PORADNIK

CYBER RATOWNIKA

IV Konferencja Naukowa
Przestępczość Teleinformatyczna XXI wieku

GDYNIA 2022

Niniejszy materiał informacyjny został przygotowany przez
Morskie Centrum Cyberbezpieczeństwa
Akademii Marynarki Wojennej w Gdyni
z okazji
IV Konferencji Naukowej Przestępczość Teleinformatyczna XXI wieku.

Poradnik Cyber Ratownika jest tłumaczeniem publikacji INTERPOL-u pt. GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS – Best practices for search and seizure of electronic and digital evidence. Tekst w języku polskim został opracowany przez panią Annę z portalu sekurak.pl jako wkład partnera do Programu Współpracy w Cyberbezpieczeństwie (PWCyber) prowadzonego przez Ministra Cyfryzacji.

Niezbędne jest stałe doskonalenie technik zabezpieczania dowodów cyfrowych i akwizycji danych, jak również udział w projektach szkoleniowych w celu ograniczenia ryzyka utraty lub uszkodzenia dowodu.

Należy pamiętać, że opisywane procedury i metody postępowania z cyfrowymi nośnikami informacji stanowią jedynie ogólnie wytyczne. W zależności od zaistniałej sytuacji, mogą one zostać zmodyfikowane w celu uzyskania jak największej efektywności wykonywanych czynności procesowych.

Wyrażamy szczerą nadzieję, że Poradnik Cyber Ratownika będzie wartościowym źródłem wiedzy dla organów ścigania i wymiaru sprawiedliwości w toku realizowanych czynności, polegających w szczególności na zabezpieczeniu dowodów cyfrowych.

sekurak.pl

INTERPOL

PORADNIK CYBER RATOWNIKA

Najlepsze praktyki przeszukania i zatrzymania dowodów elektronicznych i cyfrowych

Marzec 2021

Zastrzeżenie

Niniejszy „Poradnik Cyber Ratownika" („**Poradnik**") został przygotowany jako techniczne wytyczne dostarczające informacji i porad w zakresie podejścia do dowodów cyfrowych, które można zastosować podczas zatrzymywania i analizowania różnego rodzaju urządzeń. Niniejszy Poradnik jest przeznaczony do użytku wyłącznie przez przedstawicieli organów ścigania, którzy wykonują opisywane czynności działając na podstawie i w granicach prawa.

Ramy prawne, proceduralne i zwyczajowe w zakresie przeszukania, zatrzymania, łańcucha dowodowego, analizy, raportowania, wykorzystania w postępowaniu, oceny, dopuszczalności i wartości dowodowej znacznie się różnią w zależności od jurysdykcji. Niniejszy Poradnik nie dostarcza żadnych rekomendacji, porad lub instrukcji w zakresie porad prawnych lub proceduralnych w jakiejkolwiek jurysdykcji, a wszystkie odniesienia sugerujące, że tak jest należy odczytywać jako podlegające krajowym przepisom i procedurom w tym zakresie.

Czytelnikom zaleca się, aby podejmując jakiekolwiek czynności w oparciu o niniejszy Poradnik, weryfikowali i upewniali się, że te działania są zgodne z właściwymi przepisami prawa oraz procedurami i standardami w ich jurysdykcji.

Niniejszy Poradnik nie ma charakteru obligatoryjnego i nie ma mocy prawnej. INTERPOL nie ponosi odpowiedzialności za jakiekolwiek działania podejmowane na podstawie niniejszego Poradnika, jeśli są wbrew wymogom prawnym, regulacyjnym, administracyjnym, proceduralnym, dowodowym, zwyczajowym lub jakimkolwiek innym wymogom w zakresie pozyskiwania dowodów, zachowywania łańcucha dowodowego i in.

Niniejszy Poradnik zawiera również odnośniki do narzędzi i usług ogólnodostępnych i podlegających licencji open source (zwanych łącznie „**Narzędziami**", a każde z nich „**Narzędziem**"), które oferują różne funkcjonalności. Mogą one być przeglądane, pobierane i/lub wykorzystywane według uznania Czytelnika. W odniesieniu do powyższego, należy zwrócić uwagę na następujące kwestie:

- INTERPOL nie opracował i nie weryfikował Narzędzi, nie popiera ich, nie jest powiązany z ich dostawcami, nie udziela licencji i wsparcia w zakresie korzystania z tych Narzędzi. INTERPOL nie udziela żadnej gwarancji (wyrażonej wprost lub dorozumianej) na żadne z Narzędzi, ich przydatności i skuteczności.

- Odnośniki do innych stron internetowych zamieszczone w niniejszym Poradniku nie stanowią poparcia ze strony INTERPOL-u i są zamieszczone jedynie dla komfortu Czytelnika. Czytelnik jest odpowiedzialny za ocenę treści i przydatności treści z innych stron internetowych i wykorzystania tych Narzędzi.

- INTERPOL nie kontroluje, nie monitoruje i nie gwarantuje zawartości linków lub udostępnionych pod nimi Narzędzi, ani stosowanych przez nie praktyk gromadzenia danych, nie popiera wyrażanych tam poglądów, ani oferowanych produktów lub usług.

- W celu korzystania z niektórych Narzędzi może być konieczne utworzenie konta użytkownika, uiszczenie opłaty subskrypcyjnej lub opłaty za uaktualnienie. Rejestracja lub utworzenie konta użytkownika, albo uiszczenie opłaty może wymagać zgody ze strony organizacji Czytelnika i podlegać regulacjom w ich jurysdykcji (w tym w zakresie tworzenia fałszywych lub przybranych tożsamości). Czytelnik powinien upewnić się, że ma właściwe upoważnienie do korzystania z Narzędzi. INTERPOL nie zachęca i w żaden sposób nie zezwala na takie działania i nie będzie ponosił odpowiedzialności za żadne działania podejmowane przez Czytelnika w celu utworzenia konta lub rejestracji, ponoszenia opłat i wykorzystywania tożsamości lub tworzeniu fałszywych kont w celu korzystania z Narzędzi.

- Każde z Narzędzi może być objęte licencją, zasadami prywatności lub innymi warunkami korzystania. Czytelnik powinien uważnie zapoznać się z warunkami i zasadami prywatności dotyczącymi Narzędzi, których zamierza użyć.

- Dane wprowadzone do Narzędzi mogą być zapisane na serwerach ich dostawcy i legalność takiego działania powinna być sprawdzona przez Czytelnika. Czytelnik ponosi odpowiedzialność za weryfikację zgodności z praktykami i zasadami prywatności w jurysdykcji Czytelnika w odniesieniu do gromadzonych przez Narzędzia danych.

- Jakiekolwiek użycie Narzędzi (lub któregokolwiek z nich) odbywa się na własne ryzyko Czytelnika, a INTERPOL w żadnym wypadku nie ponosi odpowiedzialności za jakiekolwiek szkody lub straty poniesione, spowodowane lub rzekomo spowodowane z powodu użycia lub polegania na którymkolwiek z Narzędzi. Wszelkie roszczenia lub kroki prawne podejmowane w związku ze szkodą lub stratą poniesioną przez Czytelnika powinny być kierowane bezpośrednio do dostawców Narzędzia (lub Narzędzi), a nie do INTERPOL-u.

- Żadne dane, które są wprowadzane podczas korzystania z któregokolwiek z Narzędzi, nie będą w żaden sposób przekazywane do INTERPOL-u, ani mu udostępniane. Jeśli Czytelnik zdecyduje się korzystać z któregokolwiek z Narzędzi do celów informatyki śledczej, analitycznych lub śledczych, przyjmuje do wiadomości, że INTERPOL nie otrzyma żadnej informacji w tym zakresie i w żadnym momencie nie będzie sprawował nadzoru nad żadnym dowodem analizowanym lub wygenerowanym przez którekolwiek z Narzędzi.

Podziękowania

Niniejszy Poradnik opiera się na *Poradniku dowodów elektronicznych* (ang. the Electronic Evidence Guide) Rady Europy, *Podręczniku gromadzenia dowodów cyfrowych* (ang. the Digital Evidence Collection Certificate Manual) hiszpańskiego Narodowego Centrum Doskonałości w zakresie Cyberbezpieczeństwa (ang. the National Center of Excellence in Cybersecurity, INCIBE) oraz na innych zbiorach najlepszych praktyk organów ścigania w zakresie zatrzymywania i obchodzenia się z dowodami elektronicznymi. Laboratorium Informatyki Śledczej Centrum Innowacji INTERPOL-u (ang. the Interpol Innovation Centre Digital Forensics Laboratory, IC DFL) otrzymało również informacje zwrotne od ekspertów w dziedzinie informatyki śledczej z różnych części świata, aby osiągnąć konsensus w zakresie niektórych dyskutowanych lub kłopotliwych aspektów, z którymi stykają się osoby zajmujące się informatyką śledczą. INTERPOL pragnie wymienić i podziękować kolegom, których cenny wkład przyczynił się do doskonalenia organów na całym świecie:

- BRAZYLIA: Narodowemu Instytutowi Kryminalistyki Policji Federalnej Brazylii (ang. National Institute of Criminalistics Brazilian Federal Police);
- HISZPANIA: Departamentowi Cyberprzestępczości Policji Hiszpańskiej (ang. Cybercrime Unit, General Commissary of Criminal Police of Spanish National Police);
- Naukowej Grupie Roboczej ds. Dowodów Elektronicznych (ang. the Scientific Working Group on Digital Evidence, SWGDE).

INTERPOL pragnie również wyrazić szczere wyrazy wdzięczności norweskiemu Ministerstwu Spraw Zagranicznych za wsparcie i wkład w powstanie niniejszego Poradnika.

Niniejszy Poradnik będzie wykorzystywany podczas szkolenia online (listopad-grudzień 2020), prowadzonego w ramach projektu INTERPOL-u pt. *LIDER*, trzyletniej inicjatywy budowania potencjału, finansowanej przez norweski MSZ. Projekt koncentruje się na podnoszeniu kompetencji w zakresie dowodów cyfrowych beneficjentów w regionach Azji Południowej i Południowo-Wschodniej. Dzięki tym wysiłkom, kluczowi interesariusze projektu, w tym osoby zajmujące się informatyką śledczą i organa ścigania, będą miały możliwość poszerzenia swojej wiedzy w zakresie najlepszych praktyk przedstawionych w niniejszym Poradniku. Co więcej, niniejszy Poradnik posłuży jako nieocenione źródło narzędzi pośród wszystkich krajach członkowskich INTERPOL-u zapewniając, że zasady postępowania z dowodami cyfrowymi, ich pozyskiwania i zabezpieczania w celu wsparcia postępowań, będą dostępne dla funkcjonariuszy w to zaangażowanych.

Przedmowa

W celu dostarczenia wytycznych oraz wsparcia organom ścigania na całym świecie, Centrum Innowacji INTERPOL-u (ang. the INTERPOL Innovation Centre, IC) opracowało poradnik INTERPOL-u *Poradnik Cyber Ratowników: Najlepsze praktyki przeszukania i zabezpieczenia dowodów elektronicznych i cyfrowych (ang. INTERPOL Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence)*. Mam przyjemność zaprezentować niniejszy Poradnik, którego celem jest ustanowienie najlepszych praktyk obchodzenia się i wykorzystania dowodów cyfrowych w trakcie czynności przygotowania oraz podczas ich przeszukania i zatrzymania. Zidentyfikowane zostały również kluczowe względy techniczne dotyczące skutecznego zabezpieczenia danych w celu zapewnienia, że będą one wspierać organy ścigania w postępowaniach karnych i będą mogły być dopuszczone. Niniejszy Poradnik jest przeznaczony dla funkcjonariuszy organów ścigania specjalizujących się w różnych rodzajach przestępstw, którzy mogą być na miejscu zdarzenia i odpowiadać za zabezpieczenie oraz transport dowodów elektronicznych i cyfrowych. Będzie on również pomocny dla prokuratorów, aby lepiej zrozumieli zabezpieczanie i obchodzenie się z dowodami cyfrowymi.

W miarę jak nasze społeczeństwo staje się coraz bardziej połączone z technologiami cyfrowymi, które obejmują każdy aspekt naszego codziennego życia oraz pracy organów ścigania, może być trudno sobie przypomnieć sytuację, kiedy mieliście Państwo ograniczoną styczność z dowodami cyfrowymi. Dla dzisiejszej społeczności organów ścigania istnieje ciągła tendencja do prowadzenia postępowań w oparciu o pewne formy dowodów cyfrowych. Chociaż uważamy, że dowody cyfrowe rzeczywiście mają podobne cechy, co tradycyjne, to jednak istnieją również unikatowe względy, które należy wziąć pod uwagę.

Nieuchwytny charakter danych pozyskanych w formie elektronicznej, ich ulotność oraz łatwość, z jaką mogą być modyfikowane, stanowią wyzwanie dla integralności dowodów cyfrowych. Z tego względu tak ważne jest, aby osoby mające jako pierwsze styczność w dowodami cyfrowymi oraz funkcjonariusze organów ścigania potrafili prawidłowo identyfikować dowody cyfrowe i obchodzić się z tymi dowodami, tak aby późniejsze czynności mogły być wykonane w oparciu o rzetelną ich ocenę.

Wyrażam wdzięczność za wkład zespołu IC, w szczególności DFL, za podzielenie się wiedzą i doświadczeniem merytorycznym. Dziękuję również kolegom z Dyrektoratu Budowania Potencjału i Szkoleń (ang. the INTERPOL Capacity Building and Training Directorate, CBT), którzy wsparli niniejszą inicjatywę i będą wykorzystywać Poradnik w ramach projektów ukierunkowanych na podnoszenie potencjału w zakresie informatyki śledczej. Na koniec pragnę podziękować norweskiemu Ministerstwu Spraw Zagranicznych za ich hojne wsparcie.

Niniejszy Poradnik jest odzwierciedleniem nieustannych wysiłków INTERPOL-u w zakresie wspierania międzynarodowej współpracy policji i zaangażowania w pomoc krajom członkowskim w odpowiedzi na złożone wyzwania bezpieczeństwa w sferze cyfrowej.

Dyrektor Anita Hazenberg

Dyrektorat Centrum Innowacji INTERPOL-u (ang. Innovation Centre Directorate)

Spis treści

Spis ilustracji 9
1. WSTĘP 10
2. ETAP PRZYGOTOWANIA DO PRZESZUKANIA I ZATRZYMANIA 10
2.1. Planowanie 10
2.2. Miejsce dostarczenia dowodów 12
2.3. Przygotowanie narzędzi 13
3. ETAP PRZESZUKANIA I ZATRZYMANIA 15
3.1. Zabezpieczenie miejsca 15
3.2. Ocena 15
3.3. Dokumentacja 16
3.4. Zabezpieczenie i obchodzenie się z dowodem cyfrowym 17
3.4.1. Analiza live włączonych komputerów i laptopów 17
3.4.2. Brak możliwości dostępu do danych na włączonych urządzeniach 19
3.5. Etap zatrzymania 20
3.5.1 Pakowanie i transport 20
4. WZGLĘDY TECHNICZNE 20
4.1. Kopia kryminalistyczna 20
4.2. Alternatywy dla kopii kryminalistycznej 21
4.3. Funkcja HASH 22
5. SZCZEGÓLNE PROCEDURY 23
5.1. Smartfony - tablety 23
5.1.1. Względy dotyczące zabezpieczenia dowodów z telefonów 24
5.1.2. Proces zabezpieczenia dowodów z telefonów 25
5.1.3. Zabezpieczenie urządzeń z iOS 25
5.1.4. Zabezpieczenie urządzeń z Androidem 26
5.1.5 Karta SIM 28
5.1.6. Wymienne karty pamięci 28
5.1.7. Dane w chmurze 29
5.1.8. Względy dotyczące zatrzymania 29
Tradycyjna kryminalistyka 29
Dostęp 29
Izolacja sieci 29
Tezy dowodowe 30
5.2. Serwery 31
5.3. Komputery osobiste 31
5.4. Laptopy 34

5.5. Nośniki pamięci (karty, dyski flash, zewnętrzne dyski, CD i in.) 34
5.6. Inne urządzenia (aparaty, nawigacje GPS, wideorejestratory i in.) 36
5.7. Urządzenia IoT 36
5.7.1. Smartwatche 37
5.7.2. Smart TV 37
5.7.3. Inteligentne głośniki 38
5.7.4. Kamery ukryte i IP 39
5.8. Konsole do gier 40
5.9. Drony 41
5.10. Monitoring wizyjny 43
5.11. Portfele kryptowalut 44
5.12. Komputery samochodowe 49
5.13. Urządzenia pokładowe 51
REFERENCJE 53

Akronimy

CBT	INTERPOL Capacity Building and Training
CCTV	monitoring wizyjny (ang. Close Circuit Television)
CGPJ	Hiszpański organ konstytucyjny kierujący sądownictwem (ang. General Council of the Judiciary)
CNP	policja hiszpańska (hiszp. Cuerpo Nacional de Policía)
CNIC	karta SIM izolująca urządzenie od stacji przekaźnikowej
CSM	moduł CDMA (ang. CDMA Subscriber Identity Module)
CSV	format pliku CSV (ang. Comma-separated Values)
DFL	laboratorium informatyki śledczej (ang. Digital Forensics Laboratory)
DNA	kwas deoksyrybonukleinowy (ang. Deoxyribonucleic acid)
DRM	zarządzanie prawami cyfrowymi (ang. Digital Rights Management)
DSC	cyfrowe wywołanie selektywne (ang. Digital Selective Calling)
ECDIS	system zobrazowania elektronicznej mapy i informacji nawigacyjnej (ang. Electronic Chart Display and Information System)
ECU	elektroniczny moduł sterujący (ang. Electronic Control Unit)
EPIRB	nadajnik EPIRB (ang. Emergency Positioning Indicator Radio Beacon)
GB	Gigabajt (ang. Gigabyte)
GMDSS	system GMDSS (ang. Global Maritime Distress and Safety System)
GPS	system GPS (ang. Global Positioning System)
GSR	pozostałości po wystrzałach (ang. Gunshot Residue)
HD	dysk twardy (ang. Hard Drive)
HDD	dysk twardy (ang. Hard Disk Drive)
IC	Centrum Innowacji INTERPOL-u (ang. INTERPOL Innovation Centre)
ICCID	numer identyfikacyjny karty SIM (ang. Integrated Circuit Card ID)
IMEI	numer IMEI (ang. International Mobile Equipment Identity)
INCIBE	Hiszpański Narodowy Instytut Cyberbezpieczeństwa (hiszp. Instituto Nacional de Ciberseguridad)
IP	protokół IP (ang. Internet Protocol)
LRIT	system LRIT (ang. Long Range Tracking and Identification System)
NVMe	interfejs NVMe (ang. Non-Volatile Memory Express)
OS	System operacyjny (ang. Operating System)
P2P / P2MP	komunikacja P2P/P2MP (ang. Point-to-point/Point-to-multipoint)
PIN	kod PIN (ang. Personal Identification Number)
PUK	kod PUK (ang. Personal Unlocking Keys, znany jako NUC (ang. Network Unlocking Code) lub PUC (ang. Personal Unlocking Code)
RAM	pamięć operacyjna (ang. Random Access Memory)
RAID	(ang. Redundant Array of Inexpensive Disks)
RF	częstotliwość radiowa (ang. Radio Frequency)
RPAS	zdalnie sterowany system (ang. Remotely Piloted Aircraft System)
RUIM	karta RUIM (ang. Removable User Identity Module)
SMS	wiadomość SMS (ang. Short Message Service)
SSD	dysk półprzewodnikowy (ang. Solid-State Drive)
sUAS	mały bezzałogowy dron (ang. Small Unmanned Aerial System)
TB	terabajt (ang. Terabyte)
TPM	standard TPM (ang. Trusted Platform Module)
UAV	bezzałogowy statek powietrzny (ang. Unmanned Aerial Vehicle)
UAS	bezzałogowy system powietrzny (ang. Unmanned Aerial System)
UPS	zasilanie awaryjne (ang. Uninterruptible Power Supply System)

USB	magistrala USB (ang. Universal Serial Bus)
USIM	moduł USIM (ang. Universal Subscriber Identity Module)
VHF	morskie fale ultrakrótkie (ang. Very High Frequency Radio)
VMS	system monitoringu statków (ang. Vessel Monitoring System)
VIN	numer VIN (ang. Vehicle Identification Number)
WIF	format WIF (ang. Wallet Import Format)

Spis ilustracji

Obraz 1: Schemat etapu i procedury planowania 12
Obraz 2: Urządzenia: Smartfony i tablety 23
Obraz 3: Apple iPhone 25
Obraz 4: Schemat akwizycji dowodów z urządzeń z Apple iOS 26
Obraz 5: Smartfony z Androidem 27
Obraz 6: Schemat akwizycji dowodów z urządzeń z Androidem 27
Obraz 7: Karty SIM 28
Obraz 8: Karty pamięci 28
Obraz 9: Składniki zasobu chmurowego 29
Obraz 10: Kamery cyfrowe 36
Obraz 11: Smartwatche 37
Obraz 12: Smart TV 37
Obraz 13: Urządzenia takie jak Amazon Echo, Apple HomePod oraz inteligentne głośniki 38
Obraz 14: Kamery IP przesyłające obraz po sieci 39
Obraz 15: Konsole Nintendo, Sony PS Series i Microsoft XBOX jako przykłady konsol z funkcjami smart 40
Obraz 16: Drony 41
Obraz 17: Kamery CCTV wykorzystywane do monitoringu 43
Obraz 18: Portfele kryptowalutowe, wykorzystywane do przechowywania kryptowalut i innych aktywów 44
Obraz 19: Portfele papierowe 45
Obraz 20: Portfele sprzętowe 46
Obraz 21: Przykład portfela desktopowego 46
Obraz 22: Portfel desktopowy Electrum 47
Obraz 23: Przykład mobilnego portfela kryptowalut 47
Obraz 24: Portfel typu Brain (seed) 48
Obraz 25: Portfel typu Brain (seed) 48
Obraz 26: Przykłady urządzeń pokładowych z danymi i ich lokalizacją 52

PRZESZUKANIE I ZATRZYMANIE DOWODU CYFROWEGO

1. WSTĘP

Niniejszy Poradnik dostarcza wsparcia i porad dla praktyków informatyki śledczej w organach ścigania podczas czynności przeszukania i zatrzymania dowodów cyfrowych, w zakresie metod identyfikacji i obchodzenia się z dowodami, które zapewniają ich integralność.

Urządzenie elektroniczne nie powinno być zatrzymane bez spełnienia warunków wstępnych. To zespół śledczy wspólnie ze specjalistami informatyki śledczej, którzy będą pomagać w zabezpieczaniu i przetwarzaniu dowodów elektronicznych, wspólnie określają, czy ich pozyskanie i procesowanie jest istotne, czy też nie.

Z dowodami elektronicznymi, tak jak ze wszystkimi innymi tradycyjnymi dowodami, należy obchodzić się z ostrożnością, aby mogły być wykorzystane w postępowaniu. Dotyczy to zarówno integralności fizycznej urządzeń, jak i informacji oraz danych w nich zawartych. Należy mieć na uwadze, że niektóre urządzenia elektroniczne wymagają szczególnych procedur pozyskiwania, pakowania i transportowania, ponieważ są podatne na uszkodzenia przez pole elektromagnetyczne, jak i z powodu możliwości zmiany ich zawartości podczas obchodzenia się z nimi lub przechowywania ich.

Należy rozważyć możliwość pozyskania tradycyjnych (nieelektronicznych) dowodów, które nie powinny być pomijane i mieć na uwadze, że mogą mieć istotne znaczenie zarówno dla śledztwa, jak i dla późniejszego postępowania z dowodami elektronicznymi. Jest tak w przypadku wszelkich adnotacji dotyczących haseł, ustawień, kont e-mail i in. Z tymi dowodami należy postępować zgodnie z ustalonymi procedurami, aby je zabezpieczyć i zachować ich wartość dowodową.

2. ETAP PRZYGOTOWANIA DO PRZESZUKANIA I ZATRZYMANIA

2.1. Planowanie

Dane cyfrowe są dziś podstawowym filarem postępowań prowadzonych przez organy ścigania. Wraz z pojawieniem się smartfonów, mediów społecznościowych oraz usług personalizacji Internetu, takich jak usługi dostarczane Google i Apple, człowiek pozostawia po sobie cyfrowy ślad i ważne jest, aby w związku z przestępstwem ten cyfrowy ślad został uchwycony i przeanalizowany na potrzeby operacyjne oraz dowodowe. Etap przeszukania i zabezpieczenia ma decydujące znaczenie, ponieważ zapewnia zabezpieczenie urządzeń i danych na nich przechowywanych. W przypadku niewłaściwego zatrzymania i obchodzenia się ze sprzętem cyfrowym istnieje możliwość utraty danych poprzez ich usunięcie przez użytkownika, zdalne wymazanie lub zmodyfikowanie przez osoby trzecie.

Przypuśćmy, że zespół funkcjonariuszy wraz z jednym lub kilkoma specjalistami informatyki śledczej musi wykonać postanowienie prokuratora, aby wejść do domu domniemanego podejrzanego o popełnienie poważnego przestępstwa, takiego jak zabójstwo lub rozbój. Istnieje możliwość, że podejrzany na swoich urządzeniach, takich jak telefony lub komputery, może posiadać pliki lub dokumenty, które są decydujące dla rozstrzygnięcia sprawy. Dlatego urządzenia te muszą zostać przeszukane, a jeśli zostaną uznane za istotne dla postępowania, zatrzymane.

W takich przypadkach, przed rozpoczęciem jakichkolwiek czynności związanych z przeszukaniem i zatrzymaniem, należy wziąć pod uwagę szereg względów:

• Należy zorganizować spotkanie przygotowawcze w celu wymiany informacji między jednostką odpowiedzialną za prowadzenie śledztwa i innymi osobami, które będą udzielać wsparcia.

• Działania na miejscu zdarzenia wyspecjalizowanych podmiotów powinny być koordynowane i priorytetyzowane, w zależności od rodzaju sprawy. Na przykład, pierwszeństwo przed podjęciem jakichkolwiek czynności mogą mieć psy policyjne poszukujące materiałów wybuchowych lub zespoły zabezpieczające DNA.

Konieczne jest, aby jednostka odpowiedzialna za prowadzenie śledztwa przekazała z wyprzedzeniem pewne informacje potrzebne dla koordynacji działań różnych specjalistów, którzy mogą uczestniczyć w przeszukaniu i zatrzymaniu. Na spotkaniu przygotowawczym dotyczącym odpowiedniego postępowania z dowodami elektronicznymi, uczestnicy powinni mieć dostęp do wszystkich podstawowych informacji o sprawie, szczegółów postanowienia o przeszukaniu w zakresie dowodów elektronicznych, doradzić w sprawie właściwych sformułowań i wreszcie określić ostateczne miejsce dostarczenia zatrzymanych dowodów. Z punktu widzenia gromadzenia dowodów cyfrowych konieczne jest staranne przygotowanie i zaplanowanie wszystkich czynności, które będą wykonywane, z uwzględnieniem szeregu czynników, takich jak:

• **Charakter przestępstwa**. Charakter przestępstwa będzie determinował niezbędny sprzęt i przygotowanie adekwatnych procedur technicznych.

Przykładowo, w związku z seksualnym wykorzystywaniem dzieci, prawdopodobnie konieczne jest ustalenie w trakcie przeszukania faktu posiadania tego rodzaju materiałów, dlatego potrzebne będzie zabezpieczenie lub pozyskanie niezbędnych dowodów (zdjęć, filmów, czatów itd.) na miejscu zdarzenia w odpowiedni i bezpieczny sposób.

W sprawach o przestępstwa finansowe bardzo często spotyka się infrastrukturę z danymi przechowywanymi na serwerach scentralizowanych lub w chmurze, dlatego konieczne będzie precyzyjne określenie jakiego rodzaju dokumentacja elektroniczna jest poszukiwana, jaka jest optymalna metoda jej pozyskania i gdzie gromadzić pozyskane dane.

• **Wiedza techniczna podejrzanego.** Informacje o podejrzanych i ich umiejętnościach technicznych muszą być zgromadzone, ponieważ mogli oni zabezpieczyć swój sprzęt lub dane, co mogłoby skomplikować zabezpieczanie dowodów. Systemy szyfrowania lub aplikacje automatycznego usuwania danych utrudniają pozyskanie dowodów.

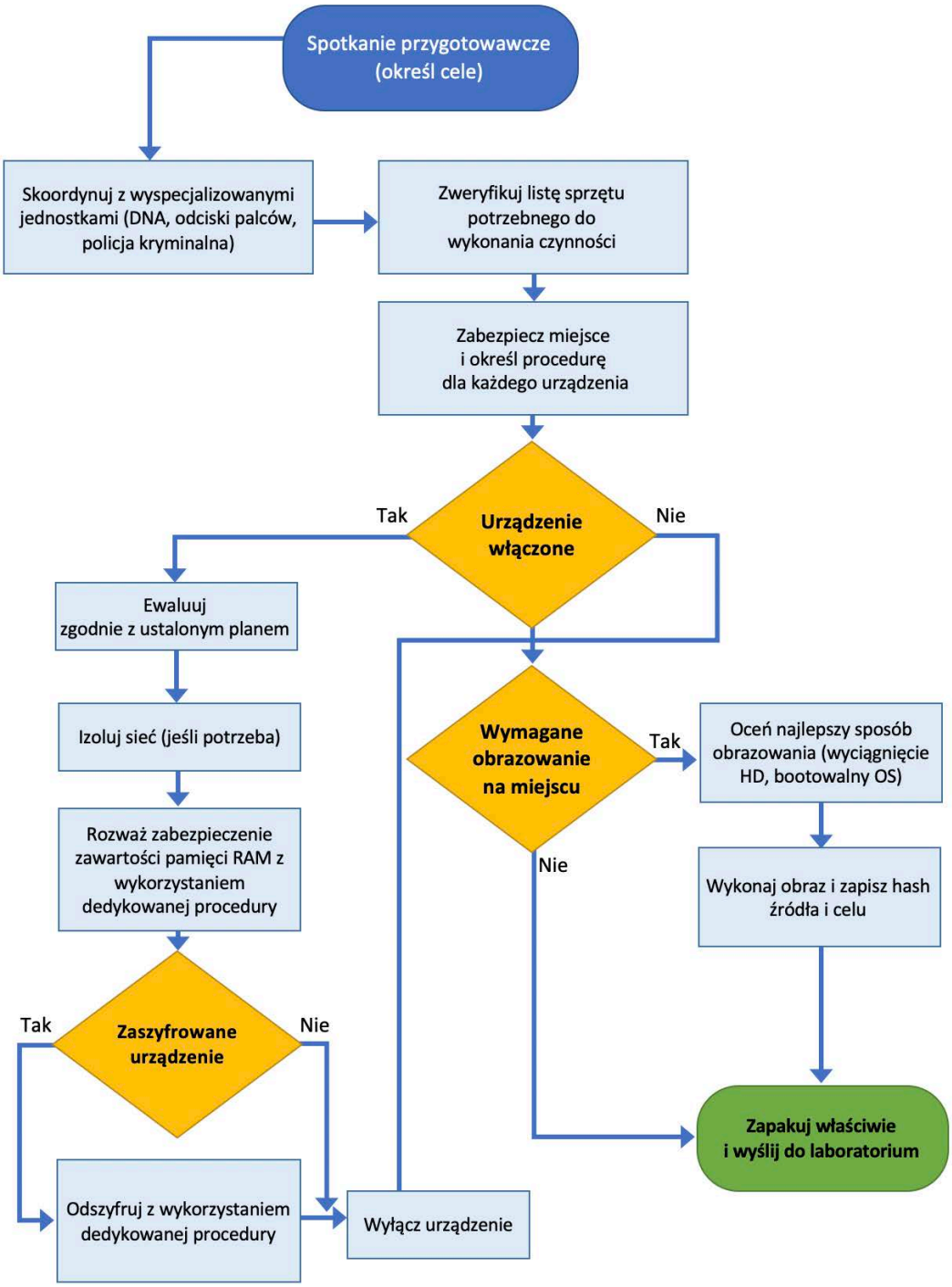
• **Miejsce przechowywania danych**. Nie jest niczym niezwykłym, że dane są przechowywane w innej lokalizacji, niż fizyczny sprzęt podejrzanego. W związku z tym konieczne jest sprawdzenie rzeczywistej lokalizacji, aby uzyskać dodatkowe upoważnienie, zwłaszcza jeśli dane są przechowywane w innej jurysdykcji lub jeśli wymagany jest dodatkowy sprzęt specjalistyczny w celu zapewnienia integralności dowodów. Wszystkie dane, które są potrzebne do przeprowadzenia czynności w związku z przetwarzaniem dowodów elektronicznych, powinny być określone w postanowieniu o przeszukaniu lub w odpowiednich procedurach poprzedzających przeszukanie i zatrzymanie.

Przy spełnianiu wymogów formalnych należy jasno i precyzyjnie określić cele czynności w odniesieniu do:

- upoważnienia do zatrzymania,
- pozyskiwania kopii kryminalistycznych na miejscu lub nie,
- analizowania urządzeń na miejscu,
- użycia aplikacji pozyskującej hasła,
- upoważnienia do zmiany hasła do kont e-mail, serwisów społecznościowych itd.

Biorąc pod uwagę liczbę różnych przypadków, powinno rozważyć najbardziej odpowiednie działania dla konkretnej sprawy. W większości sytuacji wskazane jest używanie wyrażeń, które bez wątpliwości wskazują czynności, które należy wykonać. Przykładowo, *wnioskuje się, aby zatrzymanie, kopiowanie i analiza urządzeń elektronicznych zdolnych do przechowywania informacji w postaci cyfrowej została wykonana na miejscu.* Stopień precyzji i szczegółowości będzie zależeć od jurysdykcji oraz obowiązujących w niej ram prawnych i proceduralnych.

2.2. Miejsce dostarczenia dowodów



Obraz 1: Schemat etapu i procedury planowania

Przed rozpoczęciem jakichkolwiek czynności przeszukania i zatrzymania należy określić miejsce dostarczenia dowodów.

Kopie kryminalistyczne, jak również urządzenia, które wymagają szczególnego traktowania, powinny zostać wysłane do odpowiedniego wydziału/zespołu w celu przetwarzania i analizy.

W każdym przypadku należy zadbać o odpowiednie zapakowanie i transport oraz dołączenie właściwej dokumentacji, aby zapewnić ciągłość łańcucha dowodowego, który rozpoczął się podczas zatrzymania.

2.3. Przygotowanie narzędzi

Wskazane jest posiadanie listy kontrolnej rzeczy potrzebnych do zabrania na miejsce, aby można było zweryfikować, czy wszystko, co jest potrzebne jest dostępne i jest w dobrym stanie. Przykładowa lista znajduje się poniżej (do dostosowania zgodnie z wymogami proceduralnymi i prawnymi w danej jurysdykcji).

Niezwykle ważne jest posiadanie wystarczającej liczby urządzeń, gdzie będą przechowywane obrazy kryminalistyczne, klony lub dane z zewnętrznych źródeł. Urządzenia te powinny być nowe, albo przynajmniej bezpiecznie wymazane poprzez nadpisanie wszystkich danych znaną sekwencją znaków, najczęściej 00h, aby uniknąć ewentualnego zanieczyszczenia danych.

Poniżej umieszczona jest lista składająca się z minimalnych narzędzi potrzebnych do udanego przeszukania i zatrzymania, którą funkcjonariusz musi wziąć pod uwagę:

Wyposażenie kryminalistyczne	
◯	Laptop z zainstalowanymi niezbędnymi narzędziami kryminalistycznymi (informatyki śledczej)
◯	Blokery sprzętowe
◯	Dongle z licencjami do narzędzi Dongle 1 Dongle 2 Dongle 3
◯	Wystarczający zasób pamięci zewnętrznej (zewnętrzne HDD) na obrazy i zgrywanie danych Hard Disk 1 Hard Disk 2 SD card 1
◯	HD z dodatkowym oprogramowaniem kryminalistycznym lub bootowalne urządzenia
Narzędzia do rozkręcania	
◯	Śrubokręty (płaskie, gwiazdki, sześciokątne i inne pasujące do konkretnych modeli, takich jak HP lub Apple)

◯	Szczypce (standardowe i spiczaste)
◯	Kombinerki (do przecinania przewodów)
◯	Małe pęsety
Dokumentowanie	
◯	Aparat lub kamera (do fotografowania miejsca oraz zawartości ekranu)
◯	Markery permanentne (do opisywania i identyfikacji dowodów)
◯	Etykiety (do oznaczania i identyfikowania części sprzętu, zasilaczy)
◯	Etykiety do opisywania dowodów
Materiały potrzebne do pakowania i transportu oraz eksploatacyjne	
◯	Worki na dowody
◯	Kartony na dowody takie jak USB, DVD, CD
◯	Worki antystatyczne na dowody
◯	Worki ekranowane (Faradaya) do odcięcia sygnału urządzeń mobilnych i innych, które mogą odbierać dane za pośrednictwem sieci mobilnej/Wi-Fi
Inne przedmioty	
◯	Mała latarka ze statywem

◯	Rękawiczki
◯	Duże gumki recepturki
◯	Lupa
◯	Przewody sieciowe (crossowane i skrętki)
◯	Maska

3. ETAP PRZESZUKANIA I ZATRZYMANIA

Bezpieczeństwo uczestników podczas przeszukania i zatrzymania to priorytetowa kwestia. Do tego celu służą specjalnie wyszkolone jednostki. Nikt nie powinien wchodzić na miejsce bez uprzedniego jego zabezpieczenia. Osoby znajdujące się na miejscu zdarzenia powinny pozostawać pod kontrolą w trakcie wykonywania czynności, aby uniknąć zmian lub naruszenia danych.

Opisane poniżej techniczne kroki mają charakter sugestii i są przedmiotem obowiązujących w danej jurysdykcji wymogów prawnych i proceduralnych.

3.1. Zabezpieczenie miejsca

W przypadku zabezpieczania dowodów elektronicznych celem jest uniknięcie utraty, zmiany lub zniszczenia jakiegokolwiek z dowodów. W tym celu należy podjąć następujące środki:

- Usunąć i zabronić dostępu do miejsca czynności osobom nieupoważnionym. Należy trzymać je z dala od komputerów, telefonów komórkowych i innych wrażliwych przedmiotów, w tym od źródeł zasilania. Ponadto, podejrzani nie powinni mieć możliwości komunikowania się z nikim, kto nie jest na miejscu zdarzenia, aby zapobiec zdalnemu zniszczeniu danych.
- Szybko zlokalizować najbardziej oczywiste elementy, komputery i telefony komórkowe, szczególnie te, które są podłączone do Internetu i te, które wymagają przedsięwzięcia specjalnych środków w celu zapobieżenia utracie danych.
- Sprawdzić występowanie sieci bezprzewodowych, które umożliwiają dostęp i modyfikację danych z zewnątrz.
- Odmówić wszelkiej pomocy oferowanej w czynnościach przez osoby nieupoważnione.

3.2. Ocena

Po wstępnym zabezpieczeniu miejsca zdarzenia, osoby podejmujące pierwsze czynności powinny mieć możliwość jego ogólnej oceny. Obejmuje to ogólną ocenę ilości materiału możliwego do przetworzenia, rodzaju przetwarzania oraz potrzebnego sprzętu i czasu. Jest to najlepszy moment na sporządzenie dokumentacji fotograficznej, ponieważ na tym etapie miejsce zdarzenia ulegnie niewielkim zmianom.

Chociaż tradycyjne metody prowadzenia przeszukania polegały na zachowaniu jasnego porządku, zaczynając od dokładnego przeszukania pomieszczenia, aby następnie przejść do kolejnego, to w przypadku procesowania dowodów elektronicznych przestrzeganie tej metody staje się trudne. Wynika to z faktu, że pozyskanie lub skopiowanie dowodu jest procesem powolnym, który może trwać wiele godzin. Dlatego kluczowe jest jak najszybsze rozpoczęcie przetwarzanie tych dowodów przy jednoczesnym kontynuowaniu tradycyjnego przeszukania i zatrzymania.

Warto zaznaczyć, że urządzenia cyfrowe zawierające potencjalne dowody mogą być łatwo ukryte lub znajdować się w szafkach i szufladach (karty pamięci, telefony komórkowe itd.), dlatego miejsce zdarzenia należy przeszukiwać ostrożnie, mając na uwadze fakty, które mają być dowiedzione.

3.3. Dokumentacja

Wszystkie procesy zabezpieczania i gromadzenia dowodów powinny być należycie udokumentowane, zgodnie z obowiązującymi wymogami prawnymi i proceduralnymi. W tym celu należy prowadzić wyczerpujący rejestr lokalizacji i pierwotnego stanu urządzeń.

Poniżej znajdują się przykłady prawidłowej dokumentacji miejsca zdarzenia:

- laptop: dowód numer EVI001,
- wewnętrzny dysk twardy: dowód numer EVI001A,
- nośnik USB: dowód numer EVI001B,
- DVD: dowód numer EVI001C.

W tym momencie można ocenić możliwość zatrzymania wyłącznie tych urządzeń, które zawierają informacje, do których można uzyskać fizyczny dostęp, dokumentując oględziny bez ich przetwarzania. W poprzednim przykładzie urządzenia, które zawierały dane to wewnętrzny dysk twardy, zewnętrzny nośnik USB i DVD, podczas gdy laptop bez powyższych elementów nie zawiera użytecznych informacji. Z tego względu należy unikać transportowania i przechowywania urządzeń, o których wiadomo, że nie dostarczą żadnych danych. Ta ewentualność musi być oceniona przez specjalistę, ponieważ zinwentaryzowane dowody mogą mieć związek z urządzeniem, z którego pochodzą i bez którego nie będzie możliwa ich analiza. Procedura ta będzie dyskutowana bardziej wnikliwie w sekcji opisującej szczególne procedury.

Dla każdego urządzenia należy udokumentować:

- rodzaj: komputer, dysk twardy, dysk flash, DVD itd.,
- marka i model,
- pojemność nośnika ze wskazaniem, czy jest to MB, GB lub TB,
- numer seryjny,
- stan: uszkodzony, włączony, wyłączony itd.,
- lokalizacja: położenie i konkretne miejsce,
- bezpieczeństwo: hasło dostępowe, PIN,
- komentarz: wykorzystywane wyłącznie przez dzieci, niepodłączone do Internetu itd.,

Wreszcie, wszelkie adnotacje związane z użyciem haseł, ustawień, kont e-mail, jak również plastików od kart SIM z ich ICCID, oryginalnym numerem PIN i PUK oraz wszelkie inne istotne informacje, które mogą zostać odnalezione i udokumentowane. Będą one wykorzystane w trakcie późniejszej analizy urządzeń.

3.4. Zabezpieczenie i obchodzenie się z dowodem cyfrowym

Zasadniczo stosuje się następujące zasady, jednak w przypadku niektórych urządzeń należy zapoznać się ze szczegółowymi procedurami (opisanymi w kolejnych sekcjach):

a) Jeśli urządzenie jest włączone, nie wyłączaj go.

Sprawdź, czy jest zainstalowane oprogramowanie utrudniające śledztwo: lokalne lub zdalne programy usuwające dane lub zapewniające dostęp zdalny. Zatrzymaj te procesy, nawet przez wyciągnięcie przewodu zasilającego lub wyjęcie baterii, jeśli to konieczne.

Odizoluj urządzenie od sieci, do których jest podłączone, chyba że masz upoważnienie do dostępu do usług chmurowych.

Wyłącz wygaszacze ekranu, aby nie dopuścić do hibernacji lub zatrzymania urządzenia.

Sprawdź, czy na urządzeniu uruchomiony jest jakikolwiek system szyfrowania (Bitlocker, FileVault, VeraCrypt, PGP Disk itd.).

Sprawdź, czy urządzenie jest podłączone do zasilania.

b) Jeśli urządzenie jest wyłączone, nie włączaj go, dopóki nie zostanie przetworzone w należyty sposób.

Jeśli lokalne przepisy na to zezwalają, należy zapytać podejrzanego o hasło/PIN i sprawdzić, czy są poprawne.

Nawet, jeśli urządzenie nie jest w pełni zaszyfrowane ważne jest, aby mieć hasła podejrzanego. Podejrzany mógł zaszyfrować plik lub użyć tego samego schematu hasłowania w innym systemie.

Względem urządzeń można wykonać następujące czynności:

- **Zatrzymanie**. Urządzenie jest w prosty sposób udokumentowane, opisane i zamknięte, pozostawione do podjęcia decyzji o dalszej analizie przez sąd lub inny uprawniony organ. Żadne inne czynności nie są podejmowane do czasu, aż nie zostanie ponownie otwarte.
- **Wykonanie kopii kryminalistycznej.** Do każdego dowodu zastosuj właściwą procedurę opisaną w niniejszym Poradniku.

Wykonane czynności będą musiały być udokumentowane:

- **wykorzystana procedura**: sklonowanie, zobrazowane lub inna wykorzystana procedura,
- **narzędzie**: kopiarka, bloker, oprogramowanie itd.,
- **miejsce docelowe**: docelowy dysk, plik z danymi z telefonu itd.,
- **HASH:** algorytm i uzyskana suma kontrolna,
- **obserwacje**: wszelkie zdarzenia zaistniałe podczas kopiowania.

3.4.1. Analiza live włączonych komputerów i laptopów

Konieczne jest prowadzenie wyczerpującej dokumentacji wykonywanych czynności, jak również daty i czasu ich wykonania.

Różnorodność możliwych scenariuszy podczas pozyskiwania wymaga szczególnych rozważań dla każdego z nich. Jednakże, jeśli chodzi o pozyskiwanie danych ulotnych, należy przestrzegać z góry ustalonej metodologii z uwzględnieniem kolejności ich utraty (ulotności).

Jeśli na miejscu zdarzenia używane są narzędzia kryminalistyczne, może to robić wyłącznie wykwalifikowany personel i należy zadbać o to, aby przyczyna badania dowodu na miejscu została udokumentowana i nadzorowana.

Istnieją narzędzia, które mogą pomóc w analizie live, opracowane specjalnie dla organów ścigania. Jednym z tych Narzędzi jest **FiRST,** będący częścią projektu FREETOOL policji berlińskiej (Niemcy), który jest narzędziem dla osób, które podejmują pierwsze czynności. Zamierzeniem FiRST jest poinformowanie osoby podejmującej pierwsze czynności, czy maszyna może być zamknięta (wyłączona). FiRST sprawdza, czy tradycyjna analiza post mortem może skończyć się niepowodzeniem lub być niekompletna. Obejmuje to sprawdzenie obecności oprogramowania szyfrującego lub wymazującego dyski, zasobów sieciowych/chmurowych, maszyn wirtualnych itd. Jeśli zostaną wykryte, osoba jest ostrzegana przed niebezpieczeństwem związanym z odłączeniem zasilania i zaleca się jej kontakt ze specjalistą. Więcej informacji o projekcie można znaleźć na jego oficjalnej stronie: https://freetool.ucd.ie.
Jeśli konkretne narzędzie jest niedostępne, możesz wziąć pod uwagę poniższą listę stworzoną przez Kuhlee i Völzow w celu wyboru optymalnego narzędzia akwizycji danych ulotnych (*Computer Forensik Hacks, O'Reilly, ISBN 978-3-86899-121-5*).

Ulotne dane	**Narzędzia Windows-owe**	**Narzędzia Linux-owe**
zawartość RAM	Dumpit, Winen, Mdd, FTK Imager	dd, fmem
tablice routingu, cache ARP, statystyki Kernel-a	Route PRINT, arp –a, netstat	netstat –r –n route arp -a
cache DNS	Ipconfig/displaydns	mdc dumpdb (if installed)
wylistowanie działających procesów	PsList, ListDLLs, CurrProcess, tasklist	ps –ef, lsof
wylistowanie aktywnych połączeń sieciowych		netstat –a, ifconfig
wylistowanie programów i usług używających sieci	sc queryex, netstat -ab	netstat -tunp
otwarte pliki	Handle, PsFile, Openfiles, net file	lsof, fuser
udziały sieciowe	Net share, Dumpsec	showmount –e, showmount –a smbclient -L
otwarte porty	OpenPorts, ports, netstat -an	netstat –an, lsof
połączeni użytkownicy	Psloggedon, whoami, ntlast, netusers /l	w, who –T, last
zaszyfrowane archiwa	Manage-bde (Bitlocker), efsinfo (EFS)	mount –v, ls /media

aktywne udziały sieciowe	Fsinfo, reg (mounted Devices)	mount –v, ls /media
dostęp zdalny i monitoring sieci	Psloglist	/etc/syslog.conf Port UDP 514
konfiguracja systemu i sieci	Systeminfo, msinfo32, ipconfig /all	ifconfig –a netstat -in
nośniki	Reg (Mounted Devices), Net share, netstat -a	mount –v, ls /media
data i czas	Time /T, date /T, uptime	time, date, uptime
zmienne środowiska	Cmd /c set	env, set
zawartość schowka	pclip	
zawartość dysku	FTK Imager, EnCase, Tableau Imager	dc3dd, ewfacquire, Guymager

Wiele z tych narzędzi jest dostępnych na stronie Sysinternals Microsoft-u oraz w oficjalnych repozytoriach Linux-owych.

W wyborze narzędzi konieczne jest, aby mieć na uwadze:

- Należy użyć narzędzi, które mają mniejszy wpływ na badany system. Do pozyskania pamięci RAM, na przykład aby uniknąć nadpisania danych, preferowane jest wykorzystanie małych narzędzi, takich jak "dumpit" niż wykorzystanie graficznego narzędzia, jak "FTK Imager".
- Preferowane jest również użycie narzędzi, które mają własne pliki wykonywalne i nie wykorzystują tych z badanego systemu. Podobnie, śledczy musi być w stanie umotywować w postępowaniu użyteczność i funkcjonalność narzędzia.
- Wykorzystane narzędzia powinny wyłącznie zabezpieczać dane ulotne. Dane, które będą dostępne na dysku twardym powinny być analizowane później z wykorzystaniem wcześniej opisanych procedur.
- Nośniki podejrzanego nigdy nie powinny być wykorzystane do zabezpieczania danych. Te dane muszą być zachowane na zewnętrznych nośnikach.
- Są to procesy, które mogą trwać wiele godzin. Z tego względu należy upewnić się, że systemy oszczędzania energii ich nie zakłócą.

3.4.2. Brak możliwości dostępu do danych na włączonych urządzeniach

Zdarzają się sytuacje, kiedy urządzenie jest włączone, a mimo to nie ma możliwości dostępu do jego zawartości. Może się zdarzyć, że urządzenie przeszło w tryb bezczynności lub włączył się wygaszacz ekranu, a po wyjściu z tego stanu urządzenie żąda danych uwierzytelniających, albo hasła. Pierwszą i technicznie prostą czynnością jest zażądanie tego hasła od użytkownika/właściciela. W przypadku odmowy, można zastosować kilka technik, aby uniknąć utraty danych ulotnych.

Należy zaznaczyć, że techniki te powinny być wykorzystywane przez specjalistów w przypadkach, w których jest pewne, że utrata danych ulotnych oznacza brak możliwości dostępu do zawartości pozostałej zawartości urządzenia, kiedy zostanie ona zaszyfrowana.

W pozostałych przypadkach będzie to uzasadniało wyłączenie włączonego urządzenia.

a) technika „cold-boot RAM”. Jest to technika polegająca na zamrożeniu pamięci RAM ciekłym azotem. Po wykonaniu tej czynności komputer jest wyłączany i uruchamiany z systemem operacyjnym z CD lub pendrive z narzędziami pozwalającymi wykonać zrzut pamięci RAM. Kiedy pamięć jest zamrożona w trakcie procesu wyłączania systemu, dane są zachowywane.

Ta technika opiera się na badaniach przeprowadzonych na Uniwersytecie Princeton[1] i może nie być użyteczna.

b) transport badanego urządzenia bez jego wyłączania. Inna metodą może być użycie przenośnego systemu zasilania, który podtrzymuje urządzenie do czasu przyjazdu laboratorium kryminalistycznego, gdzie będzie poddane dalszym czynnościom.

3.5. Etap zatrzymania

Protokół z przeszukania i zatrzymania zazwyczaj oznacza początek łańcucha dowodowego. Konieczne więc będzie określenie następnego miejsca oraz osób odpowiedzialnych za nadzór nad transportem zatrzymanych dowodów. Ten proces będzie uwzględniał wymogi prawne obowiązujące w danej jurysdykcji.

3.5.1 Pakowanie i transport

Wszystkie dowody z przeszukania i zatrzymania muszą spełniać następujące wymogi:

- Przed przystąpieniem do pakowania upewnij się, że cały zebrany materiał jest odpowiednio zaewidencjonowany i oznakowany.
- Jeśli to możliwe, do pakowania i transportu zatrzymanych urządzeń użyj oryginalnych opakowań.
- Dowody muszą być jednoznacznie oznakowane.
- Etykieta musi wskazywać, czy dowody były skopiowane/klonowane, czy też nie.

Do zaplombowania dowodów należy użyć odpowiednich materiałów, aby uniknąć ewentualnej manipulacji przy urządzeniach. Plomby muszą uniemożliwiać dostęp do elementów wewnętrznych (dysków twardych i pamięci) zarówno fizycznie, jak i poprzez porty.

W zależności od miejsca docelowego, dowody będą pakowane oddzielne, bez mieszania ich z inną dokumentacją lub innymi urządzeniami. Ułatwi to staranną akwizycję kopii kryminalistycznych lub bezpośrednie przekazanie do laboratorium. Każde opakowanie zawierające dowód elektroniczny powinno być oznakowane zewnętrznie ze wskazaniem identyfikatora, który określa jego rodzaj, pochodzenie i zawartość.

Środki transportu i tymczasowe nośniki muszą zapewniać integralność urządzeń, chronić przed wstrząsami i przed źródłami promieniowania elektromagnetycznego, ciepłem lub wilgocią, które mogą je uszkodzić.

4. WZGLĘDY TECHNICZNE

4.1. Kopia kryminalistyczna

Jedna z głównych zasad procesu analizy kryminalistycznej wskazuje, że poza wyjątkowymi przypadkami, badanie materiału dowodowego nie powinno być przeprowadzone z użyciem oryginalnego urządzenia. Dlatego wymagane jest wykonanie kopii lub klona danych zawartych na

[1] Halderman A., Schoen S. D., Heninger N., et alia, “Lest We Remember: Cold Boot Attacks on Encryption Keys”, artykułu opublikowanego w *Proc. 17th USENIX Security Symposium (Sec ’08), San Jose, CA, July 2008. Dostępnego na: (usenix.org)*

oryginalnym urządzeniu, aby zapobiec naruszeniu integralności. Specjalista informatyki śledczej będzie wtedy korzystał z obrazu/ze skopiowanych danych, aby wykonać analizę.

Kopia ta musi być dokładną kopią binarną oryginalnego nośnika, bez względu na jego zawartość. Można to zrobić na dwa sposoby:

a) nośnik na nośnik (klon): może to być wykonane poprzez pozyskanie dokładnej kopii binarnej oryginalnego nośnika na inny, wcześniej wyczyszczony nośnik o takiej samej lub większej pojemności,

b) nośnik do pliku (obraz): może to być wykonane przez wygenerowanie jednego lub więcej plików powiązanych ze sobą, zawierających identyczną kopię oryginalnego nośnika. Najbardziej popularne formaty to "dd" (raw) oraz "E01".

Procedury te można wykonać z wykorzystaniem sprzętowych kopiarek/imagerów, które chronią oryginalne urządzenia przed jakimkolwiek nadpisaniem lub zmianą podczas tego procesu. Jeśli do wykonywania kopii kryminalistycznych wykorzystywane jest specjalne oprogramowanie, zaleca się stosowanie sprzętowych lub programowych blokerów zapisu.

Zalety tworzenia obrazu:

- umożliwia wykonanie kopii o ustalonym rozmiarze, co ułatwia ich przechowywanie i późniejszą analizę,
- zapewnia kompresję bez utraty danych, co pozwala oszczędzić miejsce na nośniku docelowym,
- umożliwia szyfrowanie w razie potrzeby, co zapewnia większe bezpieczeństwo,
- może zwierać informacje o sprawie, dane dotyczące tworzenia obrazu, weryfikacji integralności, w tym sumy kontrolne,
- zapobiega nadpisaniu/zanieczyszczeniu kopii.

Te formaty kopii mogą być czytane bezpośrednio i bardziej wydajnie przez oprogramowanie analityczne.

4.2. Alternatywy dla kopii kryminalistycznej

Wykonanie dokładnej fizycznej kopii binarnej całego nośnika w sytuacjach na przykład zabezpieczenia serwerów, NAS-ów, wirtualnych lub zaszyfrowanych dysków nie zawsze jest możliwe.

W tych przypadkach istnieją inne techniki pozyskiwania dowodów cyfrowych.

a) Kopia logiczna wolumenu. Ta metoda jest stosowana na przykład wtedy, kiedy trzeba pozyskać zawartość zaszyfrowanego wolumenu, który jest podpięty do włączonego komputera. Aby zachować te informacje tworzona jest logiczna kopia. Gdyby wykonano kopię fizyczną dysku, uzyskano by partycję, która byłaby nieczytelna (zaszyfrowana). Kopia logiczna pozwala uzyskanie zawartości w takiej formie i w taki sam sposób, jak jej użytkownik (podejrzany).

b) Kopia logiczna pliku. Wykonuje się ją poprzez wygenerowanie, z wykorzystaniem odpowiedniego oprogramowania, kopii oryginalnych danych po wybraniu tego, co może być istotne dla sprawy. Na przykład, w środowisku firmowym, można wykonać kopię logiczną katalogu podejrzanego użytkownika. Wadą tego rozwiązania jest to, że nie zostanie zachowana zawartość niezaalokowanego obszaru oraz metadane oryginalnego systemu plików mogą nie zawsze zostać zachowane. Wykonywanie logicznych kopii kryminalistycznych nie uniemożliwia zachowania wartości dowodowej materiału. Kiedy są wykonywane, należy użyć odpowiedniego narzędzia i metody, aby zabezpieczyć przed zapisem i zachować jak najwięcej metadanych oraz skorzystać z algorytmu kryptograficznego, który pozwoli na weryfikację integralności zabezpieczonych danych.

4.3. Funkcja HASH

Funkcja HASH lub funkcja skrótu jest wykorzystywana do weryfikacji integralności danych. Innymi słowy, jest to pozyskiwanie ich "cyfrowego odcisku palca" (sumy kontrolnej).

W przypadku dowodu elektronicznego ta procedura jest stosowana podczas wykonywania kopii oryginalnych nośników, a więc jeśli wartość funkcji hashującej oryginalnej i zabezpieczonej wartości jest obliczona, muszą one być identyczne. Proces ten jest nazywany weryfikacją.

Ta procedura jest również wykorzystywana do wykrywania znanych plików pośród dowodów. Istnieją wiarygodne bazy danych plików (pochodzących z instalacji systemów operacyjnych lub innych aplikacji), takie jak NSRL (ang. National Software Reference Library), które pozwalają na ich wykluczenie, a także inne bazy danych z sygnaturami znanych plików, które pozwalają śledczym na ich identyfikację, śledzenie a nawet udostępnianie organom ścigania bez konieczności dystrybuowania oryginalnych plików.

Niektóre technologie, takie jak SSD, stają się nowym wyzwaniem dla metod weryfikacji dowodów. Ze względu na sposób działania pamięci SSD, mogą one czasami same usuwać dane, nawet jeśli są niepodłączone do żadnego interfejsu, a są jedynie włączone. Należy rozważyć alternatywy dla tradycyjnego wyliczania sum kontrolnych dla całych nośników, takie jak wyliczanie sum dla partycji logicznej lub dla plików.

5. SZCZEGÓLNE PROCEDURY

W poprzednich sekcjach wyjaśniono ogólną procedurę zachowywania integralności dowodów cyfrowych. Jednak podczas przeszukania i zatrzymania specjalista informatyki śledczej może znaleźć wiele urządzeń, które ze względu na ich charakter wymagają szczególnych procedur. Będzie to spowodowane złożonością w zakresie podłączenia niektórych z nich, obecności systemów szyfrowania, dużej ilości danych do ekstrakcji lub brakiem standardowych narzędzi.

Poniższe sekcje zawierają ogólne zasady postępowania z niektórymi urządzeniami, które mogą być często znajdowane w trakcie przeszukań i zatrzymań.

Obraz 2: Urządzenia: Smartfony i tablety

5.1. Smartfony - tablety

Telefony komórkowe stały się podstawowym źródłem dowodowym dla informatyki śledczej, ponieważ są zawsze włączone i bardzo osobiste dla każdego użytkownika. Smartfony, takie jak urządzenia Apple lub z Androidem, mogą zawierać od 16GB do 1TB danych.

Ponadto, telefon komórkowy może zawierać kartę SIM i wymienną kartę multimedialną, jeśli jest obsługiwana.

Każdy z tych elementów jest ważny dla śledztwa, ponieważ zawiera dane, które mogą umożliwić identyfikację właściciela lub zrozumieć jego aktywność przy użyciu telefonu komórkowego.

Wraz z pojawieniem się smartfonów i wprowadzeniem sklepów z aplikacjami, takich jak Google Play i iTunes Store (AppStore), użytkownik może instalować aplikacje, które mogą pozwolić na korzystanie z nowych usług, takich jak gry online, komunikatory internetowe i aplikacje do wymiany plików. W przypadku każdego telefonu komórkowego, badający powinien uzyskać dostęp do aplikacji w celu pozyskania wartościowego materiału istotnego dla sprawy, z zastrzeżeniem obowiązujących wymogów proceduralnych i prawnych w danej jurysdykcji.

5.1.1. Względy dotyczące zabezpieczenie dowodów z telefonów

Urządzenia mobilne stanowią wyzwanie dla kryminalistyki ze względu na szybkie zmiany w technologii. Obecnie w użyciu jest wiele marek i modeli urządzeń mobilnych. Wiele z tych urządzeń korzysta z zamkniętych systemów operacyjnych i opatentowanych interfejsów, co czasem utrudnia ekstrakcję dowodów cyfrowych. Do uzyskania dostępu może być niezbędna wiedza dotycząca konkretnej wersji, a podczas akwizycji danych mogą pojawić się następujące problemy:

- **Sygnały przychodzące i wychodzące** – Należy podjąć próbę zablokowania sygnałów przychodzących i wychodzących do/z urządzenia. Popularną metodą są pojemniki blokujące RF, np. worki Faradaya lub specjalne pomieszczenia. Pojemniki RF nie zawsze są skuteczne, mogą one wyczerpywać baterię, a błędy (w komunikacji) mogą powodować zmianę danych.
- **Przewody** – Przewody umożliwiające dostęp do danych mogą być unikatowe dla urządzenia i narzędzia.
- **Niszczenie danych** – Istnieją metody niszczenia danych lokalnie i zdalnie na urządzeniu mobilnym, dlatego urządzenie musi być jak najszybciej odizolowane od wszystkich sieci (np. operatora, Wi-Fi, Bluetooth). Badający powinni być świadomi, że mobilny system operacyjny może mieć zaszyte automatyczne procesy, które będą niszczyć dane przy podłączeniu zasilania lub po upływie określonego czasu. Powinni więc wybrać metodę ekstrakcji lub harmonogram, który uwzględnia te problemy, jeśli to konieczne.
- **Sterowniki** – Konflikty mogą wystąpić z powodu sterowników systemu operacyjnego, objętych patentami, niespójnymi lub właściwymi dla konkretnego vendora. Znalezienie odpowiednich sterowników może być trudne. Sterowniki dołączone do narzędzi informatyki śledczej lub pobrane ze strony internetowej mogą konkurować o przejęcie kontroli nad tym samym zasobem, jeśli zainstalowano więcej niż jedno narzędzie.
- **Zmienny charakter danych** – Dane na aktywnych (włączonych) urządzeniach mobilnych stale się zmieniają i nie istnieją dla nich metody blokowania zapisu (blokery).
- **Szyfrowanie** – Dane mogą być przechowywane w formie zaszyfrowanej, uniemożliwiającej dostęp lub analizę.
- **Narzędzia** – Narzędzia wykorzystywane do badania mogą nie być w najwyższej wersji z różnych powodów, takich jak opóźnienie w zakupie/opóźnienia budżetowe, albo wymagania dotyczące weryfikacji sprzętu, oprogramowania lub firmware.
- **Triage** – Triage urządzeń mobilnych nie jest uznawane za pełne badanie. Jednak jeśli jest wykonywany, urządzenie powinno być zabezpieczone i odizolowane od wszelkich sieci.
- **Niespójne standardy branżowe** – Producenci i operatorzy mogą używać opatentowanych metod przechowywania danych (np. zamknięte systemy operacyjne, opatentowane sposoby dostępu do danych).
- **Utrata zasilania** – Wiele urządzeń mobilnych może utracić dane lub załączyć dodatkowe mechanizmy bezpieczeństwa, kiedy zostanie wyłączone.
- **Hasła** – Mechanizmy uwierzytelnienia mogą ograniczyć dostęp do urządzenia i jego danych. Tradycyjne metody łamania haseł mogą prowadzić do trwałego zablokowania lub zniszczenia danych.
- **Wymienne nośniki pamięci** – Procesowanie wymiennych nośników, które nadal znajdują się w urządzeniu wiąże sie z ryzykiem (np. nieuzyskanie dostępu do wszystkich danych, w tym danych usuniętych, zmiana znaczników daty/czasu).
- **Moduły identyfikacyjne np. karty USIM, CSIM, RUIM** – Brak lub usunięcie tego modułu może uniemożliwić badającemu dostęp do danych w pamięci telefonu. Włożenie modułu z innego urządzenia może spowodować utratę danych.
- **Szkolenie** – Osoba zabezpieczająca i analizująca urządzenie mobilne powinna być przeszkolona w zakresie zabezpieczenia i utrzymania integralności danych.
- **Niezaalokowane /usunięte dane** – Narzędzia dla urządzeń mobilnych mogą wspierać wyłącznie logiczną akwizycję danych, co może ograniczać ilość danych, które mogą być odzyskane.

Dokumentuj zabezpieczenie urządzenia zgodnie z wytycznymi i procedurami oraz wszelkimi obowiązującymi przepisami prawa. Dokumentacja może zawierać opisy lub fotografie z miejsca zabezpieczenia, stan urządzenia (np. włączone/wyłączone, wymagane użycie kodu dostępu), opis interakcji badającego z urządzeniem oraz fizyczne cechy każdego urządzenia (np. uszkodzenie, informacje identyfikujące takie jak marka, model, numer seryjny i wszelkie znaki identyfikacyjne oraz połączenia).

Dokumentacja łańcucha dowodowego powinna być zgodna z zabezpieczeniem oraz zawierać opis lub unikatowe identyfikatory dowodów, datę i czas zabezpieczenia oraz przekazania. Zapisy powinny w pełni identyfikować każdą z osób, która była w posiadaniu dowodów (np. nazwisko, stopień, podpis).

5.1.2. Proces zabezpieczenia dowodów z telefonów

Poniższe schematy przedstawiają najlepsze praktyki w zakresie zabezpieczania dowodów oraz zatrzymywania poszczególnych rodzajów urządzeń mobilnych i mogą nie być wyczerpujące.[2] Okoliczności mogą uzasadniać odstępstwa od przedstawionych poniżej procedur. Osoby podejrzane nie powinny mieć dostępu do urządzeń (np. podejrzany wprowadza identyfikatory biometryczne lub kody).

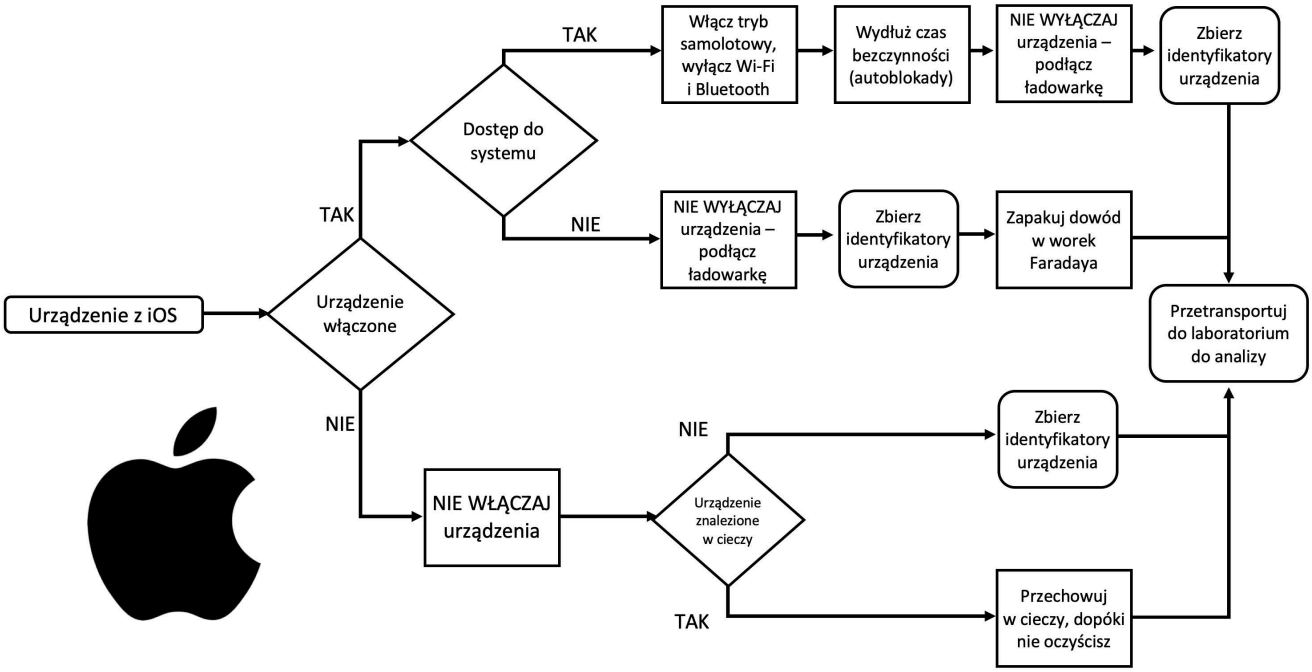
5.1.3. Zabezpieczenie urządzeń z iOS

iOS to system operacyjny dla urządzeń mobilnych stworzony i rozwijany przez firmę Apple wyłącznie dla urządzeń mobilnych tej firmy, w tym dla iPhone, iPad i iPod Touch. Poniższy schemat opisuje kroki, które należy podjąć w celu zabezpieczenia dowodów cyfrowych z urządzenia z iOS.

Wszystkie iPhone wykorzystują szyfrowanie sprzętowe i programowe, więc jeśli urządzenie posiada hasło, kod dostępu lub identyfikator twarzy (Face ID), użytkownik powinien podać informacje niezbędne do uzyskania dostępu do urządzenia, w przeciwnym razie laboratorium kryminalistyczne może nie być w stanie uzyskać dostępu do danych na nim zgromadzonych.

Obraz 3: Apple iPhone

[2] Niniejsze wytyczne są skopiowane z Najlepszych praktyk obchodzenia się i zabezpieczenia dowodów z urządzeń mobilnych (oryg. Best Practice for Mobile Device Evidence Collection and Preservation and Actuisition) v1.9 SWGDE z dn. 17.09.2020. Do Czytelnika należy zapoznanie się z najbardziej aktualną wersją tego dokumentu. Więcej informacji jest dostępnych na stronie: swgde.org/documents//published. W sekcji Referencje znajdują się wyłączenia oraz zasady udostępniania SWDGE.



Obraz 4: Schemat akwizycji dowodów z urządzeń z Apple iOS

Powyższy schemat nie jest wyczerpujący dla wszystkich wersji iOS. W celu uzyskania dostępu może być niezbędna wiedza specjalistyczna dotycząca konkretnej wersji, co może wpłynąć na powyższy schemat postępowania. Jeśli urządzenie jest włączone, może zawierać ulotne dane, w tym klucze kryptograficzne i nie powinno być wyłączane. Źródło zasilania powinno być podłączone tak szybko, jak to możliwe, aby zapobiec wyłączeniu urządzenia. Upewnij się, że zabezpieczasz również przewody do podłączenia zasilania. Jeśli to możliwe, zmień czas autoblokady, aby wydłużyć czas do automatycznego zablokowania urządzenia.

Jeśli urządzenie jest odblokowane, badający powinien przedsięwziąć kroki w celu zapobieżenia jego zablokowania, takie jak wyłączenie kodu blokady lub powtarzalna interakcja z ekranem dotykowym.

Przełącz urządzenie w tryb samolotowy i upewnij się, że Wi-Fi i Bluetooth są wyłączone. Jeśli urządzenie nie może być przełączone w tryb samolotowy, umieść je w worku Faradaya, aby zapobiec interakcji sieciowej, która potencjalnie może zmienić dane na urządzeniu. Urządzenia mobilne odcięte od sieci próbują uzyskać sygnał zwiększają moc anteny, co powoduje przyspieszone wyczerpywanie baterii. Jeśli konieczne jest podtrzymanie pracy urządzenia, należy podłączyć je do zewnętrznego źródła zasilania, na przykład power banku. Zarówno urządzenie, jak i źródło zasilania powinno być umieszczone w worku Faradaya. Jeśli źródło zasilania nie zostanie w nim umieszczone, wtedy przewód może działać jak antena i urządzenie może podłączyć się do sieci.

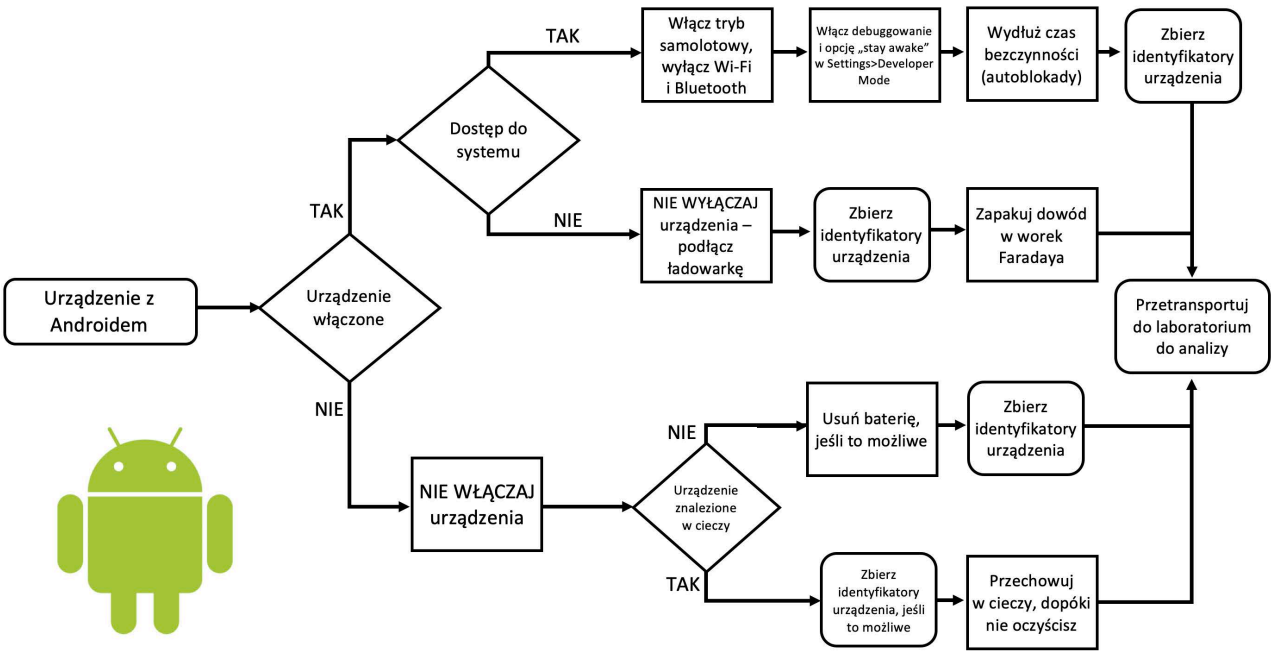
Jeśli urządzenie jest wyłączone, zostaw je wyłączone. Zbierz dane identyfikujące urządzenie, takie jak model, sieć i unikatowe identyfikatory, które są widoczne.

5.1.4. Zabezpieczenie urządzeń z Androidem

Android jest opartym o Linux-a systemem operacyjnym dla urządzeń mobilnych opracowanym przez firmę Google i posiadającym najwięcej instalacji na urządzeniach mobilnych spośród wszystkich systemów. Android jest dostępny w wielu różnych wersjach i, w przeciwieństwie do iOS, działa na urządzeniach produkowanych przez wiele firm. Poniższy schemat przedstawia kroki, jakie należy podjąć w celu akwizycji dowodów cyfrowych z urządzeń z Androidem.

Urządzenia z Androidem mogą wykorzystywać sprzętowe lub programowe szyfrowanie, więc jeśli urządzenie posiada hasło, kod dostępu lub identyfikator twarzy, użytkownik powinien podać informacje niezbędne do uzyskania dostępu do urządzenia, w przeciwnym razie laboratorium kryminalistyczne może nie być w stanie uzyskać dostępu do danych na nim zgromadzonych.

Obraz 5: Smartfony z Androidem



Obraz 6: Schemat akwizycji dowodów z urządzeń z Androidem

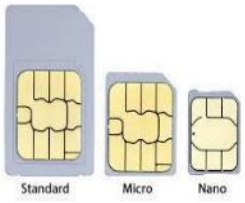
Powyższy schemat nie jest wyczerpujący dla wszystkich wersji Androida. W celu uzyskania dostępu może być niezbędna wiedza specjalistyczna dotycząca konkretnej wersji, co może wpłynąć na powyższy schemat postępowania.

Jeśli urządzenie jest włączone, może zawierać ulotne dane, w tym klucze kryptograficzne i nie powinno być wyłączane. Źródło zasilania powinno być podłączone tak szybko, jak to możliwe, aby zapobiec wyłączeniu urządzenia. Upewnij się, że zabezpieczasz również przewody do podłączenia zasilania. Jeśli to możliwe, zmień czas autoblokady, aby wydłużyć czas do automatycznego zablokowania urządzenia.

Przełącz urządzenie w tryb samolotowy i upewnij się, że Wi-Fi i Bluetooth są wyłączone. Aby mieć większe szanse na dostęp do zawartości (dowodów) w późniejszym czasie, zezwól na debugowanie USB.

Jeśli urządzenie nie może być przełączone w tryb samolotowy, należy postępować zgodnie z procedurą dla urządzeń Apple.

Jeśli urządzenie jest wyłączone, zostaw je wyłączone. Zbierz dane identyfikujące urządzenie, takie jak model, sieć i unikatowe identyfikatory, które są widoczne.



Obraz 7: Karty SIM

5.1.5. Karta SIM

Karta SIM/USIM może zawierać książkę adresową, wykaz połączeń i wiadomości SMS. Karta SIM może być chroniona kodem PIN. Jeśli próba wpisania PIN trzykrotnie zakończy się niepowodzeniem, dostęp do karty SIM jest blokowany. Aby ją odblokować potrzebny jest kod PUK, który jest umieszczony na oryginalnym plastiku, z którego wyłamano kartę SIM lub może być pozyskany od operatora. W każdym przypadku należy pozyskać ICCID, który jest identyfikatorem karty (numerem seryjnym).

Obraz 8: Karty pamięci

5.1.6. Wymienne karty pamięci

Jeśli urządzenie umożliwia korzystanie z wymiennych kart pamięci, to ta karta służy do rozszerzania pamięci telefonu. Wymienne nośniki są popularne w telefonach z systemem Android, ponieważ pozwalają użytkownikowi na przechowywanie multimediów, takich jak zdjęcia, filmy i pliki muzyczne, jak również dane aplikacji lub kopie zapasowe aplikacji, albo zawartości telefonu. Wymienne karty pamięci mogą potencjalnie być wykorzystywane przez wiele telefonów w czasie, w zależności od zwyczajów użytkownika.

Obraz 9: Składniki zasobu chmurowego

5.1.7. Dane w chmurze

Zarówno urządzenia Apple, jak i z Androidem, wymagają od użytkownika posiadania albo konta iCloud (Apple), albo Google (Android). Te usługi chmurowe pozwalają użytkownikowi backupować w chmurze dane oraz udostępniać zdjęcia, filmy i pliki muzyczne. Umożliwiają również tworzenie kopii zapasowych danych użytkownika na wypadek utraty lub w razie konieczności przeniesienia ich na nowe urządzenie.

5.1.8. Względy dotyczące zatrzymania

Tradycyjna kryminalistyka

Aby ustalić związek między urządzeniem mobilnym a jego właścicielem, konieczne może być przeprowadzenie tradycyjnych badań kryminalistycznych, takich jak badanie odcisków palców lub DNA. Jeśli podczas pozyskiwania i zabezpieczania urządzenia nie będzie obchodzić się z nim prawidłowo, dowody mogą zostać zanieczyszczone i stać się bezużyteczne. Dlatego ze wszystkimi potencjalnymi dowodami należy obchodzić się w rękawiczkach i przekazać je do odpowiedniego laboratorium, jeśli to konieczne. Tradycyjne badania kryminalistyczne (np. DNA, odciski palców) na urządzeniu mobilnym powinny być przeprowadzone przed czynnościami informatyki śledczej.

Dostęp

Hasła utworzone przez użytkownika również komplikują proces odzyskiwania danych z urządzeń mobilnych. Należy zebrać i dokumentować tego rodzaju informacje, jeśli to możliwe i zgodne z obowiązującymi w danej jurysdykcji wymogami prawnymi i proceduralnymi.

Izolacja sieci

Odłącz urządzenia mobilne od sieci, aby mieć pewność, że żadne dane nie zostaną zdalnie zmodyfikowane lub zniszczone. Urządzenia mobilne zazwyczaj mają funkcję przywracania do ustawień fabrycznych, która czyści zawartość i usuwa dane użytkownika. Ponieważ może być to wykonane osobiście lub zdalnie, konieczne jest przedsięwzięcie natychmiastowych środków ostrożności (np. oddzielenie użytkownika od urządzenia, izolacja sieci), aby zapewnić, że dowody nie zostaną zmodyfikowane lub zniszczone.

Ogólnie rzecz biorąc, dawniej badający izolowali urządzenia mobilne od sieci przełączając je w tryb samolotowy. Funkcja trybu samolotowego w nowszych wersjach systemów operacyjnych może nie wyłączać Bluetooth, Wi-Fi i innych protokołów łączności bezprzewodowej lub wyłączać je tylko tymczasowo. Badający powinni ręcznie upewnić się, że łączność sieciowa została wyłączona lub rozważyć alternatywne sposoby izolacji, takie jak umieszczenie w ekranowanym pojemniku, usunięcie karty SIM lub użycie karty CNIC dla telefonów GSM.

Osoba dokonują czynności powinna również ograniczyć wszelkie interakcje z urządzeniem, chyba że odbywa się to w kontrolowanym środowisku. Ma to na celu ochronę danych zawartych na urządzeniu oraz zapewnienie, że urządzenie nie łączy się z usługami chmurowymi i sieciami, ponieważ może to zmienić dane na urządzeniu lub umożliwić jego zdalne wymazanie.

Wyłączenie urządzenia w celu odizolowania go od sieci wiąże się z ryzykiem uruchomienia mechanizmów uwierzytelnienia (np. haseł, kodów PIN) lub włączenia zaawansowanych funkcji bezpieczeństwa, co potencjalnie może uniemożliwić dostęp do danych.

Tezy dowodowe

Osoba przekazująca urządzenie do analizy do laboratorium powinna wskazać okoliczności, które mają być udowodnione, ponieważ urządzenia takie jak smartfony zawierają wiele danych i nie wszystkie będą istotne dla sprawy.

Niektóre oprogramowanie informatyki śledczej umożliwia klonowanie danych z karty SIM na czystą kartę, przy czym oryginalne dane są kopiowane z pominięciem danych sieciowych. Telefon kojarzy rejestry połączeń, ustawienia i inne dane z konkretną kartą SIM. Jeśli telefon zostanie uruchomiony z inną kartą SIM lub bez tej karty, nie można uzyskać dostępu do tych danych i mogą one zostać utracone.

Zasady postępowania:

a) Urządzenie włączone

- Sfotografuj ekran w stanie zastanym. Sprawdź baterię i czy data oraz godzina wyświetlane przez urządzenie odpowiadają rzeczywistej dacie i godzinie w momencie zatrzymania.
- Sprawdź IMEI: wybierz * # 06 # i sfotografuj (uwaga: może to nie działać na smartfonach).
- Wykonaj logiczny obraz urządzenia za pomocą odpowiednich urządzeń, w tym odczytaj zawartość karty SIM.
- Wykonaj fizyczny obraz urządzenia, jeśli to możliwe.
- Wyłącz urządzenie. Wyjmij baterię, kartę SIM/USIM i zewnętrzne karty pamięci oraz sfotografuj to wraz z identyfikatorem dowodu.
- Wykonaj obraz kryminalistyczny karty pamięci, jak opisano w szczegółowej procedurze, jeśli nie została ona wykonana przez wyspecjalizowany zespół.
- Nie włączaj ponownie urządzenia.
- Zaplombuj wszystkie elementy i oznacz jako przetworzone.

b) Urządzenie wyłączone

- Sprawdź, czy można pozyskać obraz kryminalistyczny.
- Wyjmij baterię i zlokalizuj elementy, które należy sprawdzić: kartę SIM oraz zewnętrzne nośniki pamięci.

- Sprawdź, czy karta SIM/USIM jest chroniona kodem PIN. Jeśli próba wpisania PIN trzykrotnie zakończy się niepowodzeniem, dostęp do karty SIM jest blokowany. Aby ją odblokować potrzebny jest kod PUK, który jest umieszczony na oryginalnym plastiku, z którego wyłamano kartę SIM lub może być pozyskany od operatora. W każdym przypadku należy pozyskać ICCID, który jest identyfikatorem karty (numerem seryjnym).
- Zapisz czystą kartę SIM danymi z oryginalnej karty SIM i włóż do urządzenia. Telefon kojarzy rejestry połączeń, ustawienia i inne dane z konkretną kartą SIM. Jeśli telefon zostanie uruchomiony z inną kartą SIM lub bez tej karty, nie można uzyskać dostępu do tych danych i mogą one zostać utracone. Karta utworzona jako kopia oryginalnej zapewnia oprócz zachowania tych danych, że urządzenie nie połączy się z siecią.
- Wykonaj kopię kryminalistyczną wymiennych nośników pamięci, jeśli są obecne, postępując zgodnie ze szczegółową procedurą dla tego typu nośnika.
- Ponownie złóż urządzenie, uruchom i wykonaj kopię logiczną.
- Wykonaj fizyczny obraz urządzenia, jeśli to możliwe.
- Zaplombuj wszystkie elementy i oznacz jako przetworzone.
- Spróbuj zlokalizować i opisać oryginalne plastiki, w których były karty SIM z widocznymi kodami PIN oraz PUK.

5.2. Serwery

Serwery mogą świadczyć usługi dla innych stacji klienckich. Można je znaleźć przede wszystkim w środowiskach biznesowych, gdzie pełnią funkcje serwera plików, poczty, usług internetowych, baz danych, zarządzania użytkownikami itd. Fizycznie mogą wyglądać jak normalna stacja robocza, albo mogą być zainstalowane w szafach rack.

Przed przystąpieniem do czynności z serwerem, należy wziąć pod uwagę:

- Na co zezwala postanowienie o przeszukaniu/zatrzymaniu? Serwery mogą być podstawową częścią normalnego funkcjonowania przedsiębiorstwa, które nie musi być związane z przestępstwem. Czy uzasadnione jest pozostawienie organizacji, być może niezwiązanej z przestępstwem, bez tych usług? Czy zatrzymanie sprzętu jest naprawdę konieczne?
- Czy zapewniona jest współpraca ze strony administratora systemu lub personelu utrzymującego? Czy można im zaufać? Czy są zaangażowani w działalność przestępczą?
- Czy jasno określono, jakiego rodzaju informacje należy pozyskać?
- Czy znamy środowisko serwerowe i systemy operacyjne? Czy możemy odłączyć serwery od sieci lub nawet od zasilania, aby je odizolować?

Preferowanym sposobem zabezpieczania danych z serwerów jest wykonanie selektywnej logicznej kopii katalogu podejrzanego. Trzeba również wziąć pod uwagę pozyskanie logów zdarzeń, ustawień Active Directory, skrzynek mailowych oraz backupów.

5.3. Komputery osobiste

Pierwszym krokiem jest określenie, czy komputer jest włączony. Wiele komputerów może być w trybie oszczędzania energii z po prostu wyłączonym monitorem, w stanie uśpienia, hibernacji (Windows) i mogą sprawiać wrażenie, że są odłączone lub wyłączone. Należy sprawdzić podłączenie monitora do zasilania oraz podłączenie do stacji roboczej, a także podłączenie do zasilania lub świecenie diod LED, jeśli to może wskazywać na aktywność.

Aby zmienić stan komputera należy uniknąć naciskania włącznika, przyciska reset lub klawisza Enter. Najlepiej jest przesunąć myszkę lub użyć scroll-a, albo klawiszy shift. Należy zanotować dokładny czas tych czynności.

Jeśli urządzenie jest włączone i wykazuje aktywność, zaleca się podjęcie następujących działań:

- Sfotografuj ekran tak, aby była widoczna data, czas i strefa czasowa.
- Sprawdź aktywność użytkownika w danym momencie, taką jak aktywne ikony, paski postępu i aktywność aplikacji. Jeśli zaobserwujesz jakiekolwiek niszczące procesy, takie jak bezpieczne kasowanie, usuwanie logów lub zapisów, natychmiast je przerwij, nawet poprzez odłączenie zasilania.
- Sprawdź połączenia sieciowe, przewodowe lub bezprzewodowe.
- Wyłącz wygaszacze ekranu i opcje zasilania. Celem tego działania jest zapobieżenie zatrzymania lub wyłączenia urządzenia z utratą zastanego stanu systemu.
- Sprawdź zamontowane wolumeny i ich charakterystyki, po prostu szukając opcji szyfrowania lub udostępniania folderów innym komputerom w sieci.
- Sprawdź aktywności i połączenia z zewnętrznymi repozytoriami, takimi jak Dropbox, Google Drive, OneDrive itd. oraz aktualną aktywność w przeglądarkach, taką jak serwisy pocztowe, media społecznościowe itd.

W tym momencie należy ocenić, czy utrzymać lub rozłączyć połączenie sieciowe i odizolować sprzęt.

a) Urządzenie jest włączone

Ewaluacja na miejscu (triage). W ramach kontynuowania procesu zabezpieczania oraz w przypadkach, gdy poszukiwane są konkretne informacje i musi być to potwierdzone natychmiast (z uwagi na wymogi prawne lub proceduralne), można przeprowadzić bezpośrednie badanie dowodu w obecności strony oraz świadków. Można też wykonać kryminalistyczne kopie logiczne danych będących w obszarze zainteresowania. Ta procedura jest powszechna w przypadkach seksualnego wykorzystywania dzieci w niektórych jurysdykcjach, jednak z technicznego punktu widzenia i z uwagi na dobre praktyki należy rozważyć pewne niuanse.

Zastosowanie procedury mniej inwazyjnej. Tak samo, jak staramy się zachować urządzenie w niezmienionym stanie, aby można było zabezpieczyć inne rodzaje śladów kryminalistycznych (DNA, odciski palców itd.), tak samo korzystnie jest nie narażać oryginalnych danych z uwagi na późniejsze analizy przeprowadzane przez specjalistów w razie potrzeby.

Jeśli potrzeba skorzystać z aplikacji, muszą być one niezawodne i jeśli to możliwe, dedykowane do wykonania określonej czynności i sprawdzone przez odpowiednie laboratorium kryminalistyczne na środowisku, do którego będzie możliwy wgląd.

Procedura "Live data forensics" lub analiza live. Celem jest uzyskanie maksymalnej ilości informacji z urządzenia przed ich wyłączeniem, w tym danych ulotnych, które są istotne dla postępowania i mają być przeanalizowane później, takie jak zawartość pamięci RAM.

Jest to konieczne w urządzeniach, które zawierają zaszyfrowane wolumeny lub dyski, które są zamontowane w trakcie czynności, jak w przypadku rozwiązań BitLocker, FileVault, VeraCrypt, TrueCrypt, BestCrypt lub PGP Disk i itp. Dzięki tej procedurze uzyskamy odszyfrowane dane bez konieczności pozyskiwania hasła i bez uszczerbku dla ich pozyskania w wyniku analizy innych elementów.

Podobnie jest w przypadku szyfrowania sprzętowego przy użyciu TPM lub kluczy sprzętowych, w którym procedura ta jest wykonywana w celu uzyskania danych odszyfrowanych, gdzie w przeciwnym przypadku konieczne byłoby posiadanie całego oryginalnego systemu, aby uzyskać te informacje.

W przypadku braku możliwości uzyskania wsparcia specjalisty, korzystniej jest wyłączyć sprzęt zgodnie z procedurą opisaną w niniejszym paragrafie, aby uniknąć zniszczenia oryginalnej zawartości lub jej zanieczyszczenia i narażenia na obniżenie wartości dowodowej.

Procedura power-off. Po zakończeniu czynności zabezpieczenia live należy przystąpić do wyłączenia komputera. Optymalny sposób zależy od rodzaju urządzenia i systemu operacyjnego. Tradycyjne wyłączenie urządzenia może spowodować utratę danych, jednak w innych przypadkach konieczne będzie jego nagłe wyłączenie, aby nie utracić danych.

Systemy operacyjne, których procesowanie wymaga nagłego wyłączenia, wykonują szereg kroków, aby się wyłączyć. Te sekwencje procesów mogą powodować utratę kluczowych danych istotnych dla analizy.

Niekonwencjonalne sposoby wyłączania, które wymagają odłączenia zasilania, muszą być wykonane poprzez odłączenie przewodu od urządzenia, a nie od gniazdka ściennego, ponieważ UPS może być zainstalowany pomiędzy gniazdem ściennym a gniazdem urządzenia.

b) Urządzenie jest wyłączone

Zabezpieczone zostaną kopie kryminalistyczne lub urządzenie zostanie zatrzymane.

Nie ma powodu naruszania integralności dowodu zapisanego na komputerze poprzez włączanie go, podczas gdy jest wyłączony. W nagłych przypadkach lub w razie potrzeby pilnego zlokalizowania informacji, dane należy odczytywać w trybie read-only (tylko do odczytu) przez bloker w taki sposób, że zawartość nośnika pozostaje niezmieniona.

Po udokumentowaniu miejsca i stanu komputera oraz upewnieniu się, że jest wyłączony, należy usunąć wszelkie źródła zasilania, aby uniknąć nieoczekiwanego porażenia prądem. Dlatego przewód zasilający powinien zostać wyjęty z urządzenia, nigdy ze ściany.

Nie należy zapominać o zanotowaniu podłączonych elementów.

Obudowę komputera należy rozkręcić, aby zlokalizować nośniki. Zostaną one oznakowane zgodnie z uzgodnioną konwencją i przetworzone z wykorzystaniem odpowiednich narzędzi.

Należy wziąć pod uwagę możliwość pracy **dysków** w konfiguracji RAID. W przypadku wątpliwości, zaleca się, aby sprzęt należy zatrzymać wraz z dyskami (bez ich wyjmowania), co ułatwi późniejsze odtworzenie.

Należy sprawdzić, czy wewnątrz napędów CD/DVD nie znajdują się nośniki. W tym celu nie jest konieczne włączenie urządzenia, wystarczy umieścić specjalne narzędzie w dziurce mechanicznie odblokowującej napęd.

Pod uwagę należy wziąć również kwestie wyjaśniane wcześniej:

- Po udokumentowaniu stanu i sytuacji, w jakiej znajduje się sprzęt, całe urządzenie należy zaplombować. W ten sposób zapewniamy, że zawiera on wszystkie elementy, które mogą przechowywać informacje.
- Demontaż urządzeń nie zawsze jest prosty. Nie należy tego robić na miejscu, jeśli nie ma się wiedzy oraz odpowiednich narzędzi.
- Dostępność oryginalnego sprzętu w laboratorium może być przydatna. Na przykład, jeśli komputer posiada specjalne elementy, takie jak kontroler RAID, chip TPM lub inny szczególny element, który może być niezbędny do odtworzenia informacji. Może również umożliwić wykonanie live boot sprzętu w laboratorium, na przykład w celu zbadania obecności i zachowania złośliwego oprogramowania.

- W przypadku prostych lub standardowych urządzeń nie jest konieczne zatrzymanie kompletnego urządzenia i wystarczające jest zatrzymanie wyłącznie nośników danych, ponieważ nie będzie problemów związanych z kompatybilnością.
- Z reguły nie są zatrzymywane te nośniki, które nie mają wartości dla postępowania. Zasadniczo zatrzymanie urządzeń peryferyjnych, monitorów, myszek, klawiatur i przewodów nie jest konieczne, chyba że są nietypowe, na przykład są zastrzeżonymi modelami danej marki lub są przestarzałe i trudno dostępne. Z tego względu mogą być przydatne podczas analizy.
- Większość drukarek na poziomie użytkownika nie zawiera istotnych informacji. Mogą jednak posiadać ograniczoną pamięć, która w wyjątkowych sytuacjach może być przeanalizowana w laboratorium.

5.4. Laptopy

Stosowana będzie ta sama procedura, co w przypadku komputerów osobistych, z pewnymi szczegółami.

Przy zatrzymywaniu laptopa, należy rozważyć skorzystanie z jego dedykowanej torby, ładowarki, przewodów i akcesoriów. Po zamknięciu zostanie on zaplombowany w sposób zabezpieczający cały zestaw. Aby wyłączyć laptopa, należy najpierw wyjąć baterię (jeśli to możliwe), a następnie odłączyć przewód zasilający.

Współczesne laptopy, zwłaszcza notebooki, mają baterie i dyski twarde zintegrowane z komputerem, więc ich wyjęcie nie zawsze jest łatwe lub możliwe. Można znaleźć laptopy z dyskami typu NVMe/SSD zintegrowane z płytą główną, dla których niemożliwe będzie wykonanie kopii kryminalistycznej z wykorzystaniem metod opisanych w poprzedniej sekcji. Wiele z tych komputerów wymaga użycia specjalnych narzędzi, aby uniknąć ich uszkodzenia, więc osoby dokonujące czynności powinny być zaznajomione z procedurami demontażu.

Jednym z tych sposobów jest uruchomienie komputera z nośnika startowego (CD lub USB) ze specjalnym systemem operacyjnym. Po uruchomieniu systemu operacyjnego działającego w pamięci operacyjnej można użyć różnych narzędzi informatyki śledczych do triage lub zabezpieczenia dowodów. Istnieje wiele rozwiązań komercyjnych, jak i open source:

- CAINE (https://www.caine-live.net/),
- DEFT Linux (http://www.deftlinux.net),
- ASR data SMART Linux (http://asrdata.com/forensic-software/smartlinux/),
- KALI Linux (https://www.kali.org/downloads/).

W przypadku użycia jednego z tych systemów, badający musi pamiętać, że oryginalny dowód nie może zostać zmieniony. Z tego powodu należy korzystać z rozwiązań, które są znane i sprawdzone pod względem zapewnienia integralności oryginalnych nośników. Narzędzia i systemy wymienione powyżej nie są popierane ani promowane przez INTERPOL. W celu uzyskania informacji z tym zakresie, należy zapoznać się z oświadczeniem w zakresie wyłączenia odpowiedzialności zawartym na pierwszej stronie niniejszego Poradnika.

5.5. Nośniki pamięci (karty, dyski flash, zewnętrzne dyski, CD i in.)

Istnieje duża różnorodność nośników pamięci opartych o pamięci flash. Stają się one coraz mniejsze pod względem rozmiarów fizycznych, ale mimo to mają coraz większą pojemność. Pamięci tego typu można znaleźć ukryte lub zintegrowane z przedmiotami o różnych kształtach, dlatego specjalista, który identyfikuje te elementy, powinien znać ich wygląd.

Wraz z pojawieniem się innych nośników danych, dyski optyczne odchodzą obecnie do lamusa. Jednak nadal są elementem, który należy wziąć pod uwagę. Można znaleźć płyty pogrupowane w partie lub pojemniki z płytami.

Pamięci zewnętrzne znaleźć można praktycznie we wszystkich urządzeniach elektronicznych, od konsol do gier, telefonów, aparatów i kamer itd. Są one w stanie pomieścić w pełni funkcjonalne, kompletne systemy operacyjne, które ułatwiają zachowanie anonimowości dla czynności wykonywanych za ich pomocą.

Z drugiej strony, często spotyka się również systemy pamięci masowej na dyskach zewnętrznych, które podłączone po USB, Wi-Fi lub Ethernecie są w stanie przechowywać duże ilości danych.

Sposób postępowania:

a) obraz kryminalistyczny

Chociaż wiele urządzeń posiada przełącznik blokowania zapisu, nie należy wierzyć, że działa i robi to prawidłowo. Z tego powodu należy wykorzystywać własny sprzęt, który zapewnia odpowiednią blokadę (sprzętową lub programową).

W przypadku zewnętrznych dysków twardych możliwe jest wyodrębnienie umieszczonego w kieszeni/urządzeniu dysku, aby przeprowadzić proces kopiowania bezpośrednio z tego elementu. Procedura ta wymaga odpowiedniej dokumentacji, zarówno dla dysku wewnętrznego, jak i kieszeni/ urządzenia.

Po podłączeniu dowodu do blokera, a blokera do komputera (stacji) śledczego, można wykonać obraz kryminalistyczny.

Istnieją środki ostrożności, które należy podjąć w przypadku tych urządzeń. Czasami konieczne jest zlokalizowanie dowodu wykorzystania urządzeń zewnętrznych. Użycie wcześniej wspomnianych blokerów może nie pozwolić zarejestrować numeru seryjnego urządzenia, który jest odnotowany w systemie operacyjnym, co może być istotne, aby powiązać urządzenie z nośnikiem pamięci. Ten numer jest pobierany z chipu kontrolera i nie jest odkładany na HD, więc nie ma go w zabezpieczanym obrazie kryminalistycznym.

b) Ewaluacja (triage)

W celu uzyskania dostępu do zawartości pamięci ważne jest użycie blokerów, jak wskazano powyżej - albo programowych, dostarczonych i zweryfikowanych przez laboratoria, albo sprzętowych. W przypadku dysków optycznych, można je badać z wykorzystaniem czytnika CD/DVD, który nie pozwala na ich nadpisanie.

Dzięki wstępnemu badaniu można określić, czy są one istotne dla postępowania. Należy pamiętać, że podczas przeszukania można ujawnić ich dużą liczbę i że kopiowanie całego materiału bez wcześniejszej ewaluacji nie jest efektywne (chyba, że jest to wymogiem prawnym w danej jurysdykcji).

W przypadku zatrzymania dysków optycznych można użyć tego samego pojemnika, w którym były one przechowywane, upewniając się, że jest on zamknięty i umieszczony w zapieczętowanej torbie oznaczonej identyfikatorem. Jeśli występują pojedynczo, należy umieścić je w plastikowym etui chroniącym przed uszkodzeniem fizycznym, odpowiednio oznaczyć i zaplombować w workach na dowody. Nie zaleca się stosowania kleju bezpośrednio na płytach. Może to spowodować błędy w odczycie lub fizycznie je uszkodzić w trakcie usuwania kleju. Markery permanentne mogą być wykorzystywane do opisywania płyt. Nie zaleca się spinania płyt za pomocą gumek lub opasek, ponieważ uszkadzają one krawędzie płyt i mogą spowodować, że płyty nie będą nadawały się do użytku.

Obraz 10: Kamery cyfrowe

5.6. Inne urządzenia (aparaty, nawigacje GPS, wideorejestratory i in.)

Źródła danych w tych urządzeniach obejmują:

a) pamięć zewnętrzna: do pracy z każdym innym zewnętrznym urządzeniem pamięci masowej,

b) pamięć wewnętrzna: duża część urządzeń posiada również pamięć zintegrowaną, zwykle o ograniczonej pojemności, ale pozwalającej na przechowywanie danych, która musi być sprawdzona.

Proponuje się następującą procedurę:

- wykonaj zdjęcie po zlokalizowaniu urządzenia,
- opisz aparat wraz z jego ogólnymi danymi, zanotuj numer seryjny i nadaj numer dowodu,
- sprawdź, czy posiada zewnętrzny nośnik pamięci, jeśli tak należy go wyodrębnić i udokumentować,
- wykonaj obraz kryminalistyczny karty pamięci,
- sprawdź pamięć wewnętrzną przy włączonym aparacie (bez karty).

Jeśli ujawniona zostanie zawartość, którą należy wyodrębnić:

- wykonaj obraz łącząc urządzenie z komputerem - nie wszystkie urządzenia mają taką możliwość,
- włóż nową kartę i skopiuj na nią dane, aby uzyskać kopię logiczną,
- jeśli inne możliwości są niedostępne, zrób zdjęcie zawartości, starając się pokazać dane istotne dla postępowania,
- sprawdź w ustawieniach kamery datę, czas i strefę czasową.

Wszystkie elementy należy zaplombować razem i oznaczyć jako przetworzone.

Jeśli urządzenie nie będzie przetwarzane i będzie po prostu zatrzymane, postępuj następująco:

- udokumentuj sprzęt: fotografie, ogólne okoliczności ujawnienia, a jeśli to możliwe zlokalizuj nośniki z oprogramowaniem i przewody do podłączenia do komputera.

Jeśli to możliwe, zapakuj wszystko z wykorzystaniem oryginalnych pudełek w worki dowodowe oznaczone numerem umieszczonego w nich dowodu.

5.7. Urządzenia IoT

Oprócz opisanych powyżej tradycyjnych urządzeń, w ostatnich latach wiele urządzeń zostało określonych jako IoT lub Internet Rzeczy. Urządzenia te mogą bardzo różnić się funkcjonalnościami,

tak jak smartwatche, smart TV, wideorejestratory itd. Poniżej umieszczone są przykłady najbardziej popularnych urządzeń, które można znaleźć przy podejrzanym.

Obraz 11: Smartwatche

5.7.1. Smartwatche

Smartwatche posiadają szereg funkcji, które umożliwiają wykonywanie wielu czynności normalnie wykonywanych z wykorzystaniem smartfona. W rzeczywistości jest to urządzenie peryferyjne, przedłużenie ekranu smarfona, który nosi się w kieszeni. Smarwatch może być na podejrzanym i działać dyskretnie: nie wydawać dźwięków lub delikatnie wibrować i mogą być podłączone do urządzenia Apple lub z Androidem, więc należy ich szukać uważnie. Na rynku jest wiele smartwatchy, najbardziej popularne to Apple Watch, Xiaomi, Sony Smarwatch, Honor oraz Samsung Gear.

W zależności od przypadku, mogą zawierać informacje przydatne dla śledczych, ale należy pamiętać, że mają zazwyczaj bardzo ograniczoną pojemność, zwykle ograniczoną do książki telefonicznej, SMS i danych o nawykach sportowych.

Zazwyczaj są wyposażone w Bluetooth, niektóre mogą być wyposażone również w USB, więc można po prostu zgrać z niego zawartość jak w przypadku każdego smartfona/tableta z Androidem.

Jeśli planowane jest zatrzymanie smartwatcha, należałoby zastosować te same procedury, co podane wcześniej w sekcji dotyczącej smartfonów.

Obraz 12: Smart TV

5.7.2. Smart TV

Popularne staje się ujawnianie Smart TV, które mają możliwość łączenia się z Internetem, uruchamiania aplikacji i niektórych gier. Niektóre ze Smart TV oparte są o system Android, a inne o własne systemy operacyjne.

Konkretne funkcjonalności zależą od marki, modelu, podłączonych urządzeń peryferyjnych i zainstalowanych aplikacji.

Z perspektywy osoby podejmującej pierwsze czynności, ekstrakcja informacji z tych urządzeń może być wyzwaniem, ponieważ każdy przypadek będzie inny w zależności od wymienionych wcześniej czynników oraz systemu operacyjnego.

Większość Smart TV ma podatności bezpieczeństwa, które mogą zostać wykorzystane. Możliwości ekstrakcji oznaczają modyfikację firmware, ataki na przeglądarkę, ataki sieciowe, użycie złośliwego oprogramowania lub chip-off.

Jednak większość tych procedur nie jest prosta i wymaga skomplikowanego sprzętu (zwłaszcza chip-off) lub złożonych struktur sieciowych, które mogą nie być zgodne z aktywnością osoby podejmującej pierwsze czynności. Niewłaściwe postępowanie może "zbrickować" urządzenie i uniemożliwić dalsze próby ekstrakcji informacji.

Z reguły **proces** będzie obejmował poniższe kroki:

- przejrzyj połączenia, aby ujawnić połączenia USB, HDMI oraz połączenia sieciowe,
- sprawdź u producenta, czy dany model ma możliwość pracy bezprzewodowej (jeśli urządzenie nie jest w żaden sposób podłączone, może być odrzucone),
- sprawdź, czy urządzenie jest wyłączone, czy znajduje się w trybie czuwania,
- wykorzystaj interfejs użytkownika do zbadania konfiguracji urządzenia i stwórz dokumentację, najlepiej video,
- spróbuj ograniczyć interakcję, zapoznając się z instrukcją przed testowaniem,
- zabezpiecz opakowanie, włącznie z pilotem i przewodami zasilającymi.

Ewentualne dowody, które można znaleźć podczas przeszukania i zatrzymania:

- połączone urządzenia (do screen mirroringu, synchronizacji),
- historię przeglądania,
- zainstalowane przez użytkownika aplikacje (Facebook, Skype, Twitter, Netflix, Amazon ...), jednak hasła na tym etapie nie będą łatwe do odzyskania i mogą wymagać dalszych czynności w laboratorium.

Obraz 13: Urządzenia takie jak Amazon Echo, Apple HomePod oraz inteligentne głośniki

5.7.3. Inteligentne głośniki

Zestawy domowe pozwalają użytkownikom komunikować się z akcesoriami podłączonymi w domu po prostu za pośrednictwem aplikacji. Za pomocą framweorka Home Kit, można skonfigurować urządzenia i je kontrolować.

HomePod to urządzenie audio produkowane przez Apple, które adaptuje się do lokalizacji i dostarcza wysokiej jakości dźwięk wszędzie tam, gdzie jest odtwarzany. Wraz z Apple Music oraz Siri, umożliwia interakcję audio (muzyczną) w domu.

Ewentualne dowody, które można znaleźć podczas przeszukania i zatrzymania:

- Zazwyczaj zawierają one bardzo ograniczoną ilość danych. Zaleca się ich zatrzymanie łącznie, gdy istnieje domniemanie, że zawierają dane istotne dla postępowania. Wystarczy odłączyć je od zasilania i zatrzymać w takiej formie, w jakiej zostały znalezione. Należy wszystko udokumentować, sfotografować urządzenie, oznaczyć i je i zapakować.

Obraz 14: Kamery IP przesyłające obraz po sieci

5.7.4. Kamery ukryte i IP

Kamery IP lub ukryte kamery wykorzystywane są zazwyczaj do monitoringu na małą skalę i w przeciwieństwie do CCTV, urządzenia te mogą nie mieć lokalnego przechowywania danych. Większość dostępnych kamer IP do pracy potrzebuje wyłącznie połączenia Wi-Fi. Użytkownik może oglądać strumień z kamery na żywo z dowolnego urządzenia podłączonego do sieci. W przypadku wykupienia odpowiedniej subskrypcji możliwe jest również przechowywanie danych w chmurze i oglądanie tam materiału (zazwyczaj z kilku poprzednich dni).

Mimo to, osoby podejmujące czynności jako pierwsze muszą upewnić się, czy tego rodzaju kamery posiadają karty pamięci (zazwyczaj micro-SD), na których lokalnie przechowują dane.

Osoby podejmujące pierwsze czynności muszą być również świadome, że kamerę można ukryć wszędzie: od pluszowego misia po guzik w marynarce.

Ewentualne dowody, które można znaleźć podczas przeszukania i zatrzymania:

- W przypadku danych przechowywanych w chmurze ważne jest, aby uzyskać dane dostępowe (zazwyczaj nazwa użytkownika i hasło lub kod QR). Dane te mogą być przechowywane w samej kamerze lub komputerach/smartfonach znalezionych przy podejrzanym.
- W przypadku danych przechowywanych lokalnie zazwyczaj należy zatrzymać wyłącznie kartę pamięci. Jednak ze względu na możliwość szyfrowania, formatów objętych patentami lub nieudokumentowanych ustawień, zaleca się zatrzymywanie całego urządzenia.
- W przypadku danych dostępnych tylko na żywo (kamera tylko przesyła obraz i nie przechowuje go w chmurze, ani w pamięci lokalnej), zaleca się zatrzymanie urządzenia wyłącznie gdy istnieje przypuszczenie, że zawiera ono informacje istotne dla postępowania.
- W przypadku analizy video porównującej wcześniejsze nagrania ze znalezioną kamerą, urządzenie musi być zawsze zatrzymane.

Kiedy zatrzymanie jest niezbędne, po prostu należy odłączyć urządzenia, udokumentować wszystko, wykonać dokumentację fotograficzną urządzeń, oznakować je i zapakować.

Obraz 15: Konsole Nintendo, Sony PS Series i Microsoft XBOX jako przykłady konsol z funkcjami smart

5.8. Konsole do gier

Złożoność konsol do gier video wzrasta wraz z wydaniem każdego nowego modelu. Większość z nich zawiera wewnętrzny dysk, który może być wyciągnięty i zobrazowany zgodnie z wcześniej opisywanymi procedurami. Ze względu na powszechne szyfrowanie i stosowanie specjalnych formatów plików, niezwykle trudno jest wyodrębnić jakiekolwiek informacje w późniejszej analizie. Dodatkowo, znaczna część generowanych informacji przechowywana jest na platformach społecznościowych dla graczy i nigdy nie jest zapisywana na nośniku w urządzeniu.

Wreszcie, należy wziąć pod uwagę, że użytkownicy z innych lokalizacji mogą łatwo zmienić dane zawarte na urządzeniach i usunąć potencjalne dowody.

Ewentualne dowody, które można znaleźć podczas przeszukania i zatrzymania:

- określenie okresu, kiedy konsola była wykorzystywana do grania,
- historia przeglądania,
- niedozwolone pliki przechowywane na zasobach konsoli,
- hasła do aplikacji,
- konta użytkowników.

Obraz 16: Drony

5.9. Drony

Drony, nazywane również UAV i sUAS lub RPAS, mogą być wykorzystywane do wielu czynności, od wykonywania zdjęć w terenie do przenoszenia towarów z jednego miejsce na drugie. Z tego względu celem analizy śledczej dronów i związanych z nimi urządzeń jest identyfikacja toru lotu, danych użytkownika oraz powiązanych zdjęć oraz filmów przechowywanych na urządzeniach, które pomagają zrozumieć urządzenie i jego zastosowanie .

Dron składa się zwykle z następujących rodzajów komponentów:

- **Komponenty fizyczne**: Komponenty fizyczne, z których składa się korpus i elementy latające, można podzielić następująco:

  - **Korpus drona**: Kadłub UAV, w którym umieszczone są pozostałe elementy.
  - **Kontroler lotu**: Wykorzystywany do sterowania lotem. Stabilizuje drona i zazwyczaj odbiera dane nawigacyjne z urządzenia sterującego drogą radiową. W bardziej zaawansowanych urządzeniach, może być sterowany zdalnie w czasie rzeczywistym, jak i zaprogramowany do lotu autonomicznego.
  - **Silniki, wirniki/śmigła/skrzydła i kontrolery prędkości**: Łącznie zapewniają unoszenie się i napęd UAV. Istnieją różne konstrukcje, na przykład dedykowane do zwiększania prędkości lub długości lotu.
  - **Obudowa ochronna**: Otacza silniki i śmigła (najbardziej wrażliwe elementy każdego drona), aby zapobiec kolizji i utracie kontroli, a następnie uszkodzeniu drona.
  - **Odbiornik GPS**: Nie jest niezbędny we wszystkich dronach, ale często występuje we wiodących modelach. Ten komponent jest wykorzystywany do zarządzania położeniem UAV, funkcją powrotu do domu i autonomicznymi trasami lotu.
  - **Odbiornik radiowy**: Służy do odbierania sygnałów wejściowych sterujących otrzymywanych/zbieranych z nadajnika naziemnego.
  - **Transmiter**: Przesyła dane ręcznie wprowadzane od operatora na ziemi do drona.
  - **Światła LED**: Niektóre drony są wyposażone w światła LED (zwykle zielone i czerwone), które mogą wspierać pilota i pomagając innym użytkownikom przestrzeni powietrznej zidentyfikować drona.

- **Oprogramowanie**: Wszystkie drony zawierają aplikację lub oprogramowanie, które służy do sterowania działającym urządzeniem. Obecnie istnieje ogromny wybór aplikacji open-source służących do kontroli lotu i kontroli naziemnej, które można swobodnie pobierać i łatwo modyfikować, aby wykonywały dowolną liczbę zadań. Większość dronów jest dostarczana z aplikacjami mobilnymi, umożliwiającymi sterowanie dronem lub wyświetlanie obrazu z kamery i lokalizacji na mapie.

Drony/kontrolery są zazwyczaj wyposażone w dwa rodzaje nośników danych, które wymagają innego obchodzenia się z nimi, jak to przedstawiono poniżej:

- **Karty pamięci**: mogą być badane jak dysk twardy komputera. Można przeprowadzić ekstrakcję logiczną, jak i fizyczną, o ile narzędzia informatyki śledczej na to pozwalają. Badający musi uzyskać dostęp do karty, wyodrębnić dane, a następnie włożyć ją do urządzenia przed ponownym jego włączeniem. Niektóre urządzenia przechowują na karcie pamięci dane i jeśli wykryją, że karta nie jest dostępna, może to doprowadzić do utraty danych z drona/kontrolera. Jeśli czas i zasoby na to pozwalają, należy wykonać kopię binarną i włożyć nośnik z powrotem do urządzenia.
- **Pamięć wewnętrzna**: wymagają kompatybilnych z dronem/urządzeniem mobilnym narzędzi informatyki śledczej. Z niektórych urządzeń można dokonać fizycznej ekstrakcji pamięci. Narzędzia informatyki śledczej uruchamiają badane urządzenie w określony sposób i przeprowadzają ekstrakcję bez dokonywania jakichkolwiek zmian, czy modyfikacji danych użytkownika na badanym urządzeniu.

Z reguły proces techniczny obejmował będzie następujące czynności:

- zrób zdjęcia wyświetlacza kontrolera, jeśli jest włączony, a następnie wyłącz drona i jego elementy,
- odizoluj drona od satelitów GPS i innych urządzeń, aby upewnić się, że sygnały GPS/Wi-Fi/ sieci nie są odbierane,
- zidentyfikuj markę i model drona,
- przeszukaj drona w poszukiwaniu zewnętrznych nośników pamięci, np. kart SD,
- sfotografuj i oznacz stan drona i jego elementów,
- bezpiecznie wszystko zapakuj.

Ewentualne dowody, które można znaleźć podczas przeszukania i zatrzymania:

- historia aktualizacji,
- logi diagnostyczne,
- zarejestrowane konta e-mail,
- sparowane urządzenia,
- pliki multimedialne,
- logi dotyczące lotu/telematyczne,
- miniaturki mediów z drona,
- artefakty mapy, takie jak współrzędne geograficzne, punkty orientacyjne, lokalizacje „home”,
- oprogramowanie specyficzne dla dronów, takie jak oprogramowanie producenta do zarządzania,
- e-maile, które pokazują nowe rejestracje dronów lub powiadomienia o aktualizacjach producenta,
- pliki CSV zawierające dane telematyczne, diagnostyczne lub koordynaty GPS.

W celu uzyskania bardziej szczegółowych informacji w tym obszarze można zapoznać się z wytycznymi **INTERPOL-u Framework for Responding to a Drone Incident – For First Responders and Digital Forensics Practitioners**.

Obraz 17: Kamery CCTV wykorzystywane do monitoringu

5.10. Monitoring wizyjny

Telewizja CCTV, nazywana również monitoringiem, to wykorzystanie kamer video do transmisji sygnału do określonego miejsca, na określony zestaw monitorów. Różni się od telewizji tym, że sygnał nie jest transmitowany jawnie, chociaż może wykorzystywać połączenia P2P, P2MP, albo sieć połączeń przewodowych lub bezprzewodowych. Chociaż prawie wszystkie kamery video pasują do tej definicji to termin ten jest najczęściej stosowany w odniesieniu do kamer używanych do nadzoru w miejscach, które mogą wymagać monitorowania, takich jak banki, sklepy i inne miejsce, w których konieczne jest zapewnienie bezpieczeństwa.

System bezpieczeństwa CCTV składa się z różnych elementów, do których należą:

- **kamera CCTV**: wykorzystywana do monitoringu wizyjnego i działa jako urządzenie wejściowe do systemu monitoringu CCTV,
- **zasilacz główny**: podstawowe urządzenie zasilające,
- **zasilacz zapasowy** (opcjonalny): zapasowy zasilacz, który przydaje się w przypadku przerwy w dostawie prądu,
- **przewody**: służą do podłączenia kilku kamer CCTV do jednego rejestratora video,
- **rejestrator video**: przekształca i zapisuje sygnały wysyłane przez kamerę CCTV w formie filmu video, który jest zazwyczaj przechowywany na dysku twardym i może być automatycznie kasowany, w zależności od ustawień urządzenia,
- **przełącznik video**: przełącza tryb video pomiędzy różnymi kamerami CCTV.

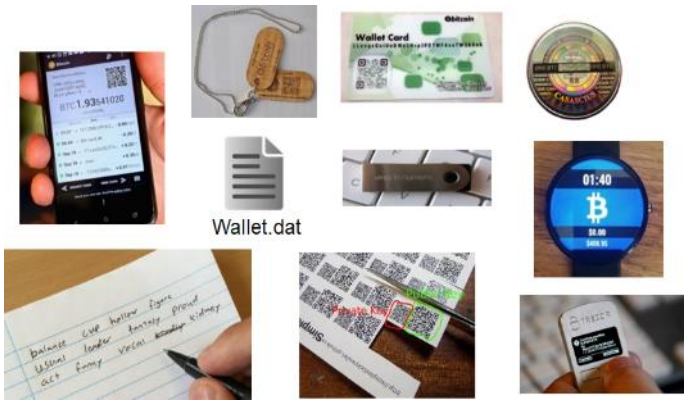
Z reguły **proces** techniczny obejmował będzie następujące czynności:

- sprawdź datę i czas ustawioną na rejestratorze i odnotuj, jeśli różni się od aktualnej,

- zrób zdjęcie ekranu(-ów),
- wyłącz rejestrator, aby uniknąć nadpisania danych,
- odłącz przewody,
- zidentyfikuj markę i model,
- sfotografuj i oznacz wszystkie elementy,
- bezpiecznie wszystko zapakuj.

Zazwyczaj komponenty systemów CCTV są zamknięte, dlatego zaleca się zatrzymanie każdej części systemu CCTV, aby uniknąć problemów w trakcie analizy.

Monitoring zdalny może być również wykorzystywany w systemach CCTV i może być wyposażony w systemy alarmowe, które ostrzegają użytkownika, kiedy wykryją ruch. Należy mieć to na uwadze podczas zbliżania się do miejsca czynności, ponieważ podejrzany może zostać zaalarmowany/ powiadomiony, jeśli policja zbliży się do miejsca, które jest monitorowane przez systemy CCTV, takie jak RING. Dlatego przy analizie systemu CCTV należy uwzględnić również użytkowników, którzy mają zdalny dostęp do tych systemów.



Obraz 18: Portfele kryptowalutowe, wykorzystywane do przechowywania kryptowalut i innych aktywów

5.11. Portfele kryptowalut

Osoby podejmujące pierwsze czynności powinny być świadome różnych rodzajów dostępu, przechowywania i transferu aktywów wirtualnych. Aby w prawidłowy sposób zająć kryptowaluty, jeśli jest to dopuszczalne w danej jurysdykcji, organy ścigania muszą przenieść środki z portfela podejrzanego na portfel kontrolowany przez organ dokonujący zajęcia.

Co więcej, osoby podejmujące pierwsze czynności muszą pamiętać, że współsprawcy mogą posiadać kopię informacji potrzebnych do dokonania transferu środków na portfel, który nie jest kontrolowany przez organ. Dlatego im szybciej kryptowaluty zostaną w sposób bezpieczny przetransferowane, tym lepiej.

Portfele kryptowalutowe mogą mieć różne kształty i formy: pliki na komputerze/telefonie, urządzenia, kody QR lub nawet ciągi słów zapisane na kartce papieru lub zapamiętane przez podejrzanego. Podczas przeszukania mogą zostać ujawnione:

- **portfele desktopowe**: Bitcoin Core, Armory, Electrum, Wasabi, Bither itd.,
- **portfele mobilne**: Mycelium, Edge, BRD, Trust itd.,
- **portfele online-owe**: BitGo, BTC.com, Coin.Space, Blockchain.com itd.,
- **portfele sprzętowe**: BitBox, Coldcard, KeepKey, Ledger, Trezor, itd.,
- **portfele papierowe**: adresy generowane na bitaddress.org, segwitaddress.org itd.
- **portfele typu brain**: seed (lista słów, która zawiera całość informacji potrzebnej do odtworzenia portfela).

Bez względu na rodzaj portfela, najważniejszą informacją, do której osoby podejmujące pierwsze czynności potrzebują uzyskać dostęp jest **niezaszyfrowany klucz prywatny**, który pozwala na prawidłowe podpisywanie transakcji i transfer środków.

W większości przypadków jednak klucz prywatny jest chroniony, albo może nie być przechowywany lokalnie. Z tego powodu, osoby podejmujące pierwsze czynności powinny poszukiwać również:

- **hasła:** wykorzystywane są do zaszyfrowania klucza prywatnego,
- **PINy**: do dostępu do portfeli sprzętowych lub telefonów,
- **poświadczenia**: nazwy użytkownika i hasła do portfeli online-owych,
- **kody QR:** mogą zawierać pełny klucz prywatny,
- **seed-y:** sekwencja słów (zazwyczaj 24 lub więcej), wykorzystywanych do odtworzenia klucza prywatnego.

Dla najbardziej popularnej kryptowaluty[3] (bitcoina), klucze prywatne to 256-bitowe liczby, które mogą być przedstawiane na wiele sposobów. Najpopularniejszy jest WIF, w którym klucze zaczynają się od '**5**', '**K**' lub '**L**', a zaszyfrowany klucz prywatny zaczyna się od '**6P**'.

Przykładowo, ten sam klucz prywatny może być wyświetlany jako:

- *Base58 Wallet Import Format (51 characters base58, starts with a '5'):*
  `5JoBSup7GzCohqzfCdU3FQmuQM8KLCu3TTKiTAtbzmWywJfzTni`
- *Base58 Wallet Import Format Compressed (52 characters base58, starts with a 'K' or 'L'):*
  `L1Yq7N6vhZV79HFVcKxLvbwCJ3qHumWhqmBbxWemTyVLJHfaUjTc`
- *Private Key BIP38 Encrypted Format (58 characters base58, starts with '6P') - password: 'asdfg':*
  `6PYLTEjqt2huN6zgG8Gc2Sdifh33tcDLoJMXXqdK52YrQWXa3fD8az9Za7`

Osoby podejmujące pierwsze czynności muszą również być w stanie zidentyfikować **klucz publiczny** (lub po prostu **adres**), który jest prawdopodobnym miejscem docelowym dla transferów lub płatności. Na przykład, adresy bitcoinowe mogą rozpoczynać się od '**1**', '**3**' or '**bc1**':

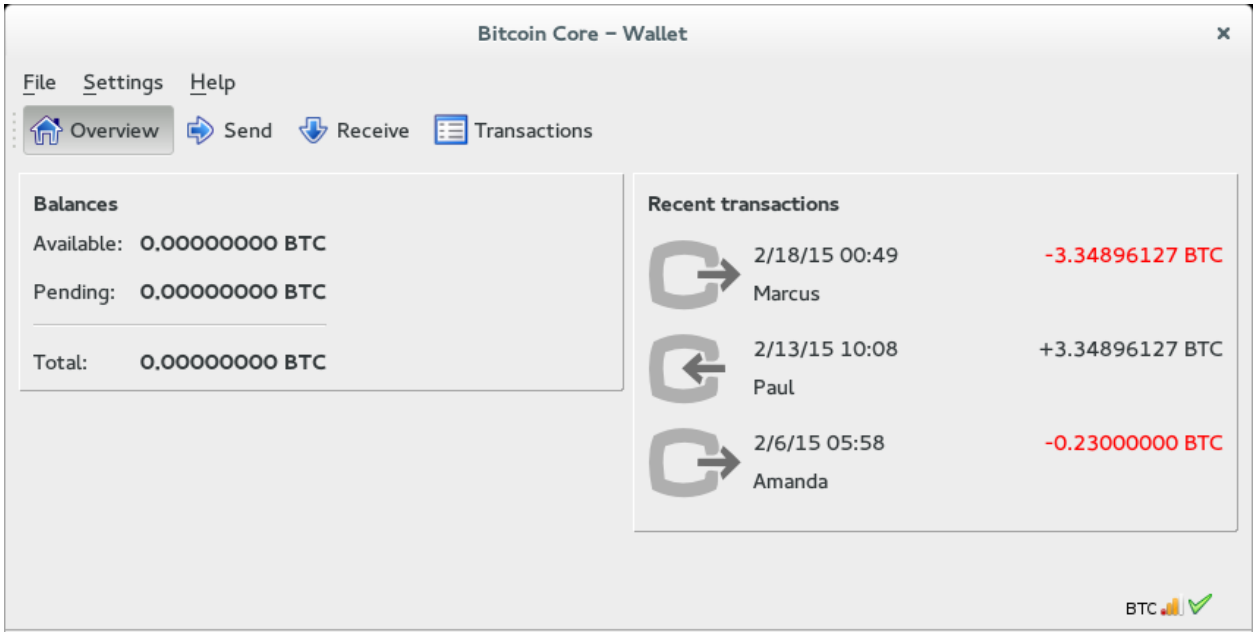
- format P2PKH: `1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2`
- format P2SH: `3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy`
- format Bech32: `bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq`

Kilka przykładów tego, co osoby podejmujące pierwsze czynności mogą ujawnić podczas przeszukania:

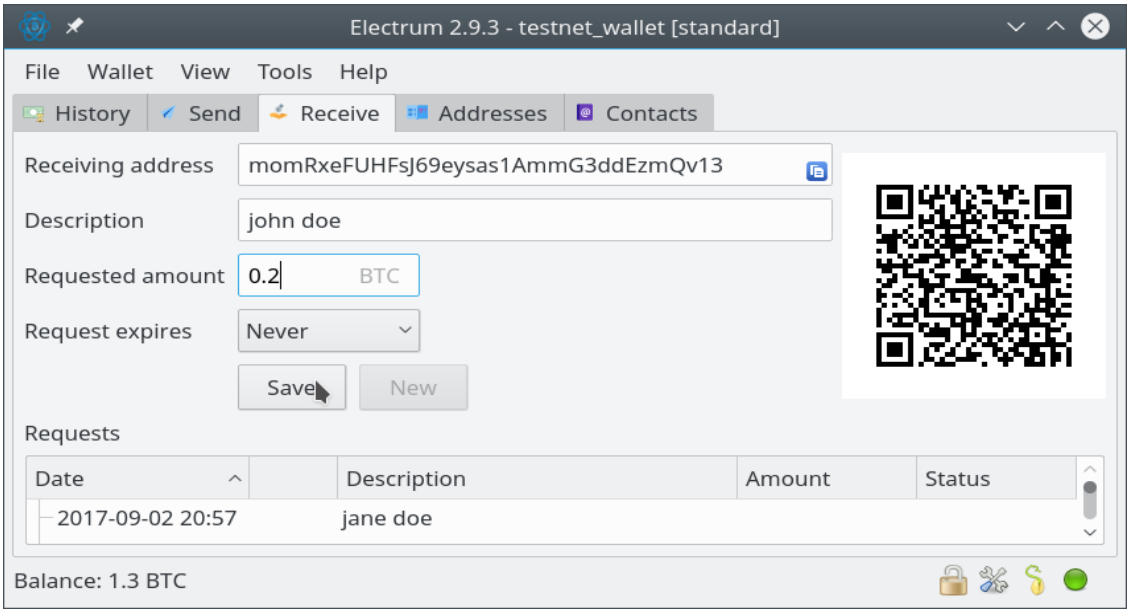
Obraz 19: Portfele papierowe

[3] Inne przykłady kryptowalut obejmują Ethereum, XRP, Bitcoin Cash, Litecoin, Monero i Zcash.

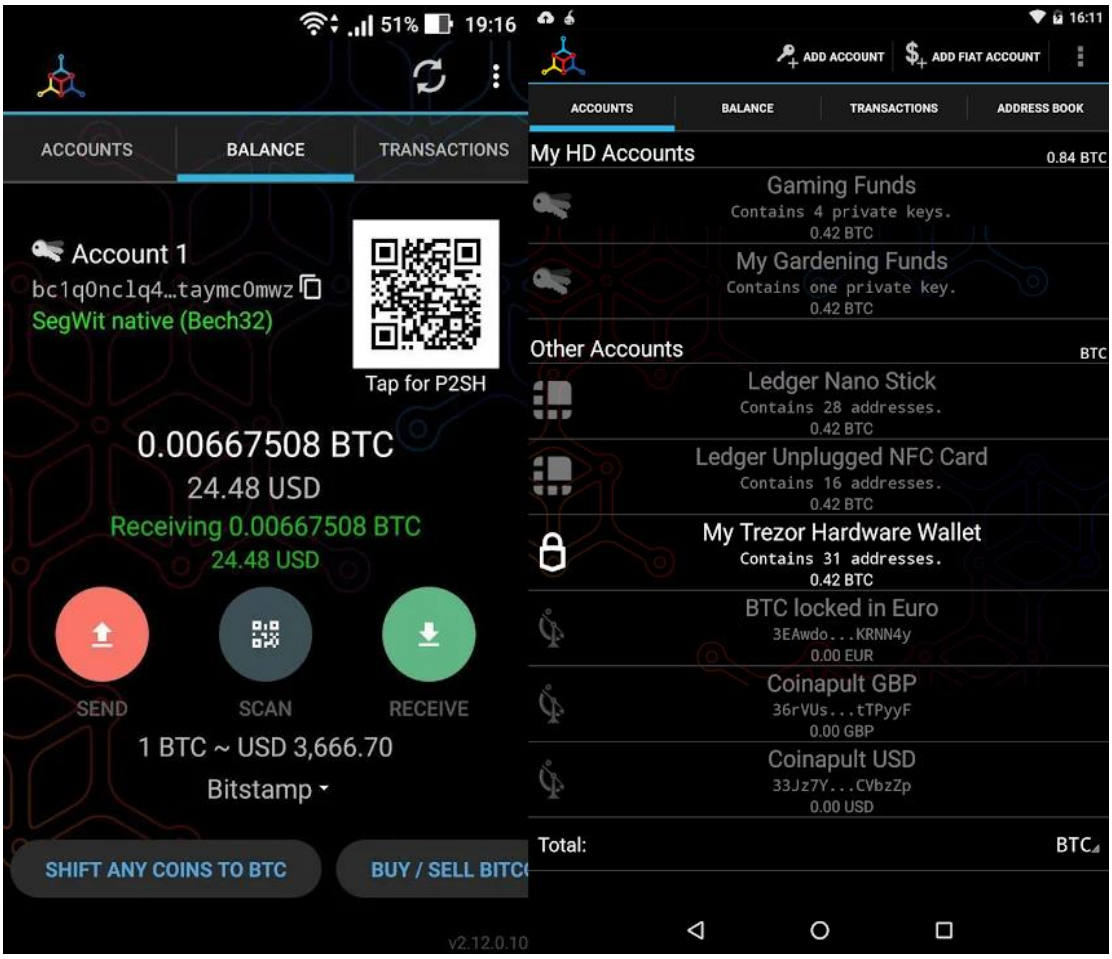
Obraz 20: Portfele sprzętowe



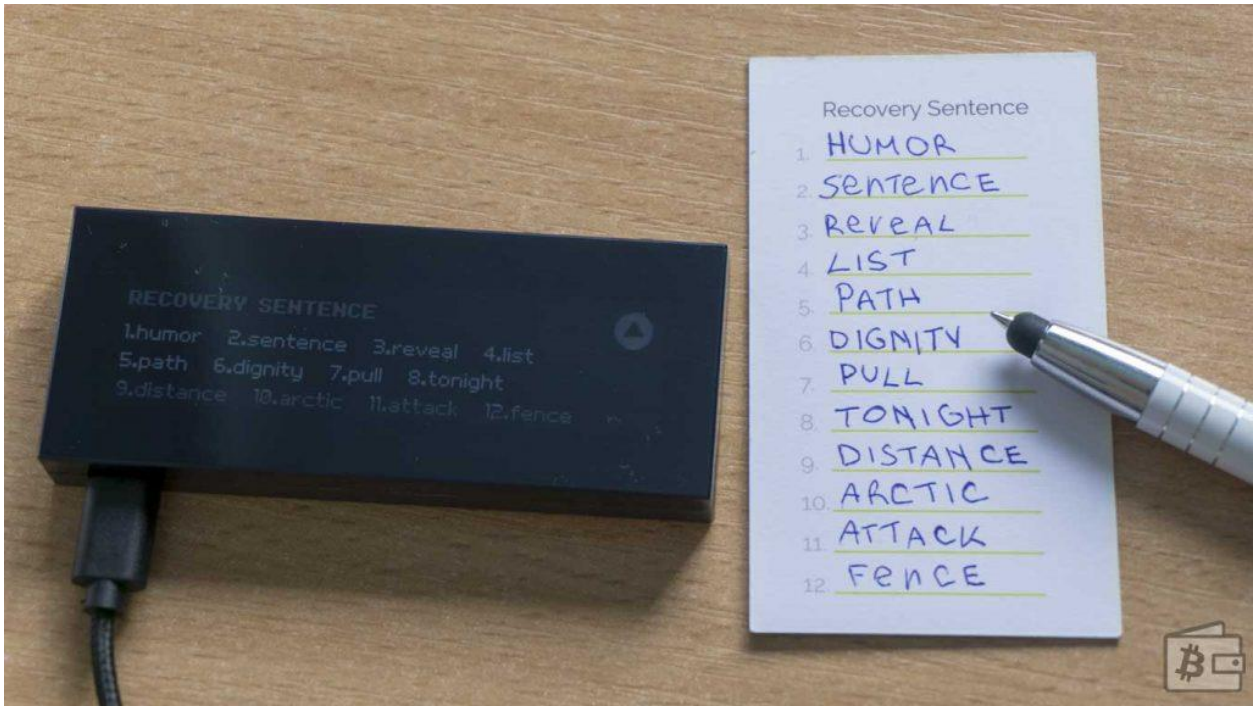
Obraz 21: Przykład portfela desktopowego



Obraz 22: Portfel desktopowy Electrum



Obraz 23: Przykład mobilnego portfela kryptowalut



Obraz 24: Portfel typu Brain (seed)

Obraz 25: Portfel typu Brain (seed)

Ważną kwestią, którą należy wziąć pod uwagę w zależności od danej jurysdykcji jest to, co zrobić z przekazanym aktywem wirtualnym: wymienić jak najszybciej na fiaty (pieniądze), czy zatrzymać na oficjalnym portfelu do czasu prawomocnego wyroku.

Na koniec, nie należy zapominać o dokumentowaniu wszystkich podjętych kroków, w tym opłat transakcyjnych, wartości bitcoinów w walucie lokalnej i ewentualnie wykorzystanych giełd. Przydatne może być załączenie zrzutów ekranów z transakcji (przy użyciu np. strony internetowej www.walletexplorer.com).

W celu uzyskania dalszych informacji, należy zapoznać się przepisami prawa w danej jurysdykcji. Aby poszerzyć wiedzę na temat wirtualnych aktywów przydane mogą być również wytyczne, takie jak Wytyczne **INTERPOL Guidelines on Darknet and Cryptocurrencies for Counter-Terrorism Practitioners**.

5.12. Komputery samochodowe

Nowoczesne pojazdy mają dwa systemy, które mogą zawierać dane istotne dla postępowania. Są to:

System telematyczny – Obejmuje różne ECU, które monitorują stan pojazdu i dane wprowadzane przez użytkownika do poruszania pojazdem, takie jak przyspieszenie, hamowanie i kierowanie. Te ECU zawierają dane o zdarzeniach w pojeździe, które mogą pomóc w ustaleniu historycznych tras, które przebył pojazd lub o sposobie jego prowadzenia.

Systemy informacyjno-rozrywkowe – Systemy zapewniające pasażerom pojazdu rozrywkę multimedialną, taką jak muzyka, audycje radiowe, streaming lub wyświetlanie lokalnie przechowywanych filmów, a także umożliwiają połączenie z Internetem lub telefonem. Jeśli użytkownik podłączy telefon do tego systemu, dane z telefonu, takie jak książka adresowa, wiadomości SMS i natychmiastowe oraz połączenia będą w nim przechowywane. Informacje te można odzyskać, kiedy urządzenie jest podłączone do systemu i sprawdzić wszelkie dane o zdarzeniach zarejestrowane przez podłączone urządzenie.

Systemy informacyjno-rozrywkowe i telematyczne stanowią wyjątkowe wyzwanie dla organów ścigania ze względu na różnice w konstrukcji sprzętu i producentów, ograniczone informacje o podstawowym oprogramowaniu i zamkniętych systemach operacyjnych, zaszyfrowane nośniki związane z DRM oraz szybkie zmiany technologii. Możliwości akwizycji mogą być ograniczone przez dostępny sprzęt i oprogramowanie ułatwiające pozyskiwanie danych. Jeśli inne techniki będą nieskuteczne, konieczne mogą być oględziny aktywnego ekranu/systemu. Badający powinni mieć świadomość, że systemy cyfrowe pojazdów są takie jak każde inne urządzenia/systemy cyfrowe i dlatego należy obchodzić się z nimi w należyty sposób, aby zapobiec zniszczeniu danych. Współczesny pojazd może zawierać wiele komputerów i/lub sieci, dlatego badający powinien przedsięwziąć odpowiednie kroki, aby odizolować pojazd od sieci bezprzewodowych (Wi-Fi, Bluetooth, komórkowych itp.).

ECU zawsze pobierają energię z akumulatora pojazdu, nawet gdy zapłon jest wyłączony. Wiele ECU, takie jak systemy informacyjno-rozrywkowe i telematyczne, wykorzystują ważne zdarzenia, takie jak odblokowanie lub otwarcie/zamknięcie drzwi, jako sygnał do przejścia w tryb niskiego poboru energii lub rozpoczęcia procedury włączania zasilania. Zminimalizowanie liczby i czasu trwania cykli zasilania pomaga zachować dane ulotne przechowywane w ECU. Badanie pojazdu w celu ujawnienia dowodów może spowodować dodatkowe cykle zasilania, co spowoduje utratę danych ulotnych. Aby zminimalizować to ryzyko, należy udokumentować dane wyświetlane na ekranie pulpitu i prawidłowo wyłączyć pojazd, aby ECU prawidłowo się zamknęły, zanim przystąpi się do procesu zabezpieczania śladów (np. linii papilarnych, DNA, GSR itp.)

Poniżej przedstawiono ogólne wytyczne dotyczące prawidłowego wyłączenia samochodu w celu zabezpieczenia dowodów:

- udokumentuj datę i godzinę wykonania czynności,
- wyłącz pojazd i wyjmij wszystkie kluczyki,
- zamknij wszystkie drzwi, a następnie otwórz drzwi kierowcy na 5 sekund,
- zamknij drzwi kierowcy i poczekaj ok. 2 minuty,
- odłącz zasilanie pojazdu (np. odłącz baterię lub przełącz samochód w tryb lawety/ transportu).

Aby sprawdzić, że samochód jest całkowicie wyłączony, należy upewnić się, że konsola pojazdu, jak również światła wewnętrzne i zewnętrzne były wyłączone przez 30-45 sekund po zamknięciu wszystkich drzwi. Należy odczekać 60 sekund.

Obchodzenie się z dowodami

Zweryfikuj nakaz przed przystąpieniem do obchodzenia się z dowodami i ich zabezpieczeniem upewniając się, że wszystkie ograniczenia zostały wskazane. Jeśli to konieczne, podczas etapu zabezpieczenia, uzyskaj dodatkowy nakaz, wykraczający poza ramy pierwotnego. Systemy ECU mogą składać się z oddzielnych ECU, zlokalizowanych w różnych miejscach w pojeździe, albo z jednej zintegrowanej jednostki ECU, która ma podwójną funkcjonalność. Ogólne wytyczne dotyczące obchodzenia się z pojazdami mającymi związek z postępowaniem są następujące:

- postępuj z dowodami zgodnie z regulaminem jednostki i zachowaj łańcuch dowodowy,
- zachowaj stan ECU zanim pojazd będzie poddany badaniom,
- jeśli badanie pojazdu (pobieranie DNA, linii papilarnych itd.) jest konieczne, omów wymogi i określ z osobą wykonującą badania ich kolejność , aby uniknąć nieumyślnego zniszczenia dowodów tradycyjnych i cyfrowych,
- zanieczyszczenia biologiczne i fizyczne stanowią wyjątkowe wyzwanie dla rekonstrukcji danych, stosuj uniwersalne środki ostrożności, aby chronić bezpieczeństwo i zdrowie badającego,
- systemy informacyjno-rozrywkowe i telematyczne mogą mieć zewnętrzne połączenia (np. komórkowe, Wi-Fi lub Bluetooth), odizoluj jeśli to możliwe pojazd od połączeń z sieciami zewnętrznymi, na przykład odłącz anteny lub modemy komórkowe, wyjmij karty SIM.

Dane, które można pozyskać z pojazdu, mogą obejmować poniższe elementy:

- **dane o pojeździe:** numer seryjny, numer części, numer VIN, numer fabryczny,
- **dane zainstalowanych aplikacji:** pogoda, ruch drogowy, Facebook oraz YouTube,
- **połączone urządzenia:** telefony, odtwarzacze multimedialne, urządzenia USB, karty SD, punkty dostępu bezprzewodowego,
- **dane nawigacyjne:** ścieżki i punkty trasy, zapisane lokalizacje, poprzednie cele, aktywne i nieaktywne trasy,
- **informacje o urządzeniach:** identyfikatory, połączenia, SMS, audio, video, obrazy,
- **zdarzenia dotyczące pojazdu:** otwieranie i zamykanie drzwi, włączanie i wyłączanie świateł, połączenia Bluetooth, Wi-FI, USB, synchronizacja GPS, dane telematyczne takie jak prędkość, hamowanie, kąt skrętu kół itd.

Każdy samochód jest inny, a jednostki ECU mogą rejestrować różne zdarzenia i przechowywać różne dane, w zależności od konfiguracji pojazdu w trakcie montażu w fabryce. Przed przystąpieniem do analizy, badający lub pierwsza osoba dokonująca czynności, powinni zweryfikować konfigurację pojazdu poprzez pozyskanie danych konstrukcyjnych, które są powiązane z numerem VIN pojazdu.

Ponadto, jeśli badający uzyska numer IMEI z ECU, może być w stanie przeprowadzić analizę danych od operatora, aby ustalić historyczne położenie pojazdu. Badający powinien również upewnić się, że stara się uchwycić powiązane dowody, takie jak CCTV, logi automatycznego rozpoznawania tablic rejestracyjnych itp. z miejsc, w których pojawiał się samochód, aby to uprawdopodobnić.

5.13. Urządzenia pokładowe

Jednostki pływające, nawet statki bliźniacze, różnią się od siebie, ponieważ wyposażenie jednostki zależy od jej przeznaczenia, a bardziej technicznie - zależy od jej klasyfikacji. Ponadto, armator lub kapitan może również zmienić możliwości jednostki po jej odbiorze, zgodnie z uznanym przez siebie optymalnym sposobem eksploatacji. Bardziej szczegółowe informacje w tym zakresie można znaleźć w "*INTERPOL Guidelines for First Responders - Digital Forensics on Shipborne Equipment*", opracowanym wspólnie z organizacją Global Fisheries Enforcement (Organized and Emerging Crime Directorate).

Klasa i rodzaj wyposażenia pokładowego zainstalowanego na każdej jednostce są powiązane z klasyfikacją i/lub perspektywami armatora. Śledczy i osoby podejmujące pierwsze czynności mogą więc spodziewać się bardzo różnego wyposażenia na poszczególnych jednostkach. W rzeczywistości konfiguracje mogą wahać się od podstawowej konfiguracji kompasu i radia VF do zaawansowanych i najnowszych urządzeń, w tym komunikacji satelitarnej. W niektórych przypadkach mostki kapitańskie przypominają bardziej kokpit samolotu.

Z uwagi na dużą różnorodność urządzeń pokładowych, osoby podejmujące pierwsze czynności powinny posiadać wiedzę na temat urządzeń pokładowych, w tym marek, serii, modeli i numerów seryjnych. Ma to kluczowe znaczenie i pozwoli im przewidzieć, jakiego rodzaju dowody mogą znaleźć na statku i zabrać ze sobą wszelkie potrzebne narzędzia (przewody, gniazda, wtyczki itd.). Ponadto, rozpoznanie wyposażenia jednostki pływającej pozwoli zaoszczędzić czas i dać wskazówki co do lokalizacji tych urządzeń oraz ich przydatności w postępowaniu. Poniżej zaprezentowano przykłady urządzeń wraz z ich lokalizacją i rodzajami przechowywanych danych.

[4] Ten proces jest skopiowany z Najlepszych praktyk SWGDE dla pojazdów v2 (oryg. Vehicle Infotainment and Telematics System) z dn. 23.06.2016. Do Czytelnika należy zapoznanie się z najbardziej aktualną wersją tego dokumentu. Więcej informacji dostępnych jest na stronie: swgde.org/documents/published. W sekcji Referencje znajdują się wyłączenia oraz zasady udostępniania SWGDE.

Urządzenie	Lokalizacja	Rodzaj danych
transponder AIS	mostek	
echosonda	mostek	
system ECDIS	mostek, kabina nawigacyjna	
system EPIRB	mostek	
system GMDSS	mostek	
GPS	mostek	
system LRIT	mostek	
system VMS	mostek	
RADAR	mostek	
DSC	mostek, kajuta kapitańska, kabina nawigacyjna	
telefon satelitarny	mostek, kajuta kapitańska, kabina nawigacyjna	

Obraz 26: Przykłady urządzeń pokładowych z danymi i ich lokalizacją

REFERENCJE

SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition

SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020). This document includes a cover page with the SWGDE disclaimer.

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.

2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems Version: 2.0 (June 23, 2016). This document includes a cover page with the SWGDE disclaimer.

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.

2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

INTERPOL

INTERPOL

INTERPOL jest największą na świecie międzynarodową organizacją policyjną. Naszym zadaniem jest wspieranie organów ścigania w naszych 194 krajach członkowskich w zwalczaniu wszelkich form przestępczości międzynarodowej. Pracujemy, aby pomóc policji na całym świecie sprostać rosnącym wyzwaniom przestępczości w XXI wieku poprzez zapewnienie zaawansowanej technologicznie infrastruktury wsparcia technicznego i operacyjnego. Nasze usługi obejmują ukierunkowane szkolenia, fachowe wsparcie śledcze, specjalistyczne bazy danych i bezpieczne kanały komunikacji policyjnej.

NASZA WIZJA:
„ŁĄCZENIE POLICJI DLA BEZPIECZNIEJSZEGO ŚWIATA"

Nasza wizja to świat, w którym każdy przedstawiciel organów ścigania będzie mógł za pośrednictwem INTERPOL-u bezpiecznie komunikować się, dzielić, a także uzyskiwać dostęp do istotnych informacji policyjnych zawsze i wszędzie, gdzie jest to potrzebne, zapewniając bezpieczeństwo obywatelom świata. Stale dostarczamy oraz promujemy innowacyjne i najnowocześniejsze rozwiązania dla globalnych wyzwań w dziedzinie porządku publicznego i bezpieczeństwa.