Rozdział 9 Kryminalistyka cyfrowa i śledztwa finansowe

Jednostka odpowiedzialna:

BayHfoD

Co-funded by
the European Union

Rozdział 9. Kryminalistyka cyfrowa i śledztwa finansowe

9.1 Wstęp

W dzisiejszym cyfrowym świecie granice między światem wirtualnym a rzeczywistym często się zacierają, co dotyczy również mrocznych machinacji handlu ludźmi w celu wyzysku pracowników (w skrócie: wyzysku pracowników lub handlu ludźmi). Rozdział szkoleniowy „Kryminalistyka cyfrowa i śledztwa finansowe" podkreśla kluczową rolę tych dwóch dyscyplin w wykrywaniu i zwalczaniu wyzysku pracowników. Kryminalistyka cyfrowa koncentruje się na analizie danych elektronicznych w celu gromadzenia cyfrowych dowodów działalności przestępczej związanej z wyzyskiem pracowników, podczas gdy śledztwa finansowe mają na celu śledzenie przepływów pieniężnych i ujawnianie sieci finansowych stojących za tymi przestępstwami. Łącząc te dwa podejścia, śledczy mogą nie tylko zidentyfikować sprawców, ale także odkryć często złożone powiązania między śladami cyfrowymi a transakcjami finansowymi, które umożliwiają wyzysk pracowników. W tym kontekście przedstawiono procedury, najlepsze praktyki, metody i możliwe narzędzia, które umożliwiają specjalistom wykorzystanie dynamicznych interakcji między komunikacją cyfrową a przepływami pieniężnymi, aby pomóc ofiarom handlu ludźmi i podjąć kroki prawne przeciwko sprawcom.

Rozdział 9 rozpoczyna się od wyznaczenia celów edukacyjnych uczestnika szkolenia (Sekcja 2). Są one wymienione osobno dla „informatyki śledczej" i „śledztw finansowych". Następnie następują definicje najważniejszych terminów tego rozdziału (Sekcja 3). Sekcja 4, stanowiąca rdzeń rozdziału 9 zawiera teoretyczne i informacyjne tło

omawianych tematów. Następnie znajduje się ćwiczenie praktyczne, które umożliwia uczestnikowi pracę z wcześniej zdobytymi informacjami teoretycznymi i ich głębsze przetworzenie (Sekcja 5). Rozdział kończy się listą źródeł (Sekcja 6).

9.2 Cele edukacyjne

Rozdział 9 wyposaża uczestników w niezbędną wiedzę z zakresu informatyki śledczej i śledztw finansowych związanych z handlem ludźmi i wyzyskiem w pracy. Po ukończeniu tego rozdziału uczestnik będzie:

Kryminalistyka cyfrowa

- rozumieć zasady informatyki śledczej, w tym gromadzenia, przechowywania i analizy danych, przy jednoczesnym zapewnieniu integralności łańcucha dostaw
- wiedzieć, jak tworzyć kopie zapasowe do celów kryminalistycznych (kopie obrazowe i logiczne)
- wiedzieć, gdzie szukać śladów cyfrowych i dowodów pozostawionych przez handlarzy ludźmi oraz co można wywnioskować z różnych źródeł dowodów cyfrowych
- rozumieć ramy prawne dotyczące dowodów cyfrowych i umieć zapewnić zgodność z wymogami proceduralnymi

Śledztwa finansowe

- identyfikować podejrzane działania finansowe, które mogą wskazywać na handel ludźmi
- stosować metodologię krok po kroku do przeprowadzania dochodzeń finansowych związanych z handlem ludźmi

- rozumieć ekonomiczne czynniki handlu ludźmi
- świadomy wyzwań związanych z dochodzeniami finansowymi, w tym z wykorzystaniem kryptowalut, kont offshore i technik zaciemniania cyfrowego
- rozumieć rolę partnerstwa publiczno-prywatnego (PPP) w dochodzeniach finansowych i współpracy międzynarodowej w zwalczaniu handlu ludźmi

9.3 Definicje

Poniżej pokrótce omówimy najważniejsze słowa kluczowe dla obu tematów.

9.3.1 Słowa kluczowe związane z informatyką śledczą

Kryminalistyka cyfrowa

Kryminalistyka cyfrowa obejmuje identyfikację, przechowywanie i badanie dowodów cyfrowych w celu wsparcia śledztw kryminalnych. Obejmuje metody pozyskiwania, analizy i dokumentowania danych w celu śledzenia cyfrowych śladów działalności przestępczej.

Kopia zapasowa danych kryminalistycznych

Tworzenie dokładnych kopii cyfrowych nośników danych z zachowaniem integralności i identyfikowalności danych (Chain of Custody). Obejmuje to fizyczne kopie zapasowe obrazów (RAW, E01) i logiczne kopie zapasowe (L01, AD1).

Łańcuch dostaw

Ciągła, chronologiczna dokumentacja postępowania z dowodami cyfrowymi w celu zapewnienia ich autentyczności i integralności w postępowaniu sądowym.

Antykryminalistyka

Środki podejmowane przez użytkownika w celu utrudnienia oceny śladów cyfrowych lub wręcz jej uniemożliwienia: Szyfrowanie (FDE, kontener, itp.); przeglądanie TOR/prywatne, wirtualizacja → usuwanie maszyny wirtualnej (VM); programy do czyszczenia, zmiany znacznika czasu itp.; ukrywanie danych, np. steganografia; wielokrotne pakowanie.

eDiscovery

Celowe wykorzystanie informatyki śledczej do analizy dużych wolumenów danych w celu wydobycia istotnych informacji na potrzeby śledztw lub postępowań sądowych. Innymi słowy, eDiscovery (elektroniczne ujawnianie) to analiza danych w konkretnych przypadkach (np. w przypadku przestępczości zorganizowanej, gospodarczej, przestępstw przeciwko bezpieczeństwu państwa). Do przeprowadzenia eDiscovery wymagana jest konkretna wiedza na temat przestępstw i konkretnej sprawy. Ponadto, ze względu na stały wzrost danych, raporty kryminalistyczne wymagają **fragmentów danych**. W ułatwieniu eDiscovery może pomóc Model Referencyjny Elektronicznego Odkrycia (EDRM), czyli ramy obejmujące standardy ujawniania i odzyskiwania danych cyfrowych, np.:

- Podstawy sprzętu komputerowego
- Podstawy informatyki śledczej
- Struktura nośników danych i systemów plików
- Krótkie wprowadzenie do narzędzi kryminalistycznych
- Podstawowe czynności kryminalistyczne
- Struktura i funkcjonalność systemu operacyjnego Windows

- Artefakty kryminalistyczne z systemów Windows

Nośniki rozruchowe do celów kryminalistycznych

Specjalistyczne systemy operacyjne (np. systemy oparte na systemie Linux lub Windows) służące do uruchamiania urządzeń cyfrowych i przeprowadzania analiz kryminalistycznych bez zmiany oryginalnych danych.

Nadmiarowa macierz niezależnych dysków (RAID)

System łączący wiele dysków twardych w celu zwiększenia bezpieczeństwa i wydajności danych, wymagający specjalistycznych technik kryminalistycznych do pozyskiwania danych.

9.3.2 Kluczowe słowa związane ze śledztwami finansowymi

Śledztwa finansowe

Badanie transakcji finansowych w celu wykrycia nielegalnych działań, takich jak pranie pieniędzy, finansowanie terroryzmu i handel ludźmi oraz identyfikacji sprawców.

Pranie pieniędzy (ML)

Proces maskowania nielegalnego pochodzenia środków poprzez serię transakcji finansowych, które mają nadawać im pozory legalności. (Odwrotność: Przeciwdziałanie praniu pieniędzy)

Poznaj swojego klienta (KYC)

Wymagania regulacyjne nakładające na instytucje finansowe obowiązek weryfikacji tożsamości i historii finansowej swoich klientów w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu.

Raporty o podejrzanych transakcjach (STR)

Raporty, które instytucje finansowe muszą składać, gdy transakcja zostanie uznana za potencjalnie podejrzaną lub powiązaną z praniem pieniędzy lub finansowaniem terroryzmu.

Analiza łańcucha bloków

Badanie transakcji kryptowalutowych w celu wykrywania nielegalnych działań, takich jak pranie pieniędzy, oszustwa lub finansowanie terroryzmu, a także śledzenia sieci przestępców.

Kryptowaluty i techniki zaciemniania

Waluty cyfrowe (np. Bitcoin, Monero) i metody takie jak miksery, wirówki czy przeskakiwanie między łańcuchami, wykorzystywane do ukrywania transakcji finansowych.

9.4 Część teoretyczna / informacyjna

9.4.1 Kryminalistyka cyfrowa

Niniejsza sekcja zawiera opis informatyki śledczej w części 9.6.2: czym jest, jak można ją kategoryzować i jak wygląda jej typowy przebieg. Ponadto, znajdują się w niej podstawowe zasady, które powinien rozważyć naukowiec lub praktyk zajmujący się informatyką śledczą. Następnie, w części 9.6.2 omówione zostały podstawowe informacje na temat kopii danych zapasowych, ponieważ budują one fundament solidnego i skutecznego procesu informatyki śledczej. Jednak dalsze wprowadzenie techniczne do informatyki śledczej (poprzez pierwszy krok tworzenia kopii zapasowej) byłoby w tym momencie zbyt daleko idące – zwłaszcza że metody analizy są zbyt różnorodne, aby je tutaj omówić. W związku z tym, nie jest celowe omawianie dalszych

kroków, zwłaszcza że mamy do czynienia z kontekstem handlu ludźmi i wyzysku pracowników. W związku z tym, w części 4.1.3 omówiona jest informatyka śledcza w kontekście handlu ludźmi.

9.4.2 Zarys ogólny

Kryminalistyka cyfrowa to zastosowanie metod naukowych do analizy i ścigania przestępstw. Zajmuje się w szczególności takimi zagadnieniami, jak:

- Gdzie powstają ślady cyfrowe?
- W jaki sposób można rozpoznawać i oceniać ślady cyfrowe?
- W jaki sposób można zabezpieczyć i wykorzystać ślady cyfrowe?

Nawet jeśli informatyka śledcza została już zdefiniowana w rozdziale 3, warto omówić ją bardziej szczegółowo. Informatyka śledcza obejmuje (1) poszukiwanie, identyfikację, (2) opis i (3) badanie dowodów cyfrowych, w tym ocenę ich wiarygodności, ważności i znaczenia dla konkretnej sprawy. Ostatnim krokiem, (4) jest również raportowanie tych dowodów (Maras, 2014). Obejmuje ona metody pozyskiwania, analizy i dokumentowania danych w celu śledzenia cyfrowych śladów działań przestępczych, czyli śladów na urządzeniach cyfrowych, które mogą i muszą być analizowane na potrzeby postępowania karnego.

Zazwyczaj w organach ścigania istnieją wyspecjalizowane jednostki zajmujące się kryminalistyką cyfrową, dlatego jednostki THB współpracują głównie z jednostkami kryminalistyki cyfrowej i zazwyczaj nie zajmują się samodzielnie kwestiami kryminalistyki cyfrowej. Dlatego najlepiej jest nawiązać i dbać o współpracę z tą jednostką. Ponadto wskazane jest zapoznanie się z różnymi stanowiskami

zawodowymi w agencji, np. czy jest tam urzędnik policyjny odpowiedzialny za IT? Urzędnik ds. cyberprzestępczości? Służba techniczna ds. dochodzeń kryminalnych? Specjalista ds. kryminalistyki cyfrowej? Kto jest za co odpowiedzialny i kiedy mogę się z kim skontaktować?

Kryminalistyka cyfrowa obejmuje identyfikację, zabezpieczenie i badanie dowodów cyfrowych, a także (1) uwzględnianie okoliczności prawnych i warunków ramowych w celu wykorzystania ich w sądzie oraz (2) zachowanie i udokumentowanie łańcucha dostaw oraz integralności danych. Kluczem do kryminalistyki cyfrowej jest zatem to, aby każdy wysiłek i każdy pojedynczy krok były odporne na zniekształcenie i nadawały się
do wykorzystania w dokumentacji sądowej.

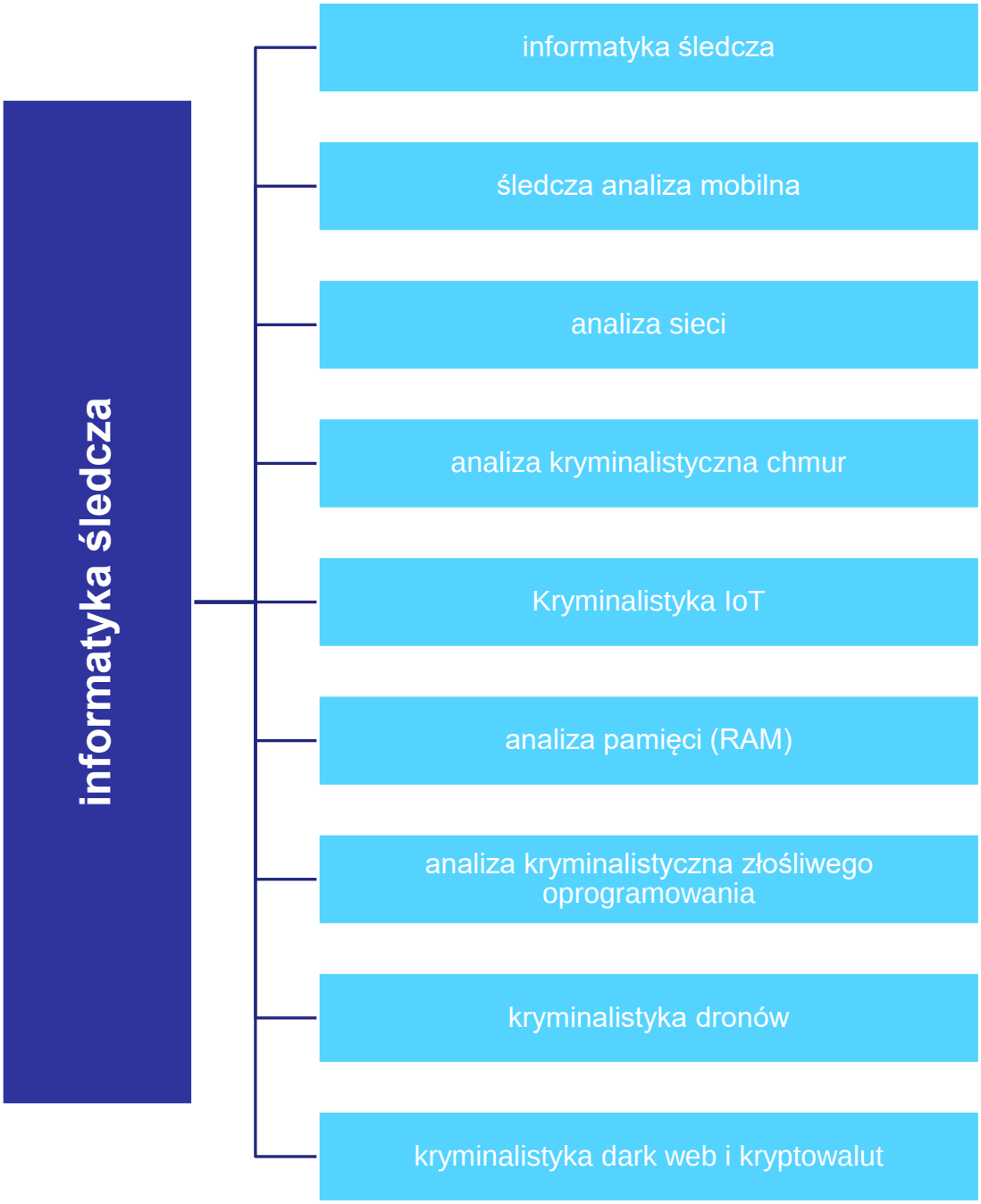
Do typowych zadań naukowców zajmujących się informatyką śledczą należą: tworzenie kopii zapasowych danych z komputerów, nośników danych, urządzeń mobilnych i magazynów internetowych; przygotowywanie i ocena dowodów komputerowych; doradztwo i wsparcie podczas przeszukań.

Ponadto, informatykę śledczą można podzielić i zaklasyfikować do różnych dziedzin. Rysunek 11 przedstawia przegląd możliwych gałęzi informatyki śledczej. Informatyka śledcza koncentruje się na odzyskiwaniu, analizowaniu i zachowywaniu dowodów cyfrowych z komputerów, w tym dysków twardych, systemów plików, systemów operacyjnych i danych aplikacji. Kluczowe techniki to obrazowanie dysków, odzyskiwanie plików i analiza rejestru (patrz np. Casey, 2011). Wyodrębniana czasem informatyka śledcza baz danych zajmuje się ich badaniem (w tym baz danych SQL i NoSQL) oraz badaniem ich metadanych, a obejmuje np. znakowanie czasu bazy danych i analizę na żywo (patrz np. Dubey, Bhatt i Negi, 2023) w celu wykrycia manipulacji

danymi lub nieautoryzowanego dostępu. Jednak informatyka śledcza baz danych może również zostać zaliczona do poddziedziny informatyki śledczej, ponieważ bazy danych są przechowywane głównie w tradycyjnych systemach komputerowych, takich jak serwery. Kryminalistyka mobilna, zwana również kryminalistyką urządzeń mobilnych, zajmuje się ekstrakcją i analizą danych przechowywanych na urządzeniach mobilnych, takich jak smartfony, tablety i systemy GPS (Dubey, Bhatt i Negi, 2023). Kryminalistyka sieciowa obejmuje analizę ruchu sieciowego w celu uzyskania informacji, wykrywania włamań

i zdobywania dowodów sądowych. W poddziedzinie kryminalistyki zapór sieciowych, wszystkie logi zapór sieciowych są badane w celu znalezienia cennych dowodów. Kryminalistyka chmurowa bada dowody przechowywane w środowiskach chmurowych, rozwiązując problemy związane z przechowywaniem danych w wielu jurysdykcjach, ograniczeniami dostępu i współpracą dostawców, dlatego wymaga specjalistycznych rozwiązań prawnych i technicznych. Kryminalistyka IoT bada cyfrowe ślady z urządzeń Internetu Rzeczy (IoT), takich jak inteligentne urządzenia domowe, urządzenia noszone, czujniki przemysłowe i systemy motoryzacyjne. Obejmuje połączenie analizy systemów wbudowanych, kryminalistyki sieciowej i tradycyjnej kryminalistyki urządzeń. Kryminalistyka pamięci (RAM) koncentruje się na ekstrakcji i analizie pamięci ulotnej (RAM) w celu wykrycia uruchomionych procesów, kluczy szyfrujących, złośliwego oprogramowania i aktywności systemu. Analiza kryminalistyczna złośliwego oprogramowania (malware) polega na analizie złośliwego oprogramowania (malware) w celu zrozumienia jego zachowania, identyfikacji jego pochodzenia i ograniczenia jego wpływu (np. poprzez statyczną i dynamiczną analizę złośliwego oprogramowania, sandboxing, inżynierię rezerw). Analiza kryminalistyczna dronów zajmuje się ekstrakcją danych z bezzałogowych statków powietrznych (UAV), w tym dzienników lotów, pamięci pokładowej, śledzenia GPS i systemów komunikacyjnych. Analiza kryminalistyczna dark webu i kryptowalut koncentruje się na nielegalnej działalności w dark webie, w tym handlu

ludźmi, handlu narkotykami i cyberprzestępczości. Techniki analizy kryminalistycznej kryptowalut pomagają śledzić transakcje w bitcoinach lub innych walutach cyfrowych w celu identyfikacji przestępców.



Rysunek 1Przykładowe gałęzie informatyki śledczej

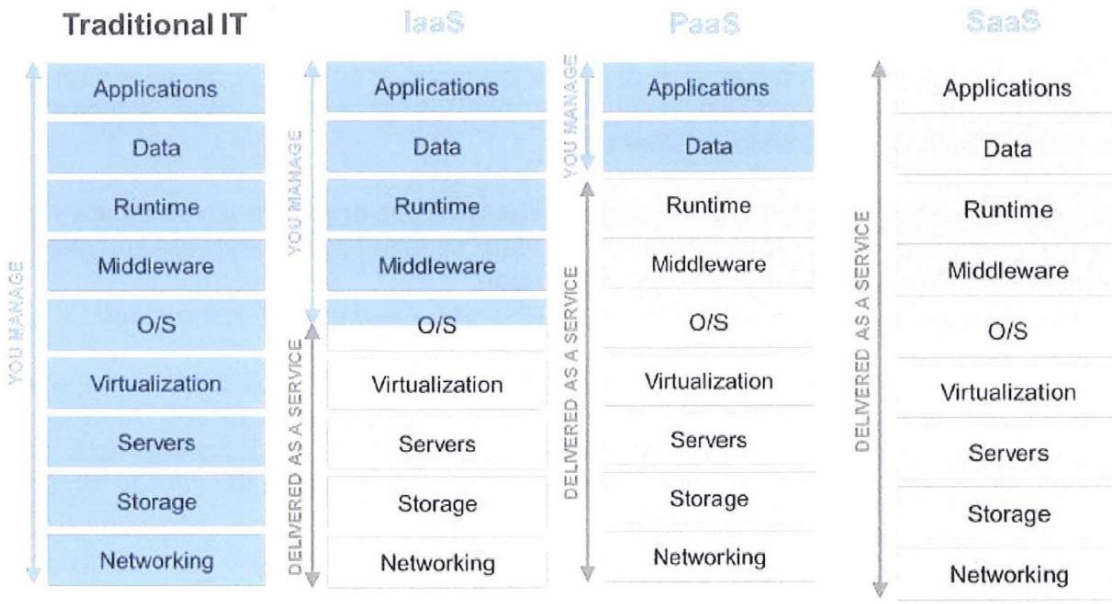
Ponadto, połączenie różnych gałęzi informatyki śledczej ze środowiskiem technologii informatycznych ma kluczowe znaczenie, ponieważ rodzaj infrastruktury decyduje o tym, gdzie przechowywane są dowody cyfrowe, w jaki sposób można uzyskać do nich dostęp i z jakimi wyzwaniami mierzą się śledczy:

„Klasyczna" analiza kryminalistyczna danych a analiza kryminalistyczna danych online

- Tradycyjna →firma IT zarządza całą swoją infrastrukturą IT lokalnie, a serwery, sieci, pamięć masowa, systemy operacyjne i oprogramowanie są fizycznie obsługiwane w obiektach firmy. Obejmuje to klasyczną informatykę śledczą, informatykę śledczą sieci i informatykę śledczą baz danych, stosowaną do maszyn fizycznych, serwerów lokalnych i sieci wewnętrznych. Typowymi źródłami dowodów są dyski twarde (HDD, SSD), lokalne bazy danych i logi systemowe. Wymaga to fizycznego dostępu, ale pełna kontrola nad sprzętem może uprościć obrazowanie i analizę śledczą.
- (IaaS →); IaaS przez Internet zapewnia podstawowe zasoby IT, takie jak serwery wirtualne i pamięć masowa. Firmy wynajmują tę infrastrukturę od dostawcy chmury. Odpowiednimi gałęziami informatyki śledczej są informatyka śledcza chmury i sieci. Głównymi źródłami danych są maszyny wirtualne, pamięci masowe w chmurze oraz logi ruchu sieciowego.
- PaaS →jako usługa (PaaS) oferuje platformę, na której programiści mogą tworzyć, testować i wdrażać aplikacje. Infrastruktura bazowa i oprogramowanie pośredniczące są zarządzane przez dostawcę. Dominującymi gałęziami są analizy śledcze baz danych i chmury obliczeniowej. Źródłami danych są głównie logi aplikacji, migawki baz danych i logi API.
- Oprogramowanie jako usługa (SaaS) zapewnia w pełni funkcjonalne oprogramowanie przez Internet. Użytkownicy uzyskują dostęp do oprogramowania za pośrednictwem

przeglądarek internetowych lub aplikacji, bez konieczności martwienia się o instalację, zarządzanie czy konserwację. Instalacja nie jest wymagana. → Tak działa na przykład Microsoft 365. Do głównych gałęzi kryminalistyki należą analiza danych w chmurze i sieci. Ważnymi źródłami danych są dzienniki audytu, historia wersji
i rejestry aktywności użytkowników.

Rysunek 11 przedstawia przegląd różnych środowisk technologii informacyjnej.



Rysunek 2Różne środowiska technologii informatycznych[1]

Nawet jeśli mamy do czynienia z odrębnymi gałęziami i należy uwzględnić rodzaj infrastruktury, to struktura procesu kryminalistyki cyfrowej zasadniczo pozostaje taka

[1]Źródło: Bawarska Policja. Dystrybucja bez zezwolenia jest zabroniona.

sama. Można ją w skrócie podsumować jako (1) pozyskanie dowodów cyfrowych, (2) ich analizę, w tym interpretację, oraz (3) ich prezentację (np. śledczym prowadzącym sprawę, sądowi) zgodnie z Dubey, Bhatt i Negi (2023). Innym ważnym modelem procesu jest multidyscyplinarny model procesu cyfrowego dochodzenia kryminalistycznego autorstwa Lutui (2016), przedstawiony na rysunku 12 .

Rysunek 3Przegląd procesu informatyki śledczej[2]

[2]Źródło: Oryginalne przedstawienie Lutui (2016), s. 601

Co więcej, poniższe wskazówki mogą pomóc osobom zajmującym się na co dzień przedmiotową tematyką w ustrukturyzowaniu procesu analizy kryminalistycznej danych cyfrowych, który zawiera niektóre elementy bardziej praktyczne niż dwa zaprezentowane wcześniej modele:

Dziewięć praktycznych elementów procesu analizy cyfrowej

1. **Przyjęcie**: otrzymanie urządzenia jako dowodu, otrzymanie wniosku o przeprowadzenie badania
2. **Identyfikacja**: identyfikacja specyfikacji i możliwości urządzenia, identyfikacja celów badania, identyfikacja podstawy prawnej badania
3. **Przygotowanie**: przygotowanie metod i narzędzi, które będą używane, przygotowanie nośników i stanowiska do analizy kryminalistycznej do egzaminu
4. **Izolacja**: ochrona dowodów, zapobieganie zdalnemu zniszczeniu danych, izolacja od sieci, Bluetooth, Wi-Fi
5. **Przetwarzanie**: przeprowadzanie badań kryminalistycznych, wykonywanie analizy kryminalistycznej, skanowanie w poszukiwaniu złośliwego oprogramowania
6. **Weryfikacja**: sprawdzenie poprawności przejęcia danych i ustaleń kryminalistycznych
7. **Dokumentowanie/Raportowanie**: sporządzenie notatki dotyczącej ustaleń i procesu, sporządzenie raportu kryminalistycznego
8. **Prezentacja**: przygotowanie eksponatów, zaprezentowanie swoich odkryć
9. **Archiwizacja**: przechowanie kopii danych w bezpiecznym miejscu, w popularnych formatach na potrzeby przyszłych zastosowań

Dla naukowca/praktyka zajmującego się informatyką śledczą ważne jest ponadto, aby pamiętać o całej procedurze dochodzenia kryminalistycznego:

Procedura dochodzenia kryminalistycznego

1. Zabezpieczone dowody przekazać specjaliście ds. informatyki śledczej
2. Przechowywać (zapisywać) dane i nośniki danych (książki, naklejki, ...)
3. Tworzyć kopie zapasowe danych: kopie zapasowe obrazów fizycznych, kopie zapasowe danych logicznych
4. Bezpiecznie przechowywać oryginalne dowody
5. Dokumentować łańcuch dostaw

Ponadto zawsze należy stosować się do kilku podstawowych zasad informatyki śledczej:

Podstawowe zasady informatyki śledczej

- Istnieją różne rodzaje tworzenia kopii zapasowych danych:
    - kopie dowodów komputerowych w formacie jeden do jednego
    - kopie zapasowe obrazów fizycznych (E01 [format pliku obrazu encase] lub RAW)
    - logiczne kopie zapasowe danych (L01, AD1 lub CTR)
- Przeprowadzenie analizy kopii zapasowych lub kopii danych (analiza post mortem)
- Nie wprowadzanie zmian do zabezpieczonych danych

- Dokładna dokumentacja tego, kto, co i kiedy zrobił, wraz z kopiami zapasowymi danych, zapewni utworzenie pełnego łańcucha dowodowego. To ostatnie wymaga (1) chronologicznej dokumentacji oraz (2) identyfikowalności w celu zabezpieczenia transferu, oceny i przekazania dowodów. Opiera się ona na zasadzie stosowania naukowo uznanych metod i sporządzania pełnej dokumentacji przez specjalistę ds. informatyki śledczej.

  Tworzenie kopii dowodów komputerowych w skali jeden do jednego...

  - zapewnia integralność i autentyczność dowodów
  - uwzględnia ochronę zapisu
  - pozwala dokonać weryfikacji

- Nie zmieniaj niczego celowo! Zmiany zachodzą szybko, np. poprzez samo uruchomienie systemu lub zamontowanie dysku twardego.
- **Bardzo ważne:** Uczyń wszystko zawsze i wszędzie możliwym do prześledzenia (dokumentacja!)

Poza tym należy znać aspekty prawne, ponieważ konieczne jest zapewnienie legalności przeszukania i zajęcia. Co więcej, jako technik kryinalistyki, zazwyczaj nie musisz martwić się o zakaz wykorzystania materiałów (= zadanie funkcjonariusza prowadzącego dochodzenie, a ostatecznie prokuratora). Wreszcie, co nie mniej ważne, w przypadku znalezisk przypadkowych zaleca się konsultację ze śledczymi.

9.4.3 Kopia zapasowa danych

W kryminalistyce cyfrowej tworzenie kopii zapasowych danych stanowi fundamentalny krok w zabezpieczaniu i analizie dowodów cyfrowych. Zapewnienie integralności i dostępności danych kryminalistycznych ma kluczowe znaczenie dla śledztw, postępowań sądowych i reagowania na incydenty cyberbezpieczeństwa. Prawidłowa kopia zapasowa danych kryminalistycznych pozwala śledczym pracować z dokładną, niezmienioną kopią oryginalnych danych, minimalizując ryzyko uszkodzenia lub utraty dowodów.

W tej sekcji omówiono kluczowe aspekty kryminalistycznego tworzenia kopii danych zapasowych, zaczynając od podstawowych zasad (sekcja 9.6.3.1), w tym integralności danych, autentyczności i łańcucha dostaw. Następnie omówiono popularne formaty kopii zapasowych i ich strukturę (sekcja 9.6.3.2), a także mechanizmy ochrony przed zapisem oparte na oprogramowaniu, zapobiegające fałszowaniu danych (sekcja 9.6.3.3). Omówiono również różne rodzaje nośników danych i ich rolę w dochodzeniach kryminalistycznych (sekcja 9.6.3.4) oraz analizę specjalistycznego oprogramowania i sprzętu do tworzenia kopii zapasowych (sekcja 9.6.3.5). Ponadto, sekcja ta obejmuje tworzenie i stosowanie nośników startowych do celów kryminalistycznych (sekcja 9.6.3.6), które ułatwiają pozyskiwanie danych z systemów działających w czasie rzeczywistym i offline. Omówiono również sieciowe metody tworzenia kopii zapasowych, w tym techniki zdalnego pozyskiwania danych (sekcja 9.6.3.7). Na koniec omówiono szczególne zagadnienia związane z obsługą złożonych systemów pamięci masowej, takich jak macierze RAID i urządzenia NAS (sekcja 9.6.3.8), krótko opisując wyzwania i najlepsze praktyki w zakresie ochrony takich struktur danych.

Dzięki zrozumieniu tych koncepcji, specjaliści i praktycy kryminalistyki sądowej mogą zapewnić niezawodne, weryfikowalne i dopuszczane przez sąd kopie zapasowe danych, tworząc podstawę rzetelnego dochodzenia kryminalistycznego.

9.4.3.1Zasady tworzenia kopii zapasowych danych kryminalistycznych

Istnieją istotne zasady, których należy przestrzegać przy tworzeniu kopii zapasowych danych:

- **Tworzenie kopii zapasowych i blokowanie zapisu**:
    - Praca wyłącznie na kopiach dowodowych, a nie na nośnikach oryginalnych
    - Tworzenie kopii kryminalistycznych w postaci obrazów strumieni bitowych lub logicznych kopii zapasowych
    - Zapobieganie zmianom oryginalnych danych lub nośników podczas tworzenia kopii zapasowej, dochodzenia i badania
    - Dostęp tylko do odczytu podczas procesu tworzenia kopii zapasowej (ochrona przed zapisem)
- **Zapewnienie integralności kopii zapasowej**:
    - Zapewnienie, że kopie zapasowe danych będą nadawały się do analizy
    - Nie dokonywanie zmian danych na kopii zapasowej (tworzenie drugiej kopii, jeśli to konieczne)
    - Wykorzystanie wyczyszczonych nośników kopii zapasowych (ryzyko zanieczyszczenia krzyżowego danych)
    - Weryfikacja kopii zapasowych obrazu (porównanie skrótów pomiędzy oryginałem i kopią po procesie tworzenia kopii zapasowej lub kopiowania)

- **Dokumentacja łańcucha dostaw**: Dokładna dokumentacja wszystkich interakcji z kopiami zapasowymi danych (utrzymywanie „łańcucha dostaw")

9.4.3.2 Przegląd i struktura popularnych formatów kopii zapasowych do celów kryminalistycznych

Zakres kopii zapasowych danych w kryminalistyce cyfrowej obejmuje dyski twarde magnetyczne i SSD z komputerów, pojedyncze urządzenia pamięci masowej, takie jak dyski USB lub pamięci flash, oraz nośniki optyczne. Można je zabezpieczyć dwiema podstawowymi metodami: **kopiami zapasowymi obrazu**, które tworzą kompleksowe kopie sektor po sektorze, lub **kopiami zapasowymi logicznymi** , które koncentrują się na określonych plikach i katalogach. Obie metody są obsługiwane przez narzędzia kryminalistyczne, takie jak X-Ways, EnCase, FTK, NUIX Imager i Magnet Acquire.

Kopia zapasowa obrazu to kopia bit po bicie urządzenia pamięci masowej, która obejmuje wszystkie dane, w tym pliki, foldery oraz nieprzydzielone, wolne i zwolnione miejsca w pamięci masowej.

Obraz różni się od klonu, ponieważ kopia zapasowa danych obrazu tworzy skompresowany plik (obraz) dysku, partycji lub systemu. Kopia zapasowa obrazu, która przechowuje dane w jednym dużym pliku, musi zostać przywrócona, zanim będzie mogła być używana. W kryminalistyce cyfrowej obrazy kryminalistyczne są wykonywane na przykład z dysku twardego podejrzanego. Obrazowanie jest zazwyczaj wykorzystywane do analizy post mortem, natomiast **klonowanie** służy do kopiowania systemów lub tworzenia identycznych konfiguracji (np. klonowanie starego dysku twardego na dysk SSD bez ponownej instalacji systemu operacyjnego). Czasami może również służyć celom kryminalistycznym. Sklonowany dysk jest natychmiast gotowy do uruchomienia i użycia. W kryminalistyce cyfrowej można na przykład wykonać dokładną kopię strumienia bitów dysku podejrzanego.

Istnieje kilka powszechnie używanych **formatów obrazów kryminalistycznych** :

- **Format RAW:** Bezpośrednia kopia strumienia bitów nośnika danych. W zależności od oprogramowania do tworzenia kopii zapasowych, tworzone są skróty MD5 całego obrazu lub poszczególnych jego fragmentów.
- **Format eksperta-świadka (EWF) (E01)**: Niezmienny format przeznaczony do celów kryminalistycznych. Nagłówek EVF zawiera metadane, takie jak liczba bloków i rozmiary sektorów. Zawiera cykliczne kontrole nadmiarowe (CRC) do weryfikacji poszczególnych bloków. Struktura segmentowana z nagłówkami, danymi i tabelami sektorów.
- **Format pliku dowodowego EnCase (Ex01):** opracowany przez Guidance/OpenText i oparty na formacie E01 . Bardziej wydajny i wydajny w porównaniu z E01, obsługiwany głównie przez EnCase. I NUIX **.**
- **Advanced Forensic Format (AFF):** Format open source, niezależny od producenta, utrzymywany przez społeczność internetową. Obsługuje warianty AFF4 i AFF4-L. Rzadziej używany w Niemczech. Kompatybilny z narzędziami takimi jak FTK Imager i Magnet Forensics AXIOM.

Badania kryminalistyczne obejmują również **logiczne kopie zapasowe**. Logiczna kopia zapasowa to kopia rzeczywistych danych na urządzeniu pamięci masowej

lub partycji, obejmująca tylko aktualnie obecne pliki i foldery, a nie nieprzypisane obszary lub usunięte dane. Logiczne kopie zapasowe są zazwyczaj tworzone na miejscu lub podczas przeszukiwania firmy oraz w systemach NAS.

9.4.3.3 Ochrona przed zapisem oprogramowania

Ochrona przed zapisem w oprogramowaniu odnosi się do narzędzi, które zapobiegają modyfikacji danych przechowywanych na nośniku danych poprzez wymuszanie dostępu tylko do odczytu. Istnieją różne programy, które zapewniają, że żadne dane nie zostaną przypadkowo zmienione lub usunięte podczas dochodzeń kryminalistycznych.

- **X-Ways forensics:** Chroni całe dyski lub określone partycje. Działa tylko po rozpoznaniu dysku przez system Windows i uzyskaniu do niego dostępu.
- **Diskpart:** Służy do ustawiania lub usuwania ochrony przed zapisem na dyskach lub woluminach. Działa dopiero po rozpoznaniu urządzenia przez system Windows.
- **FastBloc SE:** Rozwiązanie blokujące zapis programowy, umożliwiające wykonywanie analiz obrazowych na kanałach IDE, SATA, SCSI, FireWire i USB bez konieczności stosowania sprzętowych blokad zapisu.
- **Ochrona oparta na rejestrze:** włącza ochronę przed zapisem dla urządzeń pamięci masowej poprzez modyfikację ustawień systemowych w celu ograniczenia dostępu do zapisu.
- **Porty USB:** ochrona przed zapisem poprzez diskpart (niezabezpieczone) lub modyfikacje rejestru: ochrona urządzenia USB.

9.4.3.4 Nośniki danych

Magnetyczne nośniki danych, takie jak dyski twarde, przechowują dane magnetycznie na obracających się talerzach podzielonych na sektory. Sektory te mają

zazwyczaj rozmiar fizyczny 512 bajtów lub 4096 bajtów w nowoczesnych napędach, a dane są odczytywane mechanicznie za pomocą głowicy odczytująco-zapisującej.

Nośniki danych flash, takie jak dyski SSD i dyski USB, przechowują dane elektronicznie w komórkach pamięci zorganizowanych w strony i bloki. W przeciwieństwie do dysków magnetycznych, nie posiadają ruchomych części. Pamięć flash wykorzystuje kontrolery do emulowania tradycyjnej struktury opartej na sektorach, co zapewnia kompatybilność z istniejącymi systemami. Jest odporna na wstrząsy, ma kompaktowe rozmiary, oferuje dużą pojemność i zużywa mniej energii. Ma jednak również pewne wady. Jedną z istotnych wad jest ograniczona żywotność. Istnieją dwa główne rodzaje pamięci flash: NAND i NOR. Pamięć flash NAND jest tańsza i oferuje większą pojemność . Działa podobnie do urządzenia blokowego, takiego jak dysk twardy, i zawiera system plików z możliwością partycjonowania.

Dyski SSD (Solid State Drive) wykorzystują pamięć flash NAND i zostały zaprojektowane z myślą o zastąpieniu tradycyjnych dysków twardych. Zapewniają one znaczną poprawę wydajności, na przykład szybsze odczyty i zapisy danych. Hybrydowe rozwiązanie pamięci masowej, znane jako hybrydowe dyski SSD (SSHD), łączy tradycyjny magnetyczny dysk twardy z dodatkową pamięcią flash. Często używane dane są przechowywane w pamięci flash, co przyspiesza ogólną wydajność systemu poprzez buforowanie danych w celu ich szybszego pobierania.

9.4.3.5 Oprogramowanie i sprzęt do tworzenia kopii zapasowych na potrzeby kryminalistyczne

Kopie zapasowe danych kryminalistycznych wymagają połączenia specjalistycznego **oprogramowania** i narzędzi **sprzętowych** . Do najpopularniejszych narzędzi programowych należą indywidualne programy do tworzenia obrazów, takie jak:

- **FTK Imager:** Wersja przenośna i instalacyjna. Obsługuje podgląd dysków lokalnych, udziałów sieciowych i obrazów. Tworzy obrazy strumieniowe w formatach RAW, E01 i SMART. Umożliwia haszowanie, eksportowanie plików, dzielenie, scalanie obrazów i tworzenie logicznych kopii zapasowych (format AD1). Kompatybilność międzyplatformowa (Windows, Linux, macOS).
- **EnCase Imager:** autorskie narzędzie do obrazowania z zaawansowanymi funkcjami.
- **Magnet Acquire:** proste narzędzie do obrazowania na urządzeniach mobilnych i komputerach stacjonarnych.
- **NUIX Imager:** Bezpieczne obrazowanie dysków fizycznych i środowisk chmurowych. Obsługuje unikalne formaty logiczne (*.nli) z weryfikacją metadanych i hash.

Ponadto kompleksowe pakiety oprogramowania do analizy kryminalistycznej zapewniają szerszy zestaw narzędzi do analizy cyfrowej, takich jak:

- **X-Ways forensics:** Obsługuje obrazowanie dysków fizycznych i logicznych. Oferuje różne tryby obrazowania (pełny, minimalny, oczyszczony). Umożliwia tworzenie kontenerów plików, konwersję formatów i kompresję rozrzedzoną.
- **EnCase forensics:** kompleksowy pakiet do obrazowania i analizy
- **Magnet forensics IEF/AXIOM:** koncentruje się na analizie i obrazowaniu dowodów cyfrowych

Aby zapoznać się ze szczegółowym przeglądem narzędzi do analizy kryminalistycznej danych cyfrowych w kontekście THB, zapoznaj się z sekcją 9.6.4.3. Pozyskiwanie danych kryminalistycznych wymaga również użycia określonych narzędzi sprzętowych:

- **Duplikatory dysków z blokadą zapisu** służą do tworzenia dokładnych, bitowych kopii nośników danych, uniemożliwiając jednocześnie wprowadzanie zmian na nośnikach oryginalnych. Przykładami są Logicube i VOOM Hardcopy. Ponadto przenośne urządzenia kryminalistyczne to rozwiązania przeznaczone do szybkiego obrazowania w terenie i często są używane z laptopami lub dyskami zewnętrznymi.
- **Dodatkowe funkcje i narzędzia** obejmują bezpieczne kopiowanie obrazów, takie jak NUIX Evidence Mover, oraz weryfikację wartości skrótu za pomocą oprogramowania HashMyFiles, HashCalc i MD5.exe. Narzędzia te płynnie integrują się z oprogramowaniem kryminalistycznym, takim jak EnCase i X-Ways, zapewniając integralność plików obrazów E01.

W przypadku wyjmowania dysków z systemów kompaktowych, cenne wskazówki można znaleźć w takich źródłach jak iFixit, samouczkach na YouTube i oficjalnych portalach (np. TeSIT). W przypadku braku fizycznego dostępu do dysków, zaleca się użycie nośnika rozruchowego, aby ułatwić pobieranie danych.

9.4.3.6Tworzenie i używanie nośników rozruchowych do celów kryminalistycznych

Nośniki rozruchowe stanowią podstawowe narzędzie w dochodzeniu cyfrowym, szczególnie gdy nie można usunąć urządzenia pamięci masowej z komputera lub uzyskać do niego bezpośredniego dostępu albo gdy blokada zapisu nie jest dostępna.

Istnieją dwa **główne typy systemów** używanych do rozruchu:

- „Podstawowy system wejścia/wyjścia” (BIOS): Tradycyjny interfejs między sprzętem komputera a systemem operacyjnym. Obsługuje uruchamianie

do czterech systemów operacyjnych na jednym dysku. Aktywuje się natychmiast po włączeniu komputera. Zaprojektowany dla nośników danych opartych na MBR.

- „Extensible Firmware Interface" (EFI): Następca BIOS-u, obsługujący do 128 systemów operacyjnych na jednym dysku. Dostępne warianty: **UEFI** (Unified Extensible Firmware Interface) dla systemów Windows/Linux oraz **EFI** dla systemu macOS. Niezbędny dla dysków z systemem GPT. Służy do uruchamiania systemu operacyjnego na nośnikach danych GPT. Obsługiwany przez wszystkie obecne systemy operacyjne. Oferuje zwiększone bezpieczeństwo i funkcjonalność:
    - Moduł obsługi zgodności (CSM): symuluje BIOS dla sprzętu i systemu operacyjnego; tryb zgodności/tryb starszy
    - Bezpieczny rozruch: zapobiega załadowaniu złośliwego oprogramowania przed uruchomieniem systemu
    - „Zaufany" rozruch: podpisywanie plików jądra/systemu w systemie Windows 10 w celu wykluczenia złośliwego kodu
- Sekwencja rozruchowa
    - BIOS: sprawdza kolejno wskazane dyski pod kątem możliwych do uruchomienia systemów operacyjnych i przenosi proces rozruchu
    - UEFI: Zawiera wbudowanego menedżera rozruchu, który umożliwia bezpośredni wybór napędu.

Nośnik rozruchowy Linux

Nośniki startowe systemu Linux są wyposażone w szeroką gamę bezpłatnych narzędzi kryminalistycznych do zadań takich jak tworzenie kopii zapasowych, analiza

i odzyskiwanie danych. Przykładami takich narzędzi są: **Backup** (Guymager, dcfldd, ddrescue); **Analysis** (Sleuthkit , Autopsy) i **Recovery** (Foremost , TestDisk).

Popularne dystrybucje Linuksa to Knoppix, Helox, CAINE (Computer Aided INvestigative Environment), DeepThought, DEFT¸ Grml i Kali Linux.

Tworzenie nośnika startowego Linux: Systemy Linux są przechowywane w kontenerach Casper sformatowanych w systemie FAT32, a pliki generowane przez użytkownika są przechowywane na nośnikach zewnętrznych. Nośniki startowe można utworzyć za pomocą narzędzi takich jak **YUMI, Rufus** lub **Linux Live USB-Creator**. Urządzenia takie jak **Zalman** lub **IODD** mogą służyć jako urządzenia do tworzenia kopii zapasowych/rozruchowych.

Tworzenie kopii zapasowej obrazu: Zazwyczaj używa **obrazów RAW .** Polecenie „dd" jest zazwyczaj dostępne w każdym systemie Linux. Składnia: dd if=/dev/sdX of=/media/image.dd. Dzielenie dużych obrazów. Monitorowanie postępu za pomocą zaktualizowanych wersji dd lub narzędzi takich jak Pipe Viewer (pv) . Weryfikacja za pomocą algorytmów skrótu (`md5sum` lub podobnych). Scalanie części obrazu po podziale.

Alternatywne programy do tworzenia kopii zapasowych w systemie Linux to Guymager, dcfldd, dc3dd i ddrescue. Logiczna kopia zapasowa z datą jest tworzona za pomocą programu tar (Tape Archiver), który jest teraz zintegrowany z systemem Windows.

Nośnik rozruchowy oparty na systemie Windows

Nośniki rozruchowe systemu Windows zapewniają alternatywną lub uzupełniającą funkcjonalność w stosunku do nośników rozruchowych systemu Linux.

- Środowisko preinstalacji systemu Windows (WinPE): Minimalistyczny, autonomiczny system operacyjny (OS) niezależny od systemu zainstalowanego

na urządzeniu. Umożliwia analizę i obrazowanie systemu bez wpływu na dane zainstalowanego systemu operacyjnego.

- Środowisko Windows Forensic Environment (WinFE): Dostosowane środowisko WinPE skonfigurowane specjalnie do celów kryminalistycznych. Zastosowania:
    - Kopie zapasowe danych kryminalistycznych z wykorzystaniem X-Ways Forensics lub FTK Imager
    - Selekcja i podgląd dowodów
    - Omijanie uprawnień administratora w systemach docelowych
- Format obrazu systemu Windows (WIM): Przechowuje podstawowe obrazy systemu Windows (np. Pro, Home, Education). Służy do rozruchu środowiska Windows PE („boot.wim"). Podczas instalacji uruchamiany jest WinPE, a plik „install.wim" zapisywany jest na dysku twardym. Kompatybilny z narzędziami takimi jak `7zip` do inspekcji obrazu. Dostępny również w skompresowanym formacie ESD (Electronic Software Distribution).

Zaawansowane opcje nośnika rozruchowego

- Ventoy: narzędzie programowe do uruchamiania obrazów ISO bezpośrednio z dysku USB. Funkcje obejmują kompatybilność z Secure Boot i obsługę partycji GPT. Tworzy dwie partycje (FAT dla menedżera rozruchu i exFAT dla pamięci masowej ISO).
- Nośnik rozruchowy Macintosh:
    - **Tryb dysku docelowego (TDM):** umożliwia działanie komputerów Mac jako dysków zewnętrznych przez Thunderbolt lub FireWire

- **Tryb odzyskiwania:** zapewnia dostęp do narzędzi takich jak Narzędzie dyskowe i Terminal w celu tworzenia obrazów
- **Deszyfrowanie FileVault:** Wymagane są hasła lub klucze odzyskiwania w celu uzyskania dostępu
- **Zagadnienia dotyczące układu zabezpieczającego T2:** Ogranicza rozruch zewnętrzny i wymaga poświadczeń specyficznych dla urządzenia w celu obrazowania

- Nośniki Multi-Boot: Narzędzia takie jak YUMI tworzą bootowalne nośniki USB z wieloma systemami operacyjnymi (Linux, Windows, macOS). Zapewniają kompatybilność z różnymi systemami (BIOS/UEFI, ochrona integralności systemu macOS).

Specjalne uwagi dotyczące systemu macOS

- **FileVault i układ bezpieczeństwa T2:** szyfrowanie wymaga znanych danych uwierzytelniających. Układ T2 integruje funkcję bezpiecznego rozruchu i zewnętrzne ograniczenia rozruchu.
- **Napędy Fusion:** hybryda HDD i SSD, wymagająca osobnego obrazowania każdego komponentu i rekonstrukcji.

9.4.3.7Kopia zapasowa danych przez sieć

Kopie zapasowe danych w sieci stanowią skuteczną metodę obrazowania i przesyłania danych pomiędzy systemami.

EnCase i LinEn zapewniają solidną infrastrukturę do tworzenia kopii zapasowych w sieci, umożliwiając śledczym bezpieczny dostęp do zdalnych systemów i tworzenie ich obrazów.

- **Proces:**
    - Uruchom komputer docelowy za pomocą dystrybucji Linuksa do analizy kryminalistycznej, np. Deft
    - Na komputerze zapasowym uruchom EnCase Imager.
    - Nawiąż połączenie fizyczne między dwoma komputerami za pomocą kabla krosowego.
    - Przypisz statyczne adresy IP obu systemom: **Windows** : skonfiguruj za pomocą „Centrum sieci i udostępniania” w obszarze „Ustawienia karty”. **Linux** : użyj poleceń systemowych, aby ustawić adres IP.
    - Sprawdź połączenie wykonując test ping.
    - Skopiuj program LinEn na zewnętrzne urządzenie pamięci masowej i zamontuj je w systemie docelowym.
    - Przejdź do lokalizacji LinEn w systemie docelowym i uruchom ją. Wybierz opcję „Serwer” w interfejsie LinEn.
    - Na komputerze zapasowym za pomocą oprogramowania EnCase rozpocznij proces obrazowania za pomocą opcji „Dodaj dowody” i „Podgląd krzyżowy”.
- **Zalety:** Zapobiega automatycznemu dostępowi do zapisu na podłączonych urządzeniach pamięci masowej. Systemy Linux rozpoznają złożone konfiguracje sprzętowe, takie jak kontrolery RAID.

Narzędzia Unix i nośniki rozruchowe oparte na systemie Linux zapewniają elastyczność i kontrolę podczas operacji obrazowania sieci.

- **Proces:**
  - Połącz oba systemy za pomocą kabla krosowego lub standardowego kabla krosowego. W razie potrzeby użyj koncentratora sieciowego lub przełącznika.
  - Przypisz każdemu komputerowi statyczne adresy IP:

    Windows : Konfiguruj za pomocą „Centrum sieci i udostępniania”

    Linux : Ustaw adres IP za pomocą narzędzi takich jak ifconfig (np. ifconfig eth0 192.168.100.1).
  - Przetestuj łączność za pomocą polecenia ping, aby upewnić się, że oba urządzenia się komunikują.

Połączenie **dd i Netcat** umożliwia proste i wydajne przesyłanie danych przez sieć.

- **Proces:**
  - **Przygotuj komputer docelowy :** Rozpocznij nasłuchiwanie danych przychodzących za pomocą Netcat. Przykład: Zapisz dane bezpośrednio do pliku lub przekaż je do dd w celu zapisu.
  - **Przygotuj komputer źródłowy :** Przesyłaj strumieniowo dane z dysku do miejsca docelowego: W systemie Linux: Użyj dd do odczytu danych i przekierowuj je do Netcata. W systemie Windows: Użyj kompatybilnego pliku dd.exe do wykonania podobnych zadań.

- Dodatkowe uwagi **:** Wyłącz tymczasowo zapory sieciowe i oprogramowanie antywirusowe, aby uniknąć zakłóceń. Netcat może generować alerty

bezpieczeństwa, ponieważ często jest klasyfikowany jako „potencjalnie niechciany program".

Korzystanie z **protokołu SSH** gwarantuje bezpieczne przesyłanie danych, zwłaszcza podczas pracy w systemach Linux lub macOS.

- **Proces:**
  - Użyj polecenia dd , aby utworzyć kopię strumienia bitowego dysku źródłowego.
  - Prześlij dane wyjściowe za pomocą połączenia SSH do systemu docelowego, gdzie zostaną zapisane jako obraz do celów kryminalistycznych.
- **Dodatkowe funkcje**
  - **Śledzenie postępu** : Użyj narzędzi takich jak Pipe Viewer (pv), aby monitorować transfer danych w czasie rzeczywistym.
  - **Kompresja :** Przesyłaj strumieniowo dane za pomocą narzędzi kompresujących, takich jak Gzip, aby zmniejszyć wymagania dotyczące przestrzeni dyskowej.

9.4.3.8 Specjalizacje tworzenia kopii zapasowych danych

RAID (Redundant Array of Independent Disks) mają na celu zwiększenie wydajności i niezawodności poprzez dystrybucję danych na wielu dyskach twardych.

- **Rodzaje RIAD-ów:**

- **Sprzętowy RAID :** zarządzany za pomocą dedykowanej karty kontrolera RAID, oferujący solidną wydajność i niezawodność
- **RAID programowy :** kontrolowany przez system operacyjny, zazwyczaj tańszy, ale wymagający zasobów systemowych

- **Poziomy RAID:**
  - **JBOD:** wszystkie dyski twarde są połączone w jedną dużą pamięć masową; sieć pamięci masowej to duży system plików, w którym przechowywane są dane
  - **RAID0:** wszystkie dyski twarde są połączone w jeden duży system pamięci masowej; logika przechowywania danych (rozmiar paska) zapewnia, że dane są przechowywane w blokach na dyskach twardych
  - **RAID10:** Dwa lub więcej dysków twardych jest połączonych w celu utworzenia pojedynczego obszaru pamięci masowej (RAID0); obszar pamięci masowej jest lustrzany (RAID1 Mirroring)
  - **RAID5 lub RAID6:** co najmniej 3 (RAID5) lub co najmniej 4 (RAID6) dyski twarde są połączone w jeden obszar pamięci masowej; informacje o parzystości są rozłożone na dyskach. Jeśli jeden (RAID5) lub dwa (RAID6) dyski twarde ulegną awarii, ich zawartość można odzyskać z pozostałych nośników danych; W zależności od kontrolera/producenta informacje

    o parzystości można przesyłać „do przodu" lub „do tyłu" na poszczególne dyski twarde.
  - **Synology Hybrid RAID (SHR) :** wariant RAID wykorzystujący oprogramowanie Linux RAID (MD RAID i LVM2)

- **Najlepsze praktyki dotyczące tworzenia kopii zapasowych RAID** :

- Dokładna dokumentacja konfiguracji RAID (np. ustawienia BIOS-u, typ kontrolera RAID, poziom RAID, rozmiar paska).
- Kopia zapasowa wykonywana jest za pośrednictwem kontrolera RAID, np. poprzez uruchomienie systemu Linux Live CD lub WinFE, które rozpoznają sprzętowy kontroler RAID.
- Logiczna kopia zapasowa danych, jeśli to konieczne, np. za pomocą FTK Imager 'Custom Content Image'.

NAS (Network Attached Storage) to kompaktowe, autonomiczne serwery, które korzystają z dostosowanych systemów operacyjnych, zazwyczaj lekkich, dostosowanych wersji Linuksa. Wewnętrzny nośnik danych zazwyczaj składa się z dysków twardych SATA. Pierwszym krokiem jest utworzenie klasycznych kopii zapasowych obrazu. Podczas wyjmowania dysków z systemu ważne jest, aby oznaczyć, który dysk znajdował się w którym slocie. Systemy NAS posiadają interfejs oparty na przeglądarce internetowej (Web GUI). Aby uzyskać dostęp do tego interfejsu, serwer NAS musi być połączony z siecią śledczą.

9.4.4 Kryminalistyka cyfrowa w kontekście handlu ludźmi i wyzysku pracowników

Handel ludźmi, w tym wyzysk w pracy, w coraz większym stopniu opiera się na komunikacji cyfrowej, transakcjach finansowych i rekrutacji online (Europol, 2020; 2024). W związku z tym informatyka śledcza odgrywa kluczową rolę w identyfikacji sprawców, odkrywaniu wzorców wykorzystywania ofiar i zabezpieczaniu dowodów na potrzeby postępowania karnego. W niniejszym podrozdziale omówiono, jak metodologie informatyki śledczej można zastosować w sprawach handlu ludźmi, uwzględniając zarówno kwestie techniczne, jak i etyczne. Rozdział rozpoczyna się od

omówienia kluczowych źródeł dowodów cyfrowych w dziedzinie handlu ludźmi (oraz, w miarę możliwości, gromadzenia informacji, szczególnie w odniesieniu do wyzysku w pracy, rozdział 9.6.4.1). Następnie rozdział 9.6.4.2 omawia analizę dowodów cyfrowych typowych dla handlu ludźmi (np. czego szukają śledczy?). Następnie rozdział 9.6.4.3 przedstawia kilka możliwych narzędzi informatyki śledczej do wykorzystania przez organy ścigania. Następnie omówiono główne wyzwania, które są szczególnie istotne dla procesu informatyki śledczej w trakcie dochodzeń w sprawie handlu ludźmi (rozdział 9.6.4.4). Sekcja kończy się omówieniem kwestii prawnych i etycznych (sekcja 9.6.4.5). UNODC przygotowało dalszy przegląd technologii wykorzystywanych do zapobiegania i zwalczania handlu ludźmi – Moduł 14: Powiązania między cyberprzestępczością, handlem ludźmi i przemytem migrantów .

9.4.4.1Kluczowe źródła dowodów cyfrowych

Handlarze ludźmi i wyzyskiwacze korzystają z różnych platform i technologii cyfrowych, pozostawiając po sobie kluczowe ślady kryminalistyczne, ale organy ścigania mogą wykorzystać dowody cyfrowe do identyfikacji osób dokonujących handlu ludźmi i sprawców oraz znaleźć dowody prawne pozwalające oskarżyć ich o to przestępstwo (Cellebrite, 2024). Typowe źródła dowodów obejmują:

Osobiste urządzenia cyfrowe

W kontekście dochodzeń w sprawie wyzysku pracowników, osobiste urządzenia cyfrowe, takie jak telefony komórkowe i komputery, mogą stanowić kluczowe źródła dowodów. Urządzenia te często zawierają dane dotyczące komunikacji, kontaktów, transakcji finansowych i lokalizacji, które mogą ujawnić praktyki wyzysku.

- **Urządzenia mobilne** : Handlarze ludźmi często wykorzystują urządzenia mobilne do koordynowania nielegalnych działań. Dowody z tych urządzeń mogą obejmować: (1) rejestry połączeń i listy kontaktów, które ujawniają wzorce i sieci

komunikacji , (2) wiadomości tekstowe i historie czatów zawierające szczegóły dotyczące rekrutacji, koordynacji i wykorzystywania, (3) pliki multimedialne, takie jak zdjęcia i filmy, które mogą dokumentować ofiary, lokalizacje lub nielegalne działania, oraz (4) dane o lokalizacji (informacje GPS umożliwiają śledzenie ruchów i identyfikację kluczowych lokalizacji).

- **Komputery:** Kilka rodzajów przechowywanych lub w inny sposób dostępnych za pośrednictwem komputera danych może być szczególnie interesujących w kontekście badania handlu ludźmi (możliwe nakładanie się z danymi z urządzeń mobilnych): (1) zapisy komunikacji, takie jak wiadomości e-mail i SMS, aktywność w mediach społecznościowych lub reklamy online lub oferty pracy, (2) dane finansowe, takie jak transakcje bankowe i zapisy płatności lub zapisy kryptowalut, (3) dane identyfikacyjne osoby, takie jak cyfrowe kopie dokumentów tożsamości lub dane o lokalizacji, (4) zapisy dotyczące zatrudnienia i warunków pracy, takie jak umowy o pracę, nielegalne harmonogramy pracy, systemy ewidencji czasu pracy i obecności (np. w celu wykrywania nadmiernej liczby godzin pracy), (5) dane dotyczące podróży, takie jak informacje o rezerwacji podróży z linii lotniczych lub biur podróży lub zakupy biletów i trasy podróży, (6) historie aktywności w (ciemnej lub powierzchniowej) sieci, (7) dokumentacja medyczna i zdrowotna, która jest przechowywana np. z wizyt u lekarza ofiar po atakach fizycznych lub (8) dane z kamer monitorujących lub systemów bezpieczeństwa w miejscach pracy lub prywatnych nieruchomościach, pokazujące warunki życia i pracy ofiar.

Przechowywanie w chmurze

Przechowywanie danych w chmurze może być wykorzystywane przez handlarzy ludźmi ze względu na wygodę, zdalny dostęp i możliwość przechowywania dużych ilości danych, co czyni je ważnym źródłem cyfrowych dowodów w takich sprawach. Dane

gromadzone w chmurze mogą być podobne do listy przedstawionej powyżej dla urządzeń mobilnych i komputerów. Ponadto, szczególne dane, które częściej można znaleźć w chmurach, to cyfrowe kalendarze potencjalnie ujawniające przeprowadzone lub zaplanowane spotkania, trasy podróży ofiar lub inne informacje logistyczne dotyczące operacji, którymi podzielono się w sieci handlu ludźmi. W związku z tym przechowywanie w chmurze może dawać większe prawdopodobieństwo ujawnienia struktur sieci handlu ludźmi lub ofiar, które padły ofiarą zorganizowanego wyzysku pracowniczego. Dostęp do danych przechowywanych w chmurze i ich analiza wymagają jednak procedur prawnych i specjalistycznej wiedzy technicznej, aby zapewnić integralność dowodów (jeśli dane uwierzytelniające użytkownika nie są znane). Techniczne sposoby uzyskania (przynajmniej częściowego) dostępu obejmują na przykład współpracę z dostawcą usług w chmurze, stosowanie narzędzi do ekstrakcji danych z chmury, korzystanie z interfejsów API usług w chmurze, uzyskiwanie dostępu za pośrednictwem skonfiskowanych urządzeń (logowanie przy użyciu danych logowania, korzystanie z kopii zapasowych urządzeń i sprawdzanie, czy urządzenie zsynchronizowało dane z chmurą), przeprowadzanie analizy metadanych plików przechowywanych w chmurze, stosowanie analizy sieciowej (sekcja 4.1.1) lub uzyskiwanie dostępu do dzienników usług przechowywania danych w chmurze od dostawców usług w chmurze w celu np. uzyskania historii logowania lub historii pobierania plików.

Platformy komunikacyjne i rekrutacyjne

Internet zapewnia handlarzom ludźmi dostęp do potencjalnych ofiar za pośrednictwem różnych kanałów cyfrowych, w tym mediów społecznościowych i stron rekrutacyjnych (UNODC, 2019a). Fraser (2016) rozwinął temat zmian w procesach zachodzących między handlarzami ludźmi a ofiarami, wynikających z przejścia od sieci geograficznych do sieci internetowych. Fraser podkreśla, że handlarze ludźmi potrafią obecnie korzystać z mediów społecznościowych i dark webu. Artykuł opisuje również,

jak te sieci wpływają na nierównowagę sił w handlu ludźmi i kształtują doświadczenia ofiar (Fraser, 2016). Dowody cyfrowe z tych platform obejmują (1) profile i posty, które mogą zawierać próby rekrutacji, oszukańcze oferty pracy lub reklamy nielegalnych usług, (2) wiadomości bezpośrednie (ułatwiające prywatną komunikację między handlarzami a ofiarami) oraz (3) przynależność do grup wskazujących na zaangażowanie w sieci lub fora handlu ludźmi. Analiza tych elementów może ujawnić np. strategie rekrutacyjne oraz zidentyfikować zarówno ofiary, jak i sprawców.

- **Platformy mediów społecznościowych**: Raport Kunza i in. (2018) podsumowuje, które strony internetowe są wykorzystywane do celów wykorzystywania seksualnego. Wśród nich znajdują się (1) strony do oglądania i komentowania, takie jak Facebook, Instagram i Snapchat, ale także YikYak i Wispher, (2) strony do rozmów, takie jak Tinder, Blendr, WhatsApp i KIK, ale także Yellow i #1 Chat Avenue jako mniej popularne strony, (3) strony z kamerkami internetowymi, w tym Chatroulette, Omegle i Monkey, oraz (4) strony do reklamy i sprzedaży, takie jak Cityxguide, skipthegames, bedpage, seekarrangement.com lub sugar-babies.com. Nie znaleziono takiego przeglądu w odniesieniu do wyzysku pracowników. Niemniej jednak wiadomo, że **główne platformy mediów społecznościowych** są wykorzystywane do rekrutacji do pracy wyzyskującej, wraz z portalami pracy i ogłoszeniami online (patrz np. Europol, 2024).
- **Internetowe serwisy rekrutacyjne** : Nawet jeśli te portale i potencjalnie tajne strony internetowe są legalne, handlarze ludźmi mogą publikować fałszywe oferty pracy, kierując je do grup narażonych na ryzyko i poszukujących zatrudnienia. W drugim kroku handlarze wykorzystują komunikatory internetowe do wymiany danych operacyjnych, ponieważ zapewniają one bezpieczniejsze środowisko (Europol, 2024).

- **Reklamy online** : Różnica w porównaniu z platformami mediów społecznościowych, komunikatorami internetowymi i internetowymi serwisami rekrutacyjnymi polega na tym, że reklamy online mogą być postrzegane jako *komunikacja jednokierunkowa* , podczas gdy inne źródła zazwyczaj koncentrują się na *komunikacji dwukierunkowej* między osobami (np. potencjalną ofiarą a podejrzanym o handel ludźmi). Cechy reklam online dotyczących handlu ludźmi w celach przymusowych obejmują:
    - **Brak konkretów**: Ogłoszenia często zawierają niejasne opisy stanowisk z minimalną ilością szczegółów dotyczących stanowiska, obowiązków i warunków pracy. Ta niejednoznaczność ma na celu przyciągnięcie szerszego grona kandydatów bez ujawniania potencjalnych sytuacji wyzysku (Volodko, Cockbain i Kleinberg, 2020).
    - **Nierealne obietnice**: Oferty mogą obejmować nietypowo wysokie wynagrodzenia, przyspieszone rozpatrywanie wniosków wizowych lub inne korzyści, które wydają się zbyt piękne, aby były prawdziwe, a ich celem jest przyciągnięcie osób poszukujących lepszych możliwości (patrz np. Fraser, 2016).
    - **Docelowe grupy demograficzne** : Działania rekrutacyjne często koncentrują się na określonych populacjach, takich jak migranci lub osoby z ubogich środowisk, które są bardziej podatne na wykorzystywanie (Volodko, Cockbain i Kleinberg, 2020).
    - Chociaż podejmowano wysiłki mające na celu zbadanie reklam internetowych promujących wykorzystywanie seksualne przy użyciu nowoczesnych metod technologicznych, takich jak przetwarzanie języka naturalnego (NLP) (np. Perez i Rivas, 2023; Lugo-Graulich i in., 2024),

przestępstwo wyzysku pracowników, a także inne formy handlu ludźmi, wciąż nie doczekały się naukowych badań w tym obszarze.

- **Dark web kontra surface web** : Hostowane w szyfrowanych sieciach, wymagających specjalistycznego oprogramowania do dostępu, oferty i reklamy w dark webie oferują wyższy stopień anonimowości. To ukrycie stanowi poważne wyzwanie dla organów ścigania, ponieważ platformy te często wdrażają zaawansowane środki techniczne w celu ochrony tożsamości użytkowników. Z drugiej strony, oferty i reklamy w surface web są publicznie dostępne i często można je znaleźć na popularnych platformach, takich jak media społecznościowe i serwisy ogłoszeniowe. Chociaż mogą one używać zakodowanego języka i grafiki, aby uniknąć wykrycia, ich publiczny charakter pozwala organom ścigania na łatwiejszy monitoring. Handlarze wykorzystują zarówno platformę surface web, jak i dark web do reklamowania usług lub możliwości wyzysku. Istotne dowody cyfrowe w ciemnej sieci obejmują np. (1) reklamy i oferty, które mogą oferować nielegalne usługi lub oszukańcze możliwości zatrudnienia, (2) posty na forach i komunikaty, w których omawiane są metody, udostępniane informacje lub negocjowane transakcje (np. post na forum stwierdzający, że „pracownicy dostępni za niedrogą siłę roboczą") lub (3) fałszywe dokumenty uzyskane z rynków w ciemnej sieci, takie jak fałszywe wizy i zezwolenia na pracę dla nielegalnych migrantów.

Nadzór i śledzenie

Dane z nadzoru i śledzenia odnoszą się do wszelkich danych, które mogą ujawnić lokalizację, ruchy lub działania osób, często gromadzone za pośrednictwem środków elektronicznych, dlatego w grę wchodzi informatyka śledcza. Nowoczesne środowiska wyposażone w systemy nadzoru i urządzenia IoT mogą przypadkowo rejestrować

działania związane z handlem ludźmi. Śledztwo może również umożliwić (jeśli zostanie to prawnie potwierdzone) śledzenie i monitorowanie podejrzanych.

Nadzór inicjowany przez organy ścigania (zwykle wymaga nakazu sądowego)

- **Śledzenie GPS, np. śledzenie pojazdów:** może być wykorzystywane przez organy ścigania do monitorowania ruchu. Władze mogą na przykład śledzić ruch samochodu podejrzanego, który regularnie przewozi ofiary do i z różnych miejsc pracy. Wzorce w danych o lokalizacji pojazdu mogą pomóc władzom w lokalizowaniu ośrodków handlu ludźmi lub określaniu tras podróży lub godzin pracy ofiary.
- **Kamery monitorujące:** Nagrania z publicznych lub prywatnych kamer monitorujących można wykorzystać do śledzenia przemieszczania się handlarzy ludźmi lub ofiar w określonych miejscach (np. w miejscach pracy, w pobliżu granic).
- **Przechwytywanie komunikacji (podsłuchy):** Podsłuchy (np. rozmów telefonicznych, e-maili, wiadomości) mogą dostarczyć informacji na temat działalności związanej z handlem ludźmi. Podsłuchy mogą pomóc władzom podsłuchiwać handlarzy podczas organizowania podróży, płatności, gróźb wobec ofiar itp.
- **Urządzenia śledzące w telefonach komórkowych:** triangulacja komórkowa i dane GPS z telefonów komórkowych mogą być wykorzystywane do precyzyjnego określania lokalizacji ofiary lub handlarza ludźmi, a np. do mapowania ich lokalizacji w czasie.
- **Drony lub nadzór lotniczy:** Drony wyposażone w kamery można wykorzystywać do śledzenia ruchów obiektów na większych obszarach (szczególnie na obszarach

wiejskich lub trudno dostępnych, gdzie nadzór ze strony człowieka może być utrudniony).

Nadzór inicjowany przez handlarzy (dane zbierane przez handlarzy)

- **Śledzenie urządzeń mobilnych przez handlarzy** : Handlarze mogą wykorzystywać telefony ofiar lub ich własne urządzenia do śledzenia ofiar. Może to obejmować korzystanie z aplikacji śledzących GPS, a nawet instalowanie oprogramowania szpiegującego (np. mSpy, FlexiSPY) w celu monitorowania lokalizacji i komunikacji ofiary.
- **Dane o lokalizacji z urządzeń IoT** : Urządzenia IoT, takie jak smartwatche, a nawet pojazdy podłączone do sieci, mogą być wykorzystywane przez handlarzy do monitorowania lokalizacji ofiar. Rejestry z tych urządzeń można analizować, np. w celu wykrycia nietypowych godzin dostępu lub zmian w otoczeniu.
- **Monitorowanie online**: Handlarze ludźmi często monitorują konta swoich ofiar w mediach społecznościowych, aby kontrolować ich komunikację, a nawet podszywać się pod nie, aby kontrolować ich wizerunek w sieci i np. uniemożliwić im szukanie pomocy. Organy ścigania mogłyby zatem sprawdzić, czy handlarz posiadał dane logowania ofiary (ofiar) do różnych mediów społecznościowych lub innych platform.
- **Monitoring wideo i audio**: Handlarze ludźmi mogą umieszczać ukryte kamery lub urządzenia rejestrujące dźwięk w pomieszczeniach lub miejscach pracy, aby stale monitorować ofiary, np. w celu upewnienia się, że wykonują swoje zadania. Organy ścigania mogłyby skupić się na wykrywaniu takich urządzeń, a następnie analizować ich dane, aby określić zakres wyzysku pracowników i móc przedstawić wiarygodne dowody w sądzie.

Transakcje finansowe i metody płatności

Transakcje finansowe i kryptowalutowe (krajowe i międzynarodowe): Handlarze często wykorzystują systemy analizy cyfrowej do prania pieniędzy i ukrywania zysków. Kluczowe dowody cyfrowe obejmują (1) wyciągi bankowe i historie transakcji, które ujawniają nietypowe wzorce wskazujące na nielegalną działalność, (2) portfele kryptowalutowe i transakcje wykorzystywane do zacierania śladów finansowych, wymagające specjalistycznej analizy kryminalistycznej. Analiza finansowa (patrz sekcja 9.2) ma kluczowe znaczenie dla śledzenia przepływu pieniędzy, wykrywania operacji związanych z handlem ludźmi i ścigania przestępców (Thomson Reuters, 2025).

- **Tradycyjne transakcje bankowe**
- **Transakcje kryptowalutowe**
- **Systemy płatności przedpłaconych i cyfrowych**

9.4.4.2 Analiza i korelacja dowodów

Po zajęciu i zabezpieczeniu dowodów cyfrowych (np. konfiskata telefonów komórkowych, komputerów, dysków USB, kont w chmurze, danych z mediów społecznościowych), dane muszą zostać wyodrębnione z tych urządzeń lub pamięci masowych, stosując różne rodzaje analiz kryminalistycznych opisane w rozdziale 9.1.1 (np. analiza kryminalistyczna chmury; ekstrakcja danych na poziomie sprzętowym, taka jak chip-off lub metody takie jak łamanie/odszyfrowywanie haseł). Następnie śledczy mogą przeanalizować i powiązać dowody cyfrowe. Przedstawione poniżej procedury i zasady kryminalistyki cyfrowej z jednej strony mogą być jedynie przykładowe, z drugiej strony nie są całkowicie unikalne dla handlu ludźmi: wiele technik pokrywa się z cyberprzestępczością, przestępczością zorganizowaną i dochodzeniami w sprawie oszustw. Jednak niektóre aspekty sprawiają, że handel ludźmi jest wyjątkowy w tym kontekście, takie jak skupienie **się na mediach społecznościowych i ogłoszeniach**

rekrutacyjnych (w przeciwieństwie do przestępstw finansowych, sprawy dotyczące handlu ludźmi w dużym stopniu opierają się na oszustwach online i śledzeniu komunikacji). Co więcej, znaczna ilość **dowodów** (które zespoły informatyki śledczej rekonstruują) **koncentruje się na ofiarach** , ponieważ handlarze ludźmi utrzymują kontrolę nad swoimi ofiarami, np. poprzez groźby, szantaż lub śledzenie GPS. Co więcej, ofiary handlu ludźmi często nie posiadają własnych komputerów ani laptopów, lecz smartfony i konta w chmurze. To sprawia, że śledztwa w sprawie handlu ludźmi są bardziej uzależnione od **informatyki śledczej w chmurze i na urządzeniach mobilnych** (patrz sekcja 9.1.1).

W przypadku handlu ludźmi eksperci ds. informatyki śledczej mogą w szczególności zwracać uwagę na:

- **Wzory komunikacji**: Często handlarze ludźmi używają zakodowanego języka lub slangu w tekstach i dlatego szukają różnych słów kluczowych, takich jak „łatwa praca", „płatność gotówką", „darmowe podróże" w kontekście wyzysku pracowników lub „modelowanie" i „eskorta" w kontekście wykorzystywania seksualnego. Często te konkretne słowa kluczowe związane z pracą, zakwaterowaniem i płacą są używane wielokrotnie. Tong i in. (2017) odkryli na przykład, że handlarze ludźmi w USA i Kanadzie modyfikują swój język, aby uniknąć wykrycia przez organy ścigania. Ponadto zmieniają terminologię, co utrudnia opracowywanie list słów kluczowych do śledzenia reklam związanych z handlem ludźmi. Tworzy to stale ewoluujący leksykon. Na przykład zamiast wyraźnie stwierdzić „młoda dziewczyna", handlarze używają zaciemnionego tekstu, emotikonów lub slangu. (np. „Y ♥ng G!rl"). Ponadto wiele reklam nie posiada odpowiednich struktur gramatycznych, co sprawia, że tradycyjne techniki przetwarzania języka naturalnego (NLP) są mniej skuteczne. Reklamy często zawierają symbole, emotikony i niestandardowe znaki. Kolejność wyrazów jest

często niespójna, przypominając raczej wiadomości z mediów społecznościowych lub SMS-y niż pisanie struktur (np. '@' zamiast 'at' lub 'm33t' zamiast 'meet'). Złożoność unigramów, bigramów i trigramów jest wysoka. Duża zmienność słów wynika z celowego modyfikowania słów przez handlarzy w celu uniknięcia automatycznego wykrywania (nietypowe połączenia słów, rzadkie słowa, zmodyfikowane frazy słowne). Reklamy są zazwyczaj krótkie (media 133 słów) i brakuje im obszernych opisów. Tong i in. (2017) dochodzą do wniosku, że handlarze stale dostosowują swój język, co wymaga elastycznych modeli wykrywania. Same listy słów kluczowych są niewystarczające, badacze będą potrzebować modeli AI uwzględniających kontekst.

Innym sposobem na zrozumienie i odtworzenie określonych wzorców komunikacji na potrzeby informatyki śledczej jest przyjrzenie się strategiom rekrutacyjnym stosowanym przez handlarzy ludźmi. Można je podzielić na metody aktywne i pasywne (Europol, 2020): **Aktywna rekrutacja** przypomina „łowienie na haczyk", gdzie przestępcy publikują fałszywe ogłoszenia o pracę na zaufanych portalach pracy i platformach społecznościowych. Mogą nawet tworzyć fałszywe strony rekrutacyjne, które wyglądają profesjonalnie, czasami oferując czat na żywo, aby wyglądały na legalne. UNODC nazywa to zjawisko również „strategią polowania" (UNODC, 2020). Aktywna rekrutacja obejmuje głównie wiadomości bezpośrednie i czaty skierowane do osób podatnych na ataki. Może zawierać wzorce przymusu, manipulacji i fałszywych ofert pracy. Nie jest również niczym niezwykłym nagłe usuwanie wiadomości lub kont po pierwszym kontakcie (tj. gdy handlarz zauważy, że osoba, która ma być ofiarą handlu ludźmi, nie jest dostępna dla oferty(-ów) pracy). **Pasywna rekrutacja** jest bardziej dyskretna i trudniejsza do wykrycia przez organy ścigania. Działa to jak „łowienie siecią" (lub „strategia łowienia", UNODC, 2020), gdzie handlarze ludźmi monitorują ogłoszenia osób poszukujących pracy w internecie i kontaktują się z nimi bezpośrednio. Obiecują

możliwości pracy za granicą, żądając opłaty za jej znalezienie oraz pokrycie kosztów podróży lub zatrudnienia. Ofiary orientują się, że zostały oszukane dopiero po przybyciu do obcego kraju (Europol, 2020).

Na koniec, ale nie mniej ważne, wiarygodne dowody naukowe dotyczące technik badawczych dotyczących wzorców komunikacji są bardzo rzadkie (sprawdź na przykład Mapę luk dowodowych Międzynarodowej Organizacji Pracy z 2023 r., aby uzyskać możliwe aktualizacje dotyczące opracowań naukowych).

- **Śledzenie geolokalizacyjne** : Co więcej, podobnie jak w przypadku zrozumienia wzorców komunikacji, może ono pomóc w przyjęciu perspektywy sprawcy: Urządzenia umożliwiające śledzenie geolokalizacyjne mogły być wykorzystywane do monitorowania ofiary (ofiar) w czasie rzeczywistym, np. za pomocą GPS, wbudowanych kamer w smartfonach, aplikacji do udostępniania lokalizacji (Europol, 2020). Możliwość zdalnego sterowania obniża próg powstrzymywania sprawców przed wykorzystaniem przestępców, a także komplikuje działania organów ścigania w zakresie identyfikacji, jak stwierdził Europol (2020, s. 3):

  > [Podczas gdy] historycznie zorganizowane grupy przestępcze musiały sprawować fizyczną kontrolę i monopol na określone dzielnice miasta i zazwyczaj składały się z rozległej sieci członków, nowicjusze w handlu ludźmi mogą teraz sprawnie zarządzać biznesem online bez potrzeby posiadania fizycznej infrastruktury przestępczej i przy ograniczonej liczbie pracowników. W rezultacie opanowanie technologii może sprawić, że grupa przestępcza stanie się bardziej groźna, a jednocześnie trudniejsza do zidentyfikowania przez organy ścigania.

  Więcej informacji na temat śledzenia geolokalizacji można znaleźć w poprzedniej Sekcji 9.1.3.1.

- **Analiza finansowa** : Analiza finansowa i informatyka śledcza mogą iść w parze, szczególnie w odniesieniu do transakcji finansowych dokonywanych przez

handlarzy ludźmi w celu zamieszczania reklam online (Europol, 2020). Ponadto ofiary często otrzymują przelewy bankowe na rzecz handlarzy. Bardziej szczegółowe spojrzenie na finanse, transakcje finansowe i dochodzenia finansowe można znaleźć w rozdziale 9.2.

- **Identyfikacja ofiary** : W celu identyfikacji ofiary, specjaliści ds. kryminalistyki cyfrowej i praktycy mogą zastosować rozpoznawanie twarzy, aby odnaleźć ofiary np. w reklamach lub postach w mediach społecznościowych. Dodatkowo, odwrotne wyszukiwanie obrazu może ujawnić, czy ofiary były reklamowane na stronach dla dorosłych lub platformach czarnego rynku.
- **Analiza głębokiej i ciemnej sieci** : Korzystanie z forów darknetu nie jest niczym niezwykłym dla handlarzy. Śledczy mogą korzystać z narzędzi do analizy TOR i monitorowania darknetu, np. do wyszukiwania wiadomości rekrutacyjnych, treści wykorzystujących ofiary lub nielegalnych transakcji.

9.4.4.3 Podejścia i narzędzia informatyki śledczej

Aby skutecznie gromadzić i analizować dowody w sprawach handlu ludźmi i wyzysku pracowników, informatyka śledcza w dużym stopniu opiera się na:

- Kryminalistyka mobilna
- Kryminalistyka sieci i chmury
- Analiza finansowa i kryptowalutowa
- Śledztwa w darknecie

Aby przejść chronologicznie, oto istotne zasady informatyki śledczej, które należy wziąć pod uwagę w praktyce, również w kontekście handlu ludźmi: W pierwszej fazie identyfikacji i zabezpieczenia, ratownicy muszą niezwłocznie zidentyfikować

i zabezpieczyć urządzenia cyfrowe, aby zapobiec manipulacji lub utracie danych (np. odizolowanie od sieci; UNODC, 2019b). Następnie, w celu postępowania z dowodami cyfrowymi, ważne jest sporządzenie szczegółowych zapisów stanu każdego urządzenia, w tym stanu operacyjnego (włączony, wyłączony, czuwanie), modelu, wszelkich widocznych uszkodzeń. Fotografie i pisemne notatki pomagają w utrzymaniu łańcucha dowodowego i wspierają integralność dowodów (UNODC, 2019b). Ekstrakcję danych można następnie przeprowadzić za pomocą specjalistycznych narzędzi kryminalistycznych, aby odzyskać dane bez zmiany oryginalnej zawartości (patrz Sekcja 9.6.2, aby uzyskać ogólny przegląd). W przypadku niektórych urządzeń może to wiązać się z ominięciem zabezpieczeń, takich jak szyfrowanie lub hasła. Szczególnie w kontekście handlu ludźmi/(wyzysku pracowników) organy ścigania korzystają z narzędzi informatyki śledczej, które ułatwiają dochodzenie w sprawie tego przestępstwa.

Nie można przedstawić tutaj pełnego przeglądu narzędzi informatyki śledczej, które mogłyby być i są wykorzystywane w organach ścigania, ze względu na (1) różnorodność narzędzi wykorzystywanych przez różne organy ścigania w całej Europie (licząc informatykę śledczą jako całość i informatykę śledczą do celów śledztw w sprawie handlu ludźmi jako jej jedną z gałęzi), (2) powiązanie stosowania różnych technik i narzędzi, zależnych od konkretnej sprawy, oraz (3) niepubliczny dostęp do sposobu działania organów ścigania w tym zakresie, by wymienić tylko kilka powodów. Można jednak pobieżnie przedstawić niektóre narzędzia informatyki śledczej i firmy oferujące rozwiązania programowe do badania przypadków handlu ludźmi:

- **Cellebrite Pathfinder** : mobilne narzędzie do analizy kryminalistycznej, które wyodrębnia, analizuje i dekoduje dane ze smartfonów, tabletów i źródeł w chmurze. Umożliwia odzyskiwanie usuniętych wiadomości, rejestrów połączeń i lokalizacji GPS.

  Potencjalne zastosowanie w przypadku THB/wyzysku pracowników *:*

- ➔ wyciągi np. z wiadomości WhatsApp i Telegram pomiędzy handlarzami a ofiarami
- ➔ odzyskuje usunięte konwersacje, w których ofiarom obiecywano fałszywe prace
- ➔ identyfikuje lokalizacje GPS z telefonu ofiary, aby określić wzorce ruchu

- **MAGNET FORENSICS** : Firma oferuje szereg rozwiązań programistycznych na potrzeby służb bezpieczeństwa publicznego, wojska, wywiadu itp.

  MAGNET AXIOM jest szczególnie przydatny dla THB: Narzędzie to specjalizuje się w analizie komputerowej i danych w chmurze, analizując dane z dysków twardych, mediów społecznościowych, wiadomości e-mail i zaszyfrowanych plików.

Potencjalne zastosowanie w przypadku THB/wyzysku pracowników *:*

- ➔ bada wpisy w mediach społecznościowych i aktywność na portalach z ofertami pracy, gdzie handlarze zamieszczają fałszywe ogłoszenia o pracę
- ➔ wyodrębnia ukryte pliki (np. umowy ofiar, bilety lotnicze, zezwolenia na pracę) z komputerów handlarzy
- ➔ analizuje dzienniki komunikacji między wieloma podejrzanymi w różnych krajach

MAGNET OUTRIDER może również wspomóc proces dochodzeń z zakresu informatyki śledczej, skanując urządzenia mobilne z systemem iOS i Android i wykrywając np. nielegalne aplikacje, listy kontaktów, wiadomości SMS i ostatnio używane aplikacje.

Potencjalne zastosowanie w przypadku THB/wyzysku pracowników:

➔ ujawnia ukryte działania online i demaskuje handlarzy, którzy korzystają z forów dark webu lub fałszywych kont w mediach społecznościowych

➔ potrafi wykrywać fałszywe umowy o pracę, ogłoszenia o pracę i dokumenty finansowe

MAGNET GRAYKEY, specjalizujący się w łamaniu szyfrowanych urządzeń mobilnych, również może pomóc. Omija blokady ekranu i wydobywa dane z systemu plików.

Potencjalne zastosowanie w przypadku THB/wyzysku pracowników *:*

➔ Odblokowuje skonfiskowane telefony handlarzy i pomaga odzyskać rozmowy z WhatsApp, Telegram, Signal, Viber itp.

Przydatne może okazać się również inne oprogramowanie MAGNET (patrz Pizzuro, 2022).

- MSAB XRY: mobilne narzędzie kryminalistyczne wykorzystywane przez organy ścigania do wyodrębniania, analizowania i dekodowania danych z telefonów komórkowych, tabletów, urządzeń GPS i dronów.

  Potencjalne zastosowanie w przypadku handlu ludźmi/wyzysku pracowników

  ➔ wyodrębnia komunikację mobilną, potencjalnie ujawniając cyfrowe dowody związane z handlem ludźmi

  ➔ analizuje media społecznościowe i platformy pracy

  ➔ odzyskuje usunięte pliki i zdjęcia

- **Maltego**: Firma oferuje narzędzia służące do mapowania relacji między ludźmi, firmami, kontami w mediach społecznościowych i stronami internetowymi (GRAPH), do przeprowadzania wyszukiwań OSINT w celu znalezienia

podejrzanych przestępców (SEARCH), monitorowania mediów społecznościowych w czasie rzeczywistym (MONITOR) i przeprowadzania analizy sieci społecznościowych (EVIDENCE).

***Potencjalne zastosowanie w przypadku THB/wyzysku pracowników** :*

➔ odkrywa fałszywe strony internetowe służące do rekrutacji i łączy je ze znanymi handlarzami

➔ mapuje połączenia między różnymi profilami w mediach społecznościowych wykorzystywanymi do rekrutacji

➔ identyfikuje portfele kryptowalutowe i transakcje finansowe powiązane z handlarzami

https://www.maltego.com/blog/świecenie-światła-wzmacnianie-organizacji-pozarządowych-w-międzynarodowym-miesiącu-zapobiegania-handlowi-ludźmi/

- **Autopsy** : bezpłatne, otwarte narzędzie do analizy cyfrowej, stanowiące platformę do badania dysków twardych.

  ***Potencjalne zastosowanie w przypadku THB/wyzysku pracowników** :*

  ➔ odzyskuje usunięte umowy o pracę lub fałszywe dokumenty wizowe

  ➔ śledzi historię przeglądarki (np. wizyty na fałszywych stronach z ofertami pracy lub szyfrowanych platformach czatowych)

  ➔ wyodrębnia historię urządzenia USB, aby sprawdzić, czy dyski zewnętrzne były używane do przechowywania np. danych ofiary

- **ADF PRO** : oprogramowanie do informatyki śledczej i triażu przeznaczone do szybkiej analizy komputerów, dysków zewnętrznych i urządzeń mobilnych.

  ***Potencjalne zastosowanie w przypadku THB/wyzysku pracowników** :*

- ➔ Szybkie zabezpieczenie dowodów cyfrowych w miejscu nalotu (np. skanowanie mediów społecznościowych, laptopów i telefonów podejrzanych)
- ➔ Rozpoznawanie twarzy: szybka identyfikacja i dopasowywanie twarzy na obrazach i filmach (dotyczy identyfikacji ofiary i sprawcy)

- **Narzędzia do analizy łańcucha bloków** (np. Chainalysis , Elliptic , CipherTrace)

  Narzędzia te specjalizują się w śledzeniu transakcji kryptowalutowych. Często są wykorzystywane przez handlarzy do otrzymywania płatności za rekrutację lub wykorzystywanie ofiar.

  Potencjalne zastosowanie w przypadku THB/wyzysku pracowników *:*

  - ➔ śledzi transakcje Bitcoin lub kryptowaluty dokonywane przez ofiary, aż do rekrutera(-ów) stosującego wyzysk
  - ➔ łączy adresy portfeli ze znanymi sieciami handlu ludźmi
  - ➔ identyfikuje techniki prania pieniędzy wykorzystywane do ukrywania nielegalnych zysków

W kontekście procesów informatyki śledczej służących zwalczaniu handlu ludźmi, przedstawiono i krótko opisano dwa kolejne potencjalne podejścia. W pewnym stopniu mogą one również pokrywać się z już opisanymi narzędziami lub gałęziami informatyki śledczej.

Pierwszym z nich jest podejście polegające na wykorzystaniu metadanych z obrazów i filmów w handlu ludźmi do (cyfrowych) dochodzeń kryminalistycznych. Zamiast polegać wyłącznie na kosztownych obliczeniowo technikach przetwarzania obrazu, metadane obrazów i filmów mogłyby pomóc organom ścigania w identyfikacji ofiar i handlarzy (Mattmann i in., 2016). Handel ludźmi często zawiera znaki tekstowe, takie jak cechy

fizyczne ofiary, jej lokalizacja i elementy multimedialne (tj. obrazy, filmy na różnych platformach). Mattmann i in. (2016) opracowali zestaw narzędzi do analizy kryminalistycznej metadanych dla multimediów, obejmujący ImageCat (katalog obrazów) i ImageSpace. ImageCat to system ekstrakcji, transformacji i ładowania (ETL) przeznaczony do przetwarzania i katalogowania metadanych multimedialnych, szczególnie w dochodzeniach dotyczących handlu ludźmi. Potrafi on łączyć wiele reklam ze wspólnymi metadanymi (np. ta sama kamera użyta dla różnych ofiar; analiza podobieństwa) i umożliwia szybkie wyszukiwanie i pobieranie dowodów multimedialnych. W związku z tym może pomóc organom ścigania zidentyfikować zarówno ofiary, jak i handlarzy (Mattmann i in., 2016). Ponadto ImageSpace (zbudowany na ImageCat) wyodrębnia metadane multimedialne (tj. przestrzeń barw RGB, model kamery, geolokalizację, znaczniki czasu). Może przeszukiwać i przeszukiwać duże bazy danych multimedialnych, co pozwala organom ścigania wyszukiwać obrazy i filmy przy użyciu tekstu, metadanych lub podobieństwa obrazów. Ponadto interaktywne przeglądanie i wizualizacja obrazów pomaga organom ścigania wyświetlać te dowody w zorganizowanej galerii do przeglądu kryminalistycznego i zapewnia interaktywne histogramy i wykresy gęstości. ImageSpace umożliwia również dopasowywanie podobieństw między obrazami i filmami w celu grupowania powiązanych plików, pomagając śledczym śledzić np. ofiary w różnych reklamach i na różnych platformach. Co więcej, może optymalizować wyniki wyszukiwania w czasie i obsługuje optyczne rozpoznawanie znaków i ekstrakcję tekstu (tj. wyodrębnianie numerów telefonów, adresów e-mail, adresów) z obrazów i filmów. To konkretne podejście multimedialne zapewnia alternatywną metodę łączenia reklam, ofiar i handlarzy poprzez analizę wzorców metadanych zamiast samej zawartości obrazu lub wideo.

Innym podejściem, częściowo włączonym do wcześniej zaprezentowanych narzędzi i rezonującym w wielu dotychczasowych opracowaniach dotyczących dochodzeń w sprawie handlu ludźmi i informatyki śledczej, są badania z zakresu wywiadu opartego

na źródłach otwartych (OSINT). Badania OSINT polegają na gromadzeniu i analizowaniu publicznie dostępnych danych w celu wspierania śledztw. Odgrywają one kluczową rolę w kryminalistyce cyfrowej w dochodzeniach dotyczących handlu ludźmi, identyfikując wzorce, śledząc cyfrowe ślady i łącząc podejrzanych z działalnością przestępczą. Ponieważ wcześniej wspomniano o szczególnie użytecznych elementach OSINT, ten krótki rozdział na ich temat służy jedynie podkreśleniu ich znaczenia i ogromnego potencjału. OSINT jest niezbędny do identyfikacji wzorców rekrutacji i komunikacji, ponieważ pomaga odkryć kluczowe platformy, wzorce językowe i strategie rekrutacyjne wykorzystywane w aktywnych (polowania) i przelotnych (wędkowanie) metodach rekrutacji. OSINT, który można podzielić na wywiad mediów społecznościowych (SOCMINT), wywiad geoprzestrzenny (GEOINT) i wywiad ludzki (HUMINT), obejmuje m.in. monitorowanie mediów społecznościowych i ofert pracy, analizę dyskusji na forach, aktywności w dark webie oraz wyszukiwanie wsteczne obrazów i wideo. Służy do łączenia reklam online z sieciami handlu ludźmi poprzez indeksowanie i analizowanie ogłoszeń o pracę, śledzenie kryptowalut i płatności oraz analizę domen i witryn internetowych. Może być istotne dla geolokalizacji ofiar i handlarzy poprzez analizę obrazów i filmów (oraz ich metadanych) lub wykorzystanie geolokalizacji pozyskiwanej z crowdsourcingu (np. Google Street View, zdjęcia satelitarne). Ponadto OSINT może również pomóc w demaskowaniu fałszywych tożsamości i sieci poprzez krzyżowe porównywanie danych z mediów społecznościowych (lub dark webu), analizę cyfrowych śladów i sprawdzanie danych osobowych (zobacz np. https://epieos.com/ , aby uzyskać odwrotne wyszukiwanie, jeśli adres e-mail lub numer telefonu jest powiązany z konkretnymi kontami, takimi jak konto Google) lub poprzez analizę behawioralną (np. zachowania związane z publikowaniem postów, wzorce językowe, czas aktywności online).

9.4.4.4 Wyzwania w dochodzeniach z zakresu informatyki śledczej

Śledztwo w sprawach handlu ludźmi stwarza szczególne przeszkody dla informatyki śledczej, takie jak:

- Szyfrowana i samoniszcząca się komunikacja
- Usuwanie i ukrywanie danych
- Problemy z danymi transgranicznymi
- Ochrona ofiar i prywatność

Aby uzyskać bardziej systematyczny przegląd wyzwań, można je podzielić na wyzwania materialne i strukturalne.

Wyzwania związane z materią

Wyzwania związane z materią to wyzwania wynikające z zakresu informatyki śledczej i śledztw w sprawie handlu ludźmi. W związku z tym są one immanentnie związane z samym przestępstwem. Na przykład, można rozróżnić śledztwa proaktywne i reaktywne. Rozpoczęcie **śledztw proaktywnych** jest znacznie bardziej skomplikowane, ponieważ organy ścigania muszą zidentyfikować oznaki wykorzystywania, które mogłyby na nie wskazywać. Trudno jest na przykład odfiltrować te odniesienia z dużej liczby dostępnych ogłoszeń online (Europol, 2020). W związku z tym „ **śledztwa reaktywne** są łatwiejsze, ponieważ mają punkt wyjścia, taki jak zeznania zidentyfikowanej ofiary i/lub konto lub strona internetowa wykorzystywana do celów rekrutacji lub wykorzystywania” (Europol, 2020, s. 5).

Dodatkowo, sam w sobie cyfrowy materiał dowodowy, z którym śledczy mają do czynienia głównie w sprawach handlu ludźmi, stanowi wyzwanie. Ponieważ wielu handlarzy korzysta z komunikatorów internetowych, takich jak WhatsApp, Signal czy

Telegram, wbudowane szyfrowanie typu end-to-end (E2EE) utrudnia odzyskiwanie wiadomości. Kolejną kwestią jest to, że handlarze często usuwają cyfrowy materiał dowodowy (same lub korzystają z funkcji automatycznego usuwania, np. w czatach WhatsApp). Dostęp do usuniętych danych jest ograniczony, a śledczy mogą próbować uzyskać dostęp jedynie do kopii zapasowych utworzonych w przeszłości. Ponadto handlarze mogą działać w ukrytych usługach Tor (ciemna sieć, VPN), co utrudnia śledzenie. Ponadto handlarze próbują zacierać ślady poprzez ekstremalną dywersyfikację swojej obecności cyfrowej - na przykład poprzez używanie kilku kart SIM i telefonów komórkowych, różnych kont (w tym fałszywych kont) itp. Ta trudność ilustruje inne wyzwanie: śledczy zaangażowany w sprawę często musi okiełznać ogromną ilość (zwłaszcza cyfrowych) danych, przeanalizować te dane, sklasyfikować je jako istotne lub nieistotne dla przestępstwa lub przestępstw, które mają zostać oskarżone, zachować ogólny obraz i zaplanować dalsze kroki strategiczne. Z tym wyzwaniem wiąże się również inny aspekt prawny, który może stać się problematyczny: sprawa może stać się niezwykle złożona, ponieważ często można oskarżyć nie tylko handel ludźmi/wyzysk w pracy, ale także np. unikanie płacenia podatków; naruszenia prawa pracy i obowiązków związanych z ubezpieczeniem społecznym; pracę przymusową; napaść; oszustwo; fałszowanie dokumentów; lub naruszenia praw człowieka. Może to również wpłynąć na informatykę śledczą, ponieważ bardziej złożona sprawa wymaga bardziej spójnej wymiany informacji między prowadzącym sprawę śledczym a specjalistą informatyki śledczej.

Wyzwania strukturalne

Wyzwania można postrzegać jako strukturalne, gdy wynikają z systemu (np. z organizacji organów ścigania w danym kraju, okoliczności legislacyjnych). Na przykład technologie cyfrowe stosowane przez handlarzy ludźmi są stale rozwijane, dlatego organy ścigania muszą dostosowywać się do tych (najnowszych) osiągnięć technicznych,

z których korzystają sprawcy (Europol, 2020). Ponadto organy ścigania muszą pozyskać odpowiednie zasoby ludzkie do prowadzenia tych dochodzeń. Dotyczyło to nie tylko zasobów ludzkich wyspecjalizowanych śledczych ds. handlu ludźmi oraz naukowców i praktyków informatyki śledczej, ale także innego pilnie potrzebnego personelu do badania przypadków handlu ludźmi, takiego jak tłumacze ustni (na przykład do tłumaczenia danych z monitoringu telekomunikacyjnego). Podobnie, instrumenty prawne muszą zostać ulepszone, aby zapewnić ściganie i skazanie (Europol, 2020).

Rozszerzenie możliwości legislacyjnych jest szczególnie istotne, ponieważ ofiary często niechętnie składają poważne zeznania i oświadczenia, ponieważ są już narażone na silny stres psychiczny – groźby, szantaż, a także nieodłączne ryzyko publicznego skompromitowania za pośrednictwem mediów społecznościowych (np. poprzez nagłośnienie ich wykorzystywania). Łatwiejszy dostęp do dostępnych zbiorów danych na potrzeby informatyki śledczej jest zatem istotny, aby przyspieszyć śledztwa i ostatecznie wesprzeć, a nawet umożliwić ściganie karne (Europol, 2020).

Odnosząc się do aspektów prawnych, należy również wspomnieć, że wysiłki na rzecz współpracy transgranicznej mogą być utrudnione, jeśli współpraca sądowa i obowiązujące przepisy nie zostaną jasno określone. Może to utrudniać np. wymianę dowodów między krajami. W związku z brakiem ujednoliconej współpracy międzynarodowej, nie istnieje jeszcze scentralizowana globalna baza danych o handlu ludźmi, która śledziłaby aktywność handlarzy w internecie na całym świecie.

9.4.4.5 Rozważania prawne i etyczne

Ze względu na delikatny charakter spraw handlu ludźmi, dochodzenia kryminalistyczne muszą być zgodne z rygorystycznymi standardami etycznymi i prawnymi, z których część została już wcześniej przedstawiona. Dzięki uwzględnieniu tych kwestii, specjaliści ds. kryminalistyki cyfrowej mogą poruszać się w złożonym

krajobrazie dochodzeń w sprawie handlu ludźmi i wyzysku w pracy w sposób etyczny, prawny i skuteczny, zapewniając, że dążenie do sprawiedliwości jest zgodne z ochroną praw jednostki i wartości społecznych.

Podejście skoncentrowane na ofierze

Podejście skoncentrowane na ofierze priorytetowo traktuje prawa, potrzeby i dobrostan ofiar w całym procesie dochodzeniowym. Ta metodologia kładzie nacisk na traktowanie ofiar z szacunkiem i wrażliwością, zapewnienie im informacji i wsparcia oraz aktywne angażowanie ich w podejmowanie decyzji mających wpływ na ich życie. Koncentrując się na doświadczeniu ofiary, śledczy mogą budować zaufanie, które jest kluczowe nie tylko dla gromadzenia rzetelnych informacji, ale także dla zapewnienia jej odpowiednich usług wsparcia. Takie podejście nie tylko pomaga w powrocie ofiar do zdrowia, ale także wzmacnia ogólną integralność dochodzenia (Międzynarodowa Organizacja Pracy, 2018). „Bezpieczeństwo ofiar, ich rodzin i bliskich jest zawsze najważniejsze i leży w gestii śledczego i prokuratora” (Międzynarodowa Organizacja Pracy, 2018, s. 47). Podkreśla to również konieczność skupienia się nie tylko na ofierze jako jednostce, ale także na rodzinach/krewnych, ponieważ możliwość represji wobec członków rodziny ze strony handlarzy ludźmi jest immanentna. (Międzynarodowa Organizacja Pracy, 2018).

Co więcej, szczególnie w przypadku informatyki śledczej, zaleca się minimalizowanie inwazyjnego nadzoru cyfrowego poprzez skupienie się na handlarzach, a nie na ofierze/ofiarach. Należy zapewnić poufność danych ofiar w każdym momencie, aby zapobiec odwetowi lub ujawnieniu ich publicznie. Śledczy powinien unikać wywierania presji na ofiary, aby wielokrotnie relacjonowały interakcje cyfrowe (i zamiast tego korzystać z narzędzi informatyki śledczej), powinien uszanować zgodę ofiary przed uzyskaniem dostępu do urządzeń osobistych. Należy unikać agresywnych technik przesłuchań opartych na ustaleniach cyfrowych (np. konfrontowania ofiary z jej logami

czatów w sposób wywołujący stres). Kolejnym poważnym wyzwaniem w ściganiu handlarzy może być poleganie na zeznaniach ofiar, które mogą być dla nich traumatyzujące, ale potencjalnie również niewiarygodne ze względu na np. strach. W tym względzie informatyka śledcza może wzmocnić sprawę i zmniejszyć zaufanie ofiar do zeznań w sądzie, co z kolei może zmniejszyć obciążenie ofiar. Eksperci informatyki śledczej mogą ponadto zapobiec odwetowi ofiar i ponownemu handlowi ludźmi, skanując ich urządzenia, jeśli wyrażą na to zgodę/chcą, w poszukiwaniu oprogramowania szpiegującego, a następnie usuwając narzędzia śledzące.

Ochrona danych

W trakcie procesu dochodzeniowego: Ochrona osób ujawniających handel ludźmi ma kluczowe znaczenie dla zachęcania do zgłaszania przestępstw. Ponadto, ochrona sygnalistów zapewnia, że osoby zgłaszające nieprawidłowości nie spotkają się z odwetem, tworząc środowisko, w którym informacje mogą być bezpiecznie udostępniane. Ponadto, etyczne informowanie przez media i władze gwarantuje, że ofiary nie będą ponownie narażone na wiktymizację w wyniku ujawnienia, a rozpowszechniane informacje będą służyć interesowi publicznemu, nie powodując przy tym szkody.

W Module 10. poświęconym ochronie prywatności i danych UNODC przygotował przegląd zagadnień prywatności i ochrony danych , który należy uwzględnić w kwestiach związanych z cyberbezpieczeństwem.

- **Zarekwirowane dowody:** Zapewnienie integralności i poufności dowodów cyfrowych ma kluczowe znaczenie. Należy wdrożyć odpowiednie środki ochrony danych, aby zapobiec nieautoryzowanemu dostępowi, manipulacjom lub utracie dowodów. Utrzymanie jasnego łańcucha dowodowego jest kluczowe dla dopuszczalności dowodów w sądzie, ponieważ dokumentuje on sposób postępowania z dowodami od momentu ich zebrania do momentu ich

przedstawienia. Przestrzeganie norm prawnych i protokołów chroni prawa wszystkich zaangażowanych stron i podnosi wiarygodność procesu dochodzeniowego.

Współpraca międzynarodowa

Handel ludźmi i wyzysk w pracy to często przestępstwa o charakterze transnarodowym, wymagające współpracy transgranicznej. Współpraca międzynarodowa obejmuje ujednolicenie ram prawnych, wymianę informacji i koordynację działań między różnymi jurysdykcjami. To wspólne podejście zwiększa możliwości śledzenia sprawców, ochrony ofiar i skutecznego rozbijania sieci handlu ludźmi. Moduł 11 – Współpraca międzynarodowa w zwalczaniu międzynarodowej przestępczości zorganizowanej, opracowany przez UNODC, może pomóc w zapoznaniu się z możliwościami prawnymi w tym zakresie.

Proporcjonalność i konieczność

Śledztwa powinny równoważyć potrzebę informacji z poszanowaniem prywatności jednostki. Gromadzenie dowodów cyfrowych musi być proporcjonalne do wagi przestępstwa i niezbędne dla śledztwa. Zasada ta gwarantuje, że środki dochodzeniowe nie wykraczają poza granice ani nie naruszają praw podstawowych, zachowując standardy etyczne w dążeniu do sprawiedliwości.

Integracja sztucznej inteligencji

Integracja sztucznej inteligencji (AI) z informatyką śledczą zapewnia wydajność, ale budzi również obawy dotyczące dokładności i stronniczości. Zautomatyzowane narzędzia muszą być starannie projektowane i regularnie oceniane, aby zapobiegać stronniczości, która mogłaby prowadzić do niesłusznych oskarżeń lub pomijania niektórych profili ofiar. Nadzór ludzki pozostaje kluczowy dla interpretacji danych generowanych przez AI

w odpowiednim kontekście prawnym i etycznym. Wykorzystanie AI, zwłaszcza w istotnych, a nawet kluczowych momentach procesu śledczego, nie może zastępować ludzkiego osądu.

Etyczne wykorzystanie OSINT i monitorowanie darknetu

Chociaż OSINT i monitorowanie darknetu są cenne w wykrywaniu nielegalnych działań, muszą być prowadzone zgodnie z prawem. Śledczy powinni unikać nieautoryzowanego dostępu lub nieuczciwych praktyk, które mogłyby zagrozić integralności śledztwa lub naruszyć standardy etyczne. Poszanowanie prywatności i legalne pozyskiwanie informacji są fundamentalne dla utrzymania zaufania publicznego i przestrzegania praworządności.

9.5 Śledztwa finansowe

Dochodzenia finansowe są niezbędnym narzędziem w walce z przestępstwami finansowymi, takimi jak pranie pieniędzy (ML), finansowanie terroryzmu (TF) i handel ludźmi. Dochodzenia te koncentrują się na analizie transakcji finansowych w celu wykrywania nielegalnych działań, śledzenia nielegalnych funduszy oraz identyfikacji sprawców i ich sieci. Podstawowe koncepcje i cele dochodzeń finansowych koncentrują się na **śledzeniu przepływu pieniędzy** w celu wykrywania i dokumentowania przestępstw finansowych. Główne cele obejmują identyfikację sieci przestępczych, śledzenie nielegalnych funduszy oraz gromadzenie dowodów, które mogą zostać wykorzystane w postępowaniu karnym. Dobrze przeprowadzone dochodzenie finansowe usprawnia działania organów ścigania poprzez pozbawianie przestępców środków finansowych i likwidację infrastruktury finansowej wspierającej przestępczość zorganizowaną.

Znaczenie analiz finansowych w kontekście **handlu ludźmi** jest szczególnie istotne, ponieważ handlarze polegają na transakcjach finansowych, aby przemieszczać, przechowywać i prać swoje nielegalne dochody. Analizując rejestry transakcji, wyciągi bankowe i cyfrowe metody płatności, śledczy mogą odkryć powiązania finansowe między handlarzami a ich wspólnikami. Pomaga to nie tylko w ściganiu przestępców, ale także w identyfikacji ofiar poprzez wykrywanie wzorców finansowych wskazujących na wykorzystywanie. Śledztwa finansowe odgrywają zatem kluczową rolę w rozbijaniu sieci handlu ludźmi, ukierunkowując je na finansowe źródła ich utrzymania. „Jednak powszechne uznanie, wdrożenie i harmonizacja strategii i taktyk śledczych ukierunkowanych konkretnie na finanse związane z handlem ludźmi wciąż wymagają pracy" (OBWE, 2019, s. 37).

Poniższy rozdział 9.7.1 przedstawia ogólne podstawy dochodzeń finansowych, a następnie wprowadzenie do struktur biznesowych związanych z handlem ludźmi, aby podkreślić znaczenie dochodzeń finansowych w kontekście handlu ludźmi i wyzysku w pracy (rozdział 9.7.2). Rozdział 9.7.3 ilustruje krok po kroku, jak przeprowadzić dochodzenie finansowe w sprawach handlu ludźmi. Rozdział 9.7.4 przedstawia wskaźniki transakcyjne wskazujące na podejrzane działania finansowe w obszarze handlu ludźmi, a zwłaszcza wyzysku w pracy. Rozdział 9.7.5 opisuje wyzwania związane z dochodzeniami finansowymi, a rozdział 9.7.6 omawia innowacje techniczne i trendy. Rozdział 9.7.7 kończy się dodatkowymi zaleceniami.

9.5.1 Przegląd

Dochodzenia finansowe odgrywają kluczową rolę w egzekwowaniu prawa i ściganiu, szczególnie w sprawach dotyczących prania pieniędzy, finansowania terroryzmu i przestępczości zorganizowanej (FATF, 2012). Wytyczne Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF) dotyczące dochodzeń finansowych określają

podstawowe zasady, narzędzia i strategie niezbędne do prowadzenia skutecznych dochodzeń finansowych. Głównym celem dochodzenia finansowego jest **śledzenie i dokumentowanie przepływu nielegalnych środków**, co pomaga w identyfikacji sieci przestępczych, ujawnianiu struktur finansowych i budowaniu mocnych podstaw prawnych (FATF, 2012). Badając finansowe aspekty działalności przestępczej, śledczy mogą odkrywać nowe tropy, mapować całe sieci przestępcze – w tym ich powiązania międzynarodowe – oraz gromadzić cenne dowody w celu ścigania podejrzanych i konfiskaty nielegalnych aktywów.

9.5.1.1Podstawowe aspekty dochodzeń finansowych

Kluczowym elementem dochodzeń finansowych są **dochodzenia równoległe**, w których dochodzenia finansowe prowadzone są równolegle z dochodzeniami karnymi. Takie podejście zapewnia, że podczas gdy organy ścigania koncentrują się na przestępstwach takich jak handel ludźmi, korupcja czy handel narkotykami, równoległe dochodzenie finansowe śledzi przepływ pieniędzy generowanych przez te działania (FATF, 2012). Dochodzenia równoległe pomagają w śledzeniu nielegalnych aktywów, identyfikacji kolejnych podejrzanych i wspierają konfiskatę dochodów z przestępstwa. Aby zwiększyć skuteczność, często powoływane są wielodyscyplinarne zespoły zadaniowe, w których uczestniczą analitycy finansowi, biegli księgowi, eksperci ds. informatyki śledczej oraz prokuratorzy. Zespoły te usprawniają wymianę informacji wywiadowczych, ograniczają powielanie działań i zapewniają kompleksowe podejście do przestępstw finansowych (FATF, 2012).

Podstawowym celem dochodzeń finansowych jest **odzyskiwanie** i konfiskata mienia (patrz rozdział 10 „Szkolenie”). Przestępcy kierują się zyskiem finansowym jako głównym motywem, a pozbawienie ich nielegalnych dochodów osłabia ich działalność. Organy ścigania muszą śledzić, zamrażać i przejmować nielegalne aktywa, wykorzystując

zaawansowane techniki kryminalistyki finansowej. Konfiskata bez wyroku skazującego jest również zalecana jako skuteczne narzędzie prawne, umożliwiające organom ścigania przejmowanie mienia pochodzącego z przestępstwa nawet w przypadkach, gdy skazanie nie jest możliwe. Utworzenie wyspecjalizowanych jednostek ds. odzyskiwania mienia i scentralizowanych baz danych wywiadu finansowego znacząco wzmacnia dochodzenia finansowe poprzez poprawę efektywności i koordynacji.

Skuteczne dochodzenie finansowe **opiera się na wielu źródłach informacji** . Organy ścigania muszą mieć dostęp do raportów wywiadu finansowego, w tym do STR-ów, raportów o transakcjach walutowych i transgranicznych deklaracji gotówkowych. Ponadto, kluczowe tropy dostarczają rejestry bankowe i finansowe, rejestry firm, zeznania podatkowe, dane celne oraz wywiad śledczy (OSINT). Funkcjonariusze organów ścigania muszą mieć uprawnienia prawne do dostępu do tych rejestrów i ich analizy, zapewniając jednocześnie zgodność z przepisami o ochronie danych.

Techniki śledcze

W dochodzeniach finansowych stosuje się różnorodne techniki śledcze (listę technik można znaleźć w dokumencie FATF, 2012, jeśli nie wskazano innego źródła).

- **Nadzór fizyczny** : Ta technika polega na monitorowaniu podejrzanych w celu zrozumienia ich aktywności finansowej, takiej jak przepływy dużych ilości gotówki lub interakcje z pośrednikami finansowymi. Jest ona szczególnie przydatna w przypadkach prania pieniędzy i finansowania terroryzmu.
- **Wyciek śmieci** : Śledczy mogą zgodnie z prawem zbierać i analizować wyrzucone zapisy finansowe i inne dokumenty, które mogą ujawnić ukryte aktywa lub nielegalne transakcje.

- **Środki przymusowe** : Obejmują one nakazy przeszukania, wezwania sądowe i nakazy wydania dokumentów w celu uzyskania dostępu do kluczowych dokumentów finansowych, takich jak wyciągi bankowe, zeznania podatkowe i księgi rachunkowe. Prawidłowo przeprowadzone procedury przeszukania i zajęcia zapewniają legalne gromadzenie dowodów cyfrowych i fizycznych oraz ich przechowywanie w ramach łańcucha dowodowego.
- **Przechwytywanie komunikacji** : Organy ścigania mogą stosować podsłuchy, monitorowanie poczty elektronicznej i inne formy elektronicznego nadzoru w celu śledzenia transakcji finansowych i identyfikacji współspiskowców. Ta metoda jest wysoce skuteczna, ale musi być zgodna z ramami prawnymi, aby uniknąć naruszenia prywatności.
- **Operacje pod przykryciem** : W niektórych przypadkach śledczy mogą przybierać fałszywe tożsamości, aby infiltrować organizacje przestępcze i zebrać bezpośrednie dowody nadużyć finansowych. Ta technika jest zasobochłonna i wymaga intensywnego szkolenia.
- **Kontrolowane dostawy** : Ta metoda polega na śledzeniu przepływu nielegalnych środków, zarówno w gotówce, jak i za pośrednictwem przelewów cyfrowych, pod nadzorem organów ścigania. Pomaga zidentyfikować kluczowych uczestników prania pieniędzy lub sieci oszustw.
- **Rachunkowość śledcza** : Rachunkowość śledcza to specjalistyczna praktyka łącząca umiejętności księgowe, audytorskie i śledcze w celu badania dokumentacji finansowej pod kątem oznak niewłaściwego postępowania. Księgowi śledczy mogą ujawniać rozbieżności w księgach rachunkowych, wykrywać oszustwa i śledzić nielegalne działania finansowe za pomocą szczegółowych sprawozdań finansowych. Stosują zarówno metody ilościowe, takie jak analiza danych i modelowanie statystyczne, jak i podejścia jakościowe,

w tym ocenę wzorców zachowań i kultury organizacyjnej, w celu wykrywania anomalii. Prawo Benforda przewiduje rozkład częstości cyfr w naturalnie występujących zbiorach danych. Księgowi śledczy wykorzystują tę zasadę do identyfikacji nieprawidłowości w danych finansowych. Odchylenia od oczekiwanego rozkładu mogą sygnalizować potencjalną manipulację lub oszustwo. Mark Nigrini, pionier w tej dziedzinie, szczegółowo zbadał i zastosował prawo Benforda do wykrywania anomalii w danych księgowych (patrz np. Gorenc, 2019; Siavoshi, 2025).

- **Metody udowadniania dochodów** : Śledczy stosują metody bezpośrednie i pośrednie w celu ustalenia nielegalnych źródeł dochodu. Metoda wartości netto porównuje aktywa danej osoby w dwóch punktach czasowych w celu ustalenia niezgłoszonych dochodów. Metoda depozytów bankowych analizuje niewyjaśnione wpływy na rachunki bankowe. Metoda wydatków porównuje wzorce wydatków ze znanymi legalnymi źródłami dochodu.
- **Wymiana informacji finansowych** : Organy ścigania współpracują z jednostkami wywiadu finansowego (FIU), bankami i międzynarodowymi odpowiednikami w celu uzyskania raportów o podejrzanej działalności (SAR) oraz innych istotnych danych finansowych.
- **Analiza transakcji finansowych** pomaga śledczym identyfikować podejrzane wzorce bankowe, techniki warstwowe i metody integracji aktywów.
- **Kryminalistyka cyfrowa** (patrz rozdział 9.6.1) odgrywa kluczową rolę w śledzeniu internetowych przelewów pieniężnych, analizowaniu transakcji kryptowalutowych i przechwytywaniu nielegalnej komunikacji finansowej.

Wykorzystanie synergii współpracy

Jednostki analityki finansowej (FIU) odgrywają kluczową rolę w dochodzeniach finansowych, gromadząc, analizując i przekazując informacje finansowe organom ścigania. Jednostki analityki finansowej otrzymują zgłoszenia dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT), zgłoszenia transakcji (STR) oraz raporty o transakcjach transgranicznych, które mogą stanowić wczesne ostrzeżenie o przestępczej działalności finansowej. Ścisła współpraca krajowa między jednostkami analityki finansowej a śledczymi zapewnia organom ścigania dostęp do aktualnych i użytecznych informacji. Aby zwiększyć efektywność, jednostki analityki finansowej i organy ścigania powinny stworzyć bezpieczne platformy udostępniania danych w czasie rzeczywistym oraz opracować protokoły analizy informacji finansowych.

Ponieważ przestępczość finansowa ma często charakter transnarodowy, niezbędna jest również współpraca międzynarodowa. Przestępcy wykorzystują międzynarodowe systemy bankowe i zagraniczne centra finansowe do ukrywania nielegalnych funduszy. Organy ścigania muszą korzystać z umów o wzajemnej pomocy prawnej (MLAT), sieci Interpolu, Europolu i FATF, aby usprawnić transgraniczne dochodzenia. Utworzenie wspólnych zespołów dochodzeniowo-śledczych i usprawnienie ram prawnych dotyczących wymiany informacji wzmacnia globalną walkę z przestępczością finansową (FATF, 2012).

Aby usprawnić dochodzenia finansowe, organy ścigania i prokuratury powinny zintegrować analizę kryminalistyczną finansów ze wszystkimi poważnymi dochodzeniami w sprawach przestępczych, wykorzystać systemy wywiadu finansowego do analizy w czasie rzeczywistym oraz zacieśnić międzynarodową współpracę w zakresie odzyskiwania aktywów i wymiany informacji wywiadowczych. Dzięki wdrożeniu tych najlepszych praktyk, dochodzenia finansowe mogą stać się potężnym narzędziem w rozbijaniu organizacji przestępczych i zapewnieniu, że przestępstwa się nie opłacają.

9.5.1.2 Wysiłki Unii Europejskiej

Dostrzegając rosnące zagrożenie infiltracji legalnej gospodarki przez przestępczość zorganizowaną, Unia Europejska podkreśliła potrzebę wzmocnienia potencjału w zakresie dochodzeń finansowych. Strategia UE z 2021 r. w sprawie zwalczania przestępczości zorganizowanej podkreśliła znaczenie promowania wczesnych dochodzeń finansowych we wszystkich krajach UE. Podejście to ma na celu likwidację infrastruktury finansowej organizacji przestępczych, eliminację ich zysków i zapobieganie ich integracji z legalną gospodarką i społeczeństwem (Komisja Europejska, bd). Aby wesprzeć te działania, Europejska Multidyscyplinarna Platforma Przeciwko Zagrożeniom Przestępczością (EMPACT) nadała priorytet dochodzeniom finansowym w swoim programie. EMPACT ułatwia współpracę między państwami członkowskimi UE w celu zwalczania różnych zagrożeń przestępczych, w tym handlu narkotykami i handlu ludźmi, poprzez integrację dochodzeń finansowych jako wspólnego celu we wszystkich priorytetach.

Ponadto Komisja Europejska zapewnia wsparcie finansowe dla Sieci Operacyjnej ds. Przeciwdziałania Praniu Pieniędzy (AMON), globalnej sieci śledczych zajmujących się zwalczaniem prania pieniędzy, utworzonej w 2012 r. AMON ułatwia wymianę wiedzy między jednostkami ścigania i wspiera sprawną współpracę operacyjną w zakresie dochodzeń dotyczących prania pieniędzy, odzwierciedlając transgraniczny charakter tego rodzaju przestępstw.

Europol wzmocnił również swoje działania, powołując w 2020 roku Europejskie Centrum ds. Przestępczości Finansowej i Gospodarczej (EFECC). EFECC zapewnia wsparcie operacyjne państwom członkowskim UE w sprawach dotyczących przestępstw podatkowych, oszustw, korupcji, prania pieniędzy, odzyskiwania aktywów, fałszowania euro oraz przestępstw przeciwko własności intelektualnej. Celem tej inicjatywy jest

zwalczanie wysoce zaawansowanych przypadków przestępstw finansowych wymierzonych w osoby fizyczne, firmy i sektor publiczny.

Ponadto Europejska Agencja ds. Szkolenia w Dziedzinie Ścigania (CEPOL) oferuje regularne szkolenia funkcjonariuszom organów ścigania, aby pogłębić ich wiedzę na temat mechanizmów prania pieniędzy i międzynarodowych technik dochodzeń finansowych. Celem tych szkoleń jest rozwijanie umiejętności śledczych w zakresie skutecznego zwalczania finansowego wymiaru przestępczości zorganizowanej (Komisja Europejska, bd).

Podsumowując, kompleksowe podejście Unii Europejskiej do dochodzeń finansowych podkreśla ich kluczową rolę w zwalczaniu działalności przestępczej, ochronie legalnej gospodarki i zwiększaniu skuteczności egzekwowania prawa we wszystkich państwach członkowskich.

9.5.2 Handel jako biznes

Handel ludźmi działa jako biznes nastawiony na zysk, podobnie jak legalne przedsiębiorstwa, i warto spojrzeć na to z tej perspektywy, aby (1) zrozumieć kluczowe czynniki napędzające handel ludźmi oraz (2) potrzebę przeprowadzania dochodzeń finansowych. Ekonomiczne teorie przestępczości sugerują, że sprawcy dokonują racjonalnych wyborów w oparciu o potencjalne zyski, ryzyko i możliwości (patrz np. Belser, 2005). Możliwości te pojawiają się dzięki osobom poszukującym lepszych warunków ekonomicznych, czy to poprzez migrację z ubogich obszarów wiejskich do bogatszych ośrodków miejskich, czy też poprzez granice międzynarodowe. Sieci przestępcze wykorzystują te słabości, oferując fałszywe obietnice zatrudnienia, miłości lub bezpieczeństwa, wciągając ofiary w pracę przymusową, wykorzystywanie seksualne lub inne formy handlu ludźmi (np. pobieranie organów). Model biznesowy w przypadku

wyzysku w pracy przymusowej jest prosty: ofiary pracują pod przymusem lub nieświadomie, generując wysokie zyski przy minimalnych kosztach dla handlarzy. Sektory takie jak rolnictwo, budownictwo, praca domowa i hotelarstwo zapewniają ochronę przed handlem ludźmi w celach przymusowych, podczas gdy wykorzystywanie seksualne pozostaje jednym z najbardziej dochodowych rynków dla handlarzy (patrz np. Aronowitz, Theuermann i Tyurykanova, 2010) .

Pomimo wysokiej rentowności, ryzyko dla handlarzy ludźmi pozostaje niskie. Wiele ofiar obawia się organów ścigania ze względu na swój status prawny, stygmatyzację społeczną lub groźby ze strony wyzyskiwaczy. W krajach, gdzie prostytucja jest nielegalna, ofiary częściej spotykają się z aresztowaniem niż z ochroną. Ponadto wskaźniki wykrywalności i ścigania handlarzy ludźmi pozostają niskie, co wzmacnia stabilność modelu biznesowego. Siły rynkowe również odgrywają znaczącą rolę w kształtowaniu operacji handlu ludźmi. Handel ludźmi napędza nie tylko popyt ze strony konsumentów, ale także istnienie dużej liczby osób podatnych na ataki. Organizacje przestępcze dostosowują swoje metody w oparciu o ramy prawne, warunki ekonomiczne i mechanizmy egzekwowania prawa, podobnie jak legalne firmy reagujące na zmiany rynkowe (Aronowitz, Theuermann i Tyurykanova, 2010).

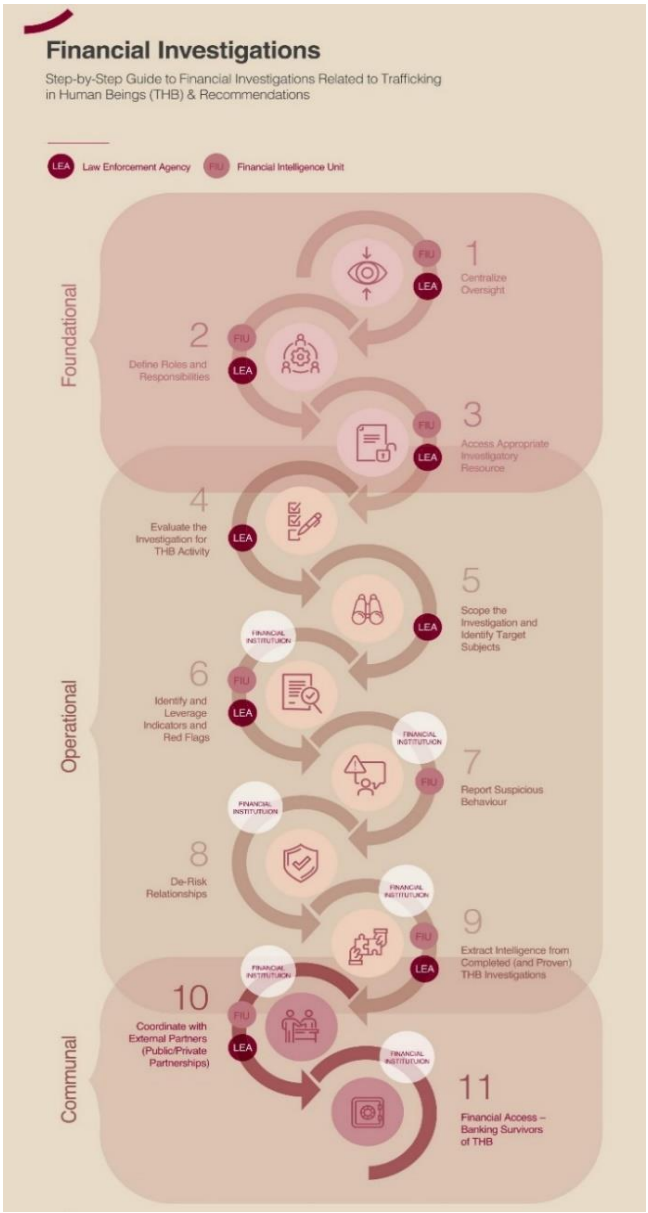
Dochodzenia finansowe w sprawie handlu ludźmi muszą uwzględniać te czynniki ekonomiczne. Analizując transakcje finansowe, marże zysku i nielegalne przepływy pieniężne, organy ścigania mogą identyfikować wzorce wykorzystywania, rozbijać sieci i osłabiać bodźce finansowe stojące za handlem ludźmi. Zrozumienie handlu ludźmi jako przedsięwzięcia ekonomicznego ma kluczowe znaczenie dla opracowania skutecznych środków zaradczych, w tym ram regulacyjnych, nadzoru finansowego i ukierunkowanych interwencji. W następnej sekcji przedstawiono ogólne ramy dochodzeń finansowych w sprawach handlu ludźmi oraz konkretne kroki, które należy podjąć.

9.5.3 Przewodnik krok po kroku po dochodzeniach finansowych związanych z handlem ludźmi (THB)

W tej sekcji przedstawiono **jedenaście kluczowych kroków** skutecznego prowadzenia dochodzeń finansowych w sprawach handlu ludźmi. Kroki te podzielono na trzy obszary: *podstawowy* , *operacyjny* i *wspólnotowy* .

Kroki podstawowe są zazwyczaj podejmowane jednorazowo w trakcie tworzenia ram dochodzeniowych i mają szerokie zastosowanie zarówno w sektorze publicznym, jak i prywatnym. Kroki operacyjne są częściej stosowane ze względu na ich znaczenie dla poszczególnych dochodzeń, choć ich wdrażanie różni się w zależności od podmiotu publicznego i prywatnego. Na przykład, kroki 7 i 8 dotyczą głównie podmiotów sprawozdawczych w sektorze prywatnym. Wreszcie, kroki wspólnotowe są podzielone pod względem zakresu zastosowania: oba sektory są zainteresowane krokiem 10, podczas gdy dostawcy usług finansowych ponoszą większą odpowiedzialność za krok 11.

Rysunek 14 przedstawia schematyczny proces krok po kroku pomiędzy lokalnymi organami ścigania a jednostkami analityki finansowej. Rysunek ten pochodzi z raportu OSCE (2020).



Rys. 4. Etapy śledztwa finansowego

Krok 1: Pierwszym krokiem w skutecznym dochodzeniu finansowym w sprawie handlu ludźmi jest **ustanowienie scentralizowanego mechanizmu nadzoru** . Zapewnia on skoordynowaną i kompleksową reakcję na każdy podejrzany przypadek, choć jego struktura może się różnić w zależności od wielkości i uprawnień danej instytucji. Organy ścigania często integrują dochodzenia w sprawie handlu ludźmi w ramach **wyspecjalizowanych jednostek** . Na przykład Departament Policji Nowego Jorku (NYPD) i londyńska Policja Metropolitalna (MPS) mają dedykowane zespoły, podczas gdy Policja w Toronto (TPS) zajmuje się sprawami handlu ludźmi w ramach swojej Jednostki ds. Przestępstw Seksualnych, uznając ich odrębność od przestępstw związanych z niedozwolonymi praktykami. Agencje federalne, takie jak FBI i Interpol, również centralizują wiedzę specjalistyczną, podobnie jak jednostki analityki finansowej (FIU), choć te ostatnie często działają z mniejszą widocznością społeczną.

W **sektorze prywatnym** , a zwłaszcza w bankach, nadzór jest mniej ustrukturyzowany ze względu na dużą liczbę transakcji i wymogi regulacyjne. Wiele instytucji utrzymuje jednak **specjalne zespoły dochodzeniowe** , które zajmują się przestępstwami finansowymi, w tym handlem ludźmi. Centralizacja działań dochodzeniowych oferuje szereg korzyści, w tym ograniczenie powielania, poprawę efektywności, poszerzenie wiedzy specjalistycznej i umożliwienie kompleksowej analizy danych. Wiąże się ona jednak również z ryzykiem, takim jak ograniczenie wiedzy do wybranej grupy i potencjalne opóźnienia w dochodzeniach. Aby zminimalizować te ryzyka, instytucje powinny promować inicjatywy dzielenia się wiedzą i zapewniać elastyczność w zakresie obowiązków dochodzeniowych, aby zapobiegać powstawaniu wąskich gardeł. Ostatecznie, o ile sprawy są rejestrowane i odpowiednio zarządzane, dochodzenia mogą być prowadzone przez różne zespoły, co przynosi korzyści zarówno interesariuszom wewnętrznym, jak i zewnętrznym.

Krok 2: Po ustanowieniu ram nadzoru nad dochodzeniami w sprawie handlu ludźmi kluczowe jest jasne określenie ról i obowiązków osób zaangażowanych. Chociaż jest to standardowa praktyka w wielu instytucjach publicznych i prywatnych, czasami jest pomijana. Jasno **określone obowiązki** pomagają zapobiegać powielaniu działań, zwiększają efektywność operacyjną i przynoszą dodatkowe korzyści, takie jak sprawniejsze planowanie sukcesji, skuteczniejsza selekcja spraw, lepsza priorytetyzacja dochodzeń oraz spójna komunikacja wewnątrz i na zewnątrz zespołu. **Dokumentowanie ról** zapewnia sprawniejsze i terminowe prowadzenie dochodzeń. Ostatecznie takie podejście opiera się na zasadzie „dziel i rządź" – gdy każdy rozumie swoją rolę, może skupić się na realizacji. Bez jasno określonych obowiązków, nawet dobrze zamierzone działania mogą skutkować niespójnym i nieskutecznym procesem dochodzeniowym.

Krok 3: Skuteczne śledztwo wymaga **dostępu do odpowiednich zasobów** , które mogą się różnić w zależności od charakteru śledztwa. Dochodzenia finansowe, szczególnie te dotyczące prania pieniędzy i handlu ludźmi, wymagają **specjalistycznych narzędzi,** różniących się od tych stosowanych w terenie. Biorąc pod uwagę złożoność śledzenia przepływów finansowych, śledczy muszą być wyposażeni w odpowiednie zasoby, aby skutecznie analizować transakcje, łączyć powiązane sprawy i dostosowywać się do zmieniających się taktyk przestępczych.

Zapewnienie śledczym niezbędnych narzędzi zwiększa efektywność, jakość śledztw i zwiększa prawdopodobieństwo skutecznych aresztowań i skazań. Kluczowe zasoby obejmują:

- **Cyfrowe systemy zarządzania sprawami:** scentralizowana baza danych do przechowywania notatek i dowodów w sprawie umożliwia lepsze śledzenie sprawy i łączenie śledztw

- **Nieograniczony dostęp do Internetu:** Śledczy mogą potrzebować dostępu do witryn o ograniczonym dostępie, takich jak platformy z treściami dla dorosłych, podczas śledzenia działań związanych z handlem ludźmi, pod warunkiem, że otrzymają odpowiednie szkolenie w zakresie zapobiegania nadużyciom.
- **Szkolenia OSINT:** Specjalistyczne szkolenia w zakresie śledztw internetowych pomagają w odkrywaniu kluczowych informacji i ochronie tożsamości śledczych.
- **Dostęp do danych wewnętrznych:** Natychmiastowa dostępność istotnych danych instytucjonalnych, takich jak rejestry transakcji czy akta wcześniejszych spraw, jest niezbędna. Pokonywanie barier technologicznych, prawnych i biurokratycznych w dostępie do danych poprawia efektywność dochodzeń.
- **Ekspercka konsultacja prawna:** Przestępstwa finansowe często dotyczą podatków, papierów wartościowych i nieruchomości, co wymaga konsultacji ze specjalistami. Wczesne zidentyfikowanie ekspertów prawnych i finansowych wzmacnia skuteczność śledztwa.

Dostęp do zasobów ma kluczowe znaczenie, jednak instytucje muszą znaleźć równowagę między efektywnością a względami prawnymi i etycznymi, dbając o to, aby śledczy działali w ramach obowiązujących przepisów, maksymalizując jednocześnie swoje możliwości śledcze.

Krok 4: Jednym z kluczowych wyzwań w dochodzeniach finansowych dotyczących handlu ludźmi jest ryzyko błędnej identyfikacji przestępstw – pomylenia innego przestępstwa z handlem ludźmi lub pominięcia jego przesłanek. Może to wynikać z braku wiedzy prawnej lub nakładania się cech przestępstw, takich jak przemyt ludzi czy naruszenia przepisów prawa pracy. Rozróżnienie tych przestępstw ma kluczowe znaczenie, szczególnie dla śledczych zarówno w sektorze publicznym, jak i prywatnym. Instytucje prywatne powinny również określić, które przestępstwa bazowe będą

analizowane przez ich wyspecjalizowane zespoły, ponieważ jednostki specjalizujące się wyłącznie w handlu ludźmi są rzadkością ze względu na ograniczone zasoby. Po uzyskaniu podstawowej wiedzy na temat przepisów dotyczących handlu ludźmi i obowiązków śledczych, śledczy mogą dopracować swoje podejście do obsługi zgłoszeń. Instytucje sektora publicznego zazwyczaj otrzymują większą liczbę zgłoszeń związanych z handlem ludźmi ze względu na ich szersze uprawnienia, podczas gdy zespoły sektora prywatnego mogą mieć mniej spraw, ale większe możliwości proaktywnego śledztwa. Strategie proaktywne obejmują:

- **Przeglądanie wcześniej zamkniętych spraw:** Starsze sprawy błędnie oznaczone jako prostytucja lub przemyt mogą zawierać pominięte dowody handlu ludźmi
- **Przeprowadzanie historycznych, niekorzystnych badań w mediach:** Przeglądanie doniesień prasowych na temat podejrzanych handlarzy ludźmi może ujawnić powiązania finansowe lub wzorce w rachunkach instytucji
- **Analiza SAR:** Analiza historycznych danych SAR może pomóc w identyfikacji przeoczonych sygnałów ostrzegawczych związanych z handlem ludźmi
- **Monitorowanie sektorów biznesu wysokiego ryzyka:** Branże takie jak salony masażu, kluby ze striptizem i pornografia są powiązane z handlem ludźmi i wymagają dokładniejszej kontroli.

Skuteczne dochodzenia finansowe wymagają zarówno działań reaktywnych, jak i proaktywnych. Ich sukces zależy jednak od jakości udostępnianych informacji wywiadowczych – zapewnienia, że dobrze udokumentowane raporty SAR dotrą do organów ścigania i szybko podejmą stosowne działania.

Krok 5: Dobrze zdefiniowany zakres śledztwa jest kluczowy, aby zapobiec rozrostowi spraw i uniknąć błędnego utożsamiania niewinnych osób z działalnością przestępczą. W dochodzeniach dotyczących handlu ludźmi handlarze ludźmi często wykorzystują konta bankowe swoich ofiar dla osobistych korzyści, dlatego kluczowe jest, aby organizacje miały politykę zapobiegającą dalszej wiktymizacji. **Priorytetem jest wyraźne rozróżnienie handlarzy od ofiar** , a następnie **identyfikacja głównych sprawców przed pośrednikami** . To podejście oparte na ryzyku optymalizuje zasoby i zapewnia skuteczność śledztwa.

Aby precyzyjnie określić zakres dochodzenia, musi ono być jak najbardziej kompleksowe od samego początku. Na przykład Model 360, opracowany przez Petera Warracka, oferuje ustrukturyzowaną metodę oceny aktywności finansowej pod kątem potencjalnego prania pieniędzy i może być stosowany zarówno w prywatnych instytucjach finansowych, jak i w organach ścigania. Model składa się z sześciu kroków:

1. **Wydarzenie wyzwalające** – dochodzenie rozpoczyna się od alertu, takiego jak SAR, flaga automatycznego monitorowania transakcji, niekorzystne informacje w mediach, wewnętrzne skierowanie lub żądanie organów ścigania.
2. **Zrozumienie klienta** – badacze zbierają informacje kontekstowe na dany temat, w tym informacje o zatrudnieniu, sytuacji finansowej i ogólnym profilu klienta.
3. **Zrozumienie aktywności finansowej** – zachowanie finansowe klienta jest oceniane w kontekście jego znanej przeszłości, aby ustalić, czy jest zgodne z oczekiwaniami.
4. **Wyeliminuj normę** – transakcje, które wydają się klientowi normalne, są filtrowane, co pozwala śledczym skupić się na naprawdę podejrzanej aktywności.

5. **Analiza pozostałej aktywności finansowej** – Śledztwo koncentruje się na aktywności, która wzbudziła początkowe podejrzenia, analizując wzorce i potencjalne powiązania z nielegalnym postępowaniem.
6. **Złóż raport i rozważ pozbycie się inwestycji** – jeśli dochodzenie potwierdzi podejrzenia, należy złożyć raport SAR do lokalnej jednostki analityki finansowej, a w przypadku organów ścigania może zostać wydany nakaz aresztowania.

Dzięki takiemu ustrukturyzowanemu podejściu zasoby śledcze koncentrują się na uzasadnionych zagrożeniach, minimalizując liczbę fałszywych alarmów i zwiększając ogólną skuteczność.

Krok 6: Zrozumienie, co stanowi podejrzaną aktywność finansową w kontekście handlu ludźmi, wymaga zarówno ogólnej wiedzy o praktykach bankowych, jak i dogłębnej znajomości metod stosowanych przez handlarzy. O ile podstawowa wiedza bankowa jest stosunkowo łatwa do zdobycia, rozpoznawanie anomalii często wymaga dostępu do obszernych danych i praktycznego doświadczenia w prowadzeniu śledztw. Biorąc jednak pod uwagę obszerną dokumentację dotyczącą zachowań finansowych handlarzy, badania mogą zrekompensować brak bezpośredniego doświadczenia.

Na poziomie makro **wskaźniki THB** można podzielić na trzy kategorie:

1. **Wskaźniki behawioralne** – są to wizualne sygnały widoczne gołym okiem, które mogą sugerować, że dana osoba jest ofiarą handlu ludźmi lub że jest handlarzem ludźmi.
2. **Wskaźniki KYC (Know Your Customer, Poznaj Swojego Klienta)** – sygnały ostrzegawcze oparte na informacjach podanych przez klienta, takie jak nieścisłości w identyfikacji lub adresie.

3. **Wskaźniki transakcyjne** – podejrzane wzorce finansowe, które mogą pojawić się w dowolnym momencie po otwarciu konta, często bez osobistej interakcji, szczególnie w związku z rozwojem bankowości cyfrowej.

Wskaźniki te mogą pojawiać się niezależnie lub w połączeniu i mogą być wykrywane przez różne zespoły w organizacji – personel pierwszej linii identyfikujący sygnały behawioralne, zespoły zbierające dane wykrywające sygnały ostrzegawcze KYC oraz zespoły monitorujące transakcje, rozpoznające anomalie finansowe. Jasna komunikacja i protokoły eskalacji są niezbędne, aby zapewnić dokładne zbadanie potencjalnie podejrzanych działań. Segmentacja wskaźników na te trzy kategorie jest zgodna z ramami opracowanymi przez Thomson Reuters i Banks Alliance w Europie, Azji i Stanach Zjednoczonych. Ich zestawy narzędzi dostarczają dodatkowych informacji, w tym względnej siły każdego wskaźnika i jego związku z konkretnymi formami handlu ludźmi, takimi jak wyzysk pracowników.

Należy pamiętać, że niektóre wskaźniki, takie jak częste zakupy w aptece, same w sobie mogą nie budzić podejrzeń. Dlatego analitycy muszą rozważyć wiele czynników łącznie, aby ustalić uzasadnione podstawy do podejrzeń. Jest to zgodne z wytycznymi agencji wywiadu finansowego, w tym:

- **FINTRAC** (Kanada, 2016): „Pojedyncza transakcja rozpatrywana w oderwaniu od reszty może prowadzić do błędnego założenia o normalności. Analiza wszystkich wskaźników może ujawnić nieznane powiązania, które razem wzięte mogłyby dać uzasadnione podstawy do podejrzeń o handel ludźmi”.
- **FinCEN** (USA, 2014): „Żadna pojedyncza czerwona flaga transakcyjna nie jest jednoznacznym wskaźnikiem działalności związanej z przemytem ludzi lub handlem ludźmi. Należy również wziąć pod uwagę dodatkowe czynniki, takie jak przewidywana aktywność finansowa klienta”.

Zarówno FINTRAC, jak i FinCEN podkreślają znaczenie ustrukturyzowanego podejścia dochodzeniowego, takiego jak Model 360 Warracka, aby zapewnić ocenę sygnałów ostrzegawczych w kontekście, a nie w izolacji. Pełną listę syntetycznych wskaźników można znaleźć w załącznikach do Kompendium Zasobów **OBWE i Przewodnika krok po kroku dochodzeń finansowych w sprawie handlu ludźmi (OBWE, 2019)** .

Krok 7: Raporty SAR odgrywają kluczową rolę w dochodzeniach finansowych zarówno w sektorze publicznym, jak i prywatnym. Tradycyjnie, raport SAR kończy dochodzenie prowadzone przez instytucję prywatną, zazwyczaj instytucję finansową, taką jak bank, która następnie przekazuje raport do swojej jednostki analityki finansowej (FIU). W przypadku instytucji publicznych raport SAR może zainicjować dochodzenie organów ścigania. Aby jednak zmaksymalizować ich potencjał, raporty SAR należy postrzegać jako cenne narzędzie w całym procesie dochodzeniowym, a nie tylko jako ostatni etap lub punkt wyjścia do dochodzeń publicznych. Mogą one dostarczać użytecznych informacji na różnych etapach, przyczyniając się do trwających dochodzeń lub dostarczając kontekstu do wewnętrznych dochodzeń w instytucjach prywatnych.

W **sektorze prywatnym** zaleca się stosowanie rozwiązań technicznych, które zmniejszą obciążenie administracyjne związane z rutynowym wprowadzaniem danych, umożliwiając śledczym skupienie się na szczegółowych aspektach podejrzanych działań. Ponadto dane z poprzednich raportów SAR powinny być łatwo dostępne, aby umożliwić identyfikację wzorców, wykrywanie unikalnych przestępstw i śledzenie zaangażowanych podmiotów. Raporty SAR powinny również odwoływać się do poprzednich raportów dotyczących tej samej siatki przestępczej, aby zbudować spójną narrację i uniknąć powielania zgłoszeń. Ważne jest, aby instytucje raportujące przestrzegały konwencji nazewnictwa ustalonych przez krajowe jednostki analityki finansowej (FIU), szczególnie w przypadku głośnych przestępstw, takich jak handel ludźmi. Przestrzeganie tych

konwencji pomaga zapewnić zgodność z oczekiwaniami regulacyjnymi, zwiększa wiarygodność instytucji w raportowaniu i pomaga w identyfikacji trendów w przestępczości finansowej. Na przykład amerykański FinCEN zaleca oznaczanie raportów SAR dotyczących handlu ludźmi jako „Doradczy handel ludźmi", podczas gdy kanadyjski FINTRAC sugeruje używanie etykiety „Project Protect". Instytucje nieposiadające tych systemów kodowania mogłyby rozważyć partnerstwa publiczno-prywatne w celu ich wdrożenia.

W **sektorze publicznym** zaleca się wykorzystywanie baz danych SAR jednostek analityki finansowej (FIU) we wszystkich dochodzeniach dotyczących handlu ludźmi, ponieważ przestępstwo to zazwyczaj wiąże się z korzyściami finansowymi. Organy ścigania powinny również korzystać z narzędzi, takich jak nakazy produkcji i nakazy sądowe, aby zachęcić banki i inne podmioty sprawozdawcze do składania raportów SAR związanych z toczącymi się dochodzeniami. Pomimo ich znaczenia, raporty SAR są krytykowane za rosnącą liczbę raportów niskiej jakości. Na przykład raport OBWE z 2014 r. podkreślił, że we Włoszech tylko 23 z 37 000 raportów SAR uznano za przydatne w dochodzeniach karnych. Brytyjska komisja ds. reformy prawa z 2019 r. wyraziła podobne obawy, sugerując potrzebę usprawnienia raportowania SAR w celu zmniejszenia liczby zgłoszeń niskiej jakości. Wdrażając niektóre z wymienionych zaleceń, takie jak odwoływanie się do historycznych raportów SAR, można poprawić jakość przyszłych raportów.

Krok 8: Po zakończeniu dochodzenia w instytucji prywatnej, takiej jak bank, należy podjąć decyzję o kontynuowaniu relacji z klientem, którego dotyczy dochodzenie. Ten proces, znany jako **„de-risking",** obejmuje w razie potrzeby zakończenie relacji. Ważne jest rozróżnienie między ofiarą a sprawcą, aby uniknąć niesłusznego ukarania ofiary, zwłaszcza w przypadkach takich jak handel ludźmi. Jeśli konto należy do ofiary handlu ludźmi, należy dołożyć starań, aby utrzymać relację, chyba że dochodzi do licznych

naruszeń lub współudziału. Do de-riskingu należy podchodzić ostrożnie, ponieważ wprowadzanie podejrzanych działań na nielegalne rynki może utrudnić dochodzenia organów ścigania. W niektórych jurysdykcjach organy ścigania mogą zażądać pozostawienia otwartych kont bankowych, aby uniknąć zakłócania dochodzeń. Jeśli de-risking okaże się konieczny, należy stosować standardowe komunikaty, aby uniknąć fałszywych oskarżeń, a także przechowywać dokumentację podmiotów, którym wcześniej umorzono ryzyko, do wglądu w przyszłości.

Krok 9: Identyfikacja rzeczywistych przypadków handlu ludźmi wyłącznie na podstawie transakcji finansowych jest trudna ze względu na brak informacji kontekstowych. Ponadto, to, czy śledczy pracują w instytucji publicznej, czy w organizacji prywatnej, wpływa na prawdopodobieństwo znalezienia rozstrzygających przypadków handlu ludźmi. Organizacje prywatne, takie jak dostawcy usług finansowych, nie mają obowiązku udowodnienia ponad wszelką wątpliwość, że doszło do przestępstwa bazowego przed złożeniem raportu bezpieczeństwa informacji (SAR) do jednostki analityki finansowej (FIU). Próg raportowania jest często niski, ponieważ instytucje finansowe widzą tylko część ogólnego obrazu. Co więcej, jednostki analityki finansowej zazwyczaj nie udzielają informacji zwrotnej na temat tego, czy raporty bezpieczeństwa informacji (SAR) prowadzą do potwierdzonych przestępstw bazowych, co utrudnia sektorowi prywatnemu weryfikację działań związanych z handlem ludźmi.

Ponieważ transparentność wyników dochodzeń finansowych w sprawie handlu ludźmi nie zawsze jest możliwa, należy wykorzystywać udowodnione przypadki, aby ułatwić szkolenia i ograniczyć przyszłe ryzyko. Dostawcy usług finansowych mogą identyfikować udowodnione przypadki handlu ludźmi poprzez:

- Przeglądanie codziennych negatywnych doniesień medialnych w celu znalezienia powiązań z wewnętrznymi dochodzeniami.

- Subskrybowanie aktualizacji od organów ścigania lub jednostek analityki finansowej na temat egzekwowania prawa w zakresie handlu ludźmi i porównywanie ich z wewnętrznymi sprawami.
- Utworzenie bezpośredniego kanału zgłaszania przypadków handlu ludźmi dla organów ścigania.

Zaleca się dzielenie się informacjami z udowodnionych przypadków handlu ludźmi z szerszym zespołem śledczym, a nie tylko ze specjalistyczną jednostką ds. handlu ludźmi . Jest to zgodne z wytycznymi w Kroku 1 (Centralizacja Nadzoru) i może podnieść morale śledczych, stworzyć poczucie celu oraz poprawić alokację zasobów lub współpracę między zespołami.

Krok 10: W ostatnich latach **znaczenie i popularność partnerstw publiczno-prywatnych (PPP) w zwalczaniu przestępstw finansowych** , w szczególności handlu ludźmi w biznesie, **znacznie wzrosły** . Globalne wysiłki na rzecz wyeliminowania handlu ludźmi doprowadziły do zacieśnienia współpracy między konkurentami w branży w celu zwalczania przestępstw finansowych. Specjaliści ds. zwalczania przestępstw finansowych zdali sobie sprawę, że handlarze ludźmi przemieszczają się między różnymi instytucjami i bankami, co skłoniło do współpracy w celu rozwiązania tych problemów. Do wiodących PPP należą brytyjska Joint Money Laundering Intelligence Taskforce (JMLIT), australijski Fintel Alliance i kanadyjski Project Protect. Stany Zjednoczone również posiadają mechanizmy, takie jak ustawa PATRIOT 314(a), dotyczące wymiany informacji.

Zachęty do udziału w partnerstwach partnerskich obejmują możliwość zapoznania się z różnorodnymi podejściami w dochodzeniach finansowych, szybsze opracowywanie wskaźników handlu ludźmi, budowanie silniejszych relacji z partnerami i organami ścigania, usprawnienie dochodzeń, dzielenie się zasobami oraz zaangażowanie w dobro

społeczne. OBWE dostrzega jednak wyzwania w nawiązywaniu efektywnej współpracy między jednostkami analityki finansowej, organami ścigania i podmiotami składającymi zgłoszenia transakcji (STR). Jednym z takich wyzwań jest jednostronny przepływ informacji z jednostek analityki finansowej, który często ogranicza ich możliwości udostępniania informacji wywiadowczych poza swoją organizacją. Informacje zwrotne na temat wysokiej jakości zgłoszeń transakcji (STR) mogą poprawić szkolenia, metody wykrywania i jakość poszukiwań i ratownictwa (SAR).

Brak informacji zwrotnej od jednostek analityki finansowej (FIU) i brak międzynarodowych baz danych dotyczących przestępców handlu ludźmi podkreślają potrzebę partnerstwa publiczno-prywatnego (PPP). Stworzenie PPP nie zawsze wymaga nowych przepisów; można wykorzystać istniejące ramy prawne. Na przykład, kanadyjski Project Protect z powodzeniem działał w ramach ram prawnych swojego rządu, koncentrując się na ogólnych typologiach i wskaźnikach, jednocześnie przestrzegając przepisów dotyczących prywatności. Kluczowe jest zrozumienie ograniczeń prawnych i praca w ich ramach, aby wspierać współpracę. Długoterminowe cele PPP mogą obejmować promowanie zmian w przepisach w oparciu o udaną współpracę. Rozpoczęcie lub udział w PPP powinno nastąpić po ustanowieniu solidnego procesu dochodzeniowego, ale wczesna współpraca jest cenna. Może ona dostarczyć spostrzeżeń, które ukształtują proces dochodzeniowy w sposób, który byłby trudny do osiągnięcia po jego wdrożeniu. Udział w PPP zwiększy kompleksowość podejścia do badania handlu ludźmi.

Krok 11: Dochodzenia w sprawie handlu ludźmi, szczególnie w sektorze bankowym, mogą mieć negatywny wpływ na ofiary. Podkreśla to wagę Kroku 4 (Ocena dochodzenia pod kątem działalności związanej z handlem ludźmi), który zapewnia jasne zdefiniowanie działań związanych z handlem ludźmi na poziomie zespołu lub instytucji. Prawidłowe wykonanie Kroku 4 może pomóc w ograniczeniu zbędnej pracy w przyszłości,

zapewniając, że niewinne osoby nie zostaną niesłusznie wykluczone. Ponieważ handlarze ludźmi często manipulują sytuacją finansową swoich ofiar, zaleca się, aby ofiarom, które uniknęły handlu ludźmi, umożliwiono odbudowę ich sytuacji finansowej.

Udanym przykładem wsparcia dla ofiar handlu ludźmi jest program uruchomiony przez HSBC w Wielkiej Brytanii w czerwcu 2019 roku. Program ten pomaga ofiarom skierowanym przez brytyjski Narodowy Mechanizm Skierowań w pokonywaniu trudności, takich jak przedstawienie dowodu adresu i tożsamości. Ponadto, projekt inicjatywy Lichtenstein Initiative na rzecz mobilizacji finansowania działań przeciwko niewolnictwu i handlowi ludźmi, opracowany we współpracy z Uniwersytetem Narodów Zjednoczonych i różnymi rządami, zgromadził kilka instytucji finansowych w celu rozszerzenia działań HSBC na różne instytucje i jurysdykcje. Scotiabank, we współpracy z programem Deborah's Gate Armii Zbawienia, mającym na celu zwalczanie handlu ludźmi, był pierwszym bankiem, który otworzył konta dla ofiar w ramach tej inicjatywy na rzecz włączenia finansowego. Oczekuje się, że inne uczestniczące instytucje finansowe pójdą w jego ślady i opracują podobne programy.

Ponieważ uwaga i wysiłki nadal koncentrują się na osobach ułatwiających handel ludźmi, **ważne jest, aby nie tracić z oczu ofiar** . Partnerstwa publiczno-prywatne i współpraca z organizacjami międzyrządowymi mogą stworzyć kompleksowe podejście do zwalczania handlu ludźmi, przynosząc korzyści nie tylko zaangażowanym instytucjom, ale także ofiarom, często przy minimalnych kosztach realizacji.

9.5.4 Identyfikacja podejrzanej aktywności finansowej

OBWE opublikowała **listę wskaźników finansowych transakcji i tzw. czerwonych flag, które mają zastosowanie w przypadku handlu ludźmi, a zwłaszcza wyzysku**

w pracy. Poniższa lista została zaczerpnięta z raportu OBWE, a trzy pozornie specyficzne wskaźniki dotyczące pobierania organów oraz siedem dotyczące wyzysku seksualnego zostały usunięte, aby uczynić ją bardziej odpowiednią dla wyzysku w pracy nawet jeśli w szczególnych przypadkach wskaźniki mogą się różnić i nakładać (OBWE, 2019, s. 61 i nast.).

- Wykorzystanie tzw. „słupów” przy transakcjach na kontach komercyjnych
- Niepłacenie podatków, odszkodowań pracowniczych i innych opłat organowi podatkowemu
- Stawka wynagrodzenia za każdy okres rozliczeniowy jest taka sama (brak zmian w przypadku nadgodzin, urlopu, zwolnienia lekarskiego, premii itp.) w przypadku stanowisk, na których budzi to wątpliwości
- Powtarzające się wypłaty wynagrodzeń w bezpodstawnie niskich kwotach (na przykład znacznie niższych niż płaca minimalna)
- Znaczny udział kapitału spółki w lokatach bezterminowych – niewspółmierne obroty finansowe
- Pożyczki udzielone przez akcjonariusza powiązanej osobie prawnej i późniejsze przeniesienie zwrotne, pożyczka fikcyjna
- Strukturyzacja za pośrednictwem podmiotów gospodarczych i przekazywanie pieniędzy za pomocą umowy pożyczki
- Nadmierne wspólne przejazdy samochodem po północy
- Brak wydatków na utrzymanie, takich jak żywność, benzyna, media i czynsz
- Zakupy w restauracji i obsługa hotelowa, brak pokoi
- Korzystanie z usług wielu osób do prowadzenia działalności bankowej

- Wysokie i/lub częste wydatki na lotniskach, w portach, innych węzłach komunikacyjnych lub za granicą, niezgodne z osobistym wykorzystaniem danej osoby lub deklarowaną działalnością gospodarczą za granicą
- Wpłaty gotówkowe realizowane w różnych miastach na terenie kraju
- Płatności na rzecz agencji zatrudnienia lub agencji rekrutujących studentów, które nie posiadają licencji/zarejestrowania lub naruszają przepisy prawa pracy
- Relatywnie wysokie wydatki na pozycje niezgodne z deklarowanym celem działalności
- Transakcje mające miejsce poza czasem trwania znanych operacji biznesowych
- Transgraniczne transfery środków niezgodne z zadeklarowanym celem działalności posiadacza rachunku i/lub pomiędzy niewyjaśnionymi wzorcami transakcji transgranicznych pomiędzy znanymi szlakami handlu ludźmi lub obszarami, na których istnieje większe ryzyko handlu ludźmi
- Szerokie wykorzystanie gotówki, w tym na zakup aktywów przedsiębiorstw
- Przelewy krajowe z firm działających w sektorach wrażliwych na oszustwa społeczne, pieniądze wypłacane są natychmiast w gotówce
- Korzystanie z instytucji nienależących do systemu finansowego (nietradycyjne)
- Korzystanie z usług kuriera gotówkowego i wielokrotne wypłaty gotówki
- Zakup weksli bankowych płatnych na rzecz kasyna bezpośrednio po dokonaniu wpłaty
- Niewyjaśnione/nieuzasadnione duże zyski dla firmy
- Wpłaty gotówkowe często nieznacznie poniżej progu sprawozdawczego
- Wpłaty gotówkowe w kilku oddziałach lub bankomatach

- Zakup przekazów pieniężnych w celu opłacania rachunków zamiast wypisywania czeków osobistych
- Konta firmowe z widocznymi potrąceniami z wynagrodzeń pracowników w różnych rodzajach kosztów, takich jak mieszkanie i żywność
- Wypłacone czeki, w przypadku których większość środków jest albo deponowana z powrotem na koncie pracodawcy, albo jest przez niego przechowywana
- Nadawca lub beneficjent z niekompletnymi danymi
- Zakup weksli bankowych płatnych na rzecz kasyna bezpośrednio po dokonaniu wpłaty
- Przelewy z różnych regionów do tych samych osób w krajach znanych z wyższego ryzyka handlu ludźmi
- Czeki z pomocą rządową wpłacane na konto, nawet jeśli posiadacz posiada znaczną sumę pieniędzy
- Przelewy/transfery elektroniczne mogą być również ustrukturyzowane
- Mieszanie gotówki z legalnymi źródłami dochodu
- Działalność rafineryjna (wymiana banknotów o niskich nominałach na banknoty o wyższych nominałach)
- Częste zakupy wielokrotności małych kwot Bitcoinów lub walut wirtualnych bezpośrednio przez klienta lub za pośrednictwem giełdy
- Przelewy środków z udziałem stron trzecich, których nazwy alternatywne podano w nawiasach
- Na konto wpływają wypłaty wynagrodzeń z legalnych, często ogólnopolskich agencji zatrudnienia, ale środki pozostają nietknięte przez długi czas

- Restauracje typu fast food: częste zakupy o niskiej wartości w stosunkowo krótkich odstępach czasu i niezgodne z oczekiwaną aktywnością
- Konto wyglądające na „lejkowe”

Poniższe studium przypadku autorstwa Francavilli Lyon i De Cock (2024) ilustruje, jak wzorce transakcji finansowych mogą służyć jako wskaźniki potencjalnego wyzysku pracowników w sektorze hotelarsko-gastronomicznym. Przykład ten podkreśla kluczową rolę analizy finansowej w identyfikacji ryzyka handlu ludźmi i wykrywaniu ukrytych form współczesnego niewolnictwa:

Sytuacja wyjściowa: Obywatel Chin otwiera konto prywatne i podaje, że pracuje w restauracji X. Analiza relacji biznesowej pokazuje, że adres tej osoby i adres restauracji X są identyczne. Część napływających wynagrodzeń jest wypłacana ponownie w gotówce lub przekazywana osobom trzecim (bez oczywistych powiązań rodzinnych). Wypłaty wynagrodzeń są dokonywane nieregularnie i w zmiennych kwotach. Podczas rozmowy między bankiem a klientem, ten ostatni powiedział bankowi, że zagraniczne płatności były alimentami, które płacił swojej byłej żonie i ich dzieciom. Jednak według KYC klient nie ma dzieci. Ponadto, zgodnie z umową o pracę, klient ma stałe stanowisko ze stałym wynagrodzeniem i nie pracuje za stawkę godzinową. Brakuje przewidywanych codziennych wydatków (jedzenie, czynsz, ubezpieczenie itp.).

Wskaźnikami w tym scenariuszu są:

- Narodowość ryzyka (klient)
- Sektor narażony na zjawisko wyzysku pracowników
- Transakcje tranzytowe
- Transakcje gotówkowe
- Brak przewidywanych codziennych wydatków

- Adres prywatny identyczny z adresem służbowym
- Sprzeczne oświadczenia klienta

9.5.5 Wyzwania w dochodzeniach finansowych

Istotnym wyzwaniem w dochodzeniach finansowych jest ewolucja **technik maskowania** stosowanych przez przestępców do ukrywania śladów finansowych. Techniki takie jak **usługi mieszania**, **przeskakiwanie łańcuchowe (chain hopping**) oraz wykorzystywanie **kryptowalut nastawionych na prywatność** stanowią poważne przeszkody dla śledczych. Na przykład usługi mieszania, znane również jako tumblery, pozwalają użytkownikom ukryć pochodzenie swoich środków poprzez ich łączenie i redystrybucję. Przeskakiwanie łańcuchowe polega na szybkiej konwersji kryptowalut między różnymi platformami, co utrudnia śledzenie przepływu środków. Ponadto kryptowaluty zapewniające prywatność, takie jak Monero i Zcash, oferują ulepszone funkcje anonimowości, co dodatkowo komplikuje działania organów ścigania.

Aby sprostać tym wyzwaniom, śledczy finansowi coraz częściej polegają na **współpracy z ekspertami w dziedzinie informatyki śledczej** . Informatyka śledcza umożliwia śledczym pozyskiwanie i analizowanie dowodów elektronicznych, takich jak zaszyfrowana komunikacja, adresy IP i metadane transakcji. To interdyscyplinarne podejście ma kluczowe znaczenie dla wykrywania ukrytych sieci finansowych i śledzenia nielegalnych przepływów finansowych przez granice. Biorąc pod uwagę transnarodowy charakter przestępstw finansowych, współpraca między instytucjami finansowymi, organami regulacyjnymi i organizacjami międzynarodowymi jest niezbędna dla skutecznego prowadzenia śledztw finansowych. „Innowacyjne metody transferu pieniędzy w połączeniu z rosnącą świadomością wśród specjalistów ds. zwalczania przestępstw finansowych, że handlarze przeskakują z instytucji do instytucji, z banku do banku, skłoniły ich do współpracy” (OBWE, 2019, s. 43).

9.5.6 Rozwój technologiczny i trendy

Ostatnie osiągnięcia technologiczne znacząco wpłynęły na przestępczość finansową, kształtując nowe metody nielegalnej działalności, a jednocześnie dostarczając udoskonalonych narzędzi do prowadzenia dochodzeń finansowych. Rozwój kryptowalut i technologii blockchain, na przykład, ułatwił rozwój różnych form przestępczości finansowej, w tym prania pieniędzy, oszustw, a nawet handlu ludźmi. Rosnące wykorzystanie **aktywów cyfrowych** umożliwia przestępcom transfer środków przez granice z zachowaniem większej anonimowości, z pominięciem tradycyjnych instytucji finansowych i kontroli regulacyjnych. Chociaż **Bitcoin** pozostaje najpopularniejszą kryptowalutą, obserwuje się coraz większe przesunięcie w stronę alternatyw bardziej nastawionych na prywatność, takich jak **Monero** i **Zcash**, co dodatkowo komplikuje działania organów ścigania.

Jednym z głównych trendów jest stosowanie **technik zaciemniania,** zaprojektowanych specjalnie dla aktywów cyfrowych. Przestępcy coraz częściej wykorzystują narzędzia takie jak **miksery** , **wirówki** i **portfele prywatne,** aby ukryć ślady transakcji i uniknąć wykrycia. Metody te utrudniają organom ścigania śledzenie nielegalnych przepływów finansowych, szczególnie w przypadkach związanych z handlem ludźmi, gdzie handlarze wykorzystują waluty cyfrowe do pobierania płatności i prania pieniędzy. Zdecentralizowany i pseudonimowy charakter transakcji opartych na blockchainie stworzył środowisko, w którym przestępczość finansowa może się rozwijać, jeśli nie zostanie zwalczona zaawansowanymi technikami śledczymi.

Jednocześnie przestępcy finansowi stają się coraz bardziej **samowystarczalni**, odchodząc od polegania na zewnętrznych sponsorach i pośrednikach. Tendencja ta jest widoczna w rosnących oszustwach cybernetycznych, atakach ransomware i oszustwach internetowych, które generują fundusze dla zorganizowanych sieci przestępczych, w tym

tych zajmujących się handlem ludźmi. Rosnące wykorzystanie fałszywych platform internetowych, fałszywych kampanii fundraisingowych i oszukańczych platform e-commerce dodatkowo zwiększyło możliwości przestępczości finansowej.

Pomimo tych wyzwań, postęp technologiczny oferuje również nowe narzędzia do walki z przestępczością finansową. **Analityka blockchain** i **sztuczna inteligencja** odgrywają kluczową rolę w dochodzeniach finansowych, pomagając organom ścigania w śledzeniu nielegalnych transakcji i identyfikowaniu podejrzanych wzorców. Systemy monitorowania transakcji oparte na sztucznej inteligencji mogą analizować ogromne ilości danych w czasie rzeczywistym, sygnalizując anomalie, które mogą wskazywać na pranie pieniędzy lub działania związane z handlem ludźmi. Ponadto narzędzia kryminalistyczne blockchain umożliwiają śledczym śledzenie ruchów kryptowalut i odkrywanie ukrytych powiązań między podmiotami przestępczymi.

9.5.7 Zalecenia

Solidne ramy prawne dotyczące ścigania przestępstw finansowych są niezbędne dla zapewnienia skutecznych dochodzeń finansowych. Międzynarodowe standardy, na przykład zalecenia **Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF)** , stanowią podstawę dla środków AML/CFT. Przepisy te nakładają na organy ścigania obowiązek prowadzenia dochodzeń finansowych, ułatwiania współpracy transgranicznej oraz egzekwowania procedur konfiskaty mienia. Na przykład, Zalecenie FATF nr 30 podkreśla znaczenie wyznaczenia właściwych organów uprawnionych do prowadzenia dochodzeń w sprawie przestępstw związanych z praniem pieniędzy i finansowaniem terroryzmu.

Z powodu wojny na Ukrainie osoby przesiedlone są narażone na zwiększone ryzyko handlu ludźmi. W odpowiedzi na to zwiększone ryzyko, organizacje takie jak Organizacja

Bezpieczeństwa i Współpracy w Europie (OBWE) opracowały specjalistyczne zasoby wspierające osoby udzielające pierwszej pomocy. OBWE oferuje na przykład „ *Kompendium szkoleń w zakresie przeciwdziałania handlowi ludźmi dla osób udzielających pierwszej pomocy* ”, które obejmuje specjalistyczne szkolenia z różnych aspektów działań przeciwko handlowi ludźmi. Wśród nich znajdują się specjalistyczne kursy poświęcone dochodzeniom finansowym, które wyposażają specjalistów w niezbędne narzędzia do identyfikacji i zwalczania nielegalnych przepływów finansowych związanych z handlem ludźmi. Link do przeglądu kursu: https://www.osce.org/cthb/562572 .

9.6 Proponowane ćwiczenia

Tabela 1Ćwiczenia w zakresie informatyki śledczej i dochodzeń finansowych

Nazwa aktywności	Ćwiczenia z zakresu informatyki śledczej
Rodzaj aktywności	Praca grupowa (np. grupy po 3-6 osób)
Czas trwania	15-35 minut
Cele edukacyjne	Identyfikacja kluczowych śladów cyfrowych i dalsze kroki
Potrzebne materiały	Przykład przypadku z wystarczającym tłem (np. wersja drukowana) • Thomas, Day i Jackson (2019) na str. 31–38 i str. 38–42 na stronie https://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Crates (2022) na str. 9–14 na stronie https://www.antislaverycommissioner.co.uk/media/h4ggz4c2/iasc-construction-report-april-2022.pdf

	• Departamentu Pracy USA (2022) pod adresem https://blog.dol.gov/2022/01/11/fighting-human-trafficking-the-legacy-of-the-el-monte-sweatshop • Lam i Skivankova (2009) na s. 23. 5 na https://www.antislavery.org/wp-content/uploads/2017/01/trafficking_and_compensation2009.pdf • KOK, niemiecka sieć organizacji pozarządowych przeciwko handlowi ludźmi (nd) na stronie https://www.kok-gegen-menschenhandel.de/menschenhandel/was-ist-menschenhandel/fallbeispiele (*użyj automatycznego tłumaczenia dla strony internetowej i wybierz podsekcję „Handel ludźmi w celu wyzysku pracowników”*) • Rozdział 8 szkolenia
Wytyczne dla osoby prowadzącej	Uczestnicy zostaną podzieleni na mniejsze grupy. Otrzymają studium przypadku, które przeczytają (3-4 min). Następnie rozpoczną dyskusję w swoich grupach i spróbują określić, jakie dowody cyfrowe najlepiej nadawałyby się do skutecznej analizy kryminalistycznej. Ponadto omówią, którzy aktorzy byliby zaangażowani i na jakim etapie procesu śledczego (10-15 min). • Jakie dowody cyfrowe są istotne? Które dowody cyfrowe są najbardziej przydatne i dlaczego? • W jaki sposób eksperci medycyny sądowej mogą wyodrębnić i przeanalizować te cyfrowe ślady?

	• W jaki sposób może pomóc w identyfikacji ofiar, handlarzy i wzorców postępowania? • Jakie wzorce lub sygnały ostrzegawcze sugerują handel ludźmi? • Jakie następne kroki powinni podjąć śledczy? • W jaki sposób dowody te mogą być wykorzystane w celu wsparcia ofiar? Następnie każda grupa zaprezentuje swoje ustalenia (5-10 min).
Odprawa	Po pracy w grupach moderator moderuje prezentację.
Wskazówki dla moderatora	Jeśli dysponujesz większą ilością czasu, możesz wykorzystać różne scenariusze przypadków, a każda grupa pokrótce przedstawi przypadek, a następnie wyniki dyskusji (zamiast, aby każda grupa pracowała nad tym samym przypadkiem).
Materiały informacyjne	*np*. studia przypadków, które należy wydrukować i udostępnić uczestnikom, potencjalnie uzupełnione o materiały zawierające imitowane fragmenty z: • Czaty WhatsApp między ofiarą a handlarzem z komunikatami w stylu: „Nie martw się papierkową robotą, zajmiemy się tym za ciebie”, „Dostaniesz darmowe zakwaterowanie i transport” lub „Spotkajmy się na dworcu autobusowym. Usuń te wiadomości”.

	• Ogłoszenia z platformy rekrutacyjnej • Rejestry transakcji bankowych • Metadane ze zdjęcia wysłanego ofierze wraz z danymi geolokalizacyjnymi • …
Warianty wdrożenia online	Możliwość prowadzenia zajęć online, twórz sesje grupowe
Nazwa aktywności	**Działalność w zakresie dochodzeń finansowych**
Rodzaj aktywności	Praca grupowa (np. grupy po 3-6 osób)
Czas trwania	15-35 minut
Cele edukacyjne	Internalizacja kroków dochodzeń finansowych i refleksja nad potencjalnymi wyzwaniami pojawiającymi się w obszarze handlu ludźmi
Potrzebne materiały	np. studium przypadku, które powinno zostać wydrukowane i udostępnione uczestnikom, potencjalnie uzupełnione materiałem zawierającym imitowane fragmenty:

	• Zapisy transakcji bankowych i wyciągi bankowe (mogą to być również po prostu tabele z kolumnami: data, opis, debet (EUR), kredyt (EUR) i saldo (EUR), pokazujące, kiedy ktoś dokonał transakcji (+ na rzecz jakiej firmy/osoby) • Listy płac • Faktury • …
Wytyczne dla osoby prowadzącej	Uczestnicy zostaną podzieleni na mniejsze grupy. Otrzymają studium przypadku, które przeczytają (3-4 min). Następnie rozpoczną dyskusję w swoich grupach i spróbują określić etapy dochodzeń finansowych (np. powtarzając każdy z poznanych wcześniej kroków). Ponadto omówią, które podmioty będą zaangażowane i na jakim etapie procesu dochodzeniowego się znajdują (10-15 min). • Jakie techniki dochodzenia finansowego należy zastosować? • W jaki sposób organy ścigania mogą współpracować z jednostkami analityki finansowej? • Jakie narzędzia prawne należy zastosować? • Jakie wyzwania można zidentyfikować? Następnie każda grupa zaprezentuje swoje ustalenia.
Odprawa	Po pracy w grupach moderator moderuje prezentację.

Wskazówki dla moderatora	Jeśli dysponujesz większą ilością czasu, możesz wykorzystać różne scenariusze przypadków, a każda grupa pokrótce przedstawi przypadek, a następnie wyniki dyskusji (zamiast, aby każda grupa pracowała nad tym samym przypadkiem).
Materiały informacyjne	*Studium przypadku powinno zostać wydrukowane i udostępnione uczestnikom* • Thomas, Day i Jackson (2019) na str. 31–38 i str. 38–42 na stronie https://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Studium przypadku Top Glove (Malezja), szczegóły dostępne na stronie 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 . Malezja: Ukryte kamery ujawniają złe warunki pracy i życia w fabryce Top Glove, co podsyca obawy dotyczące pracy przymusowej w branży rękawicowej; w tym komentarze firmy - Centrum Zasobów Biznesu i Praw Człowieka
Warianty wdrożenia online	Możliwość prowadzenia zajęć online, sesji grupowych

9.7 Bibliografia

Aronowitz, Alexis i Theuermann, Gerda i Tyurykanova, Elena. (2010). OBWE. *Analiza modelu biznesowego handlu ludźmi w celu lepszego zapobiegania przestępczości* . https://www.osce.org/files/f/documents/c/f/69028.pdf

Belser, P. (2005). *Praca przymusowa i handel ludźmi: szacowanie zysków* . Genewa: Międzynarodowe Biuro Pracy. https://ecommons.cornell.edu/bitstream/1813/99623/1/Forced_labor_no__17_Forced_labour_and_human.pdf

Cellebrite. (2024, 15 listopada). *Jak organy ścigania mogą odwrócić bieg wydarzeń w walce z handlem ludźmi dzięki dowodom cyfrowym* . https://cellebrite.com/en/how-law-enforcement-can-turn-the-tide-against-human-trafficking-with-digital-evidence/

Dubey, H., Bhatt, S. i Negi, L. (2023). *Techniki i trendy w zakresie informatyki śledczej: przegląd.* The International Arab Journal of Information Technology, *20* (4), 644-654.

Komisja Europejska. (nd). *Dochodzenia finansowe* . https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/financial-investigations_en

Europol. (2020). *Wyzwania związane ze zwalczaniem handlu ludźmi w erze cyfrowej* . https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

Europol. (2024, lipiec). *Zwalczanie zagrożeń, podejmowanie wyzwań. Reakcja Europolu na przemyt migrantów i handel ludźmi w 2023 r. i później* . Europejskie Centrum

ds. Przemytu Migrantów (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. i De Cock, M. (2024). *Zyski i ubóstwo: ekonomia pracy przymusowej* . MOP. https://www.ilo.org/sites/default/files/2024-10/Profits%20and%20poverty%20-%20The%20economics%20of%20forced%20labour_WEB_20241017.pdf

Fraser, C. (2016). Analiza rosnącej roli mediów społecznościowych w handlu ludźmi: przykłady z handlu pracą i narządami ludzkimi. *International Journal of Development Issues* , *15* (2), 98-112.

Gorenc, M. (2019). Prawo Benforda jako przydatne narzędzie do określania oszustw w sprawozdaniach finansowych. *Zarządzanie, 14* (1). 19-31. 10.26493/1854-4231.14.19-31.

Międzynarodowa Organizacja Pracy. (2018). *Badanie przypadków handlu ludźmi z wykorzystaniem podejścia skoncentrowanego na ofierze* . Międzynarodowa Organizacja ds. Migracji. https://publications.iom.int/system/files/pdf/investigating_human_trafficking.pdf

Międzynarodowa Organizacja Pracy. (30 lipca 2023 r.). *Mapa luk w dowodach dotyczących handlu ludźmi* . 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. i Williamson, C. (2018). *Media społecznościowe i proces handlu ludźmi w celach seksualnych: od nawiązywania kontaktów i rekrutacji do sprzedaży* . Ohio: University of Toledo. https://www.utoledo.edu/hhs/htsji/pdfs/smr.pdf

Lugo-Graulich, K., Meyer, LF, Souza, K., Tapp, SN, Maryfield, B. i Bostwick, L. (2024). Poprawa identyfikacji ofiar handlu ludźmi w celach seksualnych: wskaźniki handlu ludźmi w internetowych reklamach towarzyskich. *Journal of Human Trafficking* , 1-22.

Maras, M.-H. (2014). *Informatyka śledcza: cyberprzestępcy, prawo i* dowody (wydanie 2). Jones i Bartlett.

Mattmann, C., Yan GH, Manjunatha, H., Gowda N, T., Zhou, AJ, Luo, J. i McGibbney, LJ (2016). *Kryminalistyka oparta na multimedialnych metadanych w internetowych danych o handlu ludźmi* . W: Murdock, V., Clarke, CLA, Kamps, J. i J. Karlgren. *Przeszukiwanie i eksploracja informacji o charakterze pornograficznym* . s. 10–13.

OBWE. (2019, 7 listopada). *Podążając za pieniędzmi: Kompendium zasobów i przewodnik krok po kroku po dochodzeniach finansowych związanych z handlem ludźmi* . https://www.osce.org/files/f/documents/f/5/438323_0.pdf

Perez, AR i Rivas, P. (2023). Zwalczanie handlu ludźmi w cyberprzestrzeni: metodologia oparta na przetwarzaniu języka naturalnego do analizy języka w reklamach internetowych. *arXiv preprint arXiv:2311.13118* .

Pizzuro, J. (2022, 11 marca). *Wykorzystanie oprogramowania Magnet Forensics w dochodzeniach dotyczących handlu ludźmi.* MAGNET FORENSICS. https://www.magnetforensics.com/blog/leveraging-magnet-forensics-software-for-human-trafficking-investigations/

Siavoshi, M. (25 lutego 2025). *Rozwikłanie tajemnicy prawa Benforda: zastosowania w wykrywaniu oszustw* . Statology. https://www.statology.org/unraveling-the-mystery-of-benfords-law-applications-in-fraud-detection/

Thomson Reuters. (2 stycznia 2025). *Technologia i handel ludźmi: walka w słusznej sprawie.* 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, maj). *Technologia ułatwiająca handel ludźmi* . https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html

UNODC. (2019b, marzec). *Moduł 6: Praktyczne aspekty dochodzeń w sprawie cyberprzestępczości i informatyki śledczej. Postępowanie z dowodami cyfrowymi* . https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

UNODC. (2020). *Globalny raport na temat handlu ludźmi* 2020. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

Volodko, A., Cockbain, E. i Kleinberg, B. (2020). „Wykrywanie oznak" rekrutacji w sieci w celu handlu ludźmi: analiza charakterystyki reklam kierowanych do migrantów poszukujących pracy. *Trends in Organized Crime* , *23* , 7-35.

www.eradicating2project.eu

Co-funded by
the European Union