoriščanjem. Ob koncu poglavja bo udeleženec/-ka znal/-a:

Na področju digitalne forenzike

- razumeti načela digitalne forenzike, vključno z zbiranjem, zavarovanjem in analizo podatkov, pri čemer zagotavlja integriteto dokazne verige (chain of custody)
- vedeti, kako ustvariti forenzične kopije (slikovne kopije in logične kopije)
- vedeti, kje iskati digitalne sledi in dokaze, ki jih puščajo storilci, ter kaj je mogoče izpeljati iz različnih virov digitalnih dokazov
- razumeti pravni okvir digitalnih dokazov in zagotavljati skladnost s procesnimi zahtevami

Na področju finančnih preiskav

- prepoznati sumljive finančne aktivnosti, ki lahko kažejo na trgovino z ljudmi
- uporabiti metodologijo po korakih za izvedbo finančnih preiskav, povezanih s trgovino z ljudmi
- razumeti ekonomske dejavnike, ki poganjajo trgovino z ljudmi
- zavedati se izzivov pri finančnih preiskavah, vključno z uporabo kriptovalut, offshore računov in tehnik digitalnega prikrivanja

- razumeti vlogo javno-zasebnega partnerstva (PPP) pri finančnih preiskavah ter pomen mednarodnega sodelovanja v boju proti trgovini z ljudmit

## 9.3 Opredelitev pojmov

### 9.3.1 Ključni pojmi na področju digitalne forenzike

#### Digitalna forenzika

Digitalna forenzika zajema prepoznavanje, zavarovanje in pregled digitalnih dokazov za podporo kazenskim preiskavam. Vključuje metode pridobivanja podatkov, njihove analize in dokumentiranja z namenom sledenja digitalnim sledem kaznivih dejanj.

#### Forenzično kopiranje podatkov

Izdelava natančnih kopij digitalnih nosilcev podatkov ob zagotavljanju celovitosti podatkov in sledljivosti dokazov (dokazna veriga – *chain of custody*). Vključuje fizične slikovne kopije (*image*) (RAW, E01) ter logične kopije (L01, AD1).

#### Dokazna veriga

Neprekinjena, kronološka dokumentacija ravnanja z digitalnimi dokazi, ki zagotavlja njihovo avtentičnost in celovitost v sodnih postopkih.

#### Anti-forenzika

Ukrepi, s katerimi uporabnik oteži ali celo onemogoči analizo digitalnih sledi: šifriranje (FDE, šifrirani vsebniki ipd.); uporaba omrežja TOR/zasebnega brskanja; virtualizacija (npr. brisanje navideznega stroja – VM); programi za brisanje oziroma “čiščenje”,

spreminjanje časovnih žigov ipd.; skrivanje podatkov (npr. steganografija); večkratno pakiranje (več slojev “packing”).

### eDiscovery

Ciljno usmerjena uporaba digitalne forenzike za analizo velikih količin podatkov z namenom izluščiti informacije, relevantne za preiskave ali sodne postopke. Z drugimi besedami, eDiscovery (elektronsko odkrivanje) pomeni analizo podatkov za konkretne primere (npr. organizirani kriminal, gospodarski kriminal, kazniva dejanja zoper državno varnost). Za izvajanje eDiscovery so potrebna specifična znanja o kaznivih dejanjih in o konkretnem primeru. Ker količina podatkov stalno narašča, forenzična poročila praviloma temeljijo na izbranih izsekih podatkov. Pri izvedbi eDiscovery lahko pomaga tudi referenčni model Electronic Discovery Reference Model (EDRM), tj. ogrodje, ki vključuje standarde za odkrivanje in pridobivanje digitalnih podatkov, na primer:

- Osnove strojne opreme
- Osnove digitalne forenzike
- Zgradba podatkovnih nosilcev in datotečnih sistemov
- Kratek uvod v forenzična orodja
- Osnovne forenzične aktivnosti
- Zgradba in delovanje operacijskega sistema Windows
- Forenzični artefakti v sistemih Windows

### Forenzični zagonski nosilec

Specializirani operacijski sistemi (npr. na osnovi Linuxa ali Windowsa), ki se uporabljajo za zagon digitalnih naprav in izvajanje forenzičnih analiz, ne da bi pri tem spreminjali izvirne podatke..

**Redundantno polje neodvisnih diskov (RAID)**

Sistem, ki združuje več trdih diskov za večjo varnost podatkov in boljšo zmogljivost, pri čemer so za pridobivanje podatkov potrebne specializirane forenzične tehnike..

## 9.3.2 Ključni pojmi na področju finančnih preiskav

**Finančne preiskave**

Preučevanje finančnih transakcij z namenom odkrivanja nezakonitih dejavnosti, kot so pranje denarja, financiranje terorizma ali trgovina z ljudmi, ter identifikacije storilcev.

**Pranje denarja (Money laundering, ML)**

Postopek prikrivanja nezakonitega izvora sredstev prek niza finančnih transakcij, da bi sredstva navzven delovala zakonita. (Nasprotje: ukrepi za preprečevanje pranja denarja – AML.)

**Poznaj svojo stranko (Know your customer, KYC)**

Regulativna zahteva za finančne institucije, da preverijo identiteto in finančno ozadje svojih strank z namenom preprečevanja pranja denarja in financiranja terorizma.

**Prijave sumljivih transakcij (Suspicious transaction reports, STRs)**

Poročila, ki jih morajo finančne institucije posredovati, kadar ocenijo, da je transakcija potencialno sumljiva ali povezana s pranjem denarja oziroma financiranjem terorizma.

### Blockchain analiza

Preiskovanje transakcij s kriptovalutami z namenom odkrivanja nezakonitih dejavnosti, kot so pranje denarja, goljufije ali financiranje terorizma, ter sledenja mrežam storilcev.

### Kriptovalute in tehnike prikrivanja

Digitalne valute (npr. Bitcoin, Monero) ter metode, kot so mešalniki (mixers), “tumblers” oziroma storitve za mešanje transakcij, ali “chain-hopping” (preskakovanje med verigami), ki se uporabljajo za prikrivanje finančnih transakcij.

## 9.4 Teoretični del

### 9.4.1 Digitalna forenzika

To poglavje v razdelku 9.6.2 podaja pregled digitalne forenzike ter ponuja osnovne informacije o tem, kaj digitalna forenzika je, kako jo lahko kategoriziramo in kako običajno poteka digitalno-forenzični postopek. Poleg tega opisuje temeljna načela, ki jih mora upoštevati digitalni forenzik oziroma izvajalec. Nato razdelek 9.6.2 obravnava osnovno znanje o izdelavi forenzičnih kopij podatkov, saj te predstavljajo temelj zanesljivega in uspešnega digitalno-forenzičnega procesa. Vendar bi podrobnejši tehnični uvod v digitalno forenziko (prek prvega koraka, tj. izdelave kopije) na tej točki presegel namen poglavja, zlasti ker so metode analize preveč raznolike, da bi jih bilo mogoče ustrezno zajeti na tem mestu. Zato se ni smiselno poglabljati v nadaljnje korake, še posebej glede na to, da je uporaba usmerjena v kontekst trgovine z ljudmi in delovnega izkoriščanja. V skladu s tem se razdelek 4.1.3 osredotoča na digitalno forenziko v kontekstu trgovine z ljudmi.

## 9.4.2 Pregled

Forenzika je uporaba znanstvenih metod za analizo kaznivih dejanj in podporo kazenskemu pregonu. Digitalna forenzika se posebej ukvarja z vprašanji, kot so:

- Kje nastajajo digitalne sledi?
- Kako lahko digitalne sledi prepoznamo in ovrednotimo?
- Kako lahko digitalne sledi zavarujemo in uporabimo?

Čeprav je bila digitalna forenzika že opredeljena v poglavju 3, se je smiselno v tematiko nekoliko bolj poglobiti. Digitalna forenzika zajema (1) iskanje in identifikacijo, (2) opisovanje ter (3) pregled in analizo digitalnih dokazov, vključno z ocenjevanjem njihove zanesljivosti, veljavnosti in relevantnosti za konkreten primer. Kot zadnji korak (4) digitalna forenzika vključuje tudi poročanje o teh dokazih (Maras, 2014). Vključuje metode pridobivanja podatkov, analize in dokumentiranja z namenom sledenja digitalnim sledem kaznivih dejanj, torej sledem na digitalnih napravah, ki jih je mogoče in jih je treba analizirati za potrebe kazenskega pregona?

**Običajno imajo organi pregona specializirane enote za digitalno forenziko, zato enote za boj proti trgovini z ljudmi praviloma sodelujejo z digitalno-forenzičnimi enotami in se z digitalno forenziko običajno ne ukvarjajo samostojno. Zato je najbolje vzpostaviti in skrbno negovati sodelovanje s to enoto. Poleg tega je priporočljivo poznati različne strokovne vloge znotraj organizacije, na primer: ali obstaja policijski uslužbenec, odgovoren za IT? referent za kibernetsko kriminaliteto? tehnična**

**kriminalistična služba? digitalni forenzik? Kdo je za kaj odgovoren in kdaj lahko koga dosežem.**

Digitalna forenzika zajema identifikacijo, zavarovanje in preiskovanje digitalnih dokazov, pri čemer hkrati (1) upošteva pravne okoliščine in okvirne pogoje (da se zagotovi uporabnost dokazov na sodišču) ter (2) ohranja in dokumentira dokazno verigo in celovitost podatkov. Ključno pri digitalni forenziki je zato, da je vsako prizadevanje in vsak posamezen korak »sodno vzdržen« ter uporaben v sodni dokumentaciji.

Tipične naloge digitalnih forenzikov vključujejo izdelavo forenzičnih kopij podatkov iz računalnikov, podatkovnih nosilcev, mobilnih naprav in spletnih shranjevalnikov; pripravo in oceno računalniško podprtih dokazov; svetovanje in podporo med hišnimi preiskavami oziroma preiskovalnimi akcijami.

Digitalno forenziko je mogoče razdeliti in kategorizirati na različna področja. Slika 11 ponuja pregled možnih vej digitalne forenzike. Računalniška forenzika se osredotoča na pridobivanje, analizo in ohranjanje digitalnih dokazov iz računalnikov, vključno s trdimi diski, datotečnimi sistemi, operacijskimi sistemi in podatki aplikacij. Ključne tehnike so izdelava slikovne kopije diska (disk imaging), obnova datotek in analiza registra (glej npr. Casey, 2011). Forenzika podatkovnih baz (včasih navedena kot ločeno področje) se ukvarja s preučevanjem podatkovnih baz (vključno z bazami SQL in NoSQL) ter njihovih metapodatkov in lahko vključuje npr. časovno označevanje podatkovne baze ter analizo v živo (glej npr. Dubey, Bhatt & Negi, 2023) za odkrivanje manipulacij podatkov, nepooblaščenega dostopa ali nedovoljenih posegov. Hkrati pa se forenzika podatkovnih baz lahko šteje kot podpodročje računalniške forenzike, saj so podatkovne baze praviloma shranjene na klasičnih računalniških sistemih, kot so strežniki.

Mobilna forenzika oziroma forenzika mobilnih naprav se ukvarja s pridobivanjem in analizo podatkov, shranjenih na mobilnih napravah, kot so pametni telefoni, tablice in sistemi GPS (Dubey, Bhatt & Negi, 2023). Omrežna forenzika vključuje analizo omrežnega prometa z namenom pridobivanja informacij, odkrivanja vdorov in pridobivanja dokazov za pravne postopke. Na podpodročju forenzike požarnih zidov (firewall forensics) se preučujejo vsi dnevniki požarnih zidov, da se najdejo relevantni dokazi.

Forenzika v oblaku (cloud forensics) preiskuje dokaze, shranjene v okoljih oblaka, pri čemer se sooča z izzivi, povezanimi z večjurisdikcijskim shranjevanjem podatkov, omejitvami dostopa in sodelovanjem ponudnikov. Zato zahteva specializirane pravne in tehnične pristope. IoT-forenzika preučuje digitalne sledi naprav interneta stvari (IoT), kot so pametne naprave v gospodinjstvu, nosljive naprave, industrijski senzorji in avtomobilski sistemi. Pogosto vključuje kombinacijo analize vgrajenih sistemov, omrežne forenzike in klasične forenzike naprav.

Forenzika pomnilnika (RAM) se osredotoča na pridobivanje in analizo volatilnega pomnilnika (RAM) z namenom razkritja tekočih procesov, šifrirnih ključev, zlonamerne programske opreme in aktivnosti sistema v realnem času. Forenzika zlonamerne programske opreme (malware forensics) vključuje analizo zlonamerne programske opreme, da se razume njeno delovanje, ugotovi izvor in zmanjša njen vpliv (npr. s statično in dinamično analizo, uporabo peskovnikov (sandboxing) ter povratnim inženiringom).

Forenzika dronov se ukvarja s pridobivanjem podatkov iz brezpilotnih zrakoplovov (UAV), vključno z dnevniki letov, podatki iz notranjega shranjevanja, sledenjem GPS in komunikacijskimi sistemi. Forenzika temnega spleta in kriptovalut se osredotoča na nezakonite aktivnosti na temnem spletu, vključno s trgovino z ljudmi, trgovino z drogami

in kibernetsko kriminaliteto. Kriptovalutne forenzične tehnike pomagajo slediti transakcijam v Bitcoinu ali drugih digitalnih valutah, da se identificira kriminalne akterje

.

Co-funded by the European Union

Stališča in mnenja, izražena v tem besedilu, so izključno stališča avtorja(-ev) in ne odražajo stališč Evropske unije ali Evropske komisije (organa, ki je dodelil sredstva). Evropska komisija zanje ne more biti odgovorna.

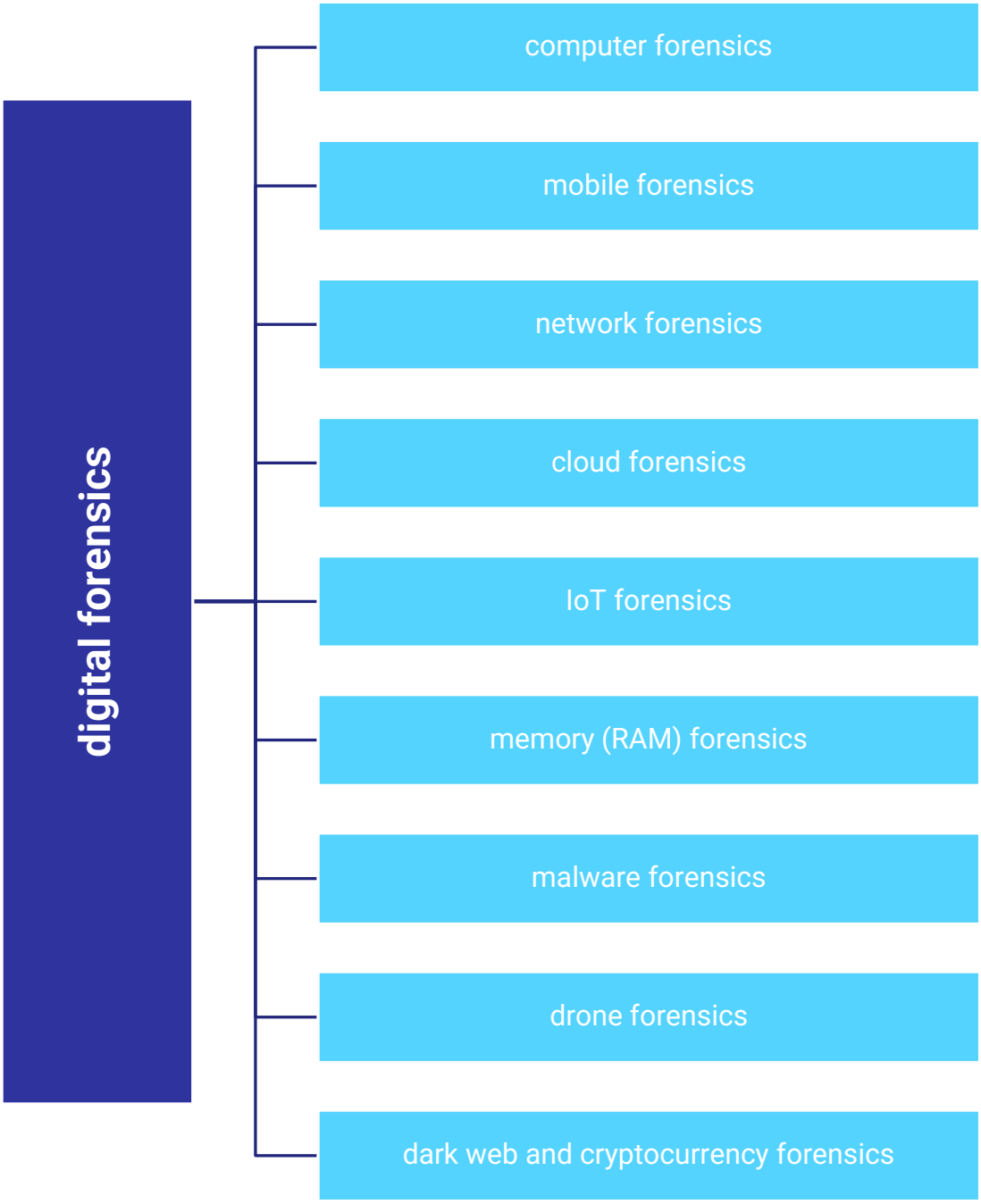


*Figure 1. Possible branches of digital forensics*

Poleg tega je ključna povezava med različnimi vejami digitalne forenzike in informacijsko-tehnološkim okoljem, saj vrsta infrastrukture določa, kje so digitalni dokazi shranjeni, kako je do njih mogoče dostopati in s kakšnimi forenzičnimi izzivi se preiskovalci soočajo:

### 'Klasična digitalna forenzika' v. spletna forenzika

- Tradicionalni IT (lokalna infrastruktura / on-premises) → podjetje upravlja celotno IT-infrastrukturo v lastnih prostorih; strežniki, omrežja, shranjevanje podatkov, operacijski sistemi in programska oprema se fizično nahajajo in upravljajo znotraj podjetja. To vključuje klasično računalniško forenziko, omrežno forenziko in forenziko podatkovnih baz, ki se izvajajo na fizičnih napravah, lokalnih strežnikih in internih omrežjih. Pogosti viri dokazov so trdi diski (HDD, SSD), lokalne podatkovne baze in sistemski dnevniki. Praviloma je potreben fizični dostop, vendar lahko popoln nadzor nad strojno opremo poenostavi izdelavo forenzičnih slikovnih kopij in analizo.
- IaaS → infrastruktura kot storitev (Infrastructure as a Service); IaaS prek interneta zagotavlja osnovne IT-vire, kot so navidezni strežniki, shranjevanje podatkov in omrežja. Podjetja to infrastrukturo najemajo pri ponudniku storitev v oblaku. Relevantni veji digitalne forenzike sta forenzika v oblaku in omrežna forenzika. Glavni viri podatkov so navidezni stroji (VM), shranjevalniki v oblaku ter dnevniki omrežnega prometa.
- PaaS → platforma kot storitev (Platform as a Service); PaaS ponuja platformo, na kateri lahko razvijalci razvijajo, testirajo in nameščajo aplikacije. Osnovno infrastrukturo in vmesno programsko opremo (middleware) upravlja ponudnik. Prevladujeta forenzika podatkovnih baz in forenzika v oblaku. Viri podatkov so

predvsem aplikacijski dnevniki, posnetki podatkovnih baz (database snapshots) in dnevniki API-jev.

- SaaS → programska oprema kot storitev (Software as a Service); SaaS zagotavlja popolnoma funkcionalno programsko opremo prek interneta. Uporabniki do programske opreme dostopajo prek spletnih brskalnikov ali aplikacij, ne da bi jim bilo treba skrbeti za namestitev, upravljanje ali vzdrževanje (namestitev ni potrebna). Primer je Microsoft 365. Na tem področju prevladujeta forenzika v oblaku in omrežna forenzika. Pomembni viri podatkov so revizijski dnevniki (audit logs), zgodovina različic in zapisi o aktivnosti uporabnikov.

Slika 11 prikazuje pregled različnih informacijskotehnoloških okolij..

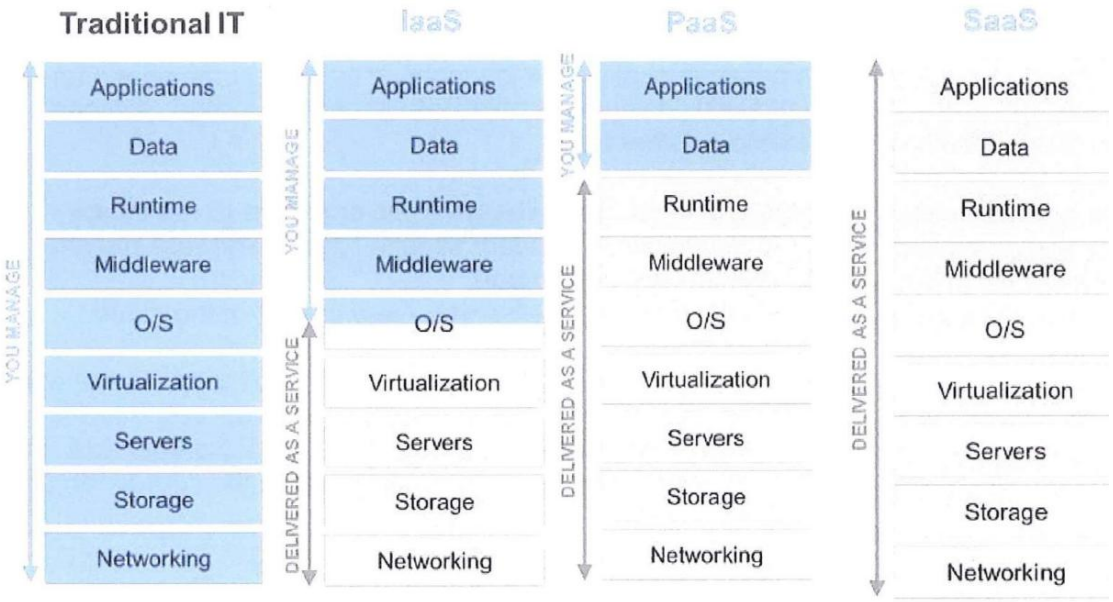


*Figure 2. Different information technology environment*[1]

Čeprav obstajajo ločene veje digitalne forenzike in je treba upoštevati vrsto infrastrukture, osnovna struktura digitalno-forenzičnega procesa večinoma ostaja enaka. Korake je mogoče na kratko povzeti kot (1) pridobivanje digitalnih dokazov, (2) njihovo analizo, vključno z interpretacijo, ter (3) njihovo predstavitev (npr. vodilnim preiskovalcem, sodišču), kot navajajo Dubey, Bhatt & Negi (2023). Drug vpliven model procesa je multidisciplinarni model digitalno-forenzične preiskave Lutui (2016), prikazan na sliki 12.

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


*Figure 3. Overview of digital forensics process*[2]

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

Poleg tega lahko izvajalcu pri strukturiranju digitalno-forenzičnega procesa pomaga tudi drug vodnik po korakih, ki vsebuje nekaj bolj praktičnih elementov kot prej predstavljena dva procesna modela:

### Devet praktičnih elementov digitalno-forenzičnega procesa

1. Sprejem: sprejmi napravo kot dokaz in prejmi zahtevo za pregled.
2. Identifikacija: ugotovi specifikacije in zmogljivosti naprave, opredeli cilje pregleda ter preveri pravno podlago za pregled.
3. Priprava: pripravi metode in orodja, ki bodo uporabljena, ter pripravi medij in forenzično delovno postajo za pregled.
4. Izolacija: zaščiti dokaz, prepreči oddaljeno uničenje podatkov ter napravo izoliraj od omrežja, Bluetootha in Wi-Fi.
5. Obdelava: izvedi forenzično pridobivanje podatkov, opravi forenzično analizo in preveri prisotnost zlonamerne programske opreme.
6. Verifikacija: potrdi pravilnost pridobitve podatkov in potrdi forenzične ugotovitve.
7. Dokumentiranje/Poročanje: vodi zapiske o ugotovitvah in postopku ter pripravi in dokončaj forenzično poročilo.
8. Predstavitev: pripravi dokazne priloge in predstavi ugotovitve.
9. Arhiviranje: kopijo podatkov varno shrani ter podatke ohrani v standardnih formatih za prihodnjo uporabo.

Za digitalnega forenzika oziroma izvajalca je pomembno tudi, da ima ves čas v mislih celoten potek forenzične preiskave:

### Postopek forenzične preiskave

1. Zasežene dokaze se preda digitalnemu forenziku.
2. Zavarovanje in evidentirano shranjevanje podatkov in podatkovnih nosilcev (evidenca, označevanje, nalepke ipd.).
3. Izdelava forenzičnih kopij podatkov: fizične slikovne kopije (image) in logične kopije podatkov.
4. Varno shranjevanje izvirnih dokazov.
5. Dokumentiranje dokazne verige (chain of custody)

Poleg tega je treba vedno upoštevati nekaj temeljnih načel digitalne forenzike:

### Temeljna načela digitalne forenzike

- zdelava forenzičnih kopij podatkov; razlikovati je treba različne vrste:
    - »ena na ena« kopije računalniško podprtih dokazov
    - fizične slikovne kopije (E01 [EnCase format slikovne kopije] ali RAW)
    - logične kopije podatkov (L01, AD1 ali CTR)
- Preiskovanje forenzičnih kopij oziroma kopij (post mortem analiza)
- Brez sprememb v zavarovanih podatkih.
- Natančna dokumentacija, kdo je kaj naredil in kdaj, pri ravnanju s forenzičnimi kopijami, da je zagotovljena dokazna veriga (chain of custody). To zahteva (1) kronološko dokumentiranje in (2) sledljivost pri zavarovanju prenosa, obravnavi ter predložitvi dokaznih predmetov. Sledi načelu, da digitalni forenzik uporablja (znanstveno) priznane metode in pripravi popolno dokumentacijo.
- Izdelava »ena na ena« kopij računalniško podprtih dokazov ob upoštevanju:

- zagotavljanja celovitosti in avtentičnosti dokazov
- zaščite pred pisanjem (write protection)
- verifikacije/preverjanja

- Ne spreminjajte ničesar namenoma. Spremembe nastanejo hitro, npr. že ob zagonu sistema ali priklopu (mount) trdega diska.
- Zelo pomembno: vedno in povsod zagotovite sledljivost (dokumentiranje!).

Poleg tega je pomembno poznati pravne vidike, saj morata biti zakonitost preiskave in zasega zagotovljeni. Poleg tega se digitalnemu forenziku praviloma ni treba ukvarjati s prepovedmi uporabe dokazov (to je naloga preiskovalca in nazadnje državnega tožilca). Nenazadnje je priporočljivo, da se ob naključnih najdbah posvetujete s preiskovalci

## 9.4.3 Kopije podatkov

V digitalni forenziki je izdelava forenzične kopije podatkov temeljni korak pri zavarovanju in analizi digitalnih dokazov. Zagotavljanje celovitosti in razpoložljivosti forenzičnih podatkov je ključno za preiskave, sodne postopke in odzivanje na kibernetske incidente. Ustrezno izdelana forenzična kopija omogoča preiskovalcem delo z natančno, nespremenjeno kopijo izvirnih podatkov, s čimer se zmanjša tveganje kontaminacije dokazov ali izgube podatkov.

Ta razdelek obravnava ključne vidike forenzičnega kopiranja podatkov, pri čemer začne z njegovimi temeljnimi načeli (razdelek 9.6.3.1), vključno s celovitostjo podatkov, avtentičnostjo in dokazno verigo (chain of custody). Nato poda pregled pogostih formatov forenzičnih kopij in njihove strukture (razdelek 9.6.3.2), temu pa sledi obravnava programskih mehanizmov zaščite pred pisanjem, ki preprečujejo posege v podatke

oziroma njihovo prirejanje (razdelek 9.6.3.3). Predstavljene so tudi različne vrste podatkovnih nosilcev in njihova vloga v forenzičnih preiskavah (razdelek 9.6.3.4), skupaj z analizo specializirane programske opreme za forenzično kopiranje ter strojnih rešitev (razdelek 9.6.3.5). Poleg tega razdelek obravnava izdelavo in uporabo forenzičnih zagonskih medijev (razdelek 9.6.3.6), ki omogočajo pridobivanje podatkov iz delujočih (live) in nedelujočih (offline) sistemov. Obravnavane so tudi omrežne metode forenzičnega kopiranja, vključno s tehnikami oddaljenega pridobivanja podatkov (razdelek 9.6.3.7). Nazadnje so predstavljeni posebni vidiki ravnanja s kompleksnimi sistemi shranjevanja, kot so polja RAID in naprave NAS (razdelek 9.6.3.8), pri čemer so na kratko izpostavljeni izzivi in dobre prakse pri zavarovanju takšnih podatkovnih struktur.

Razumevanje teh konceptov forenzičnim strokovnjakom in izvajalcem omogoča, da zagotovijo zanesljive, preverljive in sodno dopustne forenzične kopije podatkov, ki predstavljajo temelj kakovostne forenzične preiskave.

### 9.4.3.1 Načela forenzičnega kopiranja podatkov

Pri izdelavi forenzičnih kopij podatkov je treba dosledno upoštevati ključna načela:

- **Izdelava forenzičnih kopij in zaščita pred pisanjem (write-blocking):**
  - delo poteka izključno na forenzičnih kopijah, ne na izvirnem nosilcu
  - izdelava forenzičnih kopij kot bitno-identičnih slikovnih kopij (bitstream image) ali kot logičnih kopij
  - preprečevanje sprememb izvirnih podatkov ali nosilca med kopiranjem, preiskavo in pregledom

- dostop samo za branje med postopkom kopiranja (zaščita pred pisanjem) (write protection)

- **zagotavljanje integritete shranjevanja podatkov**:
  - zagotavljanje, da so forenzične kopije primerne za analizo
  - brez sprememb na kopiranih podatkih (po potrebi izdelava druge kopije)
  - uporaba predhodno izbrisanih/»očiščenih« nosilcev za kopiranje (zaradi tveganja navzkrižne kontaminacije)
  - verifikacija slikovnih kopij z uporabo zgoščenih vrednosti (hash) – primerjava hasha izvirnika in kopije po postopku kopiranja oziroma po kopirnih postopkih)

- **Dokumentiranje dokazne verige (chain of custody):** natančno dokumentiranje vseh ravnanj in posegov v zvezi s forenzičnimi kopijami podatkov (vzdrževanje dokazne verige)

### 9.4.3.2 Pregled in struktura pogostih formatov forenzičnih kopij podatkov

Obseg forenzičnega kopiranja podatkov v digitalni forenziki vključuje magnetne trde diske in SSD-je iz računalnikov, posamezne naprave za shranjevanje podatkov, kot so USB-ključki ali bliskovni pomnilniki, ter optične nosilce. Te je mogoče zavarovati na dva osnovna načina: s slikovno kopijo (image), ki ustvari celovito kopijo po sektorjih, ali z logično kopijo, ki se osredotoča na določene datoteke in imenike. Obe metodi podpirajo forenzična orodja, kot so X-Ways, EnCase, FTK, NUIX Imager in Magnet Acquire.

Slikovna kopija podatkov (image) je bitno-identična kopija nosilca podatkov, ki zajame vse podatke, vključno z datotekami, mapami ter nealokiranim, prostim oziroma sproščenim prostorom.

Slikovna kopija se razlikuje od kloniranja. Pri slikovni kopiji se ustvari stisnjena datoteka (forenzična slika) diska, particije ali sistema. Takšna kopija, ki podatke shrani v eno veliko datoteko, mora biti pred uporabo obnovljena oziroma priklopljena. V digitalni forenziki se forenzične slikovne kopije na primer izdelujejo s trdega diska osumljenca. Slikovno kopiranje se praviloma uporablja za naknadno analizo (post-mortem), medtem ko je kloniranje namenjeno kopiranju sistemov ali ustvarjanju identičnih nastavitev (npr. kloniranje starega HDD na SSD brez ponovne namestitve operacijskega sistema). Kloniranje lahko včasih služi tudi forenzičnim potrebam. Klonirani disk je takoj zagonski in uporaben. Za potrebe digitalne forenzike bi bilo na primer mogoče izdelati natančno bitno kopijo osumljenčevega diska.

Obstaja več pogosto uporabljenih formatov forenzičnih slikovnih kopij:

- RAW format: neposredna bitno-identična (bitstream) kopija nosilca podatkov. Odvisno od programske opreme za kopiranje se ustvarijo MD5 zgoščene vrednosti (hash) za celotno sliko ali za posamezne dele slike.
- Format Expert-Witness (EWF) (E01): nespremenljiv format, zasnovan za forenzično uporabo. Glava EWF vsebuje metapodatke, kot sta število blokov in velikost sektorjev. Vključuje ciklične redundančne preveritve (CRC) za preverjanje posameznih blokov. Ima segmentirano strukturo z glavami, podatki in tabelami sektorjev.

- Format EnCase Evidence File Format (Ex01): razvili Guidance/OpenText, temelji na formatu E01. V primerjavi z E01 je učinkovitejši in zmogljivejši; primarno ga podpirata EnCase in NUIX.

- Advanced Forensic Format (AFF): odprtokodni, od proizvajalcev neodvisen format, ki ga vzdržuje spletna skupnost. Podpira različici AFF4 in AFF4-L. V Nemčiji je manj pogosto uporabljen. Združljiv je z orodji, kot sta FTK Imager in Magnet Forensics AXIOM.

Digitalna forenzika vključuje tudi logične kopije. Logična kopija je kopija dejanskih podatkov na nosilcu ali particiji, pri kateri se zajamejo le datoteke in mape, ki so trenutno prisotne, ne pa nealokiranih območij ali izbrisanih podatkov. Logične kopije se običajno izdelujejo na kraju samem, na primer med preiskavami v podjetjih, ter tudi iz sistemov NAS

### 9.4.3.3 Programska zaščita pred pisanjem

Programska zaščita pred pisanjem pomeni uporabo orodij, ki preprečujejo spreminjanje podatkov na podatkovnem nosilcu tako, da uveljavijo dostop samo za branje. Obstajajo različne programske rešitve, ki zagotavljajo, da med forenzičnimi preiskavami ne pride do nenamernih sprememb ali brisanja podatkov.

- X-Ways Forensics: zaščiti celotne diske ali posamezne particije. Učinkovit je šele potem, ko Windows disk prepozna in do njega dostopa.

- Diskpart: uporablja se za nastavitev ali odstranitev zaščite pred pisanjem na diskih ali nosilcih (volumnih). Učinkovit je šele, ko Windows napravo prepozna.

- FastBloc SE: programska rešitev za blokiranje pisanja (write-blocking), ki omogoča forenzično izdelavo slikovnih kopij prek kanalov IDE, SATA, SCSI, FireWire in USB brez uporabe strojnih write-blockerjev.

- Zaščita na podlagi registra: omogoča zaščito pred pisanjem za shranjevalne naprave z spremembo sistemskih nastavitev, ki omejijo pravice pisanja.

- USB vhodi: zaščita pred pisanjem prek diskpart (ni zanesljivo) ali s spremembami v registru; zaščita na ravni USB naprave.

### 9.4.3.4 Podatkovni nosilci

Magnetni podatkovni nosilci, kot so trdi diski (HDD), shranjujejo podatke magnetno na vrtečih se ploščah, ki so razdeljene na sektorje. Ti sektorji imajo praviloma fizično velikost 512 bajtov ali pri sodobnih diskih 4096 bajtov, podatki pa se mehansko berejo z bralno/pisalno glavo.

Bliskovni podatkovni nosilci, kot so SSD-ji in USB-ključki, shranjujejo podatke elektronsko v pomnilniških celicah, organiziranih v strani in bloke. Za razliko od magnetnih diskov nimajo gibljivih delov. Bliskovni pomnilnik uporablja krmilnike, ki zaradi združljivosti z obstoječimi sistemi posnemajo tradicionalno strukturo, ki temelji na sektorjih. Je odporen na udarce, prostorsko majhen, hkrati pa lahko ponuja velike kapacitete in porabi manj energije. Ima pa tudi slabosti. Ena pomembnejših je omejena življenjska doba. V osnovi poznamo dve vrsti bliskovnega pomnilnika: NAND in NOR. NAND je cenejši in omogoča večje kapacitete. Deluje podobno kot blokovna naprava, kot je HDD, ter vsebuje datotečni sistem, ki ga je mogoče particionirati.

Pogoni SSD (Solid-State Drives) uporabljajo bliskovni pomnilnik NAND in so zasnovani kot zamenjava klasičnih trdih diskov. Prinašajo občutne izboljšave zmogljivosti, na primer hitrejše branje in pisanje podatkov. Hibridna rešitev za shranjevanje, imenovana hibridni pogon SSHD (Hybrid Solid State Drive), združuje klasični magnetni trdi disk z dodatnim bliskovnim pomnilnikom. Pogosto uporabljeni podatki se shranjujejo v bliskovni pomnilnik, kar pospeši splošno delovanje sistema, saj se podatki predpomnijo za hitrejši dostop.

#### 9.4.3.5 Programska oprema in strojna oprema za forenzično kopiranje podatkov

Forenzično kopiranje podatkov vključuje kombinacijo specializirane programske in strojne opreme. Med najpogosteje uporabljanimi programskimi orodji so posamezni programi za izdelavo slikovnih kopij (imaging), kot so:

- FTK Imager: prenosna in namestitvena različica. Omogoča predogled lokalnih diskov, omrežnih deljenih map in slikovnih kopij. Ustvarja bitno-identične slikovne kopije v formatih RAW, E01 in SMART. Omogoča izračun zgoščenih vrednosti (hash), izvoz datotek, delitev in združevanje slik, ter izdelavo logičnih kopij (format AD1). Podpira več platform (Windows, Linux, macOS).

- EnCase Imager: lastniško orodje za izdelavo slikovnih kopij z naprednimi funkcijami.

- Magnet Acquire: enostavno orodje za izdelavo kopij mobilnih naprav in računalnikov.

- NUIX Imager: varno kopiranje fizičnih diskov in podatkov v okoljih oblaka. Podpira posebne logične formate (*.nli) z metapodatki in preverjanjem zgoščenih vrednosti (hash).

Poleg tega celovite forenzične zbirke (forensic suites) ponujajo širši nabor orodij za digitalno forenziko, na primer:

- X-Ways Forensics: podpira izdelavo slikovnih kopij fizičnih in logičnih pogonov. Ponuja različne načine kopiranja (polno, minimalno, očiščeno). Omogoča ustvarjanje datotečnih vsebnikov (file container), pretvorbo formatov in redko (sparse) kompresijo.

- EnCase Forensics: celovit paket za izdelavo slikovnih kopij in analizo.

- Magnet Forensics IEF/AXIOM: osredotočen na analizo digitalnih dokazov in izdelavo slikovnih kopij.

Za specifičen pregled orodij digitalne forenzike v kontekstu trgovine z ljudmi (THB) glejte razdelek 9.6.4.3. Forenzično pridobivanje podatkov zahteva tudi ustrezna strojna orodja:

- Duplikatorji diskov z blokado pisanja (write-blocked disk duplicators) se uporabljajo za izdelavo natančnih, bitno-identičnih kopij nosilcev podatkov, pri čemer preprečujejo kakršne koli spremembe na izvirnem nosilcu. Primera sta Logicube in VOOM Hardcopy. Prenosne forenzične naprave so rešitve, namenjene hitremu kopiranju na terenu, pogosto v kombinaciji s prenosniki ali zunanjimi diski.

- Dodatne funkcionalnosti in orodja vključujejo varno kopiranje slikovnih kopij z orodji, kot je NUIX Evidence Mover, ter preverjanje zgoščenih vrednosti (hash) z uporabo programov HashMyFiles, HashCalc in MD5.exe. Ta orodja se brez težav povezujejo s forenzičnimi programi, kot sta EnCase in X-Ways, ter pomagajo zagotavljati celovitost slikovnih kopij v formatu E01.

Za odstranjevanje diskov iz kompaktnih sistemov so lahko v pomoč viri, kot so iFixit, video vodiči na YouTubu in uradni portali (npr. TeSIT). Kadar do pogonov ni mogoče fizično dostopati, je priporočljiva uporaba forenzičnih zagonskih medijev, ki omogočajo pridobivanje podatkov..

### 9.4.3.6 Izdelava in uporaba forenzičnih zagonskih medijev

Forenzični zagonski mediji so pomembno orodje v digitalni forenziki, zlasti kadar iz računalnika ni mogoče odstraniti ali neposredno dostopati do podatkovnega nosilca oziroma kadar ni na voljo blokade pisanja (write blocker).

Poznamo dve glavni vrsti zagonskih sistemov:

- Basic Input/Output System (BIOS): tradicionalni vmesnik med strojno opremo računalnika in operacijskim sistemom. Omogoča zagon do štirih operacijskih sistemov na enem disku. Aktivira se takoj po vklopu računalnika. Zasnovan je za nosilce podatkov, ki temeljijo na MBR.
- Extensible Firmware Interface (EFI): naslednik BIOS-a, ki podpira do 128 operacijskih sistemov na enem disku. Različice vključujejo UEFI (Unified Extensible Firmware Interface) za Windows/Linux in EFI za macOS. Je ključen za diske, ki temeljijo na GPT. Uporablja se za zagon operacijskega sistema na

podatkovnih nosilcih GPT. Podpirajo ga vsi sodobni operacijski sistemi. Ponuja izboljšano varnost in funkcionalnost:

- Compatibility Support Module (CSM): simulira BIOS za strojno opremo in operacijski sistem; način združljivosti oziroma “legacy mode”.
- Secure Boot: preprečuje, da bi se pred zagonom sistema naložila zlonamerna programska oprema.
- Trusted Boot: podpisovanje jedrnih/sistemskih datotek v sistemu Windows 10 za izključitev zlonamerne kode oziroma zlonamerne programske opreme.

- Zaporedje zagona (boot sequence):
  - BIOS: preverja določene pogone enega za drugim, ali vsebujejo zagonski operacijski sistem, in nato prenese zagonski proces.
  - UEFI: vključuje vgrajen zagonski upravljalnik, ki omogoča neposredno izbiro pogona

### Linux zagonski medij (forenzični)

Linux zagonski mediji so opremljeni s širokim naborom brezplačnih forenzičnih orodij za naloge, kot so izdelava kopij podatkov, analiza in obnova. Primeri takšnih orodij so: za kopiranje (Guymager, dcfldd, ddrescue), za analizo (Sleuthkit, Autopsy) in za obnovo (Foremost, TestDisk).

Med priljubljene distribucije Linuxa sodijo Knoppix, Helix, CAINE (Computer Aided INvestigative Environment), DeepThought, DEFT, Grml in Kali Linux.

Izdelava Linux zagonskega medija: Linux sistemi so shranjeni v Casper vsebnikih, formatiranih kot FAT32, uporabniško ustvarjene datoteke pa se shranjujejo ločeno (zunaj vsebnika). Zagonski medij je mogoče ustvariti z orodji, kot so YUMI, Rufus ali Linux Live USB-Creator. Naprave, kot sta Zalman ali IODD, lahko služijo kot strojna oprema za zagonski medij oziroma varnostno kopiranje.

Izdelava slikovne kopije (image backup): praviloma se uporabljajo kopije v formatu RAW. Orodje »dd« je običajno na voljo na vsakem Linux sistemu. Sintaksa je na primer: dd if=/dev/sdX of=/media/image.dd. Pri velikih slikovnih kopijah je lahko potrebno razdeljevanje na dele. Napredek je mogoče spremljati z novejšimi različicami dd ali z dodatnimi orodji, kot je Pipe Viewer (pv). Verifikacija se izvaja z uporabo zgoščevalnih algoritmov (npr. md5sum ali podobno). Po razdelitvi je treba dele slike ponovno združiti.

Alternativni programi za kopiranje v Linuxu so Guymager, dcfldd, dc3dd in ddrescue. Logična kopija podatkov se lahko izdela z uporabo tar (Tape Archiver), ki je danes na voljo tudi v okolju Windows.

### Forenzični zagonski medij na osnovi Windowsa

Windows zagonski mediji zagotavljajo alternativno ali dopolnilno funkcionalnost v primerjavi z Linux zagonskimi mediji.

- Windows Preinstallation Environment (WinPE): minimalističen, samostojen operacijski sistem (OS), neodvisen od sistema, nameščenega na napravi. Omogoča analizo sistema in izdelavo slikovnih kopij brez vpliva na podatke nameščenega operacijskega sistema.

- Windows Forensic Environment (WinFE): prilagojen WinPE, posebej konfiguriran za forenzično uporabo. Uporaba:
    - izdelava forenzičnih kopij podatkov z orodji, kot sta X-Ways Forensics ali FTK Imager
    - triaža in predogled dokazov
    - obhod skrbniških (administratorskih) privilegijev na ciljnih sistemih
- Windows Image Format (WIM): format za shranjevanje osnovnih slik Windows sistemov (npr. Pro, Home, Education). Uporablja se za zagon Windows PE (datoteka »boot.wim«). Pri namestitvi se zažene WinPE in se na trdi disk zapiše »install.wim«. Format je združljiv z orodji, kot je 7zip, za ogled vsebine slik. Lahko je na voljo tudi v stisnjenem formatu ESD (Electronic Software Distribution).

### Napredne možnosti zagonskih medijev

- Ventoy: programsko orodje, ki omogoča zagon ISO-slik neposredno z USB-ključka. Med funkcijami so združljivost s Secure Boot in podpora particijam GPT. Ustvari dve particiji (FAT za zagonski upravljalnik in exFAT za shranjevanje ISO-slik).
- Macintosh zagonski mediji:
    - Target Disk Mode (TDM): omogoča, da Mac deluje kot zunanji disk prek povezave Thunderbolt ali FireWire.
    - Recovery Mode: omogoča dostop do orodij, kot sta Disk Utility in Terminal, za izdelavo slikovnih kopij.
    - Dešifriranje FileVault: za dostop so potrebna gesla ali obnovitveni ključi.

- Posebnosti varnostnega čipa T2: omejuje zagon z zunanjih naprav in za izdelavo kopij zahteva napravi specifična poverila.

- Večzagonski medij (multi-boot): orodja, kot je YUMI, omogočajo izdelavo zagonskih USB-ključkov z več možnostmi operacijskih sistemov (Linux, Windows, macOS). Treba je zagotoviti združljivost z različnimi sistemi (BIOS/UEFI, macOS System Integrity Protection)..

**Posebni vidiki pri macOS**

- FileVault in varnostni čip T2: šifriranje zahteva znana poverila (geslo ali obnovitveni ključ). Čip T2 vključuje Secure Boot in omejitve zagona z zunanjih naprav.

- Fusion Drives: hibrid HDD in SSD, ki zahteva ločeno izdelavo slikovne kopije vsake komponente ter naknadno rekonstrukcijo.

### 9.4.3.7 Kopiranje podatkov preko omrežja

- Omrežno kopiranje podatkov je učinkovita metoda za izdelavo slikovnih kopij in prenos podatkov med sistemi.
- EnCase in LinEn zagotavljata robusten okvir za omrežno kopiranje, saj preiskovalcem omogočata varen dostop do oddaljenih sistemov in izdelavo slikovnih kopij.
- Postopek:
  - Zaženite ciljni računalnik z uporabo forenzične distribucije Linuxa, na primer Deft.

- Na računalniku za kopiranje (backup PC) zaženite EnCase Imager.
- Vzpostavite fizično povezavo med računalnikoma s križnim (crossover) kablom.
- Obema sistemoma dodelite statična IP-naslova: v Windows prek »Network and Sharing Center« v »Adapter Settings«; v Linuxu z uporabo sistemskih ukazov za nastavitev IP-naslova.
- Preverite povezavo s ping testom.
- Program LinEn kopirajte na zunanji nosilec in ga priklopite (mount) na ciljni sistem.
- Na ciljnem sistemu pojdite do lokacije LinEn in ga zaženite; v vmesniku LinEn izberite možnost »Server«.
- Na računalniku za kopiranje v EnCase začnite postopek izdelave slikovne kopije prek možnosti »Add Evidence« in »Crossover Preview«.

- Prednosti: preprečuje samodejen dostop s pisanjem do priključenih nosilcev podatkov. Linux sistemi lahko prepoznajo kompleksne strojne konfiguracije, na primer RAID krmilnike.
- Unix orodja in forenzični zagonski mediji na osnovi Linuxa omogočajo prilagodljivost in nadzor pri omrežnem kopiranju.
- Postopek:
    - Povežite oba sistema s križnim kablom (crossover) ali običajnim omrežnim kablom (patch). Po potrebi uporabite omrežno vozlišče (hub) ali stikalo (switch).

- Dodelite statična IP-naslova vsakemu računalniku: v Windows prek »Network and Sharing Center«; v Linuxu nastavite IP z orodji, kot je ifconfig (npr. ifconfig eth0 192.168.100.1).
- Preizkusite povezljivost s ping ukazom, da se prepričate, da napravi komunicirata.

Kombinacija dd in Netcat omogoča preprost in učinkovit prenos podatkov prek omrežja.

- Postopek:
  - Pripravite ciljni računalnik: z Netcat začnite poslušati dohodne podatke; podatke shranite neposredno v datoteko ali jih posredujte dd-ju za zapis.
  - Pripravite izvorni računalnik: diskovne podatke pretočite (stream) na cilj; v Linuxu uporabite dd za branje podatkov in izhod preusmerite v Netcat. V Windows uporabite združljiv dd.exe za podobna opravila.
- Dodatni vidiki: začasno onemogočite požarni zid in protivirusno zaščito, da ne motita prenosa. Netcat lahko sproži varnostna opozorila, saj je pogosto označen kot »potencialno nezaželen program«.

Uporaba SSH omogoča varen prenos podatkov, zlasti pri delu s sistemi Linux ali macOS.

- Postopek:
  - Z dd ustvarite bitno-identično kopijo izvornega diska.
  - Izhod preusmerite prek povezave SSH na ciljni sistem, kjer se shrani kot forenzična slikovna kopija.
- Dodatne funkcije:
  - Spremljanje napredka: uporabite orodja, kot je Pipe Viewer (pv), za spremljanje prenosa v realnem času.

- Stiskanje: podatke pretočite prek orodij za stiskanje, kot je Gzip, da zmanjšate zahteve po prostoru za shranjevanje.

### 9.4.3.8 Posebnosti shranjevanja podatkov

Sistemi RAID (Redundant Array of Independent Disks) so zasnovani za izboljšanje zmogljivosti in zanesljivosti z razporejanjem podatkov preko več trdih diskov.

Vrste RAID:

- strojni RAID: upravlja ga namenski RAID krmilnik; zagotavlja dobro zmogljivost in zanesljivost.
- programski RAID: nadzoruje ga operacijski sistem; običajno je cenejši, vendar je odvisen od sistemskih virov.

Nivoji RAID:

- JBOD: vsi diski (HDD) so združeni v en velik shranjevalni prostor; shranjevalni sistem predstavlja en velik datotečni sistem, v katerem se shranjujejo podatki.
- RAID0: vsi diski (HDD) so združeni v en velik shranjevalni sistem; logika shranjevanja (velikost “stripe”) zagotavlja, da so podatki razdeljeni in shranjeni v kosih na posameznih diskih.
- RAID10: dva ali več diskov (HDD) se združi v en shranjevalni prostor (RAID0), ta shranjevalni prostor pa se nato zrcali (RAID1 – mirroring).
- RAID5 ali RAID6: v en shranjevalni prostor se združijo najmanj 3 diski (RAID5) oziroma najmanj 4 diski (RAID6); paritetne informacije so porazdeljene po diskih. Če odpove en disk (RAID5) ali dva diska (RAID6), je vsebino mogoče obnoviti iz

preostalih podatkovnih nosilcev. Odvisno od krmilnika/proizvajalca se lahko paritetne informacije po posameznih diskih rotirajo “naprej” ali “nazaj”.

- Synology Hybrid RAID (SHR): različica RAID, ki uporablja Linux programski RAID (MD RAID in LVM2).

Dobre prakse pri kopiranju podatkov iz RAID:

- natančno dokumentiranje konfiguracije RAID (npr. nastavitve BIOS, vrsta RAID krmilnika, RAID nivo, velikost “stripe”).
- kopiranje prek RAID krmilnika, npr. z zagonom sistema z Linux Live CD ali WinFE, ki prepoznata strojni RAID krmilnik.
- po potrebi izdelava logične kopije podatkov, npr. s FTK Imager možnostjo »Custom Content Image«.

Sistemi NAS (Network Attached Storage) so kompaktni, samostojni strežniki, ki uporabljajo prilagojene operacijske sisteme, običajno lahke, prilagojene različice Linuxa. Notranji podatkovni nosilci so praviloma SATA trdi diski. Prvi korak je izdelava klasičnih slikovnih kopij (image). Pri odstranjevanju diskov iz sistema je pomembno označiti, kateri disk je bil v katerem ležišču (slotu). NAS sistemi imajo brskalniški uporabniški vmesnik (Web GUI). Za dostop do tega vmesnika mora biti NAS priključen v preiskovalno omrežje

### 9.4.4 Digitalna forenzika v kontekstu trgovine z ljudmi in delovnega izkoriščanja

Trgovina z ljudmi, vključno z delovnim izkoriščanjem, se vse bolj opira na digitalno komunikacijo, finančne transakcije in spletno novačenje (Europol, 2020; 2024). Posledično ima digitalna forenzika ključno vlogo pri identifikaciji storilcev, razkrivanju

vzorcev izkoriščanja žrtev in zavarovanju dokazov za kazenski pregon. Ta podrazdelek obravnava, kako je mogoče digitalno-forenzične metodologije uporabiti v primerih trgovine z ljudmi, pri čemer upošteva tako tehnične kot etične vidike. Razdelek se začne s predstavitvijo ključnih virov digitalnih dokazov na področju trgovine z ljudmi (THB) ter, kjer je mogoče, virov, relevantnih posebej za delovno izkoriščanje (razdelek 9.6.4.1). Nato razdelek 9.6.4.2 obravnava analizo digitalnih dokazov, značilnih za THB (npr. kaj preiskovalci iščejo?). Sledi razdelek 9.6.4.3, ki prikazuje nekaj možnih digitalno-forenzičnih orodij za uporabo v organih pregona. Nato so predstavljeni glavni izzivi, ki so posebej relevantni za digitalno-forenzični proces v preiskavah THB (razdelek 9.6.4.4). Razdelek se zaključi s pravnimi in etičnimi vprašanji, ki jih je treba upoštevati (razdelek 9.6.4.5). Dodatni pregled tehnologij za preprečevanje in boj proti trgovini z ljudmi je pripravil tudi UNODC – Module 14: Links between Cybercrime, Trafficking and Smuggling of Migrants.

### 9.4.4.1 Ključni viri digitalnih dokazov

Storilci trgovine z ljudmi in izkoriščevalci uporabljajo različne digitalne platforme in tehnologije ter pri tem za seboj puščajo ključne forenzične sledi, organi pregona pa lahko digitalne dokaze uporabijo za prepoznavanje trgovine z ljudmi, identifikacijo storilcev ter pridobitev dokazov za kazenski pregon (Cellebrite, 2024). Pogosti viri dokazov vključujejo:

#### Osebne elektronske naprave

V preiskavah delovnega izkoriščanja so osebne digitalne naprave, kot so mobilni telefoni in računalniki, lahko ključni viri dokazov. Te naprave pogosto vsebujejo komunikacijo, kontakte, podatke o finančnih transakcijah in lokacijske podatke, ki lahko razkrijejo izkoriščevalske prakse.

- Mobilne naprave: storilci pogosto uporabljajo mobilne naprave za koordinacijo nezakonitih aktivnosti. Dokazi iz teh naprav lahko vključujejo: (1) dnevnike klicev in sezname stikov, ki razkrivajo vzorce komunikacije in omrežja, (2) SMS-sporočila in zgodovino klepetov, ki lahko vsebujejo podrobnosti o novačenju, koordinaciji in izkoriščanju, (3) multimedijske datoteke, kot so fotografije in videoposnetki, ki lahko dokumentirajo žrtve, lokacije ali nezakonita dejanja, ter (4) lokacijske podatke (GPS), s katerimi je mogoče slediti premikom in identificirati ključne lokacije.

- Računalniki: različne vrste shranjenih podatkov oziroma podatkov, do katerih je mogoče dostopati prek računalnika, so lahko posebej pomembne za preiskave trgovine z ljudmi (možno je tudi prekrivanje z podatki iz mobilnih naprav): (1) komunikacijski zapisi, kot so e-pošta in sporočila, aktivnosti na družbenih omrežjih ter spletni oglasi ali objave delovnih mest, (2) finančni podatki, kot so bančne transakcije in plačilni zapisi ali zapisi o transakcijah s kriptovalutami, (3) osebni identifikacijski podatki, kot so digitalne kopije osebnih dokumentov, ter lokacijski podatki, (4) evidence o zaposlitvi in delovnih pogojih, kot so pogodbe o zaposlitvi, nezakoniti urniki dela, sistemi evidentiranja delovnega časa in prisotnosti (npr. za ugotavljanje čezmernih delovnih ur), (5) potovalni podatki, kot so rezervacije pri letalskih družbah ali turističnih agencijah oziroma nakupi vozovnic in potovalni načrti, (6) zgodovina aktivnosti na spletu (na odprtem ali temnem spletu), (7) zdravstvena in medicinska dokumentacija, npr. zapisi o obiskih zdravnika po fizičnih napadih na žrtve, ali (8) posnetki nadzornih kamer oziroma podatki iz varnostnih sistemov na delovnih mestih ali v zasebnih objektih, ki prikazujejo bivalne in delovne razmere žrtev.

### Hramba v oblaku

Shranjevanje v oblaku lahko storilci uporabljajo zaradi priročnosti, oddaljenega dostopa in možnosti shranjevanja velikih količin podatkov, zato je v takšnih primerih pomemben vir digitalnih dokazov. Podatki, pridobljeni iz shranjevanja v oblaku, so lahko podobni tistim, ki so bili zgoraj navedeni za mobilne naprave in računalnike. Poleg tega so v shranjevanju v oblaku pogosto prisotni tudi specifični podatki, kot so digitalni koledarji, ki lahko razkrijejo izvedena ali načrtovana srečanja, premike žrtev oziroma potovanja ali druge logistične informacije o aktivnostih, ki so bile deljene znotraj mreže trgovine z ljudmi. Zato lahko shranjevanje v oblaku z večjo verjetnostjo razkrije strukturo mreže ter identificira žrtve, ki so izpostavljene organiziranemu delovnemu izkoriščanju.

Dostop do podatkov, shranjenih v oblaku, in njihova analiza pa zahtevata ustrezne pravne postopke in posebno tehnično znanje, da se zagotovi celovitost dokazov (zlasti če uporabniška poverila niso znana). Tehnični načini za (vsaj delni) dostop so na primer sodelovanje s ponudnikom storitev v oblaku, uporaba orodij za ekstrakcijo podatkov iz oblaka, uporaba API-jev oblačnih storitev, dostop prek zaseženih naprav (prijava z uporabniškimi poverili, uporaba varnostnih kopij naprav ter preverjanje, ali se je naprava sinhronizirala z oblakom), analiza metapodatkov datotek, shranjenih v oblaku, uporaba omrežne forenzike (razdelek 4.1.1) ali pridobitev dnevniških zapisov storitve pri ponudniku (npr. zgodovina prijav ali zgodovina prenosov datotek).

### Komunikacijske platforma in platforme za novačenje

Internet storilcem omogoča dostop do potencialnih žrtev prek različnih digitalnih kanalov, vključno z družbenimi omrežji in spletnimi stranmi za zaposlovanje (UNODC, 2019a). Fraser (2016) podrobneje pojasnjuje, kako se z premikom od geografskih k spletnim omrežjem spreminjajo procesi med storilci trgovine z ljudmi in žrtvami. Fraser

izpostavlja, da storilci danes znajo uporabljati družbena omrežja in temni splet. Prispevek tudi prikazuje, kako ta omrežja vplivajo na neravnovesje moči v trgovini z ljudmi in oblikujejo izkušnje žrtev (Fraser, 2016). Digitalni dokazi s teh platform lahko vključujejo (1) profile in objave, ki lahko vsebujejo poskuse novačenja, zavajajoče ponudbe za delo ali oglase za nezakonite storitve, (2) zasebna sporočila (ki omogočajo neposredno komunikacijo med storilci in žrtvami) ter (3) članstva v skupinah, ki lahko kažejo na vključenost v mreže trgovine z ljudmi ali povezane forume. Analiza teh elementov lahko razkrije na primer strategije novačenja ter pomaga identificirati tako žrtve kot storilce.

- Družbena omrežja: poročilo Kunz idr. (2018) povzema, katere spletne strani se uporabljajo za namene spolnega izkoriščanja. Med njimi so (1) platforme za ogled in komentiranje, kot so Facebook, Instagram in Snapchat, pa tudi YikYak in Wispher, (2) platforme za pogovore, kot so Tinder, Blendr, WhatsApp in KIK, pa tudi Yellow in #1 Chat Avenue kot manj pogoste platforme, (3) spletne strani za "webcam" interakcije, vključno s Chatroulette, Omegle in Monkey, ter (4) strani za oglaševanje in prodajo, kot so Cityxguide, skipthegames, bedpage, seekingarrangement.com ali sugar-babies.com. Za delovno izkoriščanje takšnega pregleda ni bilo mogoče najti. Kljub temu je znano, da se za novačenje za izkoriščevalsko delo uporabljajo glavna (mainstream) družbena omrežja, skupaj s spletnimi portali za zaposlitev in malimi oglasi (glej npr. Europol, 2024).

- Spletna mesta za zaposlovanje/novačenje: tudi če so ti portali in morebitne strani z malimi oglasi legitimni, lahko storilci objavljajo zavajajoče ponudbe za delo in ciljajo ranljive skupine, ki iščejo zaposlitev. V naslednjem koraku storilci za izmenjavo operativnih podrobnosti pogosto uporabijo aplikacije za neposredno sporočanje, saj zagotavljajo "varnejše" okolje za komunikacijo (Europol, 2024).

- Spletni oglasi: razlika v primerjavi z družbenimi omrežji, aplikacijami za sporočanje in spletnimi mesti za zaposlovanje je v tem, da je spletni oglas mogoče razumeti kot enosmerno komunikacijo, medtem ko so ostali viri praviloma namenjeni dvosmerni komunikaciji med osebami (npr. potencialno žrtvijo in domnevnim storilcem). Značilnosti spletnih oglasov, povezanih s trgovino z ljudmi z namenom delovnega izkoriščanja, vključujejo:

    - Pomanjkanje konkretnih informacij: oglasi pogosto navajajo nejasen opis dela z minimalnimi podrobnostmi o nalogah, odgovornostih ali delovnih pogojih. Takšna nedoločnost je namenjena privabljanju širšega kroga kandidatov, ne da bi razkrila morebitne izkoriščevalske okoliščine (Volodko, Cockbain & Kleinberg, 2020).

    - Nerealistične obljube: ponudbe lahko vključujejo nenavadno visoke plače, pospešeno urejanje vizumov ali druge ugodnosti, ki se zdijo »predobre, da bi bile resnične«, z namenom privabiti osebe, ki iščejo boljše priložnosti (glej npr. Fraser, 2016).

    - Ciljane skupine: novačenje je pogosto usmerjeno v specifične skupine, kot so migranti ali osebe iz ekonomsko prikrajšanih okolij, ki so bolj izpostavljene izkoriščanju (Volodko, Cockbain & Kleinberg, 2020).

Čeprav so bile izvedene raziskave spletnih oglasov za spolno izkoriščanje z uporabo sodobnih tehnoloških metod, kot je obdelava naravnega jezika (NLP) (npr. Perez & Rivas, 2023; Lugo-Graulich idr., 2024), delovno izkoriščanje in druge oblike trgovine z ljudmi na tem področju še vedno nimajo dovolj znanstvenih raziskav.

Temni splet v primerjavi z odprtim spletom: temni splet gostuje na šifriranih omrežjih, do katerih je mogoče dostopati le s specializirano programsko opremo; objave in oglasi na temnem spletu praviloma omogočajo višjo stopnjo anonimnosti. Takšna prikritost predstavlja velik izziv za organe pregona, saj te platforme pogosto uporabljajo napredne tehnične ukrepe za zaščito identitete uporabnikov. Nasprotno so objave in oglasi na odprtem spletu javno dostopni in jih pogosto najdemo na uveljavljenih platformah, kot so družbena omrežja in strani z malimi oglasi. Čeprav lahko uporabljajo kodiran jezik in podobe, da se izognejo odkrivanju, javna dostopnost omogoča lažje spremljanje s strani organov pregona. Storilci uporabljajo tako odprti kot temni splet za oglaševanje storitev ali izkoriščevalskih "priložnosti". Relevantni digitalni dokazi na temnem spletu lahko vključujejo na primer: (1) male oglase in ponudbe, ki lahko oglašujejo nezakonite storitve ali zavajajoče zaposlitvene priložnosti, (2) objave in komunikacijo na forumih, kjer se razpravlja o metodah, izmenjujejo informacije ali dogovarjajo transakcije (npr. objava v smislu »delavci na voljo za nizkocenovno delo«), ali (3) ponarejene dokumente, pridobljene na tržnicah temnega spleta, kot so ponarejeni vizumi in delovna dovoljenja za osebe brez urejenega statusa.

### Nadzor in sledenje

Podatki o nadzoru in sledenju se nanašajo na vse podatke, ki lahko razkrijejo lokacijo, gibanje ali ravnanja posameznikov; pogosto se zbirajo z elektronskimi sredstvi, zato je pri tem ključna digitalna forenzika. Sodobna okolja, opremljena z nadzornimi sistemi in napravami interneta stvari (IoT), lahko nehoteno zabeležijo aktivnosti, povezane s trgovino z ljudmi. Preiskava lahko (če je to pravno dopustno in ustrezno odrejeno) omogoči tudi sledenje in spremljanje osumljencev.

### Nadzor, ki ga odredijo organi pregona (praviloma zahteva sodno odredbo)

- GPS sledenje, npr. sledenje vozilom: organi pregona ga lahko uporabijo za spremljanje premikov. Organi lahko na primer sledijo gibanju avtomobila osumljenca, ki žrtve redno prevaža na različne lokacije dela in nazaj. Vzorci v lokacijskih podatkih vozila lahko pomagajo pri lociranju "žarišč" trgovine z ljudmi ali pri prepoznavanju potovalnih poti žrtev oziroma njihovega delovnega ritma (npr. delovnih ur).
- Nadzorne kamere: posnetki CCTV iz javnih ali zasebnih nadzornih kamer se lahko uporabijo za sledenje gibanju storilcev ali žrtev na določenih lokacijah (npr. na delovnih mestih, v bližini meja).
- Prestrezanje komunikacij (prisluškovanje): prisluškovanje (npr. telefonskim klicem, e-pošti, sporočilom) lahko zagotovi vpogled v aktivnosti, povezane s trgovino z ljudmi. Prisluškovanje lahko organom omogoči spremljanje, kako storilci dogovarjajo prevoze, plačila, grožnje žrtvam ipd.
- Sledilne funkcije na mobilnih telefonih: mobilna triangulacija in GPS podatki mobilnih telefonov se lahko uporabijo za natančno določanje lokacije žrtve ali storilca, na primer za kartiranje lokacij skozi čas.
- Droni oziroma zračni nadzor: droni, opremljeni s kamerami, se lahko uporabijo za spremljanje gibanja na večjih območjih, zlasti na podeželju ali na težko dostopnih območjih, kjer je drugačno fizično opazovanje oteženo.

### Nadzor s strani storilcev (podatki, ki jih zbirajo storilci)

- Sledenje mobilnim napravam s strani storilcev: storilci lahko uporabljajo telefone žrtev ali lastne naprave za sledenje žrtvam. To lahko vključuje uporabo aplikacij za GPS-sledenje ali celo namestitev vohunske programske opreme (npr. mSpy, FlexiSPY) za spremljanje lokacije žrtve in njenih komunikacij.

- Lokacijski podatki iz naprav IoT: naprave interneta stvari, kot so pametne ure ali celo povezana vozila, lahko storilci uporabijo za spremljanje lokacije žrtev. Dnevniške zapise (logs) teh naprav je mogoče analizirati, na primer za ugotavljanje nenavadnih časov dostopa ali sprememb v okolju.
- Spletno spremljanje: storilci pogosto spremljajo profile žrtev na družbenih omrežjih, da nadzorujejo njihovo komunikacijo, ali se celo predstavljajo kot žrtev, da nadzorujejo njen spletni »profil« in ji na primer preprečijo iskanje pomoči. Organi pregona lahko zato preverijo, ali je imel storilec poverila žrtve (uporabniško ime/geslo) za prijavo v družbena omrežja ali druge platforme.
- Video- in avdio-nadzor: storilci lahko v prostore ali na delovna mesta namestijo skrite kamere ali naprave za snemanje zvoka, da žrtve neprekinjeno nadzorujejo, na primer ali opravljajo naloge. Organi pregona se lahko osredotočijo na odkrivanje takšnih naprav in nato ovrednotijo pridobljene podatke, da opredelijo obseg delovnega izkoriščanja ter zagotovijo zanesljive dokaze za sodišče.

### Finančne transakcije in metode plačevanja

Finančne transakcije in transakcije s kriptovalutami (domače in mednarodne): storilci pogosto izkoriščajo digitalne sisteme in kanale za pranje denarja ter prikrivanje dobičkov. Ključni digitalni dokazi vključujejo (1) bančne izpiske in zgodovino transakcij, ki lahko pokažejo nenavadne vzorce, značilne za nezakonite dejavnosti, ter (2) kripto denarnice in kripto transakcije, ki se uporabljajo za zakrivanje finančnih sledi in zato zahtevajo specializirano forenzično analizo. Finančna analiza (glej poglavje 9.2) je ključna pri sledenju denarnim tokovom, razbijanju mrež trgovine z ljudmi in kazenskem pregonu storilcev (Thomson Reuters, 2025).

- tradicionalne bančne transakcije

- transakcije s kriptovalutami
- predplačniški in digitalni plačilni sistemi

### 9.4.4.2 Analiza in korelacija dokazov

Po zasegu in zavarovanju digitalnih dokazov (npr. zaseg mobilnih telefonov, računalnikov, USB-ključkov, dostopov do računov v oblaku, podatkov z družbenih omrežij) je treba podatke iz teh naprav oziroma shranjevalnikov pridobiti z uporabo različnih vrst forenzike, opisanih v razdelku 9.1.1 (npr. forenzika v oblaku; pridobivanje podatkov na strojni ravni, kot je »chip-off«, ali metode, kot so razbijanje gesel oziroma dešifriranje). Nato lahko preiskovalci digitalne dokaze analizirajo in medsebojno povezujejo.

Spodaj predstavljeni digitalno-forenzični postopki in načela so po eni strani zgolj primeri, po drugi strani pa niso povsem specifični za trgovino z ljudmi (THB): številne tehnike se prekrivajo s preiskavami kibernetske kriminalitete, organiziranega kriminala in goljufij. Vendar pa nekatere značilnosti v tem kontekstu THB vendarle razlikujejo, na primer poudarek na družbenih omrežjih in oglasih za novačenje (za razliko od finančnih kaznivih dejanj so primeri THB pogosto močno odvisni od spletnega zavajanja in sledenja komunikaciji). Poleg tega je velik del dokazov, ki jih digitalno-forenzične ekipe rekonstruirajo, izrazito osredotočenih na žrtve, saj storilci nadzorujejo žrtev oziroma žrtve na primer z grozilnimi sporočili, izsiljevanjem ali GPS-sledenjem. Žrtve trgovine z ljudmi pogosto nimajo lastnih računalnikov ali prenosnikov, temveč predvsem pametne telefone in račune v oblaku. To pomeni, da so preiskave THB bolj odvisne od mobilne forenzike in forenzike v oblaku (glej razdelek 9.1.1).)

**V primerih trgovine z ljudmi so lahko digitalni forenziki posebno pozornost namenijo:**

- Vzorci komunikacije: storilci pogosto uporabljajo kodiran jezik ali sleng v sporočilih, zato preiskovalci iščejo različne ključne besede, kot so »lahko delo«, »plačilo v gotovini«, »brezplačno potovanje« v kontekstu delovnega izkoriščanja ali »modeling« in »escort« v kontekstu spolnega izkoriščanja. Pogosto se določene ključne besede, povezane z delom, nastanitvijo in plačilom, ponavljajo. Tong idr. (2017) so na primer ugotovili, da storilci v ZDA in Kanadi prilagajajo jezik, da bi se izognili zaznavi s strani organov pregona. Poleg tega spreminjajo terminologijo, zaradi česar je težko razvijati sezname ključnih besed za sledenje oglasom, povezanim s trgovino z ljudmi. Tako nastaja nenehno spreminjajoč se »leksikon«. Namesto da bi na primer izrecno zapisali »mlado dekle«, storilci uporabljajo prikrit zapis, emojije ali sleng (npr. »Y❤ng G!rl«). Številni oglasi so tudi slovnično neurejeni, zato so klasične tehnike obdelave naravnega jezika (NLP) manj učinkovite. Oglasi pogosto vsebujejo simbole, emojije in nestandardne znake. Besedni red je pogosto nekonsistenten in bolj podoben družbenim omrežjem ali SMS-sporočilom kot strukturiranemu pisanju (npr. »@« namesto »at« ali »m33t« namesto »meet«). Kompleksnost unigrama, bigrama in trigrama je visoka. Velika variabilnost besed je posledica tega, da storilci namenoma spreminjajo zapise besed, da bi se izognili avtomatiziranemu odkrivanju (nenavadne besedne zveze, redke besede, spremenjene fraze). Oglasi so praviloma kratki (mediana 133 besed) in ne vsebujejo obširnih opisov. Tong idr. (2017) zaključujejo, da storilci jezik nenehno prilagajajo, zato so potrebni prilagodljivi modeli zaznave. Sami seznami ključnih besed niso dovolj; preiskovalci potrebujejo kontekstno občutljive modele umetne inteligence.
- Drug način za razumevanje in sledenje specifičnim komunikacijskim vzorcem v digitalni forenziki je analiza strategij novačenja, ki jih uporabljajo storilci. Te je mogoče razdeliti na aktivne in pasivne metode (Europol, 2020). Aktivno novačenje

je podobno »ribolovu s trnkom« (hook fishing), pri katerem storilci objavljajo lažne oglase za delo na zaupanja vrednih zaposlitvenih portalih in tržnicah na družbenih omrežjih. Včasih celo ustvarijo lažne rekrutacijske spletne strani, ki delujejo profesionalno in lahko vključujejo tudi klepet v živo, da delujejo legitimno. UNODC ta pojav poimenuje tudi »lovska strategija« (hunting strategy) (UNODC, 2020). Aktivno novačenje večinoma vključuje neposredna sporočila in klepete, usmerjene v ranljive posameznike, ter lahko kaže vzorce prisile, manipulacije in zavajajočih ponudb za delo. Pogost pojav je tudi nenadno brisanje sporočil ali računov po začetnem stiku (npr. ko storilec ugotovi, da potencialna žrtev ni dovzetna oziroma »dosegljiva« za ponujeno delo).

- Pasivno novačenje je bolj prikrito in ga organi pregona težje zaznajo. Deluje kot »ribolov z mrežo« (net fishing) oziroma »ribolovna strategija« (fishing strategy) (UNODC, 2020), kjer storilci spremljajo objave iskalcev zaposlitve na spletu in jih nato neposredno kontaktirajo. Obljubljajo zaposlitev v tujini ter zahtevajo plačilo za »zagotovitev« dela in kritje stroškov potovanja ali posredovanja. Žrtve pogosto ugotovijo, da so bile zavedene, šele ob prihodu v tujo državo (Europol, 2020)

  Nenazadnje je zanesljivih znanstvenih dokazov o preiskovalnih tehnikah za prepoznavanje komunikacijskih vzorcev zelo malo (za morebitne posodobitve znanstvenih ugotovitev si je smiselno ogledati npr. Evidence Gap Map Mednarodne organizacije dela, 2023).

- Geolokacijsko sledenje: podobno kot pri razumevanju komunikacijskih vzorcev lahko pomaga, če preiskava upošteva perspektivo storilca. Naprave, ki omogočajo geolokacijsko sledenje, so lahko uporabljene za spremljanje žrtve oziroma žrtev v realnem času, na primer prek GPS, vgrajenih kamer v pametnih telefonih ali aplikacij za deljenje lokacije (Europol, 2020). Možnost oddaljenega nadzora

znižuje prag zadržkov pri izkoriščanju in hkrati otežuje prizadevanja organov pregona pri prepoznavanju storilcev, kot navaja Europol (2020, str. 3):

> *[Medtem ko] so v preteklosti morale organizirane kriminalne združbe izvajati fizični nadzor in vzpostaviti monopol nad določenimi mestnimi območji ter so praviloma vključevale veliko mrežo članov, lahko novi akterji na področju trgovine z ljudmi (THB) danes učinkovito upravljajo »spletni posel« brez potrebe po fizični kriminalni infrastrukturi in z manjšim številom sodelujočih. Posledično lahko obvladovanje tehnologije kriminalno združbo naredi bolj nevarno, hkrati pa manj prepoznavno za organe pregona.*

Več o geolokacijskem sledenju je predstavljeno v prejšnjem razdelku 9.1.3.1.

- Finančna analiza: finančna analiza in digitalna forenzika se lahko dopolnjujeta, zlasti pri finančnih transakcijah, ki jih storilci izvajajo za objavo spletnih oglasov (Europol, 2020). Poleg tega žrtve pogosto izvajajo bančna nakazila storilcem. Podrobnejši pogled na finance, finančne transakcije in finančne preiskave je v razdelku 9.2.

- Identifikacija žrtev: pri identifikaciji žrtev lahko digitalni forenziki uporabijo prepoznavanje obrazov, na primer za iskanje žrtev v oglasih ali objavah na družbenih omrežjih. Poleg tega lahko povratno iskanje slik (reverse image search) pokaže, ali so bile žrtve oglaševane na spletnih straneh za odrasle ali na platformah črnega trga.

- Analiza temnega in globokega spleta: uporaba forumov temnega spleta pri storilcih ni neobičajna. Preiskovalci lahko uporabijo forenziko TOR in orodja za

spremljanje temnega spleta, na primer za iskanje novačitvenih sporočil, vsebin izkoriščanja žrtev ali nezakonitih transakcij.

### 9.4.4.3 Pristopi in orodja digitalne forenzike

Za učinkovito zbiranje in analizo dokazov v primerih trgovine z ljudmi (THB) in delovnega izkoriščanja se digitalna forenzika v veliki meri opira na:

- mobilno forenziko
- omrežno in oblačno forenziko
- finančno analizo in analizo kriptovalut
- preiskovanje temnega spleta

Da nadaljujemo kronološko, so tukaj ključna načela digitalne forenzike, ki jih je treba v praksi upoštevati tudi v kontekstu THB. V prvi fazi (identifikacija in zavarovanje) morajo prvi odzivni akterji hitro prepoznati in zavarovati digitalne naprave, da preprečijo posege v podatke ali njihovo izgubo (npr. izolacija od omrežij; UNODC, 2019b). Pri ravnanju z digitalnimi dokazi je nato pomembno podrobno evidentirati stanje vsake naprave, vključno z operativnim stanjem (vključena, izključena, stanje pripravljenosti), modelom in morebitnimi vidnimi poškodbami. Fotografije in pisne opombe pomagajo pri vzdrževanju dokazne verige (chain of custody) in podpirajo celovitost dokazov (UNODC, 2019b). Pridobivanje podatkov (data extraction) je nato mogoče izvesti s specializiranimi forenzičnimi orodji, ki omogočajo pridobitev podatkov brez spreminjanja izvirne vsebine (glej razdelek 9.6.2 za splošen pregled). Pri nekaterih napravah to lahko vključuje premagovanje varnostnih mehanizmov, kot so šifriranje ali gesla. Zlasti v kontekstu trgovine z ljudmi oziroma (delovnega izkoriščanja) organi pregona uporabljajo digitalno-forenzična orodja, ki olajšajo preiskovanje tega kaznivega dejanja.

Celovitega pregleda, katera digitalno-forenzična orodja bi se lahko uporabljala in se dejansko uporabljajo v organih pregona, tukaj ni mogoče podati zaradi (1) raznolikosti praks in rešitev, ki jih uporabljajo različni organi pregona po Evropi (tako na področju digitalne forenzike na splošno kot pri preiskovanju THB kot specifični podveji), (2) prepletene uporabe tehnik in orodij, ki je odvisna od konkretnega primera, ter (3) omejene javne dostopnosti informacij o tem, kako organi pregona na tem področju delujejo, če navedemo le nekaj razlogov. Kljub temu je mogoče na splošno (orientacijsko) predstaviti nekatere digitalno-forenzične rešitve in podjetja, ki ponujajo programska orodja za preiskovanje primerov THB:

- Cellebrite Pathfinder: orodje za mobilno forenziko, ki omogoča pridobivanje, analizo in dekodiranje podatkov iz pametnih telefonov, tablic in virov v oblaku. Omogoča tudi obnovitev izbrisanih sporočil, dnevnikov klicev in GPS lokacij.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  ➔ pridobi npr. sporočila WhatsApp ali Telegram med storilci in žrtvami

  ➔ obnovi izbrisane pogovore, v katerih so žrtvam obljubljali lažna delovna mesta

  ➔ dentificira GPS lokacije iz telefona žrtve za kartiranje vzorcev gibanja

- MAGNET FORENSICS: Podjetje ponuja več programskih rešitev za javno varnost, vojsko in obveščevalno skupnost ipd.

- MAGNET AXIOM je posebej relevanten za preiskave trgovine z ljudmi (THB): orodje je specializirano za računalniško in oblačno forenziko ter analizo podatkov s trdih diskov, družbenih omrežij, e-pošte in šifriranih datotek.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

- ➔ preišče objave na družbenih omrežjih in aktivnosti na zaposlitvenih portalih, kjer storilci objavljajo lažne oglase za delo
- ➔ pridobi skrite datoteke (npr. pogodbe žrtev, letalske vozovnice, delovna dovoljenja) z računalnikov storilcev
- ➔ analizira komunikacijske dnevnike med več osumljenci v različnih državah

- MAGNET OUTRIDER lahko prav tako koristno podpira digitalno-forenzični preiskovalni proces, saj pregleda mobilne naprave iOS in Android ter lahko odkrije na primer nezakonite oziroma sumljive aplikacije, seznam stikov, SMS-sporočila in nedavno uporabljene aplikacije.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  - ➔ razkrije prikrite spletne aktivnosti in odkrije, ali storilci uporabljajo forume temnega spleta ali lažne račune na družbenih omrežjih
  - ➔ lahko zazna ponarejene pogodbe o zaposlitvi, lažne oglase za delo in finančne evidence

- MAGNET GRAYKEY, ki je specializiran za odklepanje šifriranih mobilnih naprav, lahko prav tako pomembno prispeva. Orodje obide zaklep zaslona in omogoča pridobitev podatkov iz datotečnega sistema.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  - ➔ odklene zasežene telefone storilcev in pomaga pri obnovi pogovorov v aplikacijah WhatsApp, Telegram, Signal, Viber ipd.

  Prav tako so lahko koristne tudi druge rešitve podjetja MAGNET (glej Pizzuro, 2022).

- MSAB XRY: orodje za mobilno forenziko, ki ga uporabljajo organi pregona za pridobivanje, analizo in dekodiranje podatkov iz mobilnih telefonov, tablic, GPS naprav in dronov.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  ➔ pridobi mobilno komunikacijo, ki lahko razkrije digitalne dokaze, relevantne za THB

  ➔ analizira podatke z družbenih omrežij in zaposlitvenih platform

  ➔ obnovi izbrisane datoteke in fotografije

- Maltego: Podjetje ponuja orodja za kartiranje odnosov med osebami, podjetji, računi na družbenih omrežjih in spletnimi mesti (GRAPH), za izvajanje OSINT iskanj o domnevnih storilcih (SEARCH), za spremljanje družbenih omrežij v realnem času (MONITOR), ter za analizo družbenih omrežij (EVIDENCE).

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  ➔ razkrije lažne rekrutacijske spletne strani in jih poveže z znanimi storilci

  ➔ prikaže povezave med različnimi profili na družbenih omrežjih, ki se uporabljajo za novačenje

  ➔ identificira kripto denarnice in finančne transakcije, povezane s storilci

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

- Autopsy: brezplačno, odprtokodno digitalno-forenzično orodje, ki ponuja platformo za preiskave trdih diskov.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

➔ obnovi izbrisane pogodbe o zaposlitvi ali ponarejene vizumske dokumente

➔ sledi zgodovini brskanja (npr. obiski lažnih zaposlitvenih spletnih strani ali šifriranih klepetalnih platform)

➔ pridobi zgodovino uporabe USB naprav, da se ugotovi, ali so bili zunanji nosilci uporabljeni za shranjevanje npr. podatkov o žrtvah

- ADF PRO: je programska oprema za digitalno forenziko in triažo, namenjena hitri analizi računalnikov, zunanjih diskov in mobilnih naprav.

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  ➔ hitro zavarovanje digitalnih dokazov na kraju hišne preiskave/akcije (npr. pregled družbenih omrežij osumljencev, prenosnikov in telefonov)

  ➔ prepoznavanje obrazov: hitro prepoznavanje in ujemanje obrazov na fotografijah in videoposnetkih (uporabno pri identifikaciji žrtev in storilcev)

- Orodja za analizo verig blokov (blockchain) (npr. Chainalysis, Elliptic, CipherTrace)

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

  Potencialna uporaba v primeru THB/delovnega izkoriščanja:

  ➔ sledi transakcijam v Bitcoinu ali drugih kriptovalutah, ki so jih žrtve izvedle v korist izkoriščevalskih posrednikov/novačevalcev

  ➔ poveže naslove denarnic z znanimi mrežami trgovine z ljudmi

  ➔ identificira tehnike pranja denarja, uporabljene za prikrivanje nezakonitih dobičkov

Za digitalno-forenzične procese v boju proti trgovini z ljudmi (THB) sta predstavljena še dva dodatna pristopa, ki sta na kratko opisana. Deloma se lahko prekrivata z že predstavljenimi orodji ali področji digitalne forenzike.

Prvi pristop je uporaba metapodatkov iz slik in videoposnetkov v preiskavah trgovine z ljudmi. Namesto da bi se preiskava zanašala zgolj na računsko zahtevne tehnike računalniškega vida, lahko metapodatki slik in videoposnetkov organom pregona pomagajo pri prepoznavanju žrtev in storilcev (Mattmann idr., 2016). Trgovino z ljudmi pogosto spremljajo besedilni znaki, kot so fizične značilnosti žrtve, lokacija ter multimedijski elementi (tj. slike in videoposnetki na različnih platformah). Mattmann idr. (2016) so razvili orodja za metapodatkovno forenziko multimedije, ki vključujejo ImageCat (katalog slik) in ImageSpace.

ImageCat je sistem za ekstrakcijo, transformacijo in nalaganje podatkov (ETL), zasnovan za obdelavo in katalogizacijo metapodatkov multimedijskih vsebin, zlasti v kontekstu preiskav THB. Omogoča povezovanje več oglasov na podlagi skupnih metapodatkov (npr. ista kamera uporabljena pri fotografiranju različnih žrtev; analiza podobnosti) ter hitro iskanje in pridobivanje multimedijskih dokazov. Tako lahko organom pregona pomaga pri identifikaciji tako žrtev kot storilcev (Mattmann idr., 2016).

ImageSpace (nadgradnja na ImageCat) pridobiva metapodatke multimedije (npr. RGB barvni prostor, model kamere, geolokacija, časovni žigi). Omogoča iskanje in poizvedovanje po obsežnih bazah multimedije, kar organom pregona omogoča iskanje slik in videoposnetkov po besedilu, metapodatkih ali podobnosti slik. Interaktivno pregledovanje in vizualizacija slik omogočata urejen prikaz dokaznega gradiva v obliki galerije za forenzični pregled ter ponujata interaktivne histograme in prikaze gostote. ImageSpace omogoča tudi ujemanje podobnosti med slikami in videoposnetki za združevanje povezanih datotek, kar preiskovalcem pomaga pri sledenju žrtvam skozi

različne oglase in platforme. Poleg tega lahko sčasoma optimizira rezultate iskanja ter podpira optično prepoznavanje znakov (OCR) in ekstrakcijo besedila (npr. pridobivanje telefonskih številk, e-poštnih naslovov, naslovov) iz slik in videoposnetkov. Ta multimedijski pristop predstavlja alternativno metodo povezovanja oglasov, žrtev in storilcev z analizo vzorcev metapodatkov, ne pa zgolj vsebine slike ali videa.

Drug pristop, ki je delno že zajet v prej predstavljenih orodjih in se kot rdeča nit pojavlja v dosedanjih razpravah o preiskovanju trgovine z ljudmi (THB) ter digitalni forenziki, je raziskovanje na podlagi odprtih virov (OSINT – open-source intelligence). OSINT pomeni zbiranje in analizo javno dostopnih podatkov za podporo preiskavam. V okviru digitalne forenzike pri preiskavah THB ima OSINT pomembno vlogo, saj pomaga prepoznati vzorce, slediti digitalnim sledem ter povezovati osumljence s kaznivimi ravnanji. Ker so bili posamezni OSINT elementi že večkrat omenjeni, je namen tega kratkega razdelka predvsem poudariti njegovo pomembnost in velik potencial.

OSINT je ključen za prepoznavanje vzorcev novačenja in komunikacije, saj pomaga odkrivati ključne platforme, jezikovne vzorce in strategije novačenja, ki se uporabljajo pri aktivnih (»lovskih«) in pasivnih (»mrežnih«) metodah. OSINT, ki ga je mogoče razdeliti na obveščevalno dejavnost na družbenih omrežjih (SOCMINT), geolokacijsko oziroma geospatialno obveščevalno dejavnost (GEOINT) ter pridobivanje informacij prek ljudi (HUMINT), med drugim vključuje spremljanje družbenih omrežij in objav delovnih mest, analizo razprav na forumih, aktivnosti na temnem spletu ter povratno iskanje slik in videoposnetkov. OSINT lahko služi tudi povezovanju spletnih oglasov z mrežami trgovine z ljudmi, na primer z avtomatiziranim zbiranjem in analizo oglasov za delo, s sledenjem kriptovalutnim transakcijam in plačilom ter z analizo domen in spletnih strani. Pomemben je lahko pri geolociranju žrtev in storilcev, na primer z analizo slik in videoposnetkov (ter njihovih metapodatkov) ali z uporabo množično podprtih geolokacijskih virov (npr.

Google Street View, satelitski posnetki). Poleg tega lahko OSINT pomaga razkriti lažne identitete in mreže, na primer s primerjanjem podatkov z družbenih omrežij (ali temnega spleta), z analizo digitalnih sledi in preverjanjem povezav osebnih podatkov med računi (npr. https://epieos.com/ za povratno preverjanje, ali je e-poštni naslov ali telefonska številka povezana z določenimi računi), ali pa z vedenjsko analizo, kot so vzorci objavljanja, jezikovne značilnosti in časovna dinamika spletnih aktivnosti.

### 9.4.4.4 Izzivi digitalne forenzike

Preiskovanje primerov trgovine z ljudmi predstavlja za digitalno forenziko posebne izzive, na primer:

- šifrirano komunikacijo in komunikacijo s samodejnim brisanjem,
- brisanje ter prikrivanje podatkov,
- čezmejne zaplete pri dostopu do podatkov ter
- vprašanja varstva žrtev in njihove zasebnosti.

Za bolj sistematičen pregled izzivov jih je smiselno razdeliti na vsebinske (na kaznivo dejanje vezane) in strukturne izzive.

#### Vsebinsko pogojeni izzivi

Vsebinsko pogojeni izzivi so tisti, ki izhajajo iz same narave digitalne forenzike in preiskovanja trgovine z ljudmi. Gre torej za izzive, ki so imanentni kaznivemu dejanju kot takemu. Pri tem lahko ločimo med proaktivnimi in reaktivnimi preiskavami. Proaktivne preiskave je bistveno težje začeti, ker morajo organi pregona najprej prepoznati znake izkoriščanja, ki lahko kažejo na trgovino z ljudmi oziroma izkoriščanje. Posebej zahtevno

je na primer iz velikega števila spletnih oglasov izločiti tiste, ki vsebujejo relevantne indike (Europol, 2020). Zato so »reaktivne preiskave lažje, ker imajo izhodišče, kot je izpoved identificirane žrtve in/ali račun ali spletno mesto, uporabljeno za namene novačenja ali izkoriščanja« (Europol, 2020, str. 5).

Poleg tega izzive predstavlja tudi sama narava digitalnih dokazov, s katerimi se preiskovalci v primerih THB najpogosteje srečujejo. Ker številni storilci uporabljajo aplikacije za takojšnje sporočanje, kot so WhatsApp, Signal ali Telegram, vgrajeno šifriranje od konca do konca (end-to-end encryption, E2EE) otežuje pridobivanje vsebine sporočil. Pogosta je tudi namerna odstranitev digitalnih sledi: storilci dokaze izbrišejo sami ali pa uporabljajo funkcije samodejnega brisanja (npr. v klepetih WhatsApp). Dostop do izbrisanih podatkov je omejen, zato lahko preiskovalci pogosto poskušajo pridobiti le varnostne kopije (backupe), ki so nastale v preteklosti. Storilci lahko delujejo tudi prek skritih storitev omrežja Tor (temni splet, uporaba VPN), kar dodatno otežuje sledenje. Poleg tega skušajo sledi zabrisati z izrazito razpršitvijo svoje digitalne prisotnosti, na primer z uporabo več SIM kartic in telefonov ter številnih računov (tudi lažnih).

Ta zahtevnost ponazarja še en pomemben izziv: preiskovalec mora pogosto obvladovati zelo veliko količino (zlasti digitalnih) podatkov, jih pregledati, razvrstiti glede na relevantnost za kaznivo dejanje oziroma kazniva dejanja, ohraniti pregled nad celoto in načrtovati nadaljnje strateške korake. S tem je povezan tudi pravni vidik, ki lahko postane problematičen: primer se lahko močno zaplete, saj pogosto ni mogoče obravnavati zgolj trgovine z ljudmi oziroma delovnega izkoriščanja, temveč tudi na primer davčno utajo, kršitve delovnopravne zakonodaje in obveznosti socialne varnosti, prisilno delo, telesne poškodbe, goljufijo, ponarejanje listin ali kršitve človekovih pravic. To vpliva tudi na digitalno forenziko, saj kompleksnejši primer praviloma zahteva več in bolj

usklajene izmenjave informacij med vodilnim preiskovalcem in digitalno-forenzičnim strokovnjakom.

### Strukturni izzivi

Izzive lahko opredelimo kot strukturne, kadar izhajajo iz samega sistema, na primer iz organizacije organov pregona v posamezni državi ali iz zakonodajnih okoliščin. Digitalne tehnologije, ki jih uporabljajo storilci, se namreč nenehno razvijajo, zato se morajo organi pregona sproti prilagajati (naj)nov(ejš)im tehničnim rešitvam, ki jih uporabljajo storilci (Europol, 2020). Ob tem morajo organi pregona zagotoviti tudi ustrezne kadrovske vire. Ne gre le za specializirane preiskovalce THB in digitalno-forenzične strokovnjake oziroma praktike, temveč tudi za drugo nujno osebje, potrebno za preiskovanje primerov THB, na primer tolmače in prevajalce (npr. za prevajanje podatkov iz nadzora telekomunikacij).

Hkrati je treba izboljšati tudi zakonodajne instrumente, da bi se zagotovila učinkovita preiskava, pregon in obsodba storilcev (Europol, 2020). Širitev oziroma krepitev zakonodajnih možnosti je še posebej pomembna, ker žrtve pogosto niso pripravljene podati obsežnih izpovedb in izjav, saj so že tako pod velikim psihološkim pritiskom – zaradi groženj, izsiljevanja in tudi zaradi tveganja javnega sramotenja prek družbenih omrežij (npr. z javnim razkritjem njihovega izkoriščanja). Zato je lažji dostop do razpoložljivih podatkovnih zbirk za potrebe digitalne forenzike pomemben, da se preiskave lahko nadaljujejo, okrepijo in da se na koncu podpre oziroma sploh omogoči kazenski pregon (Europol, 2020).

Pri pravnih vidikih je treba omeniti tudi, da so lahko čezmejna prizadevanja za sodelovanje otežena, če sodno sodelovanje in uporabljiva pravila niso jasno določena. To

lahko zavira na primer izmenjavo dokazov med državami. V povezavi s pomanjkanjem standardiziranega mednarodnega sodelovanja trenutno še ni centralizirane globalne podatkovne zbirke o trgovini z ljudmi, ki bi omogočala globalno spremljanje spletnih aktivnosti storilcev.

### 9.4.4.5 Pravni in etični vidiki

Zaradi občutljive narave primerov trgovine z ljudmi morajo forenzične preiskave dosledno upoštevati stroge etične in pravne standarde, od katerih so bili nekateri že predstavljeni zgoraj. Z vključevanjem teh vidikov lahko strokovnjaki digitalne forenzike etično, zakonito in učinkovito krmarijo po kompleksnem področju preiskav THB in delovnega izkoriščanja ter zagotovijo, da je prizadevanje za pravico skladno z varstvom pravic posameznikov in družbenih vrednot.

#### Na žrtev osredotočen pristop

Na žrtev osredotočen pristop daje prednost pravicam, potrebam in dobrobiti žrtev skozi celoten preiskovalni proces. Ta metodologija poudarja spoštljivo in občutljivo obravnavo žrtev, zagotavljanje obveščenosti in podpore ter njihovo aktivno vključevanje v odločitve, ki vplivajo na njihovo življenje. S poudarkom na izkušnji žrtve lahko preiskovalci gradijo zaupanje, ki je ključno ne le za pridobivanje točnih informacij, temveč tudi za ustrezno usmerjanje žrtve v podporne storitve. Tak pristop ne prispeva samo k okrevanju žrtev, temveč tudi krepi celovitost preiskave (Mednarodna organizacija dela, 2018). »Varnost žrtev ter njihovih družinskih članov in bližnjih je ves čas najpomembnejša in je odgovornost preiskovalca ter tožilca« (Mednarodna organizacija dela, 2018, str. 47). To dodatno poudarja, da se je treba osredotočiti ne le na žrtev kot posameznika, temveč

tudi na njeno družino oziroma sorodnike, saj je tveganje povračilnih ukrepov zoper družinske člane s strani storilcev stalna realnost (Mednarodna organizacija dela, 2018).

Z vidika digitalne forenzike je priporočljivo, da se invazivno digitalno spremljanje čim bolj omeji in se pri tem, kjer je to mogoče, osredotoči na storilce, ne na žrtev oziroma žrtve. Zaupnost podatkov žrtev je treba zagotoviti ves čas, da se prepreči povračilne ukrepe ali javno razkritje. Preiskovalec naj se izogiba pritiskanju na žrtve, da bi večkrat podrobno obnavljale digitalne interakcije (namesto tega naj se, kolikor je mogoče, uporabijo forenzična orodja), ter naj spoštuje informirano soglasje žrtve pred dostopom do osebnih naprav. Izogibati se je treba tudi agresivnim tehnikam zasliševanja, ki izhajajo iz digitalnih ugotovitev (na primer soočanju žrtve z izpisi klepetov na način, ki sproži stres ali ponovno podoživljanje).

Eden večjih izzivov pri kazenskem pregonu storilcev je lahko prevelika odvisnost od izpovedbe žrtve, ki je lahko za žrtev travmatizirajoča, hkrati pa zaradi strahu tudi manj zanesljiva. V tem pogledu lahko digitalna forenzika okrepi dokazni položaj in zmanjša potrebo po naslanjanju na izpoved žrtve na sodišču, kar lahko posledično zmanjša breme za žrtve. Digitalno-forenzični strokovnjaki lahko poleg tega prispevajo k preprečevanju povračilnih ukrepov in ponovne viktimizacije oziroma ponovnega trgovanja z ljudmi tako, da – če žrtev to želi in se s tem strinja – pregledajo njene naprave za vohunsko programsko opremo ter po potrebi odstranijo sledilna orodja.

### Varstvo podatkov

- V preiskovalnem postopku je zaščita oseb, ki razkrijejo aktivnosti, povezane s trgovino z ljudmi, ključna za spodbujanje prijav kaznivih dejanj. Zaščita žvižgačev zagotavlja, da tisti, ki se opogumijo in spregovorijo, ne bodo izpostavljeni povračilnim ukrepom, s čimer se krepi okolje, v katerem je mogoče informacije varno deliti. Poleg tega etično poročanje medijev in pristojnih organov zmanjšuje

tveganje sekundarne viktimizacije, saj preprečuje, da bi bile žrtve dodatno prizadete zaradi izpostavljenosti, in zagotavlja, da posredovane informacije služijo javnemu interesu, ne da bi povzročale škodo.

- UNODC je v okviru Modula 10 (Zasebnost in varstvo podatkov) pripravil pregled vidikov zasebnosti in varstva podatkov, ki jih je treba upoštevati pri zadevah, povezanih s kibernetskim področjem.
- Zaseženi dokazi: zagotavljanje celovitosti in zaupnosti digitalnih dokazov je bistvenega pomena. Vzpostavljeni morajo biti ustrezni ukrepi varstva podatkov, da se preprečijo nepooblaščen dostop, nedovoljeni posegi ali izguba dokazov. Ohranjanje jasne dokazne verige (chain of custody) je nujno za dopustnost dokazov na sodišču, saj dokumentira ravnanje z dokaznim gradivom od zbiranja do predstavitve. Spoštovanje pravnih standardov in protokolov varuje pravice vseh vpletenih ter krepi verodostojnost preiskovalnega postopka.

### Mednarodno sodelovanje

Trgovina z ljudmi in delovno izkoriščanje sta pogosto čezmejni kaznivi dejanji, zato je nujno sodelovanje med državami. Mednarodno sodelovanje vključuje usklajevanje pravnih okvirov, izmenjavo informacij in koordinacijo dejavnosti med različnimi jurisdikcijami. Tak skupen pristop krepi zmožnost sledenja storilcem, zaščite žrtev ter učinkovitega razbijanja mrež trgovine z ljudmi. Modul 11 UNODC – Mednarodno sodelovanje v boju proti transnacionalnemu organiziranemu kriminalu – lahko ponudi koristen vpogled v pravne možnosti na tem področju.

### Sorazmernost in nujnost

Preiskave morajo uravnotežiti potrebo po informacijah s spoštovanjem zasebnosti posameznika. Zbiranje digitalnih dokazov mora biti sorazmerno s težo kaznivega dejanja in nujno potrebno za izvedbo preiskave. To načelo zagotavlja, da preiskovalni ukrepi ne presežejo potrebnega obsega in ne posegajo v temeljne pravice, s čimer se ohranjajo etični standardi ob hkratnem zasledovanju pravičnosti.

### Uporaba UI

Vključevanje umetne inteligence v digitalno forenziko prinaša večjo učinkovitost, hkrati pa odpira vprašanja glede točnosti in pristranskosti. Avtomatizirana orodja morajo biti skrbno zasnovana in redno preverjana, da se preprečijo pristranskosti, ki bi lahko vodile do neupravičenih obtožb ali do tega, da bi bili določeni profili žrtev spregledani. Človeški nadzor ostaja ključen, saj je treba rezultate, ki jih generira UI, razlagati v ustreznem pravnem in etičnem okviru. Zlasti pri pomembnih oziroma ključnih točkah preiskovalnega postopka uporaba umetne inteligence ne sme nadomestiti človeške presoje.

### Etična uporaba OSINT in spremljanje temnega spleta

Čeprav sta OSINT in spremljanje temnega spleta dragocena pri odkrivanju nezakonitih dejavnosti, ju je treba izvajati znotraj pravnih okvirov. Preiskovalci se morajo izogibati nepooblaščenemu dostopu ali zavajajočim praksam, ki bi lahko ogrozile integriteto preiskave ali kršile etične standarde. Spoštovanje zasebnosti in zakonito pridobivanje informacij sta temeljna za ohranjanje zaupanja javnosti in utrjevanje načela pravne države.

## 9.5 Finančne preiskave

Finančne preiskave so bistveno orodje v boju proti finančnim kaznivim dejanjem, kot so pranje denarja (ML), financiranje terorizma (TF) in trgovina z ljudmi. Osredotočajo se na analizo finančnih transakcij z namenom odkrivanja nezakonitih dejavnosti, sledenja nezakonitim sredstvom ter identifikacije storilcev in njihovih mrež. Temeljni koncepti in cilji finančnih preiskav izhajajo iz načela »sledi denarju«: cilj je razkriti in dokumentirati finančna kazniva dejanja. Ključni cilji vključujejo prepoznavanje kriminalnih mrež, sledenje nezakonitim sredstvom ter zbiranje dokazov, ki so uporabni v kazenskem pregonu. Dobro izvedena finančna preiskava krepi delo organov pregona, saj storilcem odvzema finančne vire in razgrajuje finančno infrastrukturo, ki podpira organizirani kriminal.

Pomen finančnih analiz v kontekstu trgovine z ljudmi je še posebej izrazit, saj so storilci odvisni od finančnih transakcij za premikanje, shranjevanje in »pranje« nezakonito pridobljenih sredstev. S pregledom transakcijskih evidenc, bančnih izpiskov in digitalnih načinov plačevanja lahko preiskovalci odkrijejo finančne povezave med storilci in njihovimi sodelavci. To ne prispeva le k učinkovitejšemu kazenskemu pregonu, temveč lahko pomaga tudi pri identifikaciji žrtev, saj se z analizo finančnih tokov lahko prepoznajo vzorci, značilni za izkoriščanje. Finančne preiskave tako pomembno prispevajo k razbijanju mrež trgovine z ljudmi, ker ciljajo na finančne »življenjske linije«, ki takšne mreže ohranjajo. Ob tem pa velja opozoriti: »Kljub splošnemu priznanju pomena finančnega vidika je širše sprejemanje, izvajanje in usklajevanje preiskovalnih strategij in taktik, usmerjenih posebej v finance trgovine z ljudmi, še vedno v razvoju« (OVSE, 2019, str. 37).

V nadaljevanju razdelek 9.7.1 predstavi splošne osnove finančnih preiskav, nato sledi uvod v poslovne strukture trgovine z ljudmi, da se poudari relevantnost finančnih preiskav za področje THB in delovnega izkoriščanja (razdelek 9.7.2). Razdelek 9.7.3 po korakih prikazuje, kako izvesti finančno preiskavo v primerih trgovine z ljudmi. Razdelek 9.7.4 predstavi transakcijske indikatorje, ki lahko kažejo na sumljive finančne aktivnosti na področju THB, zlasti delovnega izkoriščanja. Razdelek 9.7.5 opisuje izzive finančnih preiskav, razdelek 9.7.6 obravnava tehnične inovacije in trende, razdelek 9.7.7 pa sklene z dodatnimi priporočili.

## 9.5.1 Pregled

Finančne preiskave imajo ključno vlogo pri delu organov pregona in tožilstva, zlasti v primerih pranja denarja (ML), financiranja terorizma ter organiziranega kriminala (FATF, 2012). Smernice FATF o finančnih preiskavah opredeljujejo temeljna načela, orodja in strategije, potrebne za učinkovito izvajanje finančnih preiskav. Osnovni cilj finančne preiskave je slediti in dokumentirati gibanje nezakonitih sredstev, s čimer se lažje prepoznajo kriminalne mreže, razkrijejo finančne strukture in zgradijo trdni pravni primeri (FATF, 2012). Z analizo finančnega vidika kaznivih dejanj lahko preiskovalci pridobijo nove sledi, izrišejo celotne kriminalne mreže – vključno z njihovimi čezmejnimi povezavami – ter zberejo dragocene dokaze za kazenski pregon osumljencev in odvzem nezakonito pridobljenega premoženja

### 9.5.1.1 Ključni vidiki finančnih preiskav

Ključna sestavina finančnih preiskav so vzporedne preiskave, pri katerih finančna preiskava teče vzporedno s kazensko preiskavo. Tak pristop zagotavlja, da se ob tem, ko se organi pregona osredotočajo na kazniva dejanja, kot so trgovina z ljudmi, korupcija ali

trgovina z drogami, hkrati izvaja tudi finančna preiskava, ki sledi denarnim tokovom, ustvarjenim s temi dejavnostmi (FATF, 2012). Vzporedne preiskave pomagajo izslediti nezakonito pridobljeno premoženje, prepoznati dodatne osumljence ter podpreti odvzem protipravno pridobljene premoženjske koristi. Za večjo učinkovitost se pogosto vzpostavljajo multidisciplinarne delovne skupine, ki združujejo finančne analitike, forenzične računovodje, strokovnjake za digitalno forenziko in tožilce. Takšne ekipe izboljšajo izmenjavo obveščevalnih podatkov, zmanjšajo podvajanje dela in omogočijo celovitejši pristop k preiskovanju finančne kriminalitete (FATF, 2012).

Pomemben cilj finančnih preiskav je tudi izterjava in odvzem premoženja (glej poglavje usposabljanja 10). Storilce praviloma vodi finančni dobiček, zato jim odvzem nezakonitih prihodkov oslabi delovanje. Organi pregona morajo z naprednimi forenzično-finančnimi metodami izslediti, začasno zamrzniti in zaseči protipravno pridobljeno premoženje. Kot učinkovito pravno orodje se priporoča tudi odvzem premoženja brez obsodilne sodbe, ki omogoča zaseg premoženja tudi v primerih, ko obsodba ni mogoča. Vzpostavitev specializiranih enot za izterjavo premoženja in centraliziranih baz finančnoobveščevalnih podatkov lahko bistveno okrepi finančne preiskave, saj izboljša učinkovitost in koordinacijo.

Uspešna finančna preiskava temelji na več virih informacij. Organi pregona morajo imeti dostop do finančnoobveščevalnih poročil, vključno s poročili o sumljivih transakcijah (STR), poročili o gotovinskih transakcijah in čezmejnimi prijavami prenosa gotovine. Poleg tega pomembne sledi zagotavljajo bančni in finančni zapisi, registri podjetij, davčne evidence, carinski podatki ter OSINT. Ključno je, da imajo pristojni organi ustrezna zakonska pooblastila za dostop in analizo teh evidenc, ob hkratnem spoštovanju pravil varstva osebnih podatkov.

## Preiskovalne metode

Pri finančnih preiskavah se uporablja vrsta preiskovalnih tehnik (za navedene tehnike glej FATF, 2012, če ni naveden drug vir).

- Fizično opazovanje: ta tehnika vključuje spremljanje osumljencev, da se razume njihove finančne aktivnosti, na primer premiki večjih količin gotovine ali stiki s finančnimi posredniki. Posebej uporabna je v primerih pranja denarja in financiranja terorizma.
- Preiskovanje odpadkov (»trash runs«): preiskovalci lahko skladno z zakonodajo zbirajo in analizirajo zavržene finančne evidence in druge dokumente, ki lahko razkrijejo skrito premoženje ali nezakonite transakcije.
- Prisilni ukrepi: sem sodijo hišne preiskave, sodne odredbe, pozivi in odredbe za predložitev dokumentacije, s katerimi se pridobijo ključni finančni podatki, kot so bančni izpiski, davčne evidence in poslovne knjige. Pravilno izvedeni postopki preiskave in zasega zagotavljajo zakonitost zbiranja digitalnih in fizičnih dokazov ter ohranjanje dokazne verige (chain of custody).
- Prestrezanje komunikacij: organi pregona lahko izvajajo prisluškovanje, nadzor e-pošte in druge oblike elektronskega nadzora za sledenje finančnim transakcijam in identifikacijo sostorilcev. Metoda je zelo učinkovita, vendar mora biti izvedena v okviru zakonitih pooblastil, da se preprečijo nedopustni posegi v zasebnost.
- Prikrite preiskovalne dejavnosti: v nekaterih primerih lahko preiskovalci prevzamejo lažne identitete, da se infiltrirajo v kriminalne združbe in zberejo neposredne dokaze o finančnih nepravilnostih. Ta tehnika je kadrovsko in časovno zahtevna ter zahteva specializirano usposabljanje.

- Kontrolirane dostave: metoda vključuje sledenje premiku nezakonitih sredstev (v gotovini ali prek digitalnih prenosov) pod nadzorom organov pregona. Pomaga prepoznati ključne akterje v mrežah pranja denarja ali goljufij.
- Forenzično računovodstvo: gre za specializirano področje, ki združuje znanja računovodstva, revizije in preiskovalnih veščin za pregled finančnih evidenc z namenom odkrivanja nepravilnosti. Forenzični računovodje lahko odkrijejo neskladja v knjigah, zaznajo goljufije in sledijo nezakonitim finančnim tokovom na podlagi podrobne analize finančnih izkazov. Uporabljajo kvantitativne metode (npr. podatkovno analitiko in statistično modeliranje) ter kvalitativne pristope (npr. oceno vedenjskih vzorcev in organizacijske kulture) za prepoznavanje odstopanj. Benfordov zakon opisuje pričakovano porazdelitev števk v naravno nastalih podatkovnih nizih; forenzični računovodje ga uporabljajo za prepoznavanje nepravilnosti v finančnih podatkih, saj lahko odstopanja od pričakovane porazdelitve kažejo na manipulacijo ali goljufijo. Mark Nigrini, pionir na tem področju, je Benfordov zakon obsežno raziskoval in ga uporabljal za odkrivanje anomalij v računovodskih podatkih (glej npr. Gorenc, 2019; Siavoshi, 2025).
- Metode dokazovanja prihodkov: preiskovalci uporabljajo neposredne in posredne metode za ugotavljanje nezakonitih virov prihodkov. Metoda neto premoženja primerja premoženje posameznika v dveh časovnih točkah, da se oceni neprijavljen dohodek. Metoda bančnih pologov analizira nepojasnjene prilive na bančne račune. Metoda izdatkov primerja vzorce porabe z znanimi zakonitimi viri dohodkov.
- Izmenjava finančnoobveščevalnih podatkov: organi pregona sodelujejo s finančnoobveščevalnimi enotami (FIU), bankami in mednarodnimi partnerji za

pridobivanje poročil o sumljivih aktivnostih (SAR) in drugih relevantnih finančnih podatkov.

- Pregled finančnih transakcij: analitika transakcij preiskovalcem pomaga prepoznati sumljive bančne vzorce, tehnike plastenja (layering) ter načine integracije premoženja (asset integration).
- Digitalna forenzika (glej razdelek 9.6.1): ima pomembno vlogo pri sledenju spletnim denarnim prenosom, analizi transakcij s kriptovalutami in prestrezanju nezakonitih finančnih komunikacij.

### Izkoriščanje sinergij sodelovanja

Finančnoobveščevalne enote (FIU) imajo ključno vlogo pri finančnih preiskavah, saj zbirajo, analizirajo in posredujejo finančnoobveščevalne informacije organom pregona. FIU prejemajo razkritja v okviru AML/CFT, poročila o sumljivih transakcijah (STR) ter poročila o čezmejnih transakcijah, ki lahko predstavljajo zgodnje opozorilne signale o nezakonitih finančnih aktivnostih. Močno nacionalno sodelovanje med FIU in preiskovalci zagotavlja, da imajo organi pregona pravočasne in operativno uporabne informacije. Za večjo učinkovitost bi morale FIU in organi pregona vzpostaviti varne platforme za deljenje podatkov v realnem času ter razviti protokole za analizo finančnoobveščevalnih podatkov.

Ker je finančna kriminaliteta pogosto čezmejna, je nujno tudi mednarodno sodelovanje. Storilci izkoriščajo mednarodne bančne sisteme in offshore finančna središča za prikrivanje nezakonitih sredstev. Organi pregona morajo pri čezmejnih preiskavah učinkovito uporabljati mehanizme mednarodne pravne pomoči (MLAT), Interpol, Europol in mreže FATF. Vzpostavljanje skupnih preiskovalnih skupin ter

poenotenje oziroma poenostavitev pravnih okvirjev za izmenjavo informacij krepi globalni boj proti finančni kriminaliteti (FATF, 2012).

Za dodatno krepitev finančnih preiskav bi morali organi pregona in tožilstva finančno forenziko vključevati v vse večje preiskave kaznivih dejanj, izkoriščati sisteme finančne obveščevalne dejavnosti za analizo v realnem času ter okrepiti mednarodno sodelovanje pri izterjavi premoženja in izmenjavi obveščevalnih podatkov. Z upoštevanjem teh dobrih praks lahko finančne preiskave postanejo močno orodje za razbijanje kriminalnih združb in zagotavljanje, da se kazniva dejanja ne izplačajo.

### 9.5.1.2 Prizadevanja Evropske unije

Ker je organizirani kriminal vse bolj prisoten tudi v legitimnem gospodarstvu, je Evropska unija poudarila potrebo po krepitvi zmogljivosti za finančne preiskave. Strategija EU za boj proti organiziranemu kriminalu iz leta 2021 je izpostavila pomen spodbujanja zgodnjih finančnih preiskav v vseh državah članicah EU. Namen takšnega pristopa je razgraditi finančno infrastrukturo kriminalnih združb, odvzeti nezakonite dobičke ter preprečiti, da bi se kriminalni prihodki in vpliv prelivali v zakonito gospodarstvo in družbo (European Commission, n.d.). V podporo tem prizadevanjem je Evropska multidisciplinarna platforma proti kriminalnim grožnjam (EMPACT) med prednostne naloge uvrstila tudi finančne preiskave. EMPACT omogoča sodelovanje med državami članicami EU pri obravnavi različnih kriminalnih groženj, vključno s trgovino z drogami in trgovino z ljudmi, pri čemer finančne preiskave vključuje kot skupni cilj vseh prednostnih področij.

Poleg tega Evropska komisija finančno podpira Operativno mrežo za boj proti pranju denarja (AMON), globalno mrežo preiskovalcev na področju preprečevanja pranja denarja, ustanovljeno leta 2012. AMON omogoča izmenjavo znanja med enotami organov pregona ter podpira hitro operativno sodelovanje pri preiskavah pranja denarja, kar odraža čezmejno naravo tovrstnih kaznivih dejanj.

Europol je svoja prizadevanja dodatno okrepil z ustanovitvijo Evropskega centra za finančni in gospodarski kriminal (EFECC) leta 2020. EFECC državam članicam EU zagotavlja operativno podporo v primerih davčnih kaznivih dejanj, goljufij, korupcije, pranja denarja, izterjave in odvzema premoženja, ponarejanja evra ter kaznivih dejanj s področja intelektualne lastnine. Namen te pobude je učinkoviteje obravnavati zelo kompleksne oblike finančne kriminalitete, usmerjene proti posameznikom, podjetjem in javnemu sektorju.

Evropska agencija za usposabljanje na področju kazenskega pregona (CEPOL) poleg tega redno izvaja usposabljanja za uslužbence organov pregona, s katerimi krepi razumevanje shem pranja denarja in tehnik čezmejnih finančnih preiskav. Cilj teh usposabljanj je okrepiti zmogljivosti preiskovalcev za učinkovito obravnavo finančnih razsežnosti organiziranega kriminala (European Commission, n.d.).

Skupno gledano celovit pristop Evropske unije k finančnim preiskavam poudarja njihovo ključno vlogo pri motenju delovanja kriminalnih združb, varovanju zakonitega gospodarstva ter krepitvi učinkovitosti organov pregona v državah članicah.

## 9.5.2 Trgovanje z ljudmi kot poslovni model

Trgovina z ljudmi deluje kot dobičkonosno, tržno naravnano »poslovanje«, podobno kot zakonite gospodarske dejavnosti. Ta perspektiva je uporabna, da (1) bolje razumemo ključne gonilnike trgovine z ljudmi in (2) utemeljimo potrebo po finančnih preiskavah. Ekonomske teorije kriminalitete predpostavljajo, da storilci sprejemajo racionalne odločitve na podlagi pričakovanih dobičkov, tveganj in priložnosti (glej npr. Belser, 2005). Priložnosti se pojavljajo zaradi posameznikov, ki iščejo boljše ekonomske razmere, bodisi z migracijami iz revnejših podeželskih območij v bogatejša urbana središča bodisi prek državnih meja. Kriminalne mreže te ranljivosti izkoriščajo z lažnimi obljubami zaposlitve, ljubezni ali varnosti ter žrtve zvabijo v delovno ali spolno izkoriščanje oziroma druge oblike trgovine z ljudmi (npr. odvzem organov).

Poslovni model delovnega izkoriščanja je razmeroma preprost: žrtve delajo pod prisilo ali brez polnega zavedanja izkoriščevalnih razmer, s čimer ustvarjajo visoke dobičke, storilci pa imajo pri tem nizke stroške. Sektorji, kot so kmetijstvo, gradbeništvo, gospodinjsko delo in gostinstvo, lahko zagotavljajo »kritje« za delovno izkoriščanje, medtem ko spolno izkoriščanje ostaja eden najbolj donosnih »trgov« za storilce (glej npr. Aronowitz, Theuermann in Tyurykanova, 2010).

Kljub visoki dobičkonosnosti tveganja za storilce pogosto ostajajo nizka. Mnoge žrtve se organov pregona bojijo zaradi svojega pravnega statusa, družbene stigme ali groženj izkoriščevalcev. V državah, kjer je prostitucija nezakonita, so žrtve lahko bolj izpostavljene tveganju kaznovanja kot zaščiti. Poleg tega sta odkrivanje in pregon storilcev pogosto razmeroma redka, kar prispeva k vzdržnosti takšnega »poslovnega modela«. Tržne sile pomembno vplivajo na delovanje mrež trgovine z ljudmi. Trgovine z ljudmi ne spodbuja zgolj povpraševanje potrošnikov, temveč predvsem obstoj velikega »bazena« ranljivih oseb. Kriminalne združbe svoje metode prilagajajo pravnim okvirom,

gospodarskim razmeram in učinkovitosti nadzornih mehanizmov, podobno kot zakonita podjetja odzivajo na tržne spremembe (Aronowitz, Theuermann in Tyurykanova, 2010).

Finančne preiskave trgovine z ljudmi morajo zato upoštevati te ekonomske gonilnike. Z analizo finančnih transakcij, dobičkovnih marž in nezakonitih denarnih tokov lahko organi pregona prepoznajo vzorce izkoriščanja, motijo delovanje mrež ter zmanjšujejo finančne spodbude, ki trgovino z ljudmi poganjajo. Razumevanje trgovine z ljudmi kot ekonomske dejavnosti je ključno za razvoj učinkovitih protiukrepov, vključno z regulativnimi okviri, finančnim nadzorom in ciljno usmerjenimi intervencijami. Naslednji razdelek predstavi splošni okvir finančnih preiskav v primerih THB ter opredeli konkretne korake, ki jih je treba pri tem izvesti.

### 9.5.3 Smernice za finančne preiskave, povezane s trgovino z ljudmi

Ta razdelek opisuje **enajst ključnih korakov** za učinkovito izvajanje finančnih preiskav v primerih trgovine z ljudmi. Koraki so razdeljeni na tri področja: temeljne, operativne in skupnostne.

Temeljni koraki se praviloma izvedejo enkrat ob vzpostavitvi preiskovalnega okvira in se na splošno uporabljajo tako v javnem kot v zasebnem sektorju. Operativni koraki se uporabljajo pogosteje, ker so neposredno povezani s posameznimi preiskavami, vendar se njihovo izvajanje razlikuje med javnimi in zasebnimi subjekti. Na primer, 7. in 8. korak se nanašata predvsem na poročevalske subjekte v zasebnem sektorju. Skupnostni koraki pa so razdeljeni glede na uporabo: oba sektorja imata skupen interes pri 10. koraku, medtem ko imajo ponudniki finančnih storitev večjo odgovornost pri 11. koraku.

Slika 14 prikazuje shematičen postopek tega vodiča po korakih med organi pregona (LEA) in finančnoobveščevalnimi enotami (FIU). Slika je povzeta po OVSE (2020).

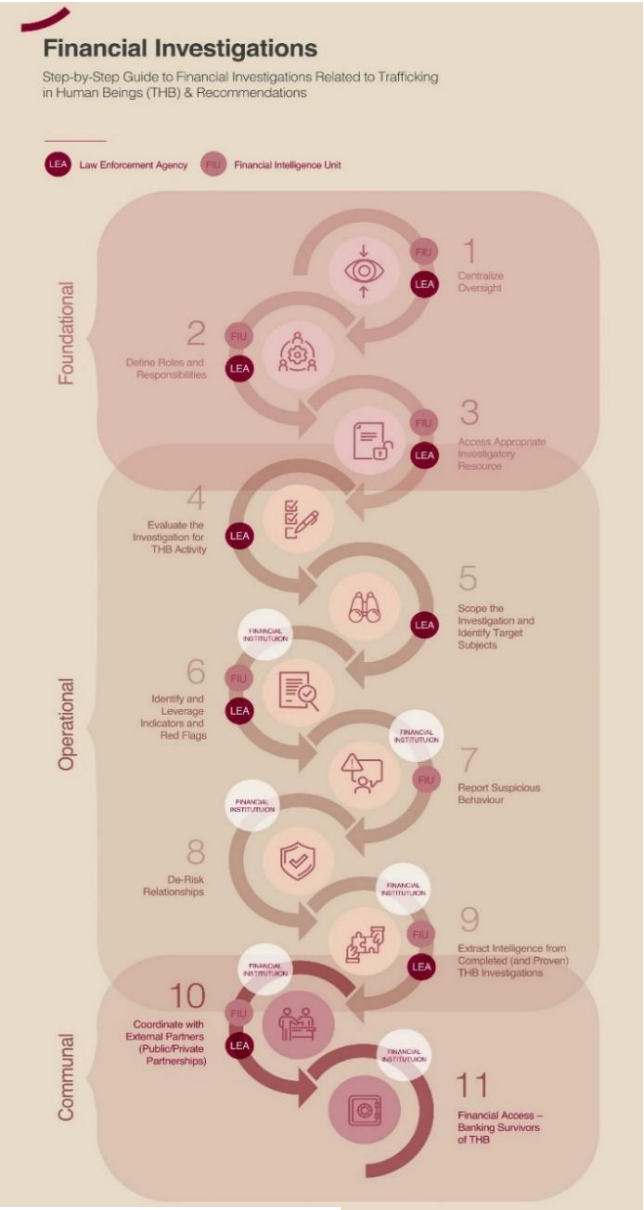


*Figure 4. Steps of a financial investigation*

**Korak 1**: Prvi korak k uspešni finančni preiskavi v primerih trgovine z ljudmi je vzpostavitev centraliziranega mehanizma usmerjanja in nadzora. To omogoča usklajen in celovit odziv na vsak sumljiv primer, pri čemer se lahko konkretna ureditev razlikuje glede na velikost institucije in njen mandat. Organi pregona pogosto vključijo preiskovanje trgovine z ljudmi v specializirane enote. Tako imajo na primer newyorška policija (NYPD) in londonska Metropolitanska policija (MPS) namenske ekipe, medtem ko policija v Torontu (TPS) primere obravnava znotraj enote za spolna kazniva dejanja, pri čemer priznava razlikovanje med trgovino z ljudmi in kaznivimi dejanji, povezanimi z »vice« (npr. prekrškovno obravnavanimi dejavnostmi). Tudi zvezne agencije, kot sta FBI in Interpol, centralizirajo strokovno znanje, enako velja za finančnoobveščevalne enote (FIU), čeprav te pogosto delujejo z manj javne vidnosti.

V zasebnem sektorju, zlasti v bankah, je nadzor običajno manj strukturiran zaradi velikega obsega transakcij in regulatornih zahtev. Kljub temu številne institucije vzdržujejo specializirane preiskovalne ekipe za finančno kriminaliteto, vključno s trgovino z ljudmi. Centralizacija preiskovalnih naporov ima več prednosti: zmanjšuje podvajanje dela, povečuje učinkovitost, krepi strokovnost in omogoča celovitejšo analizo podatkov. Ima pa tudi tveganja, na primer, da znanje ostane omejeno na ozek krog ljudi ali da pride do zamud zaradi preobremenjenosti enote. Za zmanjšanje teh tveganj naj institucije spodbujajo deljenje znanja in ohranjajo določeno fleksibilnost pri razporejanju preiskovalnih nalog, da se preprečijo »ozka grla«. V praksi lahko preiskave izvajajo tudi različne skupine, če so primeri ustrezno evidentirani in vodeni, kar koristi tako notranjim kot zunanjim deležnikom.

**Korak 2:** Ko je vzpostavljen okvir nadzora nad preiskavami trgovine z ljudmi, je ključno jasno opredeliti vloge in odgovornosti vseh vključenih. Čeprav je to v mnogih javnih in

zasebnih institucijah standardna praksa, se včasih spregleda. Jasna razdelitev odgovornosti preprečuje podvajanje aktivnosti, povečuje operativno učinkovitost in prinaša dodatne koristi, kot so lažje načrtovanje nasledstev, učinkovitejša triaža primerov, boljše določanje prioritet ter doslednejša komunikacija znotraj ekipe in navzven. Dokumentiranje vlog prispeva k temu, da so preiskave izvedene bolj učinkovito in pravočasno. Gre za načelo »razdeli in obvladaj«: ko vsi razumejo svojo vlogo, se lahko osredotočijo na izvedbo. Brez jasnih odgovornosti lahko tudi dobronamerna prizadevanja vodijo v nedosleden in manj učinkovit preiskovalni proces.

**Korak 3:** Uspešna preiskava zahteva dostop do ustreznih virov, ki se lahko razlikujejo glede na naravo preiskave. Finančne preiskave, zlasti na področju pranja denarja in trgovine z ljudmi, zahtevajo specializirana orodja, ki se razlikujejo od tistih, ki se uporabljajo pri terenskih aktivnostih. Zaradi kompleksnosti sledenja finančnim tokovom morajo imeti preiskovalci na voljo zadostne vire za učinkovito analizo transakcij, povezovanje sorodnih primerov ter prilagajanje spreminjajočim se taktikam storilcev.

Zagotavljanje potrebnih orodij in virov preiskovalcem povečuje učinkovitost, izboljšuje kakovost preiskovanja ter povečuje verjetnost uspešnih prijetij in obsodb. Ključni viri vključujejo:

- Digitalni sistemi za vodenje primerov: centralizirana baza za shranjevanje zapiskov in dokazov omogoča boljše sledenje primerom ter povezovanje povezanih preiskav.
- Neomejen dostop do interneta: preiskovalci lahko pri spremljanju dejavnosti, povezanih s trgovino z ljudmi, potrebujejo dostop tudi do omejenih spletnih vsebin (npr. platform z vsebinami za odrasle), pri čemer morajo imeti ustrezno usposabljanje in jasna pravila, ki preprečujejo zlorabe.

- Usposabljanje za OSINT: specializirano usposabljanje za spletne preiskave pomaga odkriti ključne informacije ter hkrati zaščititi identiteto in varnost preiskovalcev.
- Dostop do internih podatkov: takojšnja razpoložljivost relevantnih institucionalnih podatkov (npr. transakcijskih zapisov ali preteklih spisov) je bistvena. Odpravljanje tehnoloških, pravnih in birokratskih ovir pri dostopu do podatkov izboljšuje učinkovitost preiskav.
- Strokovno pravno svetovanje: finančna kazniva dejanja pogosto vključujejo tudi davčna, vrednostnopapirna in nepremičninska vprašanja, zato je smiselno zgodaj vključiti specialiste. Zgodnja identifikacija pravnih in finančnih strokovnjakov okrepi rezultate preiskave.

Čeprav je dostop do virov ključen, morajo institucije ves čas uravnotežiti učinkovitost s pravnimi in etičnimi zahtevami ter zagotoviti, da preiskovalci delujejo v okviru predpisov, hkrati pa čim bolj izkoristijo svoje preiskovalne zmogljivosti.

**Korak 4**: Eden ključnih izzivov pri finančnih preiskavah, povezanih s trgovino z ljudmi (THB), je tveganje napačne opredelitve kaznivega dejanja – bodisi da se drugo kaznivo dejanje zmotno obravnava kot THB bodisi da se spregledajo indikatorji THB. Do tega lahko pride zaradi pomanjkljivega poznavanja pravnega okvira ali zaradi prekrivanja značilnosti z drugimi ravnanji, kot so tihotapljenje ljudi ali kršitve delovne zakonodaje. Jasno razlikovanje med temi pojavi je bistveno, zlasti za preiskovalce v javnem in zasebnem sektorju. Zasebne institucije bi morale dodatno opredeliti, katera predhodna kazniva dejanja (predicate offences) bodo obravnavale njihove specializirane ekipe, saj so izključno THB-enote zaradi omejenih virov redke.

Ko je vzpostavljeno temeljno razumevanje zakonodaje, povezane s THB, ter preiskovalnih pristojnosti, lahko preiskovalci natančneje oblikujejo pristop k obravnavi prijav in napotitev. Organi javnega sektorja običajno prejemajo večje število THB-povezanih napotitev zaradi širšega mandata, medtem ko imajo ekipe v zasebnem sektorju praviloma manj primerov, vendar pogosto več možnosti za proaktivno preiskovanje. Proaktivne strategije vključujejo:

- pregled že zaključenih primerov: starejši primeri, ki so bili napačno označeni kot prostitucija ali tihotapljenje, lahko vsebujejo spregledane elemente THB
- izvedbo zgodovinskih pregledov negativnih medijskih objav: pregled medijskih poročil o osumljenih storilcih lahko razkrije finančne povezave ali vzorce v računih znotraj institucije
- analizo SAR: pregled zgodovinskih SAR-podatkov lahko pomaga prepoznati spregledane rdeče zastavice, povezane s THB
- spremljanje sektorjev z visokim tveganjem: panoge, kot so masažni saloni, striptiz klubi in pornografija, se v različnih okoljih povezujejo s THB in zato zahtevajo večjo pozornost

Učinkovite finančne preiskave zahtevajo kombinacijo reaktivnih in proaktivnih ukrepov. Njihov uspeh pa je odvisen od kakovosti izmenjanih obveščevalnih podatkov – zlasti od tega, da dobro dokumentirana poročila o sumljivih aktivnostih (SAR) pravočasno dosežejo organe pregona in sprožijo smiselne, ciljno usmerjene aktivnosti.

**Korak 5:** Jasno opredeljen obseg preiskave je ključen, da primer ne postane preobsežen in neobvladljiv ter da se po pomoti ne poveže nedolžnih oseb s kriminalno dejavnostjo. V preiskavah trgovine z ljudmi (THB) storilci pogosto zlorabljajo bančne

račune žrtev za lastno korist, zato je bistveno, da imajo organizacije vzpostavljene politike in postopke, ki preprečujejo dodatno viktimizacijo. Prednostna naloga je jasno razlikovanje med storilci in žrtvami, nato identifikacija ključnih storilcev pred obravnavo sekundarnih omogočevalcev. Takšen pristop, ki temelji na oceni tveganja, omogoča optimalno uporabo virov in večjo učinkovitost preiskovanja.

Za natančno določitev obsega preiskave mora biti ta že na začetku čim bolj celovito zastavljena. Primer 360 modela, ki ga je razvil Peter Warrack, ponuja strukturiran način za ocenjevanje finančnih aktivnosti z vidika možnega pranja denarja in se lahko uporablja tako v zasebnih finančnih institucijah kot tudi pri organih pregona. Model obsega šest korakov:

1. Sprožilni dogodek – Preiskava se začne z opozorilom, na primer s poročilom o sumljivih aktivnostih (SAR), zaznavo v avtomatiziranem sistemu spremljanja transakcij, negativnimi medijskimi objavami, interno napotitvijo ali zahtevo organov pregona.
2. Razumite stranko – Zberite kontekstualne informacije o obravnavani osebi (ali subjektu), vključno z zaposlitvijo, finančnim položajem in splošnim profilom.
3. Razumite finančno aktivnost – Finančno vedenje stranke ocenite v primerjavi z znanim ozadjem ter preverite, ali je skladno s pričakovanji.
4. Izločite običajno – Transakcije, ki so za stranko videti običajne, izločite, da se lahko osredotočite na resnično sumljive aktivnosti.
5. Analizirajte preostalo finančno aktivnost – Osredotočite se na aktivnosti, ki so sprožile začetni sum, ter analizirajte vzorce in morebitne povezave z nezakonitim ravnanjem.

6. Poročajte in razmislite o prekinitvi poslovnega razmerja – Če preiskava potrdi sum, vložite SAR pri pristojni FIU; v primerih, ki jih vodijo organi pregona, lahko sledi tudi predlog za izdajo odredbe za prijetje.

Takšen strukturiran pristop zagotavlja, da so preiskovalni viri usmerjeni v dejanske grožnje, zmanjšuje število lažno pozitivnih zaznav in izboljšuje splošno učinkovitost.

**Korak 6:** Razumevanje, kaj pomeni sumljiva finančna aktivnost v kontekstu trgovine z ljudmi (THB), zahteva tako splošno poznavanje bančnih praks kot tudi poglobljeno razumevanje načinov delovanja storilcev. Temeljno bančno znanje je razmeroma enostavno pridobiti, vendar prepoznavanje odstopanj pogosto zahteva dostop do obsežnih podatkov ter praktične izkušnje pri preiskovanju. Kljub temu pa lahko pomanjkanje neposrednih izkušenj vsaj delno nadomesti strokovno raziskovanje, saj je o finančnih vzorcih in vedenjih storilcev na voljo veliko dokumentacije in analiz.

Na makro ravni lahko indikatorje trgovine z ljudmi (THB) razvrstimo v tri kategorije:

1. Vedenjski indikatorji – nanašajo se na osebno zaznavne, vizualne znake in vedenjske vzorce, ki lahko kažejo, da je posameznik ujet v trgovino z ljudmi ali da je nekdo v vlogi storilca.
2. Indikatorji v okviru KYC (Know Your Customer / »Poznaj svojo stranko«) – opozorilni znaki, ki izhajajo iz podatkov, ki jih posreduje stranka, na primer neskladja v identifikacijskih dokumentih, naslovih ali drugih osnovnih informacijah.
3. Transakcijski indikatorji – sumljivi finančni vzorci, ki se lahko pojavijo kadarkoli po odprtju računa, pogosto brez neposrednega stika s stranko, zlasti zaradi širjenja digitalnega bančništva.

Ti indikatorji se lahko pojavijo samostojno ali v kombinaciji, pogosto pa jih v organizaciji zaznajo različne ekipe – na primer zaposleni v prvi liniji lahko prepoznajo vedenjske znake, ekipe za zbiranje in preverjanje podatkov lahko opazijo KYC »rdeče zastavice«, ekipe za spremljanje transakcij pa zaznajo finančna odstopanja. Zato so jasna pravila komuniciranja in protokoli za eskalacijo ključni, da se potencialno sumljive okoliščine ustrezno preveri in temeljito preišče.

Razdelitev indikatorjev v te tri kategorije je skladna z okviri, ki so jih razvili Thomson Reuters in bančne zveze (Banks Alliance) v Evropi, Aziji in ZDA. Njihovi priročniki in »toolkiti« ponujajo dodatne vpoglede, vključno z oceno relativne »teže« posameznih indikatorjev ter povezavo z določenimi oblikami trgovine z ljudmi, na primer z delovnim izkoriščanjem.

Pomembno je poudariti, da nekateri indikatorji (npr. pogosti nakupi v lekarni) sami po sebi še niso nujno sumljivi. Zato morajo analitiki vedno presojati več dejavnikov hkrati, da lahko utemeljijo razumen sum. To je skladno tudi s smernicami finančnoobveščevalnih organov, med drugim tudi z usmeritvami, vključno z:

- FINTRAC (Kanada, 2016) poudarja: »Posamezna transakcija, obravnavana ločeno, lahko vodi v napačen vtis normalnosti. Šele upoštevanje vseh indikatorjev lahko razkrije neznane povezave, ki skupaj lahko predstavljajo utemeljene razloge za sum trgovine z ljudmi (THB).«

- FinCEN (ZDA, 2014) navaja: »Nobena posamezna transakcijska ‘rdeča zastavica’ ni jasen indikator dejavnosti, povezane s tihotapljenjem ljudi ali trgovino z ljudmi. Upoštevati je treba tudi dodatne dejavnike, na primer pričakovani finančni profil stranke.«

- Tako FINTRAC kot FinCEN zato poudarjata pomen strukturiranega preiskovalnega pristopa, kot je Warrackov 360 model, ki omogoča, da se finančne 'rdeče zastavice' presojajo v kontekstu in ne izolirano. Za celovit seznam sintetiziranih indikatorjev glejte priloge v publikaciji OVSE Compendium of Resources and Step-by-Step Guide to Financial Investigations Related to Trafficking in Human Beings (OSCE, 2019).

**Korak 7:** Poročila o sumljivih aktivnostih (SAR) imajo ključno vlogo pri finančnih preiskavah tako v javnem kot zasebnem sektorju. Tradicionalno SAR v zasebnem sektorju pomeni zaključek interne preučitve (najpogosteje v finančni instituciji, na primer v banki), nakar institucija poročilo posreduje svoji finančnoobveščevalni enoti (FIU). V javnem sektorju pa lahko SAR predstavlja sprožilec za začetek preiskave organov pregona. Da bi se njihov potencial res izkoristil, je smiselno na SAR gledati kot na uporabno orodje skozi celoten preiskovalni proces – ne le kot na »zadnji korak« zasebne preučitve ali kot začetni impulz za javno preiskavo. SAR lahko prispeva obveščevalne informacije v različnih fazah, bodisi kot dopolnilo že tekočim preiskavam bodisi kot kontekst za interne preglede v zasebnih institucijah.

V zasebnem sektorju je priporočljivo uporabljati tehnične rešitve, ki razbremenijo administrativni del vnosa rutinskih podatkov, da se preiskovalci lahko osredotočijo na vsebinski del sumljivih aktivnosti. Prav tako naj bodo podatki iz preteklih SAR enostavno dostopni, saj omogočajo prepoznavanje vzorcev, odkrivanje specifičnih kaznivih dejanj ter sledenje vpletenim osebam in subjektom. Pri novih SAR je smiselno sklicevanje na prejšnja poročila, povezana z isto kriminalno mrežo, da se zgradi koherentna »zgodba« in se izogne podvajanju poročanja. Pomembno je tudi, da poročevalske institucije upoštevajo poimenovalne konvencije, ki jih določijo nacionalne FIU, zlasti pri odmevnih

kaznivih dejanjih, kot je trgovina z ljudmi (THB). Takšna usklajenost prispeva k skladnosti z regulatornimi pričakovanji, krepi verodostojnost poročanja in pomaga pri prepoznavanju trendov finančne kriminalitete. Na primer: ameriški FinCEN priporoča označevanje SAR, povezanih s THB, z oznako »Advisory Human Trafficking«, kanadski FINTRAC pa predlaga oznako »Project Protect«. Institucije, ki nimajo takšnih kodnih sistemov, bi lahko razmislile o javno-zasebnih partnerstvih za njihovo uvedbo.

V javnem sektorju je priporočljivo, da se baze SAR, ki jih vodijo FIU, uporabljajo pri vseh preiskavah trgovine z ljudmi, saj je ta kriminal praviloma povezan s finančno koristjo. Organi pregona lahko dodatno uporabijo mehanizme, kot so odredbe za predložitev podatkov in hišne preiskave (production orders, warrants), da spodbudijo banke in druge poročevalske subjekte k vlaganju SAR, povezanih z odprtimi preiskavami. Kljub pomembnosti pa so SAR pogosto tarča kritik zaradi naraščajočega števila poročil nizke kakovosti. Tako je poročilo OVSE iz leta 2014 navajalo, da je bilo v Italiji od 37.000 SAR za kazenske preiskave uporabnih le 23. Tudi britanska komisija za pravno reformo je leta 2019 izpostavila podobne pomisleke in opozorila na potrebo po izboljšavah pri poročanju SAR, da bi se zmanjšal obseg nekakovostnih prispevkov. Z upoštevanjem nekaterih zgoraj navedenih priporočil (npr. sklicevanje na zgodovinske SAR) se lahko kakovost prihodnjih poročil opazno izboljša.

**Korak 8:** Po zaključku interne preučitve v zasebni instituciji, na primer v banki, je treba sprejeti odločitev, ali se bo poslovno razmerje s preiskovano stranko nadaljevalo. Ta proces se pogosto označuje kot »de-risking« in lahko pomeni tudi prekinitev poslovnega razmerja. Ključno je jasno razlikovati med žrtvijo in storilcem, da se žrtev ne kaznuje neupravičeno, kar je pri primerih trgovine z ljudmi še posebej pomembno. Če račun pripada žrtvi trgovine z ljudmi, naj bo cilj praviloma ohranitev razmerja, razen če obstajajo

večkratne kršitve ali znaki soudeležbe. Pri »de-riskingu« je potrebna previdnost, saj lahko potiskanje sumljivih aktivnosti v neformalne oziroma nezakonite kanale oteži preiskovanje organom pregona. V nekaterih jurisdikcijah lahko organi pregona banki tudi predlagajo ali zahtevajo, da račun ostane odprt, da se preiskava ne prekine ali ogrozi. Če je prekinitev poslovnega razmerja vendarle potrebna, je smiselno uporabljati standardizirana obvestila, ki ne vsebujejo obtoževanja ali neutemeljenih namigov, ter voditi evidenco o že »de-riskanih« osebah oziroma subjektih za prihodnjo referenco.

**Korak 9:** Prepoznavanje dejanskih primerov trgovine z ljudmi (THB) zgolj na podlagi finančnih transakcij je zahtevno, ker pogosto manjka kontekstualnih informacij. Poleg tega na verjetnost, da se pride do dokončnih ugotovitev, vpliva tudi to, ali preiskovalec deluje v javni instituciji ali v zasebni organizaciji. Zasebne organizacije (npr. ponudniki finančnih storitev) pred vložitvijo SAR pri FIU praviloma niso dolžne dokazati »onkraj razumnega dvoma«, da je prišlo do predhodnega kaznivega dejanja. Prag poročanja je pogosto nižji, ker finančne institucije vidijo le del celotne slike. Poleg tega FIU običajno ne dajejo povratnih informacij o tem, ali so SAR dejansko vodili do potrditve predhodnega kaznivega dejanja, zato zasebni sektor težje potrjuje, ali je šlo za THB-povezano aktivnost.

Ker popolna transparentnost glede izida finančnih preiskav THB ni vedno mogoča, je smiselno potrjene primere uporabljati za usposabljanje in prihodnje obvladovanje tveganj. Ponudniki finančnih storitev lahko potrjene primere THB prepoznajo tako, da:

- Z rednim spremljanjem dnevnih posodobitev negativnih medijskih objav (adverse media) in preverjanjem morebitnih povezav z internimi preiskavami.
- Z naročanjem na posodobitve organov pregona ali FIU o izvrševanju zakonodaje na področju THB ter s primerjavo teh informacij z internimi primeri.

- Z vzpostavitvijo neposrednega kanala za napotitve oziroma posredovanje informacij s strani organov pregona v povezavi s preiskavami THB.

Priporočljivo je, da se obveščevalne informacije iz potrjenih primerov THB deli s širšo preiskovalno ekipo in ne zgolj s specializirano THB-enoto. To je skladno z usmeritvami iz 1. koraka (centraliziran nadzor) in lahko pozitivno vpliva na motivacijo preiskovalcev, okrepi občutek smisla pri delu ter poveča verjetnost, da se zagotovijo dodatni viri ali vzpostavi učinkovitejše sodelovanje med ekipami.

**Korak 10:** V zadnjih letih sta se pomen in razširjenost javno-zasebnih partnerstev (PPP) pri preprečevanju in odkrivanju finančne kriminalitete, zlasti trgovine z ljudmi (THB), izrazito povečala. Globalna prizadevanja za odpravo THB so okrepila sodelovanje tudi med sicer konkurenčnimi akterji v industriji, saj se je pokazalo, da storilci premikajo finančne tokove med različnimi institucijami in bankami. Strokovnjaki za preprečevanje finančne kriminalitete zato vse pogosteje sodelujejo, da bi takšne dejavnosti učinkoviteje zaznali in prekinili. Med vidnejšimi PPP pobudami so britanski Joint Money Laundering Intelligence Taskforce (JMLIT), avstralska Fintel Alliance in kanadski Project Protect. Tudi ZDA imajo mehanizme za izmenjavo informacij, na primer določbe iz US: PATRIOT Act 314(a).

Motivacija za sodelovanje v PPP vključuje izpostavljenost različnim pristopom finančnega preiskovanja, hitrejši razvoj indikatorjev THB, krepitev odnosov s strokovnimi kolegi in organi pregona, kakovostnejše preiskave, delitev virov ter prispevek k širšemu družbenemu dobremu. OVSE (OSCE) pa hkrati prepoznava izzive pri vzpostavljanju učinkovitega sodelovanja med FIU, organi pregona in subjekti, ki poročajo o sumljivih transakcijah (STR). Eden od izzivov je enosmeren tok informacij, saj FIU pogosto ne morejo (ali ne smejo) deliti obveščevalnih podatkov zunaj svoje organizacije. Povratne

informacije o kakovostnih STR bi lahko izboljšale usposabljanja, metode zaznavanja ter kakovost SAR/STR poročanja.

Pomanjkanje povratnih informacij FIU in odsotnost mednarodnih baz podatkov o storilcih THB dodatno poudarjata potrebo po PPP. Pri vzpostavitvi PPP ni vedno potrebno spreminjati zakonodaje; pogosto je mogoče uporabiti obstoječe pravne okvire. Primer je kanadski Project Protect, ki je deloval znotraj nacionalnega pravnega okvira in se osredotočal na splošne tipologije ter indikatorje, ob hkratnem spoštovanju zakonodaje o varstvu zasebnosti. Ključno je razumeti pravne omejitve ter delovati znotraj njih, da se sodelovanje lahko razvija. Dolgoročni cilji PPP lahko vključujejo tudi zagovorništvo za spremembe zakonodaje, ki temeljijo na uspešnih praksah sodelovanja.

Vzpostavitev ali vključitev v PPP naj praviloma sledi vzpostavitvi trdnega preiskovalnega procesa, vendar je zgodnje sodelovanje kljub temu dragoceno. Lahko prinese vpoglede, ki pomagajo oblikovati preiskovalni proces na način, ki bi ga kasneje, ko so postopki že utrjeni, težje dosegli. Sodelovanje v PPP praviloma poveča celovitost pristopa k preiskovanju trgovine z ljudmi (THB).

**Korak 11:** Preiskave trgovine z ljudmi (THB), zlasti v bančnem sektorju, lahko na žrtve vplivajo tudi negativno. To dodatno poudarja pomen 4. koraka (oceni preiskavo z vidika možne THB-aktivnosti), ki zagotavlja, da so aktivnosti, povezane s THB, na ravni ekipe ali institucije jasno opredeljene. Če je 4. korak pravilno izveden, lahko kasneje zmanjša nepotrebno delo, saj pomaga preprečevati, da bi bile nedolžne osebe po pomoti izključene ali obravnavane kot visoko tvegane. Ker storilci pogosto manipulirajo s finančnim položajem žrtev, je priporočljivo, da se osebam, ki so se iz trgovine z ljudmi umaknile, omogoči obnova in krepitev njihovega finančnega profila.

Kot primer dobre prakse podpore preživelim navajajo program, ki ga je HSBC v Združenem kraljestvu uvedel junija 2019. Program pomaga preživelim, napotenim prek britanskega Nacionalnega napotitvenega mehanizma (National Referral Mechanism), pri ovirah, kot sta dokazilo o naslovu in identifikacija. Poleg tega je pobuda Lichtenstein Initiative – Blueprint for Mobilizing Finance Against Slavery and Trafficking, ki je nastala v partnerstvu z United Nations University in več vladami, povezala več finančnih institucij z namenom razširitve HSBC-jevih prizadevanj na različne institucije in jurisdikcije. Scotiabank je v sodelovanju s programom Salvation Army Deborah's Gate proti trgovini z ljudmi kot prva banka v okviru te pobude finančne vključenosti odprla račune za preživele. Pričakovati je, da bodo tudi druge vključene finančne institucije sledile in razvile podobne programe.

Ob vse večji osredotočenosti na osebe in strukture, ki omogočajo ali izvajajo THB, je pomembno, da se ne izgubi izpred oči žrtev. Javno-zasebna partnerstva ter sodelovanje z medvladnimi skupinami lahko vzpostavijo celovit pristop k preprečevanju in preiskovanju THB, ki koristi ne le vključenim institucijam, temveč tudi žrtvam – pogosto z razmeroma nizkimi stroški izvedbe.

## 9.5.4 Prepoznavanje sumljivih finančnih aktivnosti

OSCE je objavila seznam transakcijskih finančnih indikatorjev oziroma »rdečih zastavic«, ki so uporabni pri prepoznavanju trgovine z ljudmi (THB), zlasti v kontekstu delovnega izkoriščanja. Spodnji seznam je povzet po poročilu OVSE; izvirniku so bili odstranjeni trije indikatorji, ki so se nanašali specifično na odvzem organov, ter sedem indikatorjev, ki so se nanašali na spolno izkoriščanje, da bi bil seznam primernejši za

delovno izkoriščanje. V posameznih primerih se lahko indikatorji razlikujejo, prekrivajo ali pojavljajo v kombinaciji (OVSE, 2019, str. 61 in dalje).

- Uporaba posrednikov pri uporabi poslovnega računa.
- Neplačevanje davkov, prispevkov za nezgodno zavarovanje pri delu in drugih obveznosti do davčnih organov.
- Znesek izplačila plače je v vsakem plačilnem obdobju identičen (brez sprememb za nadure, dopust, bolniško, dodatke, nagrade ipd.) pri delih, kjer bi spremembe običajno pričakovali.
- Ponavljajoča se izplačila plač v nerazumno nizkih zneskih (npr. bistveno pod minimalno plačo ali običajno plačno lestvico).
- Pomemben delež kapitala podjetja v vlogah brez ročnosti, nesorazmerno glede na promet/poslovanje.
- Posojila, ki jih družbenik odobri povezani pravni osebi in se nato sredstva prenesejo nazaj; navidezno (fiktivno) posojilo.
- Strukturiranje prek gospodarskih subjektov in prenos denarja s posojilno pogodbo.
- Pretirano oziroma nenavadno pogosto skupno prevažanje (ride sharing) po polnoči.
- Odsotnost običajnih življenjskih izdatkov (npr. hrana, gorivo, komunala, najemnina).
- Nakupi v restavracijah in naročila sobne strežbe, brez evidentiranih stroškov nočitev/sob.
- Uporaba več različnih oseb za izvajanje bančnih transakcij.

- Visoki in/ali pogosti izdatki na letališčih, v pristaniščih, drugih prometnih vozliščih ali v tujini, ki niso skladni z osebno rabo ali deklarirano poslovno dejavnostjo v tujini.
- Gotovinski pologi v različnih mestih po državi.
- Plačila agencijam za zaposlovanje ali študentskim posrednikom, ki niso licencirani/registrirani ali imajo ugotovljene kršitve delovne zakonodaje.
- Razmeroma visoki izdatki za nakupe, ki niso skladni z navedeno poslovno dejavnostjo.
- Transakcije izven siceršnjega časa poslovanja podjetja.
- Čezmejni prenosi sredstev, ki niso skladni z navedeno poslovno namembnostjo računa, in/ali nepojasnjeni vzorci čezmejnih transakcij po znanih poteh trgovine z ljudmi oziroma z območji, kjer je tveganje za THB višje.
- Obsežna uporaba gotovine, tudi pri nakupu poslovnih sredstev/premoženja.
- Domača nakazila podjetij iz sektorjev, občutljivih za socialne goljufije, pri čemer se denar takoj zatem dvigne v gotovini.
- Uporaba institucij ali ponudnikov, ki ne spadajo v klasični finančni sistem (netradicionalni ponudniki).
- Uporaba gotovinskih kurirjev in ponavljajoči se gotovinski dvigi.
- Nepojasnjeni oziroma neupravičeni visoki dobički podjetja.
- Gotovinski pologi tik pod pragom za poročanje.
- Gotovinski pologi na več različnih poslovalnicah ali bankomatih.

- Uporaba denarnih nakaznic (money orders) za plačevanje računov namesto osebnih čekov oziroma običajnih bančnih plačil.
- Poslovni računi, pri katerih so vidni odbitki od plač zaposlenih pod različnimi stroškovnimi postavkami (npr. nastanitev, hrana).
- Unovčenje plačilnih čekov, pri čemer se večina sredstev bodisi ponovno nakaže na račun delodajalca bodisi jo obdrži delodajalec.
- Pošiljatelj ali prejemnik z nepopolnimi podatki.
- Nakup bančnih menic takoj po gotovinskih pologih.
- Prenosi iz različnih regij na iste prejemnike v državah, ki so znane kot višje tvegane za delovanje mrež trgovine z ljudmi.
- Nakazila socialnih pomoči na račun, čeprav ima imetnik očitno na voljo znatna sredstva.
- Elektronski prenosi (nakazila) so lahko prav tako strukturirani (razdrobljeni).
- Mešanje gotovine z zakonitimi viri prihodkov.
- »Rafiniranje« gotovine (menjava bankovcev majhnih apoenov v večje apoene).
- Pogosti nakupi Bitcoina ali drugih virtualnih valut v večkratnih manjših zneskih, neposredno ali prek menjalnic.
- Prenosi, ki vključujejo tretje osebe, pri čemer so v oklepajih navedena alternativna imena/aliasi.
- Račun prejema izplačila plač od zakonitih (pogosto nacionalnih) kadrovskih agencij, vendar sredstva nato ostanejo nedotaknjena daljše obdobje.

- Pogosti nakupi nizke vrednosti v kratkih časovnih intervalih in neskladno s pričakovano aktivnostjo.
- Račun deluje kot »lijak« (funnel account), tj. prejema sredstva, ki se hitro prenesejo naprej ali dvignejo, brez jasne gospodarske logike

Naslednja študija primera iz Francavilla Lyon & De Cock (2024) ponazarja, kako lahko vzorci finančnih transakcij služijo kot kazalniki morebitnega delovnega izkoriščanja v gostinskem sektorju. Ta primer poudarja ključno vlogo finančne analize pri prepoznavanju tveganj trgovine z ljudmi in odkrivanju prikritih oblik sodobnega suženjstva.

*Primer: Moški kitajski državljan odpre osebni račun in navede, da dela v restavraciji X. Analiza poslovnega razmerja pokaže, da sta naslov te osebe in naslov restavracije X enaka. Del prejetih izplačil plače se ponovno dvigne v gotovini ali prenese na tretje osebe (brez očitne družinske povezave). Izplačila plače se izvajajo neredno in v različnih zneskih. Med pogovorom med banko in stranko je stranka banki povedala, da so tuja plačila preživninska plačila, ki jih plačuje svoji nekdanji ženi in za njune otroke. Po podatkih KYC pa stranka nima otrok. Poleg tega ima stranka po pogodbi o zaposlitvi stalno zaposlitev s fiksno plačo in ne dela po urni postavki. Manjkajo pričakovani vsakodnevni izdatki (hrana, najemnina, zavarovanja ipd.).*

Indikatorji v tem primeru so sledeči:

- Državljanstvo
- Tvegan sektor za delovno izkoriščanje
- Pretočne transakcije (pass-through transakcije)
- Gotovinske transakcije

- Odsotnost pričakovanih vsakodnevnih izdatkov
- Zasebni naslov je enak naslovu delovnega mesta
- Nasprotujoče si izjave stranke

### 9.5.5 Izzivi finančnih preiskav

Pomemben izziv pri finančnih preiskavah je spreminjajoča se narava tehnik prikrivanja, ki jih storilci uporabljajo za prikrivanje finančnih sledi. Tehnike, kot so mešalne storitve, preskakovanje verig (chain-hopping) in uporaba kriptovalut, osredotočenih na zasebnost, preiskovalcem povzročajo velike ovire. Mešalne storitve, znane tudi kot »tumblers«, uporabnikom omogočajo, da zabrišejo izvor svojih sredstev tako, da jih združijo in nato ponovno razdelijo. Preskakovanje verig (chain-hopping) vključuje hitro pretvarjanje kriptovalut med različnimi platformami, kar otežuje sledenje gibanju sredstev. Poleg tega kriptovalute za zasebnost, kot sta Monero in Zcash, ponujajo izboljšane funkcije anonimnosti, kar dodatno otežuje prizadevanja organov pregona.

Za soočanje s temi izzivi se finančni preiskovalci vse pogosteje opirajo na sodelovanje z digitalno-forenzičnimi strokovnjaki. Digitalna forenzika preiskovalcem omogoča pridobivanje in analizo elektronskih dokazov, kot so šifrirane komunikacije, IP-naslovi in metapodatki transakcij. Ta interdisciplinarni pristop je ključen za razkrivanje skritih finančnih omrežij in sledenje nezakonitim finančnim tokovom prek meja. Glede na čezmejno naravo finančnih kaznivih dejanj je sodelovanje med finančnimi institucijami, nadzornimi organi in mednarodnimi organizacijami bistveno za učinkovite finančne preiskave. »Inovativni načini premikanja denarja v kombinaciji z vse večjim zavedanjem strokovnjakov za preprečevanje finančnega kriminala, da trgovci z ljudmi preskakujejo od

institucije do institucije, od banke do banke, so jih spodbudili k sodelovanju.« (OVSE, 2019, str. 43).

## 9.5.6 Tehnološki napredek in trendi

Nedavni tehnološki razvoj je pomembno vplival na finančni kriminal, saj oblikuje nove metode nezakonitih dejavnosti, hkrati pa zagotavlja izboljšana orodja za finančne preiskave. Vzpon kriptovalut in tehnologije veriženja blokov (blockchain) je na primer omogočil različne oblike finančnega kriminala, vključno s pranjem denarja, goljufijami in celo trgovino z ljudmi. Povečana uporaba digitalnih sredstev storilcem omogoča, da sredstva prenašajo prek meja z večjo stopnjo anonimnosti ter se izognejo tradicionalnim finančnim institucijam in regulatornim nadzorom. Čeprav je Bitcoin še vedno najbolj znana kriptovaluta, se vse bolj opaža premik k alternativam, bolj usmerjenim v zasebnost, kot sta Monero in Zcash, kar dodatno otežuje prizadevanja organov pregona.

Eden glavnih trendov je uporaba tehnik prikrivanja, posebej zasnovanih za digitalna sredstva. Storilci se vse pogosteje zanašajo na orodja, kot so mešalniki (mixers), »tumblers« in denarnice, usmerjene v zasebnost, da zabrišejo sledi transakcij in se izognejo odkrivanju. Te metode organom otežujejo sledenje nezakonitim finančnim tokovom, zlasti v primerih, povezanih s trgovino z ljudmi, kjer storilci uporabljajo digitalne valute za prejemanje plačil in pranje protipravno pridobljenih sredstev. Decentralizirana in psevdonimna narava transakcij na osnovi blockchaina je ustvarila okolje, v katerem lahko finančni kriminal uspeva, če ga ne omejujejo napredne preiskovalne tehnike.

Hkrati postajajo storilci finančnih kaznivih dejanj vse bolj samooskrbni in se odmikajo od odvisnosti od zunanjih financerjev ali posrednikov. Ta trend je viden v porastu kibernetsko podprtih goljufij, napadov z izsiljevalsko programsko opremo (ransomware) in spletnih prevar, ki ustvarjajo sredstva za mreže organiziranega kriminala, vključno s tistimi, ki se ukvarjajo s trgovino z ljudmi. Vse pogostejša uporaba goljufivih spletnih tržnic, lažnih kampanj zbiranja sredstev in zavajajočih platform e-trgovine je dodatno razširila priložnosti za finančni kriminal.

Kljub tem izzivom tehnološki napredek prinaša tudi nova orodja za boj proti finančnemu kriminalu. Analitika veriženja blokov (blockchain analytics) in umetna inteligenca (UI) imata vse pomembnejšo vlogo pri finančnih preiskavah, saj organom pomagata slediti nezakonitim transakcijam in prepoznati sumljive vzorce. Sistemi za spremljanje transakcij, podprti z UI, lahko v realnem času analizirajo ogromne količine podatkov ter označijo anomalije, ki lahko kažejo na pranje denarja ali aktivnosti, povezane s trgovino z ljudmi. Poleg tega forenzična orodja za blockchain preiskovalcem omogočajo sledenje premikom kriptovalut in razkrivanje prikritih povezav med kriminalnimi subjekti.

## 9.5.7 Priporočila

Trden pravni okvir za pregon finančnih kaznivih dejanj je nujen za zagotavljanje učinkovitih finančnih preiskav. Mednarodni standardi, na primer priporočila, ki jih je določila Skupina za finančno ukrepanje (FATF), zagotavljajo podlago za ukrepe AML/CFT. Ti predpisi od organov pregona zahtevajo izvajanje finančnih preiskav, omogočanje čezmejnega sodelovanja ter izvajanje postopkov za odvzem premoženja.

Priporočilo FATF 30 na primer poudarja pomen določitve pristojnih organov, ki imajo pooblastila za preiskovanje kaznivih dejanj pranja denarja in financiranja terorizma.

Zaradi vojne v Ukrajini se razseljene osebe soočajo s povečanim tveganjem za trgovino z ljudmi. Kot odziv na to povečano ranljivost so organizacije, kot je Organizacija za varnost in sodelovanje v Evropi (OVSE), razvile ciljno usmerjene vire za podporo prvim posredovalcem. OVSE na primer ponuja »Compendium of Anti-Trafficking Training Courses for First Line Responders«, ki vključuje specializirana usposabljanja o različnih vidikih prizadevanj za preprečevanje trgovine z ljudmi. Med njimi so tudi posebni tečaji, osredotočeni na finančne preiskave, ki strokovnjakom zagotavljajo potrebna znanja in orodja za prepoznavanje in zajezitev nezakonitih finančnih tokov, povezanih s trgovino z ljudmi. Povezava do pregleda tečajev: https://www.osce.org/cthb/562572.

## 9.6 Predlagane aktivnosti

*Tabela 1. Aktivnost za digitalno forenziko in finančne preiskave*

| Ime aktivnosti | Aktivnost – digitalna forenzika |
|---|---|
| **Vrsta aktivnosti** | Skupinsko delo (npr. skupine po 3-6 oseb) |
| **Trajanje** | 15-35 minut |
| **Učni ciji** | Identifikacija ključnih digitalni sledi in naslednjih korakov |
| **Gradiva** | Primeri z opisi ozadja zadeve (npr. natisnjeni izročki)<br>• 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<br>• 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<br>• Lam & Skivankova (2009) on p. 5 at https://www.antislavery.org/wp-content/uploads/2017/01/trafficking_and_compensation2009.pdf<br>• 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'* )<br>• Training chapter 8 |
| **Smernice za izvajalca** | Udeleženci bodo razdeljeni v manjše skupine. Prejeli bodo študijo primera, ki jo bodo prebrali (3–4 min).<br>Nato bodo v skupinah začeli razpravo in poskušali opredeliti, kateri digitalni dokazi bi bili najprimernejši za uspešno digitalno forenzično obravnavo. Poleg tega bodo razpravljali, kateri akterji bi bili vključeni in na kateri točki preiskovalnega postopka (10–15 min)<br>• Kateri digitalni dokazi so relevantni? Kateri digitalni dokazi so najbolj uporabni in zakaj? |

| | |
|---|---|
| | • Kako lahko forenzični strokovnjaki pridobijo in analizirajo te digitalne sledi?<br>• Kako lahko to pomaga pri identifikaciji žrtev, storilcev in vzorcev?<br>• Kateri vzorci ali opozorilni znaki (»red flags«) nakazujejo trgovino z ljudmi?<br>• Katere naslednje korake naj preiskovalci izvedejo?<br>• Kako se lahko ti dokazi uporabijo za podporo žrtvam?<br>Nato bo vsaka skupina predstavila svoje ugotovitve (5–10 min) |
| **Razprava** | Izvajalec vodi razpravo po predstavitvi vsake od skupin. |
| **Nasveti za izvajalca** | Če imate na voljo več časa, lahko uporabite različne študije primerov. Vsaka skupina na kratko predstavi svoj primer in nato rezultate razprave (namesto da bi vse skupine obravnavale isti primer). |
| **Gradiva** | Npr. študije primerov, ki jih natisnete in razdelite udeležencem, po možnosti dopolnjene z gradivom z imitiranimi izseki iz:<br>• WhatsApp klepetov med žrtvijo in storilcem, z npr. sporočili: »Ne skrbi glede papirjev, to bomo uredili mi.«, »Dobili boste brezplačno nastanitev in prevoz.« ali »Dobiva se na avtobusni postaji. Izbriši ta sporočila.«<br>• oglasov z rekrutacijske platforme |

| | |
|---|---|
| | • izpiskov bančnih transakcij<br>• metapodatkov fotografije, ki je bila poslana žrtvi, z geolokacijskimi podatki<br>• … |
| **Spletna izvedba** | Izvedba je možna tudi na daljavo – za skupinsko nalogo oblikujte ločene (breakout) sobe. |
| **Ime aktivnosti** | **Aktivnost – finančne preiskave** |
| **Vrsta aktivnosti** | Skupinsko delo (npr. skuine po 3-6 oseb) |
| **Trajanje** | 15-35 minut |
| **Učni cilji** | Ponotranjiti korake finančnih preiskav ter razmisliti o morebitnih izzivih, ki se pojavljajo na področju trgovine z ljudmi. |
| **Gradiva** | Npr. študije primera, ki jo natisnete in razdelite udeležencem, po potrebi dopolnjeno z gradivom z imitiranimi izseki:<br>• Bančni transakcijski zapisi in bančni izpiski (lahko tudi zgolj tabela s stolpci: datum, opis, breme (EUR), dobro (EUR) in stanje (EUR), ki prikazuje, kdaj je nekdo izvedel transakcijo in komu/podjetju je bila namenjena). |

| | |
|---|---|
| | • Plačilne liste / evidence izplačil plač.<br>• Računi (fakture)<br>• … |
| **Usmeritve za izvajalca** | Udeleženci bodo razdeljeni v manjše skupine. Prejeli bodo študijo primera, ki jo bodo prebrali (3–4 min).<br>Nato bodo v skupinah začeli razpravo in poskušali opredeliti korake finančne preiskave (npr. tako, da gredo skozi posamezne korake, ki so jih spoznali prej). Poleg tega bodo razpravljali, kateri akterji bi bili vključeni in na kateri točki preiskovalnega postopka (10–15 min).<br>• Katere tehnike finančne preiskave je treba uporabiti?<br>• Kako lahko organi pregona pri tem sodelujejo s FIU?<br>• Katera pravna orodja je treba uporabiti?<br>• Katere izzive je mogoče prepoznati?<br>Nato bo vsaka skupina predstavila svoje ugotovitve |
| **Razprava** | Izvajalec vodi razpravo po predstavitvi vsake od skupin. |
| **Nasveti za izvajalca** | Če imate na voljo več časa, lahko uporabite različne študije primerov. Vsaka skupina nato na kratko predstavi svoj primer in rezultate razprave (namesto da bi vse skupine obravnavale isti primer). |

| | |
|---|---|
| **Gradiva** | *Študije primera, ki naj jih prejmejo udeleženci:*<br>• 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<br>• 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 |
| **Spletna izvedba** | Izvedba je možna tudi na daljavo – za skupinsko nalogo oblikujte ločene (breakout) sobe. |

## 9.7 Viri

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


**www.eradicating2project.eu**

Co-funded by
the European Union