WYKRYWANIE CYBERZAGROŻEŃ I ZAPOBIEGANIE IM

Co-funded by the
Erasmus+ Programme
of the European Union

Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA

Spis treści

1. Wprowadzenie do informatyki śledczej

Informatyka śledcza jest bezpośrednio związana z reagowaniem na incydenty, będąc jednym z najważniejszych jego elementów, niezbędnym do uzyskania informacji o zdarzeniach i działaniach wykonywanych w analizowanym systemie. Informatyka śledcza ma również znaczenie kryminalistyczne, badając przeszłe działania na urządzeniach, próbując zidentyfikować i zebrać dowód przestępstwa, który mógłby pomóc w decyzji w sądzie.

"niemożliwe jest, aby przestępca działał, zwłaszcza biorąc pod uwagę intensywność przestępstwa, bez pozostawienia śladów tej obecności". (Doktor Edmond Locard, s.d.)[1]

Informatyka śledcza *Rozumiana jest jako gałąź kryminalistyki, która bada i stosuje proces pozyskiwania, analizowania i zachowywania dowodów cyfrowych tak, aby były one* prawnie dopuszczalne i technicznie niepodważalne w sądzie.

Dowód cyfrowy to wszelkie dane lub informacje cyfrowe, prawnie dopuszczalne (uzyskanie) i technicznie niepodważalne (pochodzenie, integralność i niezaprzeczalność).

Informacja cyfrowa to wszystkie dane przechowywane lub przesyłane w formie cyfrowej, takie jak logi, dokumenty, e-maile, baza danych, ruch sieciowy, wśród wielu innych.

Cel informatyki śledczej i reagowania na incydenty:

- Identyfikowanie, gromadzenie i zabezpieczanie dowodów cyberprzestępstwa;
- Interpretuj, dokumentuj i przedstawiaj dowody w taki sposób, aby były one dopuszczalne w sądzie;
- Zrozumienie technik i metod stosowanych przez przestępców;
- Reaguj na incydenty, aby zapobiec stratom własności intelektualnej, finansowej i reputacji podczas ataku;
- Znać przepisy prawne obowiązujące w różnych regionach;
- Poznaj procesy manipulowania platformą cyfrową, typy danych i systemy operacyjne;
- Określenie odpowiednich narzędzi do badań kryminalistycznych;
- Odzyskaj usunięte pliki, ukryte pliki i dane tymczasowe, które mogą być wykorzystane jako dowody;
- Wspieranie prokuratury w dochodzeniach dotyczących cyberprzestępczości;
- Zabezpieczyć organizację przed podobnymi zdarzeniami w przyszłości.

---

[1] https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard

1.1. Obowiązki eksperta

Analityk kryminalistyczny podobnie jak biegły z zakresu informatyki jest prawnie odpowiedzialny za analizę zawartości cyfrowej sprzętu, który zostanie mu powierzony, dostarczając raport zwany cyfrową ekspertyzą kryminalistyczną. Po zapoznaniu się z sankcjami za odmowę lub niedopełnienie obowiązków należy odczytać przed organem sądowym lub sędzią następujące zdanie: "Zobowiązuję się z honorem do wiernego wypełnienia powierzonych mi obowiązków" i podpisać oświadczenie o zobowiązaniu. W ten sposób biegły zobowiązuje się do przeprowadzenia analizy i cyfrowego raportu kryminalistycznego, przy czym biegli będący funkcjonariuszami publicznymi i interweniujący przy wykonywaniu swoich obowiązków są zwolnieni z terminu zobowiązania. Zostanie poinformowany o procesie i o pytaniach, na które należy odpowiedzieć. Sankcje za odmowę lub niewykonanie zobowiązania są obecne w portugalskim Kodeksie postępowania karnego w art. 91, no. 4. Jeśli chodzi o dostarczenie raportu biegłego, art. 157 tego samego kodeksu postępowania karnego stanowi, że raport musi zawierać odpowiedzi i wnioski należycie uzasadnione i musi zostać przedstawiony w terminie nieprzekraczającym 60 dni.

Konieczne jest, aby raport przedstawiał tylko prawdziwe informacje, gdyż za podanie nieprawdziwych informacji grozi kara pozbawienia wolności od 6 miesięcy do 3 lat lub grzywna nie krótsza niż 60 dni, zgodnie z art. 360.

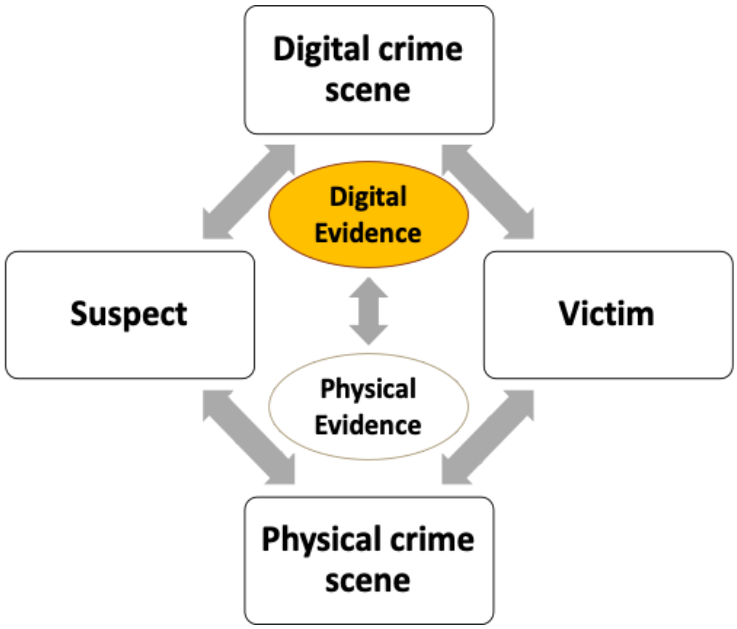
1.2. Aplikacja informatyki śledczej

Obszary działania informatyki śledczej są coraz bardziej wszechstronne, gdzie wcześniej analizowane byłyby tylko dyski twarde i inne nośniki służące do przechowywania informacji, teraz konieczne może być zbieranie i analizowanie danych w pamięciach lotnych (performance w live-data forensics) czy nawet danych o ruchu sieciowym (network forensics), danych przechowywanych na urządzeniach mobilnych (mobile forensics), danych przechowywanych w systemach rozproszonych w chmurach w Internecie, wśród wielu innych.

Edmond Locard (Figure 1), stwierdził, że:

"niemożliwe jest, aby przestępca działał, zwłaszcza biorąc pod uwagę intensywność przestępstwa, bez pozostawienia śladów tej obecności"

W przestępstwach, które w jakiś sposób wiążą się z komponentem cyfrowym, przestępstwach cyberinstrumentalnych i cyberzależnych (R.Bravo) i zgodnie z wypowiedzią Edmonda Locarda, istnieje większa możliwość pozostawienia dowodów cyfrowych, związanych z wykorzystaniem środków cyfrowych.



Rysunek 1 - Schemat Edmonda Locarda

Źródło: https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard

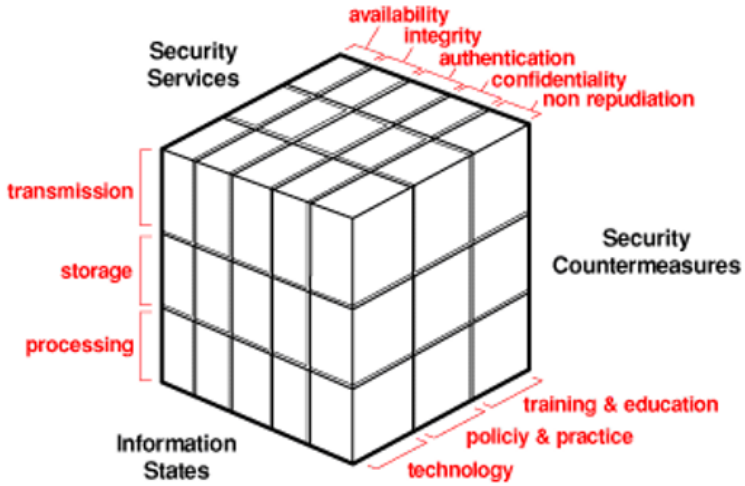
Cyfrowa kryminalistyka nie jest uważana za naukę ścisłą i możliwe jest, że ten sam raport z informatyki śledczej analizowany przez różne osoby może być różnie rozumiany, dlatego zasadnicze znaczenie ma zapewnienie podstawowych zasad bezpieczeństwa informacji (rys. 2), poufności, integralności i niezaprzeczalności. W ten sposób informatyka śledcza będzie z konieczności:

PRAWNIE DOPUSZCZALNA I TECHNICZNIE NIEPODWAŻALNA

Stosowanie powszechnie akceptowanych technik, przestrzeganie przepisów prawa krajowego w dążeniu do udzielenia na każde badane pytanie jak najpełniejszej odpowiedzi, przy czym 7 powodów jest najpełniejszą formą odpowiedzi:

"Co? Gdzie?, Kiedy?, Jak?, Kto?, Dlaczego? i Ile?".

Inspektor-koordynator Rogério Bravo - policja sądowa



Rysunek 2 - Bezpieczeństwo informacji

Źródło: John McCumber

Poufność

Do czasu rozstrzygnięcia przez sąd osoby zamieszane w sprawę są i muszą pozostać niewinne, a dostęp do ich danych jest całkowicie ograniczony do samego biegłego, który nie może ich udostępnić osobom trzecim.

Autentyczność

Dowody muszą być autentyczne. Wytworzony przez osoby, które mogą o nim odpowiedzieć. W przeciwnym razie dowód jest uznawany w sądzie za nieistotny.

Integralność

Informacje zawarte w urządzeniach muszą być za wszelką cenę zachowane w stanie pierwotnym. Ekspert jest odpowiedzialny za stosowanie technik zmieniających integralność informacji.

Brak odmowy

Jeśli chodzi o sprawowanie funkcji eksperckich, "nierepublikowanie" odpowiada stosowaniu powszechnie akceptowanych technik, umożliwiając wykorzystanie kontrekspertyzy w celu uzyskania tych samych rezultatów.

1.3. Wyzwania związane z informatyką śledczą

Metody i techniki informatyki śledczej stoją obecnie przed wielkimi wyzwaniami, zmuszając śledczych do ciągłej potrzeby badań i udoskonaleń. Tradycyjnie, śledczy zajmujący się informatyką śledczą systematycznie starają się przyjrzeć artefaktom w poszukiwaniu ewentualnej wskazówki, która może być dowodem przestępstwa. Jednak wraz z rozwojem technologii, procedury i podejścia do poszukiwania takich dowodów przestępstwa muszą być ulepszane i dostosowywane. Istnieje wiele nowych, małych wyzwań, z którymi kryminalistyka musi sobie poradzić, jednak przedstawiamy krótkie podsumowanie w 3 kategoriach:

Dane techniczne:

- Różne rodzaje przechowywania;
- Szyfrowanie;
- Stegnografia;
- Techniki antyforensyczne;
- Acquisition and Analysis in Live Data Forensics;
- Ukrywanie i usuwanie danych;
- Zmienność danych;
- Udziały w sieci;
- ...

Legals:

- Prywatność;
- Ochrona danych osobowych;
- Opóźnienie w dostosowaniu prawa do rzeczywistości technologicznej;
- Działając na miejscu zbrodni;
- Analiza i obróbka danych;
- ...

Zasoby:

- Wzrost ilości danych;
- Złożoność rozproszonych systemów przechowywania danych;
- ...

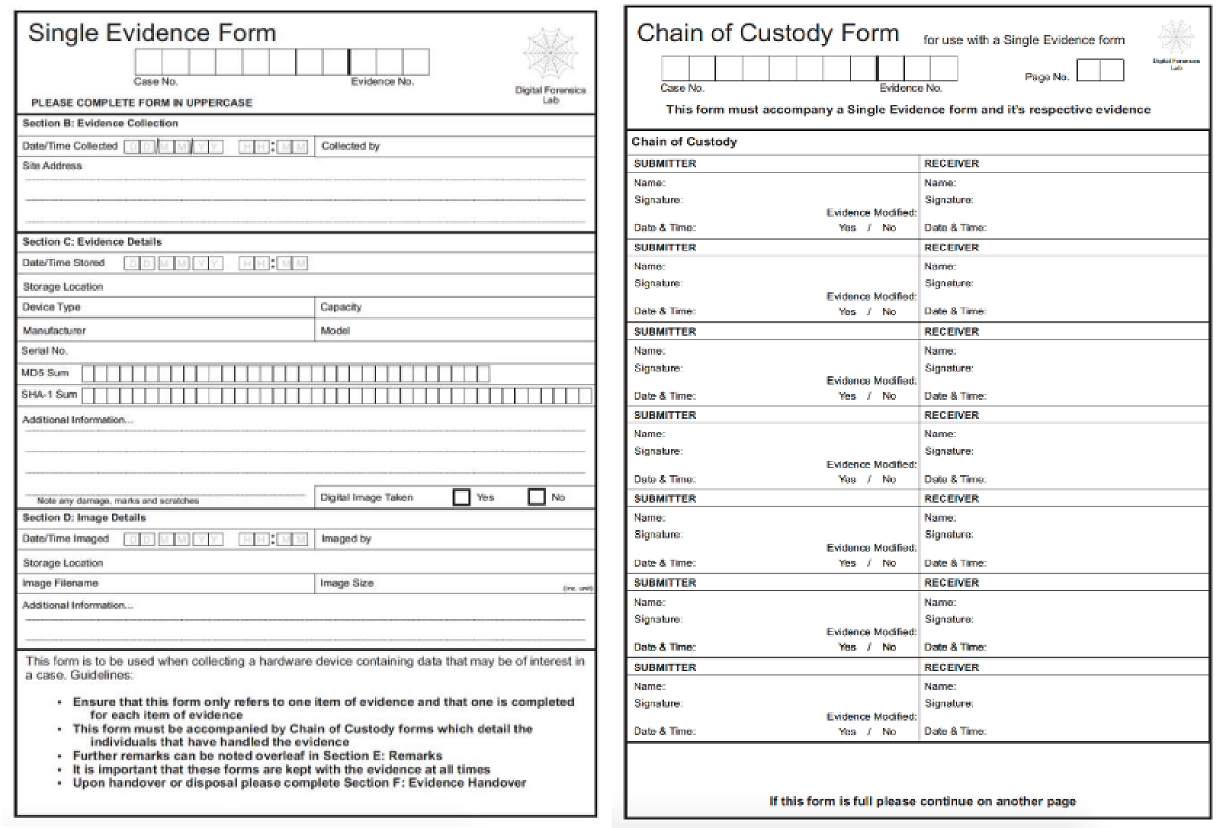
1.4. Standardy międzynarodowe

Podmioty, które starają się opracować przewodniki dobrych praktyk w obszarze informatyki śledczej są liczne, bu nasze odniesienia to ISO/IEC, NIST, ENISA, SANS i inne, które starają się upowszechniać i rozwijać wiedzę w tym obszarze. Można więc wyróżnić kilka ważnych dokumentów w rozwoju funkcji eksperta ds. informatyki śledczej, a mianowicie:

- **RFC 3227:2002** Przewodnik po pozyskiwaniu i zabezpieczaniu dowodów cyfrowych
- **NIST 800-86** Przewodnik po integracji technik kryminalistycznych w reagowaniu na incydenty
- **NIST 800-144** Przewodnik po bezpieczeństwie i prywatności w chmurze
- **NIST 800-101** Przewodnik po kryminalistyce urządzeń mobilnych
- **ISO/IEC 20000-1:2018** Technika informatyczna - Zarządzanie usługami
- **ISO/IEC 27001:2013** Definicja systemu zarządzania bezpieczeństwem informacji (ISMS)
- **ISO/IEC 27002:2013** Przewodnik po dobrych praktykach w zakresie bezpieczeństwa informacji
- **ISO/IEC 27005:2018** Zarządzanie ryzykiem w zakresie bezpieczeństwa informacji
- **ISO/IEC 27032:2012** Przewodnik po cyberbezpieczeństwie
- **ISO/IEC 27037:2012** Przewodnik po identyfikacji, zbieraniu, pozyskiwaniu i zabezpieczaniu dowodów cyfrowych

1.5. Łańcuch dowodowy

Łańcuch dowodowy to dokument/formularz, który musi być wypełniony przez osobę przejmującą sprzęt. Dokument ten musi zawsze towarzyszyć samemu sprzętowi, zachowując datowany zapis wszystkich osób, które miały pieczę nad sprzętem. Przedstawiono przykład łańcucha nadzoru (Rysunek 3).



Single Evidence Form

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected D D M M Y Y H H : M M — Collected by

Site Address

Section C: Evidence Details

Date/Time Stored D D M M Y Y H H : M M

Storage Location

Device Type — Capacity

Manufacturer — Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches — Digital Image Taken ☐ Yes ☐ No

Section D: Image Details

Date/Time Imaged D D M M Y Y H H : M M — Imaged by

Storage Location

Image Filename — Image Size (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Chain of Custody Form — for use with a Single Evidence form

Case No. Evidence No. Page No.

Digital Forensics Lab

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: — Evidence Modified: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Rysunek 3 - Formularz łańcucha dowodowego

Źródło: https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=wx99T&1661384494937

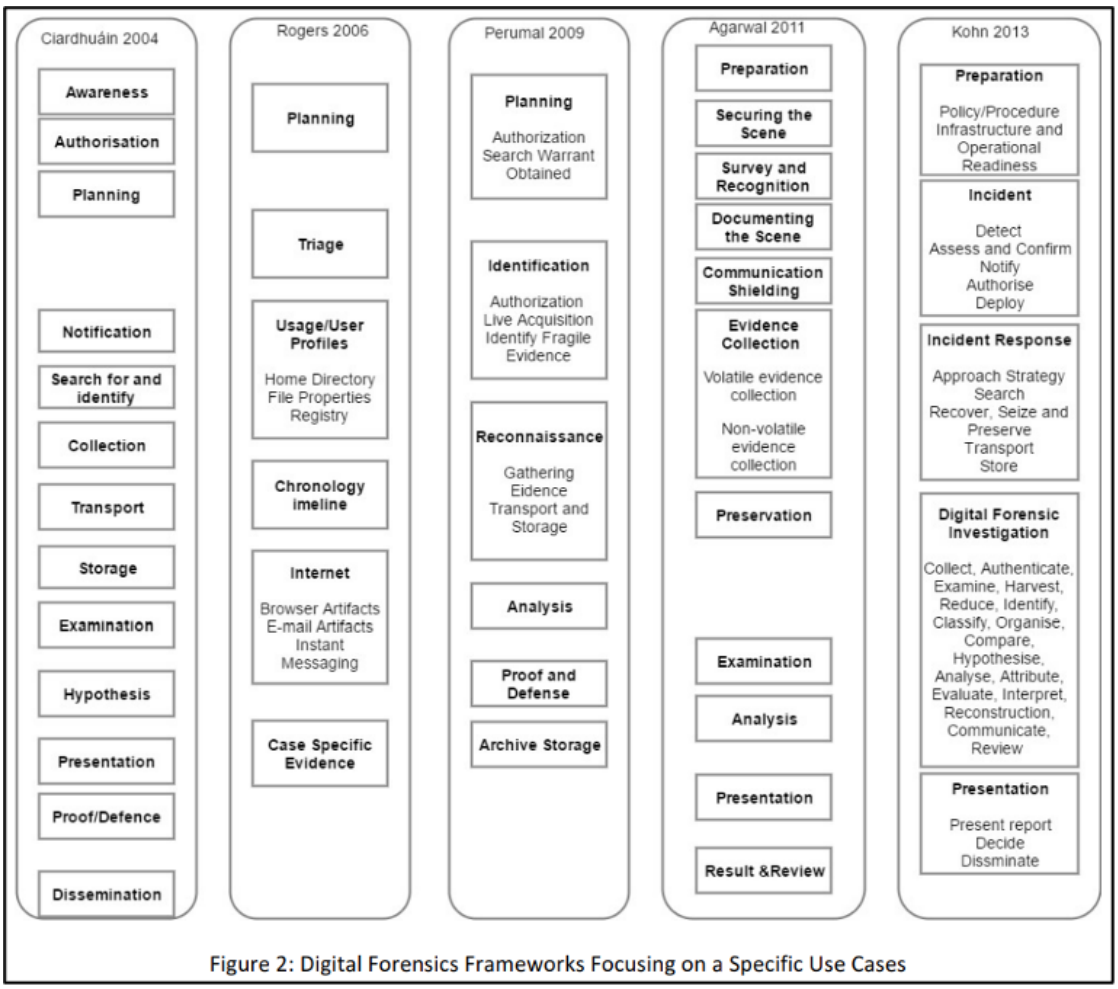
1.6. Modele procesów w analizie kryminalistycznej

Każdy śledczy ma swoją własną metodę i metodykę pracy w trakcie przeprowadzania analizy kryminalistycznej, nie ma też standardowego modelu dla każdego rodzaju śledztwa, który zazwyczaj kieruje się dotychczasowym doświadczeniem każdego śledczego.

Z biegiem czasu pojawiły się różne metodologie, które określają potrzebę sekwencji ogólnych kroków w dochodzeniu kryminalistycznym, zwykle definiowanych jako "zbieranie dowodów, zabezpieczenie lub badanie, analiza".

Zaproponowano kilka modeli dochodzeniowych, zwanych również " Digital Forensics Investigation Frameworks "(Rysunek 4), przy czym te są jednymi z najbardziej popularnych:

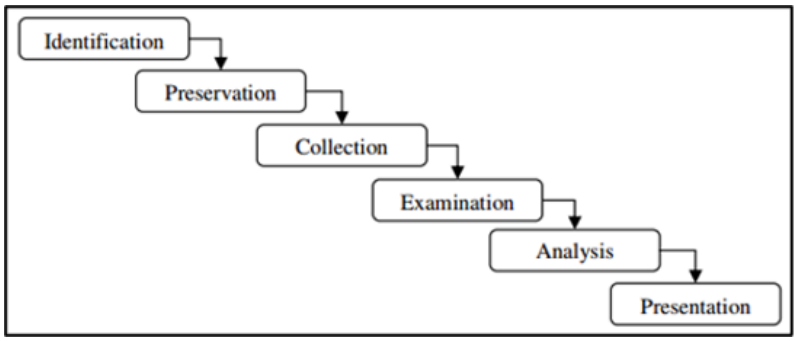
- Model DFRWS - Digital Forensic Research Workshop (Palmer et al. 2001)
- ADFM - Abstract digital forensics model (Reith et al. 2002)
- IDIP - Integrated Digital Investigation Process (Carrier et al. 2003)
- EIDIP - Enhanced Integrated Digital Investigation Process (Baryamureeba & Tushabe 2004).
- CFFTPM - Computer Forensics Field Triage Process Model (Rogers et al. 2006)
- SRDFIM - Systematic Digital Forensic Investigation Model (Agarwal et al. 2011)
- IDFPM - Integrated Digital Forensic Process Model (Kohn et al. 2013)
- EDRM - Electronic Discovery Reference Model (https://edrm.net, 2014)



Rysunek 4 - Ramy dochodzenia w dziedzinie informatyki śledczej

Źródło: Rysunek 2 z artykułu https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf

W 2001 roku w badaniach wynikających z Warsztatów Badań Cyfrowych zaproponowano 6-stopniową ramę, przedstawioną na rysunku 5.



Rysunek 5 - Ramy DFRWS

Jest to do dziś jedna z głównych metodologii cyfrowego śledztwa kryminalistycznego i ta, którą będziemy się kierować. Każdy z etapów został opisany poniżej:

Identyfikacja - kiedy badacz musi zidentyfikować wszystkie istotne informacje i określić strategię ich pozyskania. Badacz może mieć do czynienia z typowym urządzeniem pamięci masowej, takim jak dysk twardy, karta pamięci, lub inaczej dane cyfrowe mogą wymagać zebrania z danych o ruchu sieciowym, danych lotnych, takich jak dane pamięciowe, urządzeń mobilnych lub IoT, lub jakichkolwiek innych urządzeń do przechowywania danych cyfrowych. Na tym etapie, przygotowanie przed użyciem technik i narzędzi, jest niezwykle ważne, aby zapewnić autentyczność, integralność i niezaprzeczalność wszystkich dowodów w sądzie.

Zachowanie - jest to etap, który ma na celu realizację takich zadań, jak ustanowienie właściwego zarządzania sprawami i zapewnienie akceptowalnego łańcucha dowodowego w sądzie. Ten etap jest kluczowy dla zapewnienia, że dane są zbierane bez żadnych zewnętrznych zanieczyszczeń i analizowane prawidłowo.

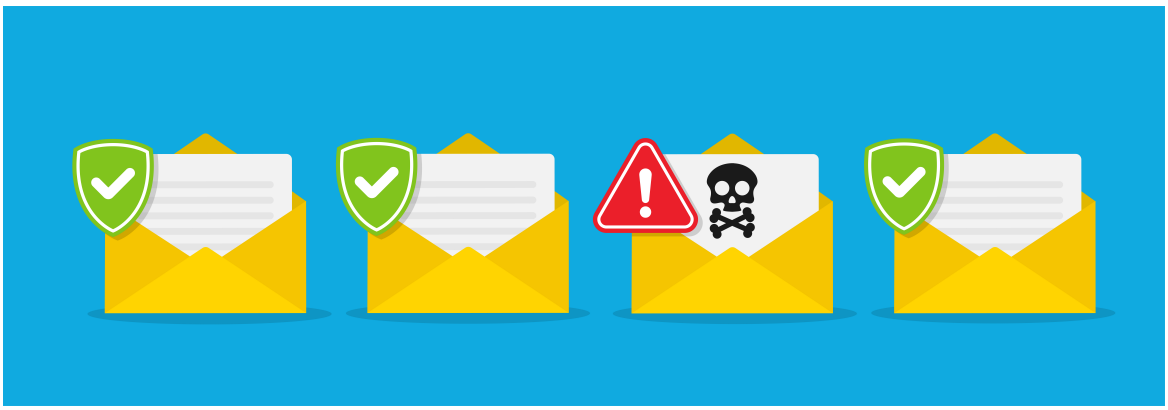
Zbieranie - Ten etap odnosi się do pozyskania dowodów cyfrowych i tradycyjnie może być dokonany poprzez klonowanie lub kryminalistyczne obrazowanie urządzenia pamięci masowej. Pozyskanie danych zmiennych lub innych istotnych i zmiennych danych może mieć decydujące znaczenie dla etapu dochodzenia, zwłaszcza gdy dane związane z pozyskaną pamięcią masową są zaszyfrowane. Zebrane na tym etapie dane stanowią dane wejściowe lub źródło danych dla etapu analizy.

Badanie - Jest to faza poszukiwania pożądanych danych, obejmująca m.in. techniki wyszukiwania, odzyskiwania usuniętych danych, deszyfrowania danych, łamania haseł, analizy złośliwego oprogramowania, analizy wzorców. Faza ta jest powiązana z fazą analizy, gdyż np. po identyfikacji dokumentów konieczna będzie ich analiza, uwzględniająca odpowiedź na żądane pytania.

Analiza - analiza wszystkich zebranych danych. Jest to najbardziej czasochłonna faza, ze względu na konieczność przeprowadzenia dokładnego wyszukiwania i identyfikacji wszystkich istotnych artefaktów. W większości przypadków zdarza się, że zebrane dane występują w postaci danych nieustrukturyzowanych, co wymaga zastosowania specjalnych narzędzi i bardziej czasochłonnej analizy w celu zidentyfikowania potencjalnych cyfrowych danych dowodowych, gdzie w grę wchodzą dane ustrukturyzowane, takie jak zapisy, bazy danych, pliki danych, pliki systemowe, strony internetowe i inne.

Prezentacja - Jest to ostatnia faza procesu cyfrowej analizy kryminalistycznej, w której należy przedstawić sędziemu raport końcowy ze wszystkimi istotnymi danymi. Raport ten powinien być złożony w formie papierowej, ze wszystkimi artefaktami uznanymi za istotne. W przypadku wątpliwości dotyczących informacji presente w złożonym raporcie, wymagane jest zeznanie eksperta w sądzie w celu dostarczenia odpowiednich wyjaśnień .

2. Zabezpieczanie i gromadzenie dowodów cyfrowych na miejscu przestępstwa/zdarzenia



Aby analiza została przeprowadzona w jak najlepszym stanie, konieczne będzie również prawidłowe wykonanie zabezpieczenia i zebrania. W tym rozdziale podejdziemy do działań na miejscu zdarzenia w taki sam sposób jak do działań na miejscu przestępstwa, gdyż w obu są oczywiste podobieństwa, ale każde z nich siłą rzeczy będzie miało swoją specyfikę i cechy szczególne, których nie będziemy tu przedstawiać.

INCYDENT

"Incydent komputerowy to przerwa lub awaria jakościowa w usłudze informatycznej" Źródło: Podręcznik "ITIL V3 - Funkcjonowanie usług" (OGC, 2007)

Aby zaistniał incydent, musi koniecznie dojść do naruszenia dostępności, autentyczności, integralności lub poufności danych.

To właśnie sieci Computer Security Incident Response Team (CSIRT) umożliwiają gromadzenie danych dotyczących incydentów komputerowych, w tym celu opracowały wspólną taksonomię (Źródło: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf) klasyfikacji incydentów, klasyfikując je za pomocą 2 wektorów, według typu incydentu i według typu zdarzenia.

ENISA również rozwijała i promowała wiedzę na temat dobrych praktyk w zakresie identyfikacji i zarządzania incydentami, regularnie publikując na ten temat (czytaj: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection).

ENISA w 2010 r. opublikowała dokument "Incident Management Guide" (https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management), w którym klasyfikuje incydenty na kategorie w zależności od stopnia ich ciężkości, co przedstawiono na rysunku 6.

Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Rysunek 6 - Klasyfikacja zdarzeń

Źródło: Incident Management Guide (ENISA 2010)

2.1. Międzynarodowe standardy reagowania na incydenty

Podmiotów, które starają się opracować przewodniki dobrych praktyk w zakresie reagowania na incydenty jest wiele, jednak naszymi referencjami są ISSO/IEC, NIST oraz ENISA. Można zatem wskazać kilka ważnych dokumentów w rozwoju funkcji eksperta ds. informatyki śledczej, a mianowicie:

- **Przewodnik zarządzania incydentami** (ENISA 2010)
- **ISO/IEC 27035:2016** Przewodnik zarządzania incydentami bezpieczeństwa informacji dla średnich i dużych organizacji
- **ISO/IEC 27037:2012** Przewodnik po identyfikacji, zbieraniu, pozyskiwaniu i zabezpieczaniu dowodów cyfrowych
- **NIST 800-86** Przewodnik po integracji technik kryminalistycznych w reagowaniu na incydenty
- **NIST IR 8796** Analiza bezpieczeństwa urządzeń mobilnych i wearables dla osób udzielających pierwszej pomocy
- **ISO/IEC 27001:2013** Definicja systemu zarządzania bezpieczeństwem informacji (ISMS)
- **ISO/IEC 27002:2013** Przewodnik po dobrych praktykach w zakresie bezpieczeństwa informacji
- **ISO/IEC 27005:2018** Zarządzanie ryzykiem w zakresie bezpieczeństwa informacji
- **ISO/IEC 27032:2012** Przewodnik po cyberbezpieczeństwie

Norma ISO/IEC 27002 - Zarządzanie incydentami bezpieczeństwa informacji definiuje różnicę pomiędzy **zdarzeniem** a **incydentem,** gdzie zdarzenie może nie zawsze prowadzić do incydentu, ale incydent zawsze prowadzi do zdarzenia.

2.2. Zarządzanie incydentami i łagodzenie ich skutków

Norma ISO/IEC 27035 definiuje 5 kroków w zarządzaniu incydentami i łagodzeniu ich skutków, a mianowicie:

1. Przygotowanie i planowanie
2. Wykrywanie i rejestracja
3. Ocena i decyzja
4. Odpowiedź
5. Wyciągnięte wnioski

1.Przygotowanie i planowanie to etap identyfikacji wszystkich krytycznych aktywów instytucji, wewnętrznych procesów dostępu do informacji, tworzenia systemów monitorowania pozwalających na identyfikację incydentów, a także wszystkich obowiązków i procedur w przypadku wystąpienia incydentu.

Przygotowanie

- Przygotowanie laboratorium cyfrowego
- Określenie lidera zespołu
- Określenie członków zespołu i zakresu odpowiedzialności
- Przygotowanie briefingu / strategii interwencji

Briefing

- Strategia interwencji?
- Sprzęt potrzebny do zabrania na miejsce zdarzenia?
- Jaki rodzaj metod (narzędzi) zbierania/pozyskiwania danych?
- Jaka jest aktywność sieciowa?
- Zmienność zgromadzonych danych?
- Czy sprzęt mógł być skonfigurowany tak, aby zniszczyć dowody?
- Jak będziemy przechowywać/transportować dowody cyfrowe?
- Powiązane urządzenia, podręczniki, itp ?
- Zidentyfikować ewentualne konflikty interesów?
- Ocena ryzyka

2. Wykrywanie i rejestrowanie to z konieczności faza identyfikacji zdarzeń i odróżniania zdarzenia lub kolejnych zdarzeń od ewentualnego incydentu .

Podobnie jak w przypadku każdego innego przestępstwa, ponieważ zdarzenie mogło zostać celowo sprowokowane przez wewnętrznego pracownika organizacji. W związku z tym powinniśmy wziąć pod uwagę wcześniejsze przygotowanie do działania według poniższych punktów:

- Zabezpieczanie miejsca zbrodni
- Zbieranie informacji wstępnych
- Dokumentowanie miejsca zbrodni
- Zbieranie i zabezpieczanie dowodów
- Pakowanie i transport
- Łańcuch dowodowy

W celu umożliwienia sprawnego podejmowania decyzji należy przeprowadzić maksymalne możliwe **zbieranie informacji**, odpowiednie do rodzaju ewentualnego zdarzenia. W ten sposób powinniśmy wziąć pod uwagę wszystkie rodzaje informacji, które mogą być pozyskane, takie jak:

- Typ połączenia (Wi-Fi/Ethernet)
- Jakie komputery służą do łączenia się z internetem?
- Lokalizacja systemów i określenie, kto ma dostęp
- Szczegóły dotyczące urządzeń wymiennych i właściwości użytkownika
- Uzyskanie szczegółów dotyczących topologii sieci
- Uzyskanie szczegółowych informacji o innych urządzeniach peryferyjnych podłączonych do komputera
- Czy są jakieś inne pytania w tym temacie, na które nie udzielono odpowiedzi?

Z tych informacji powinniśmy wziąć pod uwagę informacje otaczające, takie jak:

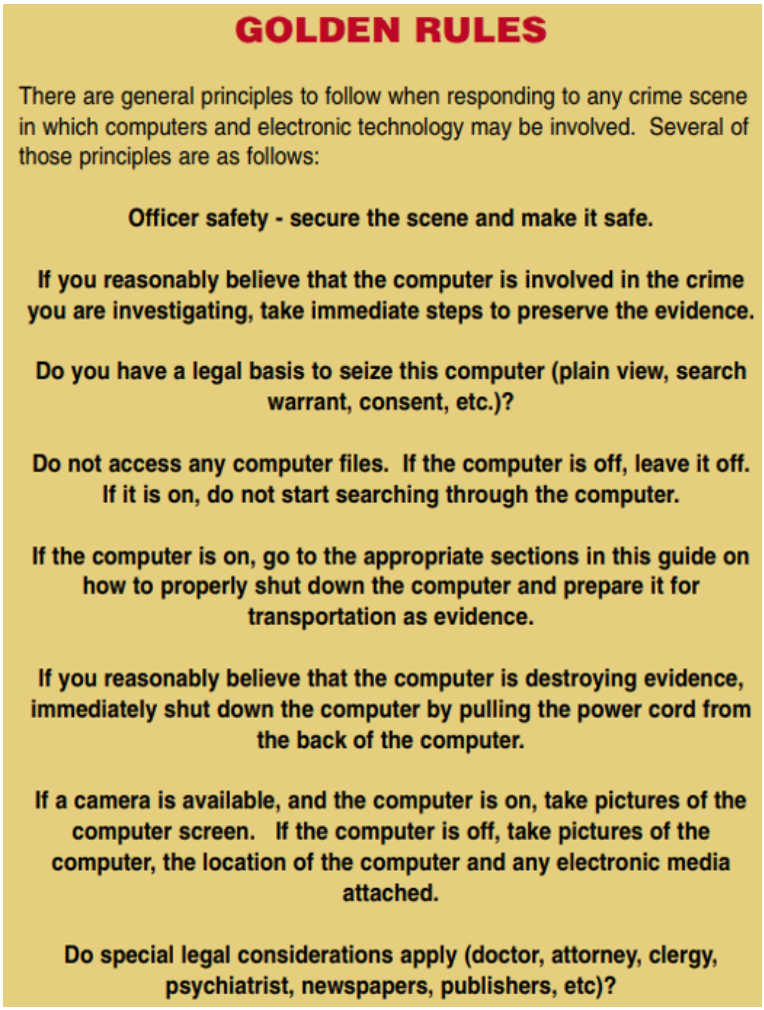
- Jakie usługi są oferowane przez organizację?
- Kim są osoby dotknięte zdarzeniami? Czy zostały one poinformowane?
- Czy istnieją logiczne środki ochrony (antywirus, firewall, IDS, IPS)? Alarmy?
- Jakie środki bezpieczeństwa fizycznego są stosowane?
- Czy istnieją zapisy z kamer przemysłowych
- Określenie liczby komputerów i komputerów podłączonych do internetu
- Sprawdź najnowsze wymiany sprzętu
- Poziom dostępu pracowników? Ostatnie zwolnienia?
- Poziomy dostępu Administracyjny/Administrator?
- Polityka bezpieczeństwa organizacji?
- Procedury podane w celu opanowania incydentu?
- Lista podejrzanych? Dlaczego są podejrzani?
- Logi systemowe? Logi sieciowe? Coś podejrzanego?
- Użycie systemu po incydencie? Polecenia CMD/Shell? Skrypty? Zadania? Procesy?
- Procedury analizy po zdarzeniu?

Zespół reagujący na incydent powinien wziąć pod uwagę zbieranie zmiennych danych, które są ewentualnie krytyczne dla szybkiego podejmowania decyzji dotyczących wszystkich przeszłych zdarzeń. Dlatego ważne jest, aby działać w różny sposób w zależności od tego, czy komputer jest włączony czy wyłączony (Figure 7).

Jak znaleźć komputer?

Rysunek 7 - pierwsze działanie

Departament Bezpieczeństwa Krajowego USA opublikował krótki przewodnik dla First Responders, zatytułowany "Best Practices for seizing Electronic Evidence", który ma coś, co nazywają złotymi zasadami, co jest przedstawione na Rysunku 8.

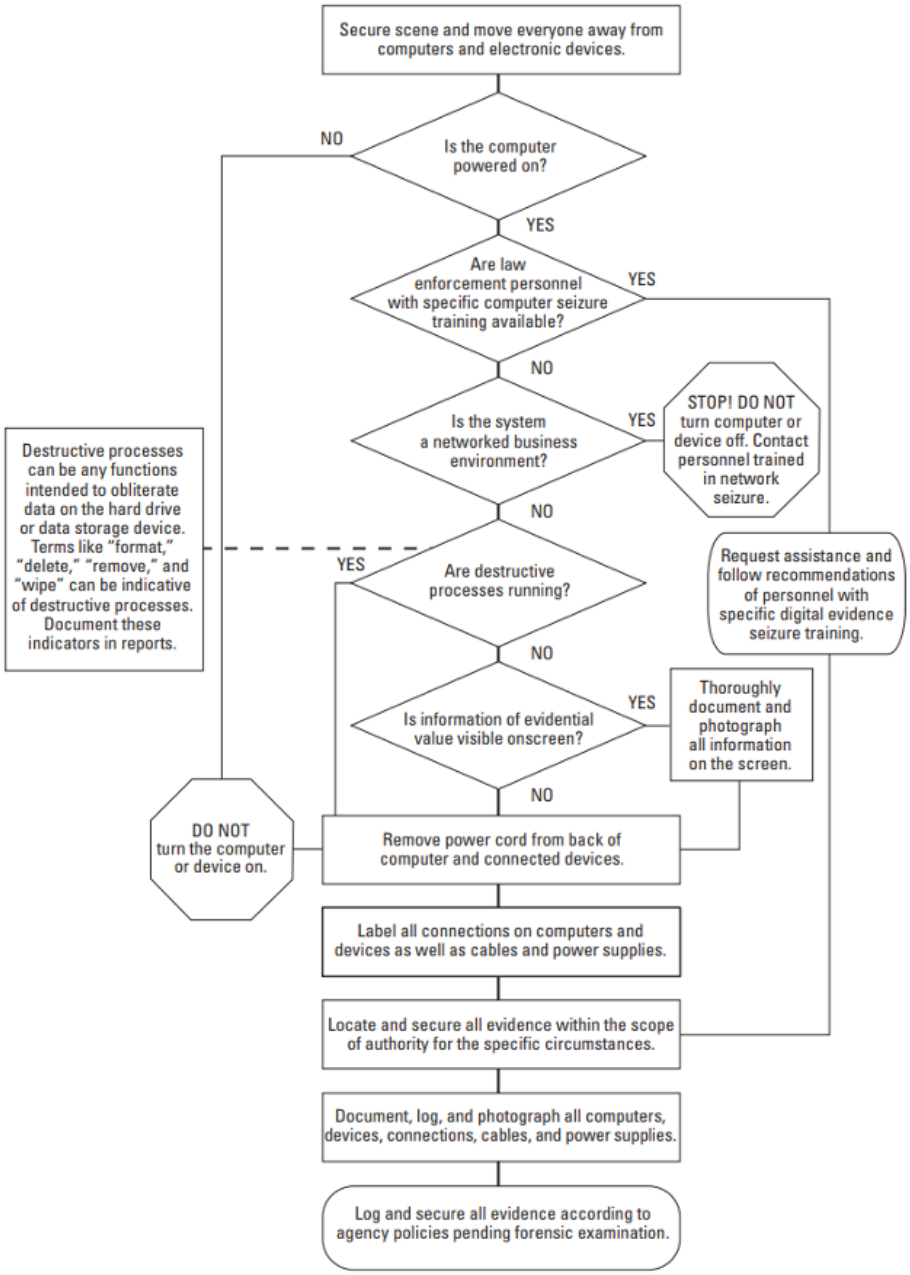


Rysunek 8 - Najlepsze praktyki w zakresie przejmowania dowodów elektronicznych

Źródło: https://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf

Zasady te obowiązują obecnie i należy się do nich stosować podczas reagowania na incydenty bezpieczeństwa.

Z kolei Departament Sprawiedliwości USA - Narodowy Instytut Sprawiedliwości opublikował schemat przepływu podsumowujący proces zbliżania się do urządzeń, nazwany "Collecting Digital Evidence Flow Chart" (Rysunek 9).



Rysunek 9 - Schemat przepływu gromadzenia dowodów cyfrowych

Źródło: Collecting Digital Evidence Flow Chart. US Department of Justice - National Institute of Justice (2010).

W związku z tym możemy określić następujące procedury:

1. Zapewnienie bezpieczeństwa fizycznego i elektronicznego.
2. Jeśli komputer jest wyłączony:

· Upewnij się, że nie jest włączony (odłącz kabel zasilający/wyciągnij baterię, jeśli jest)

· Oznaczyć/fotografować wszystkie komponenty i urządzenia peryferyjne

· Identyfikacja urządzeń pamięci masowej

· Sprawdź dane/czas BIOS-u (bez dysku twardego)

3. Jeśli komputer jest włączony:

· Rozłączenie komunikacji (odłączenie kabla sieciowego/wyjęcie karty SIM)

· Sfotografuj ekran i całą jego zawartość (opisz widoczną zawartość)

· Jeśli istnieje potrzeba gromadzenia danych lotnych i nielotnych:

· Wykonaj akwizycję danych na żywo (zgodnie z kolejnością zmienności)

· Sprawdź, czy urządzenia pamięci masowej są zaszyfrowane

· Odłącz komputer od zasilania

· Etykietowanie/fotografowanie wszystkich komponentów i urządzeń peryferyjnych

· Identyfikacja urządzeń pamięci masowej

· Sprawdź datę/czas BIOS-u (bez dysku twardego)

4. Jeśli w grę wchodzi urządzenie mobilne (smartfon/tablet):

· Jeśli urządzenie jest wyłączone, nie należy go włączać

· Jeśli urządzenie jest włączone :

· Sfotografuj wyświetlacz (jeśli jest dostępny)

· Tryb lotu Pu tinto

· Zawsze upewnij się, że urządzenie podłączone do akumulatora ma wystarczające zasilanie, aby utrzymać je w stanie aktywnym do czasu analizy

· Użyj torby/worka Faradaya (rysunek 10)

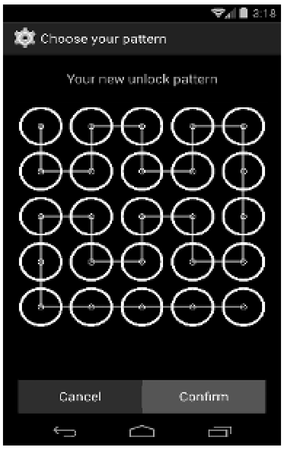
Rys. 10 - Torba Faradaya

Oznaczyć/fotografować wszystkie elementy

· Zbierz wszystkie dodatkowe urządzenia pamięci masowej (karty pamięci, karty SIM itp.).

· Dokumentuj wszystkie czynności związane z przejęciem urządzenia mobilnego

· Pytanie o kody dostępu (PIN/wzór), PIN karty SIM i kody PUK (sprawdzić woreczki do przenoszenia urządzeń - rysunek 11)



Rysunek 11 - Kod standardowy

Jak przechowywać i transportować?

· Nosić rękawice

· Nie zakrywać informacji identyfikujących

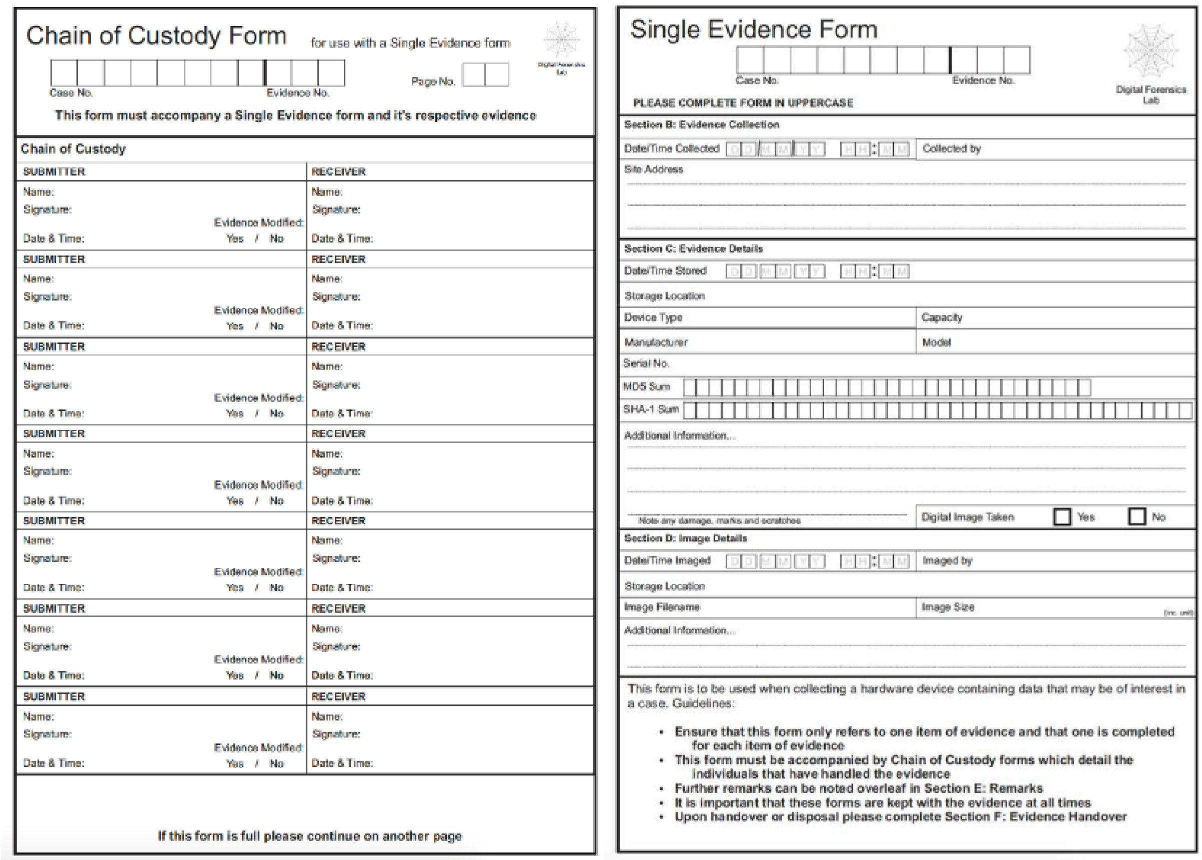
· Dowody cyfrowe z otworami i ruchomymi elementami powinny być zabezpieczone plombami lub taśmą zabezpieczającą przed manipulacją.

· Urządzenia powinny być przechowywane w torbach rozpraszających ładunki elektrostatyczne i torbach Faradaya.

· Dokumentować

· Udokumentować w odpowiednim sprawozdaniu i podpisać przez wszystkich zaangażowanych.

· Wypełnij formularz Chain of Custody sprzętu (Rysunek 12)



Chain of Custody Form for use with a Single Evidence form

Case No. Evidence No. Page No.

Digital Forensics Lab

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:

If this form is full please continue on another page

Single Evidence Form

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected D D M M Y Y H H : M M Collected by

Site Address

Section C: Evidence Details

Date/Time Stored D D M M Y Y H H : M M

Storage Location

Device Type Capacity

Manufacturer Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken Yes No

Section D: Image Details

Date/Time Imaged D D M M Y Y H H : M M Imaged by

Storage Location

Image Filename Image Size (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

Rysunek 12 - Łańcuch dowodowy

Źródło: https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=wx99T&1661384494937

3.Ocena i decyzja to faza po uzyskaniu wiedzy o istnieniu możliwego incydentu, zebraniu wszystkich użytecznych informacji o tym, co się stało, prowadząca do podjęcia decyzji o potwierdzeniu incydentu bezpieczeństwa IT. Wraz z tym potwierdzeniem musi nastąpić szybka reakcja w celu jego złagodzenia i rozwiązania .

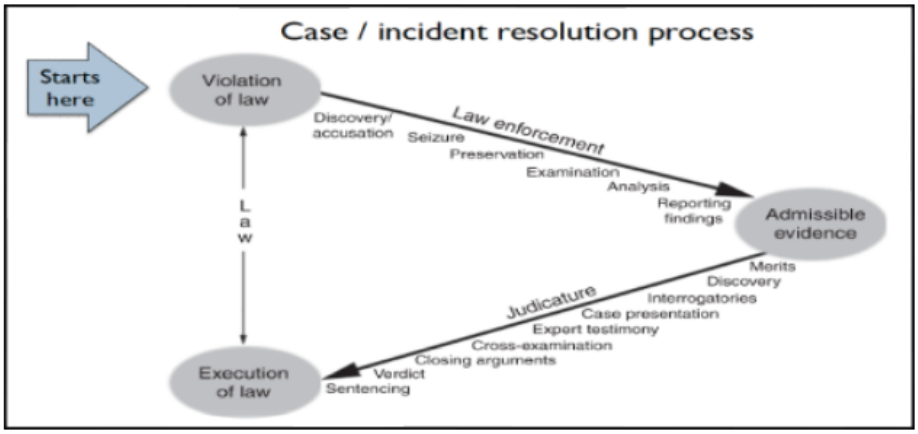
4.Reakcja to etap, w którym następuje klasyfikacja incydentu, zgodnie z tym, co zostało określone w fazie 1, kategoryzacja incydentu i klasyfikacja jego powagi, przeprowadzenie niezbędnych procedur w celu jego złagodzenia i rozwiązania, wykorzystanie mechanizmów zarządzania kryzysowego oraz zgłoszenie incydentu do właściwych organów, w przypadku Portugalii są to Policja Sądowa (PJ), Krajowe Centrum Cyberbezpieczeństwa (CNCS) oraz Krajowa Komisja Ochrony Danych (CNPD).

5.Lessons Learned jest jednym z najbardziej potrzebnych etapów, ponieważ umożliwia wdrożenie środków, aby podobny incydent się nie powtórzył, a także wykorzystanie wygenerowanej wiedzy do poprawy systemu bezpieczeństwa organizacji.

Patrz: https://www.cncs.gov.pt/certpt/coordenacao-da-resposta-a-incidents/

2.3. Związek między procesem rozwiązywania incydentów a informatyką śledczą

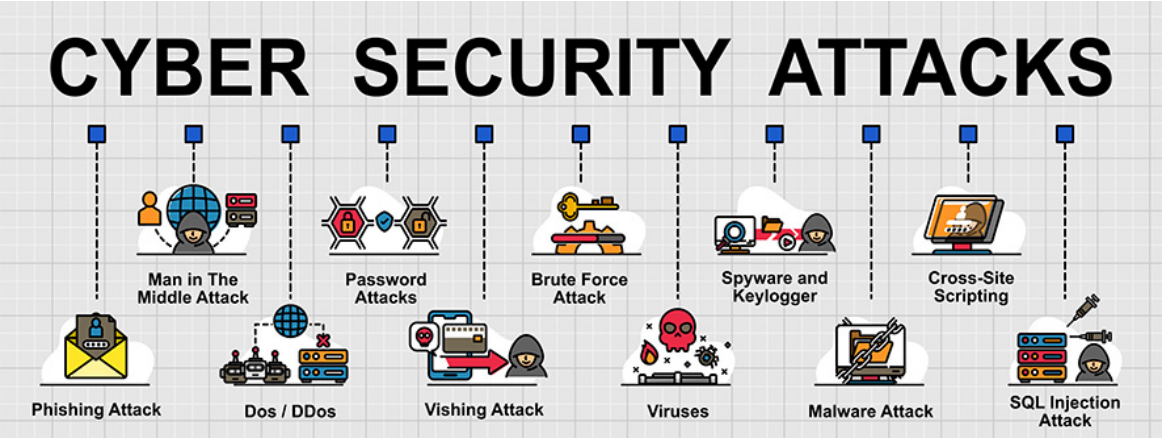
Procedury te odnoszą się do informatyki śledczej (Rysunek 13) w każdym przypadku wykrycia incydentu, gdy chcemy dowiedzieć się więcej na jego temat, próbując postawić sprawcę przed sądem. W procesie zarządzania incydentem mamy więc ten sam proces dochodzeniowy, wskazany w punkcie 1.6, dotyczący 6 kroków ram analizy.



Rysunek 13 - Proces rozwiązywania incydentów

Źródło: http://www.c-jump.com/bcc/t155t/Week03a/W24_0030_overview_of_caseinci.htm

3. Procedury pozyskiwania dowodów cyfrowych



Informatyka śledcza to proces pozyskiwania, analizowania i zabezpieczania dowodów cyfrowych, przy zastosowaniu standaryzowanych procedur, które pozwalają na zachowanie integralności obrazu dowodowego.

Konieczne jest zatem zapewnienie, aby kryminalistyczne pozyskanie urządzeń pamięci masowej odbywało się zgodnie z przyjętymi na szczeblu międzynarodowym najlepszymi praktykami, a jedną z nich jest uprzednia sterylizacja dysku twardego, na który trafi kopia danych, co opisano w kolejnym punkcie.

3.1. Procedura sterylizacji

Procedury sterylizacji mają na celu zapewnienie, że nasze urządzenie docelowe jest gotowe do odbioru oryginalnej informacji. Sterylizacja ma na celu zapisanie wszystkich bitów naszego dysku zbiorczego z wartością 0 (zero), co zapewnia, że żadna wcześniejsza informacja nie jest na nim obecna.

Po sterylizacji zawsze konieczna jest walidacja, sprawdzająca czy sterylizacja przebiegła w prawidłowy sposób. Po tej walidacji możemy przystąpić do formatowania dysku na odpowiedni system plików.

Istnieje wiele programów, które pozwalają na przeprowadzenie tej procedury sterylizacji dysku i sformatowania go do pożądanego systemu plików. Tutaj zademonstrujemy ten proces używając narzędzi obecnych w większości dystrybucji Linuksa, lsblk,fdisk i dc3dd.

Pierwszym krokiem jest identyfikacja tarczy przeznaczonej do sterylizacji. Bardzo ważne jest, aby ta identyfikacja była jednoznaczna i potwierdzona tyle razy, ile jest to konieczne. Wysterylizowany dysk nie może być odzyskany.

3.1.1. Identyfikacja urządzenia

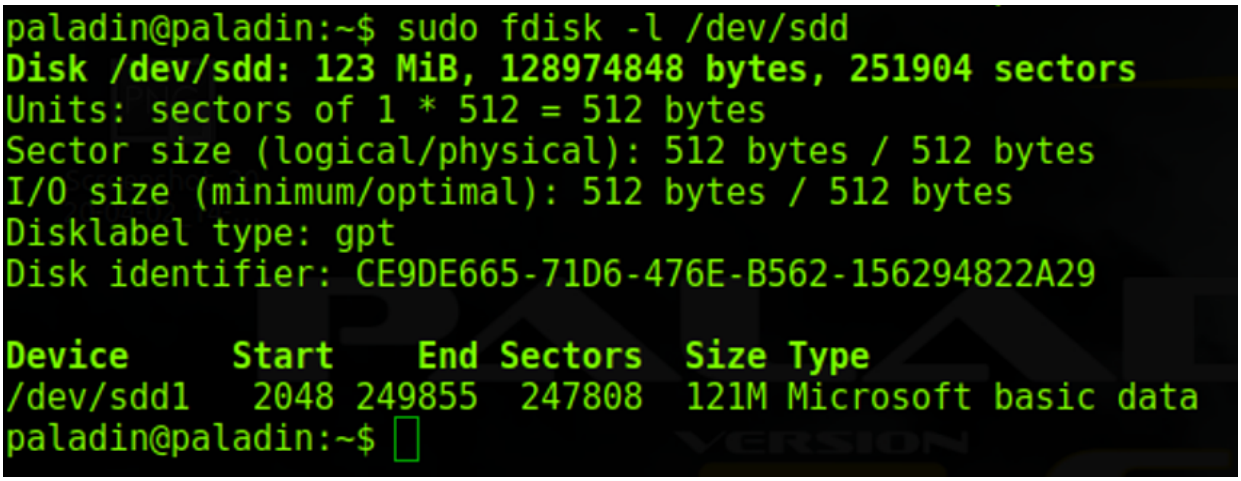
Identyfikacja urządzenia odbywa się za pomocą serii poleceń. W pierwszej kolejności należy określić jakie woluminy zainstalowane są na komputerze, który ma być użyty. Dobrą praktyką jest używanie komputera z podłączonym tylko dyskiem do sterylizacji, uruchamiając system operacyjny z płyty liveCD lub pamięci USB. Zmniejsza to możliwość wystąpienia błędów w identyfikacji dysku:

$ lsblk | grep sd*

To polecenie wyświetli listę wszystkich urządzeń pamięci masowej rozpoznawanych przez system operacyjny. Wyświetlone zostaną wszystkie dyski, a także ich rozmiar i partycje. Polecenie to pomaga nam jedynie dowiedzieć się, jak nazywa się nasz dysk w komputerze.

W razie wątpliwości możemy jeszcze użyć polecenia (Rysunek 14)

*fdisk -l /dev/sd**



Rysunek 14 - identyfikacja urządzenia

To polecenie daje nam więcej informacji o pożądanym dysku.

3.1.2. Sterylizacja dysku docelowego

Proces sterylizacji to nic innego jak zapisanie całego dysku wartością 0 (zero), czyli zmuszenie wszystkich bitów dysku twardego do nabrania wartości zero.

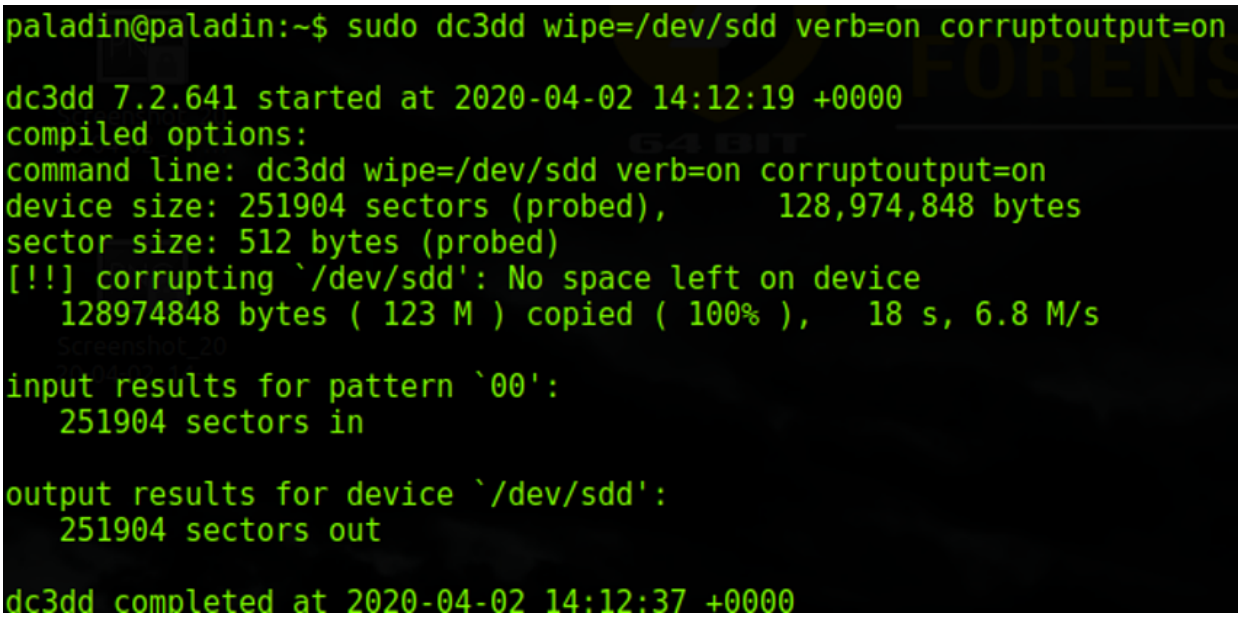
Do tego zadania można użyć takich narzędzi jak Live-CD DBAN (www.dban.org) lub w systemie Windows the Eraser (eraser.heidi.ie).

W systemie Linux możemy użyć poleceń (Rysunek 15)

dc3dd wipe=/dev/sdd verb=on corruptoutput=on

lub

dcfldd if=/dev/zero of=/dev/sdb bs=8k conv=noerror,sync



Rysunek 15 - Sterylizacja dysku docelowego

Polecenie to wykonuje zapis wszystkich bitów dysku twardego, więc będzie to trwało tym dłużej, im większy jest dysk twardy. W naszym przykładzie urządzenie o pojemności zaledwie 123mb potrzebowało 18 sekund na zapis, jednak dysk twardy o pojemności 1 TB, może zająć ponad 8 godzin. Należy również pamiętać, że w zależności od technologii dysku twardego, czas ten może być wyższy lub niższy, w zależności od jego prędkości zapisu.

W systemie Microsoft Windows, sterylizacja dysku docelowego, może być wykonana poprzez polecenie diskpart.

Przeprowadzenie identyfikacji dysku docelowego przez:

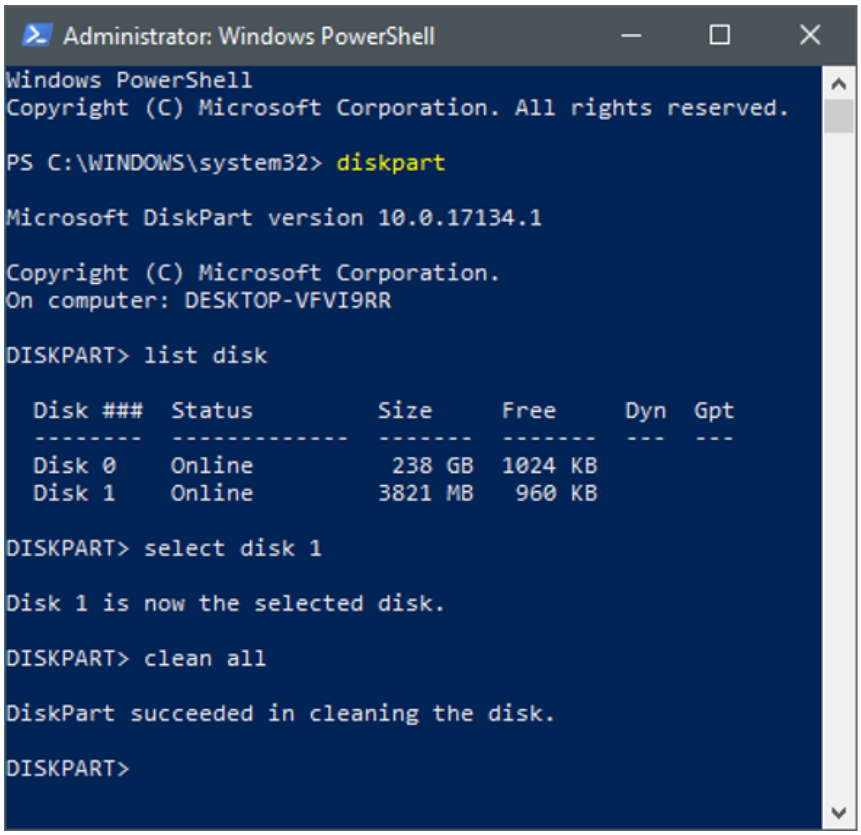
LIST DISK (identyfikacja urządzenia)

LIST VOLUME (identyfikacja głośności)

SELECT DISK 1 (wybierz dysk, który ma być sterylizowany)

Przeprowadzenie sterylizacji (Rysunek 16)

CZYSTE WSZYSTKO



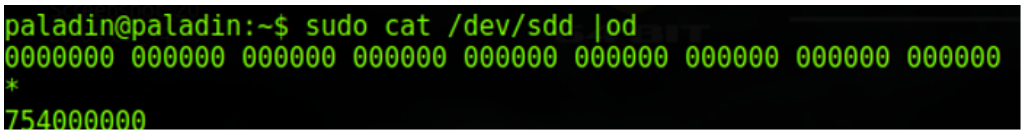
Rysunek 16 - Sterylizacja dysku docelowego w systemie Windows

3.1.3. Weryfikacja sterylizacji

Na koniec należy sprawdzić, czy zapis na dysku twardym był skuteczny, w tym celu wykonujemy polecenie:

cat /dev/sdb |od

Jeśli zapis zakończył się sukcesem, wyjściem polecenia będzie 0000000, co oznacza, że na dysku twardym zapisano same zera (Rysunek 17).



Rysunek 17 - weryfikacja sterylizacji

Polecenie "cat" wyświetli zawartość urządzenia, natomiast argument "|od" przekonwertuje tę zawartość na bazę ósemkową, dzięki czemu wyświetlone zostaną tylko zera, gdy sterylizacja zakończyła się sukcesem.

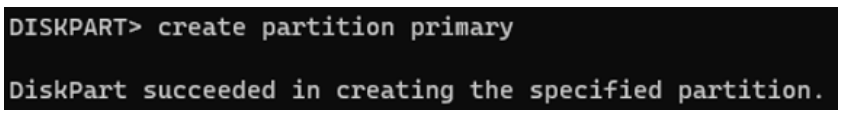
Oprócz przedstawionych procedur istnieją inne metody i różne polecenia, które można wykorzystać, takie jak wyświetlanie w formacie szesnastkowym lub inne.

3.1.4. Formatowanie

Po sterylizacji konieczne jest sformatowanie dysku, umożliwiające odbieranie danych.

Formatowanie to można jeszcze wykonać za pomocą programu Diskpart, w następujący sposób:

Tworzenie partycji podstawowej (Rysunek 18)



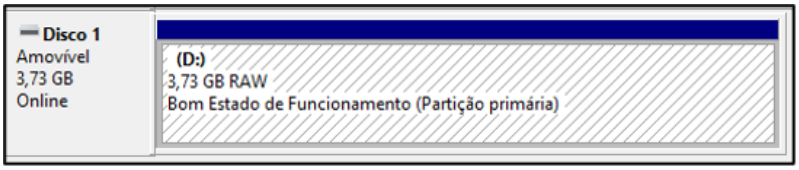
Rysunek 18 - Tworzenie partycji głównej

Formatowanie NTFS (.Rysunek 19)

```
DISKPART> select partition 1

Partition 1 is now the selected partition.

DISKPART> format fs=ntfs quick

  100 percent completed

DiskPart successfully formatted the volume.
```

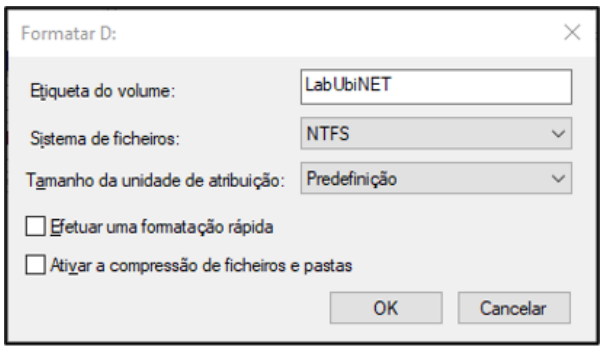
Rysunek 19 - Formatowanie

Ze środowiska graficznego można korzystać z aplikacji Zarządzanie dyskami poprzez polecenie DISKMGMT.MSC (Rysunek 20).



Rysunek 20 - Zarządzanie dyskami

Kliknij prawym przyciskiem myszy na wybrany dysk i wybierz "Formatuj", następnie wskaż nazwę i żądany system plików. Można wybrać szybkie formatowanie, ponieważ dysk został wcześniej wysterylizowany (Rysunek 21).



Rysunek 21 - Formatowanie przy użyciu Zarządzania dyskami

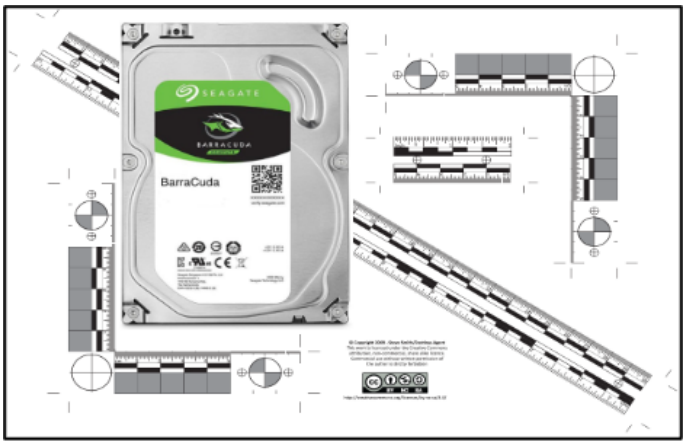
3.2. Identyfikacja urządzeń do przechowywania danych

Urządzenia pamięci masowej przeszły w ostatnich latach szybką ewolucję, co wymaga od analityka kryminalistycznego uważności i badania każdego analizowanego sprzętu, dążąc do poznania wszystkich urządzeń do przechowywania danych, które dany sprzęt obsługuje. W ten sposób analityk może dążyć do identyfikacji wszystkich takich urządzeń (rys. 22).

Rysunek 22 - Identyfikacja urządzeń pamięci masowej

3.3. Reportaż fotograficzny

Po zidentyfikowaniu sprzętu i odpowiednich urządzeń do przechowywania danych należy zarejestrować ich obecny stan. W tym celu należy przypisać każdemu elementowi wyposażenia wewnętrzne oznaczenie i sfotografować urządzenia pod różnymi kątami (Rysunek 23), używając skali metrycznej i zwracając szczególną uwagę na ewentualne uszkodzenia. Są to informacje, które mogą być ważne w sądzie.



Rysunek 23 - Reportaż fotograficzny

3.4. Dystrybucje zakresów kryminalistycznych

Biorąc pod uwagę techniki i procedury pozyskiwania i analizy nośników danych, istotne jest posiadanie wiedzy na temat kryminalistycznych dystrybucji systemu Linux. Posiadają one zestaw narzędzi, które umożliwiają pozyskiwanie i analizę informacji z uwzględnieniem najlepszych praktyk. Są to z reguły dystrybucje Live, które nie wymagają instalacji na komputerze, ale pozwalają na podłączenie dysków bez obaw o blokowanie zapisu, gdyż przychodzą natywnie skonfigurowane bez automatycznego montowania ich w systemie.

Dystrybucje, na które wskazujemy, są następujące:

- **CAINE (Computer Aided INvestigative Environment Live CD/DVD)**
- **DFF (Digital Forensics Framework)**
- **SANS SIFT (Sans Investigative Forensics Toolkit)**
- **Paladin Edge (Sumuri)**

3.5. Techniki pozyskiwania

Procedury akwizycji mają decydujące znaczenie dla zagwarantowania integralności dowodów cyfrowych i ułatwienia procesu ich analizy, stanowiąc jedną z technik stosowanych w ramach dobrych praktyk informatyki śledczej, która gwarantuje dopuszczalność pozyskanych dowodów w sądzie.

Pozyskiwaniem nazywamy binarną kopię bitową urządzeń do przechowywania danych, istnieje też tzw. kopia kryminalistyczna lub duplikat (rysunek 24).

Rysunek 24 - Duplikator urządzeń pamięci masowej

Źródło: https://security.opentext.com/tableau/hardware/details/td2u

W każdym z zastosowanych typów zbiorów kryminalistycznych należy pamiętać, że dysk docelowy powinien mieć większą pojemność niż dysk źródłowy.

3.5.1. Blokada zapisu

W procedurach akwizycji należy zastosować urządzenie sprzętowe (Rysunek 25) blokujące zapis na dysku źródłowym. W ten sposób zagwarantowana jest integralność danych na tym dysku, chroniąca dysk przed niezamierzonymi zmianami, np. ze strony systemu operacyjnego lub programu antywirusowego, a także walidacja danych kopiowanych na dysk docelowy.

Rysunek 25 - Blokada zapisu

Źródło: www2.guidancesoftware.com

Jeśli nie masz dostępu do sprzętowej blokady zapisu, możesz użyć programowych blokad zapisu. Wymagają one większej ostrożności w sprawdzaniu poprawności ich działania, gdyż zależą od systemu operacyjnego, z którego korzystamy. Kilka przykładów przedstawiono na Rysunku 26.

Rysunek 26 - Oprogramowanie kryminalistyczne z blokadą zapisu

Blokadę zapisu w systemie operacyjnym Microsoft Windows można wykonać poprzez utworzenie klucza rejestru

"HKLMSYSTEMSet001StorageDevicePoliciesWriteProtect", zgodnie z poniższym opisem:

- "regedit" w trybie administratora i przejdź do następującej ścieżki:
"HKEY_LOCAL_MACHINE\SYSTEM\SetCurrentControl\SetControl"
- Utwórz nowy klucz w "Control" o nazwie: **"StorageDevicePolicies"**
- Dodaj nową wartość typu "DWORD (32-bit)", o nazwie: **"WriteProtect"**
- Zmień jego informacje z "**0**" na "**1**"
- Przetestuj zamek z kilkoma urządzeniami pamięci masowej

3.5.2. Porównanie aplikacji do zamówień publicznych

Możliwe jest przeprowadzenie procedur akwizycji kryminalistycznej w kilku systemach operacyjnych, ponieważ istnieje wiele aplikacji posiadających zdolność do wykonania tego zadania, czego przykładem jest Rysunek 27 porównawczy dla tych samych aplikacji.

Tool	Platform			Input Sources				Encoding		Output Formats			
	❖	🐧		Physical Disk	Logical Volume	Files	Folders	Compression	Encryption	Raw	E01	Ex01	Split
FTK Imager 3.2	✓			✓	✓		✓	✓	✓	✓	✓		✓
FTK Imager CLI 3.1.1	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
EnCase Forensic Imager 7.0	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
dd		✓	✓	✓	✓	✓	✓			✓			
dcfldd		✓		✓	✓	✓	✓			✓			✓
dd_rescue		✓		✓	✓	✓	✓			✓			
dd.exe	✓			✓	✓	✓	✓	✓	✓	✓			
dc3dd	✓	✓		✓	✓	✓	✓			✓			✓
ewfacquire		✓	✓	✓	✓					✓	✓	✓	✓

Rysunek 27 - Porównanie wniosków o udzielenie zamówienia publicznego

Źródło: Vandeven, Sally, The SANS Institute, 2014 r.

Czytaj: https://www.raedts.biz/forensics/forensic-imaging-tools-compared-tested/

3.5.3. Przejęcie systemu Linux

Pozyskiwanie poprzez system operacyjny Linux, wśród innych zastosowań, może odbywać się poprzez dcfldd lub dc3dd, aplikacje wywodzące się ze znanego dd.

Urządzenie i jego tablica partycji muszą być zidentyfikowane

mmls /dev/sdb

Przejęcie przez dclfdd:

dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=10G md5log=md5.txt sha256log=sha256.txt hashconv=after bs=512 conv=noerror,sync split=10G of=diskimage.dd

Lub nabycie poprzez dc3dd:

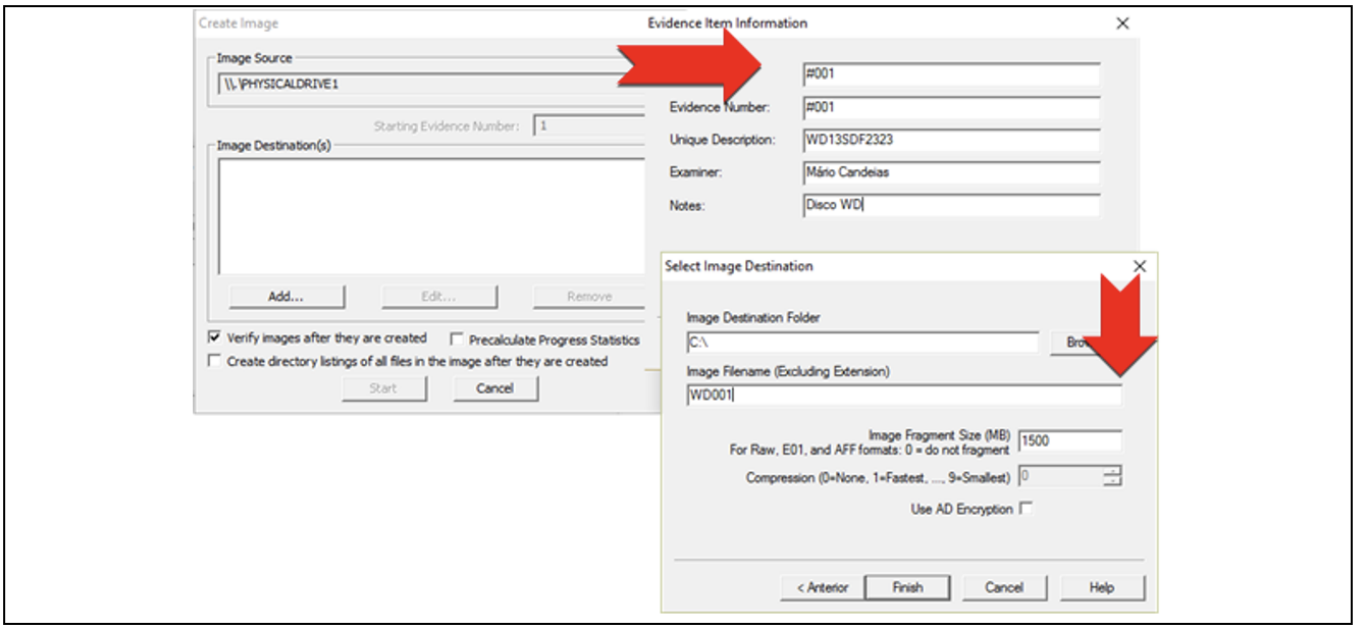
dc3dd if=/dev/sdb hash=md5,sha256 hlog=hash_log.log= diskimage.log rec=off of=diskimage.dd

Należy sprawdzić pliki dziennika, identyfikując zgodność haseł zawartości dysku źródłowego z zawartością obrazu kryminalistycznego utworzonego w tej procedurze. Ważne jest również zweryfikowanie zawartości nieczytelnej, czyli bad sectorów, które w obu procedurach pozostaną bez wartości zapisanej, pozostawiając tę przestrzeń z wartością 0 (zero).

3.5.4. Przejęcie systemu Windows

Akwizycja poprzez system operacyjny MS Windows, wśród innych aplikacji, może odbywać się poprzez znaną darmową aplikację FTK Imager firmy Acess Data.

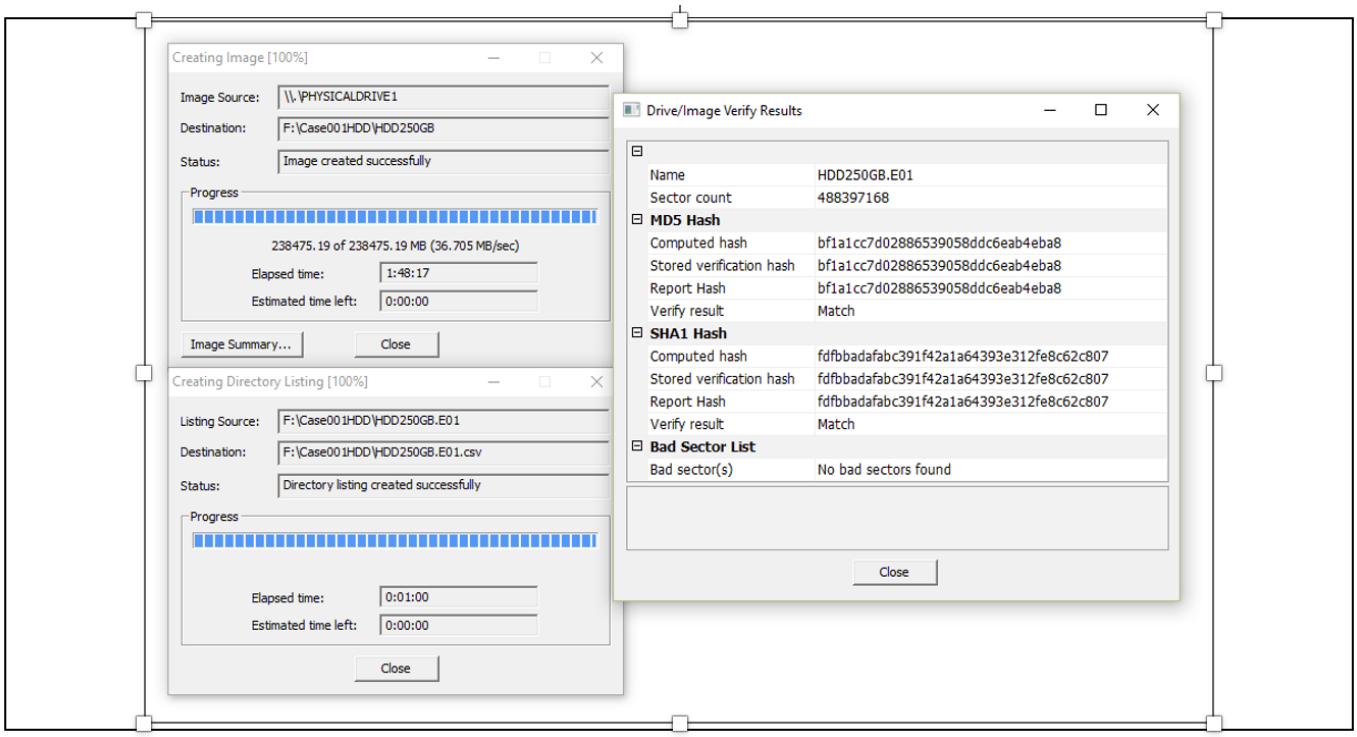
W programie FTK Imager należy wybrać opcję Create Disk Image / Physical Drive, jak na rysunku Rysunek 28.



Rysunek 28 - Procedura akwizycji za pomocą kamery AccessData FTK Imager

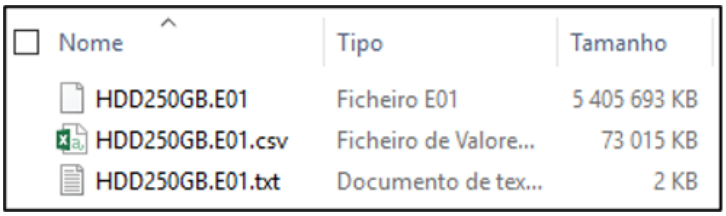
Przed rozpoczęciem procedur akwizycji możliwe jest zaznaczenie opcji tworzenia listy wszystkich plików, które powstaną po akwizycji i zostaną zapisane w formacie ".csv".

Po rozpoczęciu akwizycji pojawi się okno walidacji, z walidacją korespondencji hashowej, a także informacją o nieodczytanych sektorach, zwanych również bad sectorami (Rysunek 29).



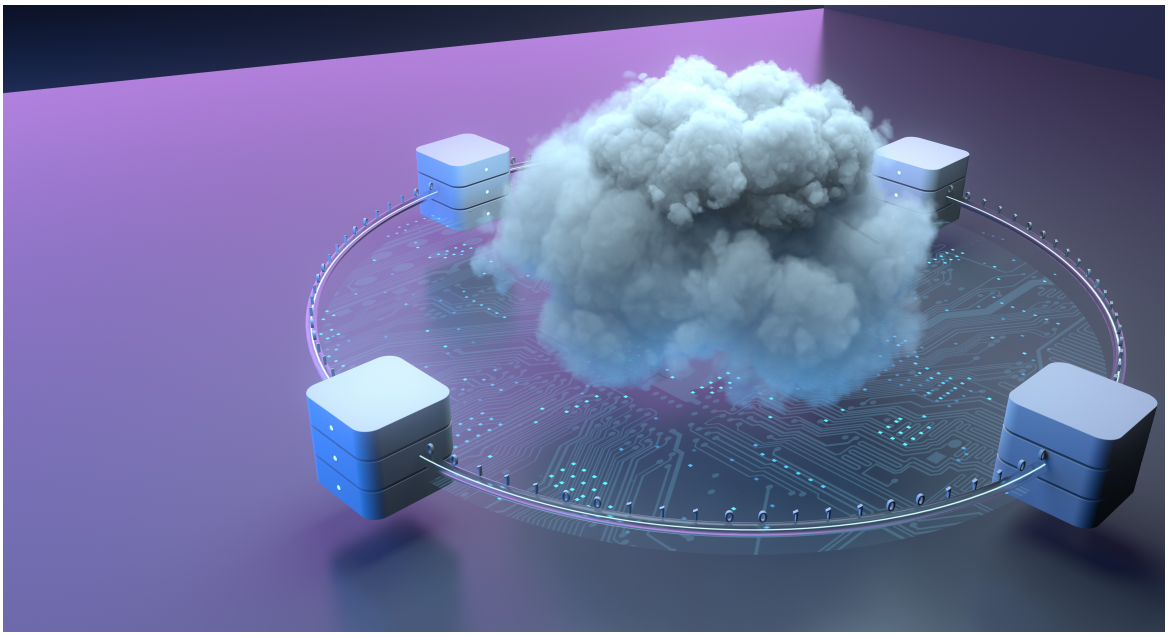
Rysunek 29 - Wynik akwizycji przy użyciu AccessData FTK Imager

Te same informacje będziemy mieli również w pliku tekstowym, zapisanym w tej samej lokalizacji co plik obrazu kryminalistycznego (Rysunek 30). Plik ".csv" również będzie w tej samej lokalizacji, jeśli wybraliśmy tworzenie listy plików.



Rysunek 30 - Pliki powstałe w wyniku akwizycji za pomocą AccessData FTKImager

4. Pozyskiwanie i analiza informacji ulotnych



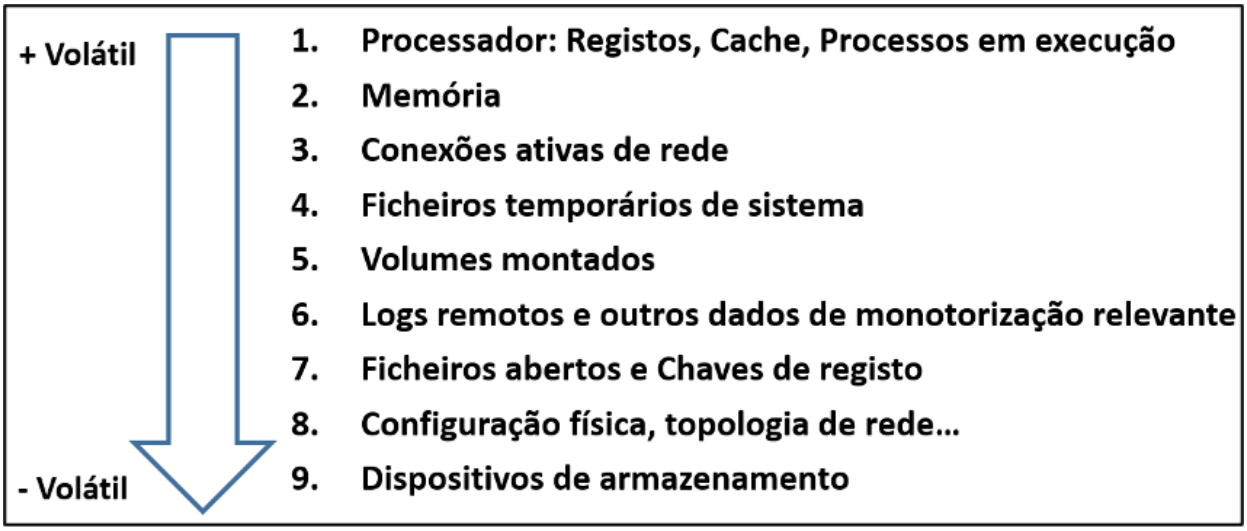
Informacje ulotne to informacje, które są tracone w momencie wyłączenia systemu lub utraty zasilania. Informacje lotne zazwyczaj znajdują się w pamięci fizycznej lub w pamięci RAM i składają się z informacji o procesach, połączeniach sieciowych, otwartych plikach, schowku itp. Informacje te opisują stan systemu w danym momencie.

Podczas wykonywania analizy live-data forensics, jedną z pierwszych rzeczy, które badacze powinni zebrać jest zawartość pamięci RAM. Zbierając tę informację jako pierwszą, minimalizuje się wpływ zbieranych przez nich danych na zawartość pamięci RAM, jednakże przechwytywanie to może powodować niestabilność systemu lub nawet prowadzić do powstania Blue Screen of Death (BSoD), co skłoniło kilku autorów do wskazania, że procedury te powinny być wykonywane po zebraniu innych ulotnych informacji, będąc traktowane priorytetowo w zależności od sytuacji.

Niektóre ze szczególnych rodzajów ulotnych informacji, które powinny być zbierane:

- Pamięć RAM
- Data i godzina systemowa
- Informacje o sieci
- Zalogowani użytkownicy
- Pliki otwarte
- Połączenia sieciowe
- Informacje o uruchomionych procesach
- Mapowanie między procesami i portami
- Status sieci
- Zawartość schowka
- Informacje o usługach i kierowcach
- Historia wykonanych poleceń
- Napędy mapowane
- Akcje
- Hasła i klucze kryptograficzne

Spośród nich należy dla każdego konkretnego przypadku określić, która informacja jest bardziej zmienna i będzie ważniejsza do uzyskania w pierwszej kolejności. Tutaj możliwa kolejność informacji w kolejności zmienności (Rysunek 31).



Rysunek 31 - Możliwa sekwencja informacji w kolejności zmienności

4.1. Proces przechwytywania ulotnych informacji

Przede wszystkim należy zadbać o stabilność naszej maszyny roboczej. Jednym z problemów, z jakimi można się spotkać, jest automatyczny restart maszyny, spowodowany automatycznymi aktualizacjami systemu operacyjnego. Dlatego warto wyłączyć, nie aktualizacje systemu operacyjnego, ale ich zdolność do wymuszania restartu maszyny. Takie ponowne uruchomienie mogłoby na przykład przerwać akwizycję dysku lub analizę obrazu.

Inną dobrą praktyką jest odmowa dostępu do zapisu na dyskach wymiennych, co zapobiega zmianom na dyskach źródłowych.

Dane ulotne to wszelkie dane, które mogą zostać utracone po wyłączeniu systemu, takie jak zapis połączenia ze stroną internetową, który jest nadal obecny w pamięci RAM lub w schowku systemowym. Zbieranie tych danych musi odbywać się podczas pracy systemu.

Live-Data Forensics, to technika stosowana do zbierania danych, które są zmienne i mogą zostać utracone w przypadku utraty zasilania przez urządzenie.

Memory DUMP to procedura zapisywania w pliku, wszystkich danych znajdujących się w danym momencie w pamięci fizycznej komputera.

Podczas gromadzenia tego typu danych należy wziąć pod uwagę kolejność zmienności danych, dostosowując gromadzenie do kategorii danych, która jest najbardziej interesująca. Jeśli naszym celem jest zidentyfikowanie wysłania wiadomości e-mail na określony adres, nie miałoby większego sensu nadawanie priorytetu identyfikacji procesów zamiast zbierania haseł, lub poświadczeń dostępu, umożliwiających dostęp do adresu e-mail.

Bardzo ważne jest, aby zbieranie danych na żywo było odpowiednio udokumentowane, najlepiej poprzez stworzenie zespołu zbierającego składającego się z co najmniej dwóch osób, aby zapewnić, że procedury zbierania są wykonywane przez jedną osobę, podczas gdy druga dokumentuje zastosowany proces zbierania.

Ważne jest również zagwarantowanie minimalnej zmiany w analizowanym systemie, a jeśli trzeba dokonać jakiejkolwiek zmiany, należy ją zarejestrować w raporcie dla przyszłej pamięci.

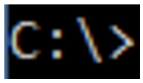
Zalecenia dotyczące stosowania skryptów:

· Użycie zmiennych środowiskowych
(np.: cmd: %COMPUTERNAME% / PS: $env:Computername)

· Uruchomienie w trybie administratora

4.1.1. Rodzime narzędzia systemowe

Biorąc pod uwagę minimalny ślad cyfrowy na urządzeniu, powinniśmy w miarę możliwości wykorzystywać narzędzia kryminalistyczne do zbierania przydatnych informacji, które pozwolą na bardziej efektywną analizę. Przykładem tego są informacje związane z szyfrowaniem całego dysku. System operacyjny MS Windows umożliwia jednak wykonywanie poleceń i skryptów za pomocą natywnych narzędzi, będąc doskonałą możliwością pozyskania niezbędnych informacji przy minimalnym śladzie cyfrowym.

Wiersz poleceń	Wiersz poleceń systemu MS Windows jest natywnie jednym z najczęściej wykorzystywanych w gromadzeniu informacji o systemie, umożliwiając wykonanie wielu programów służących do tego celu	
Instrumentacja zarządzania systemem Windows (WMI)	Windows Management Instrumentation umożliwia dostęp do systemu operacyjnego poprzez linię komend Windows Management Instrumentation i jest doskonałym sposobem na uzyskanie informacji o systemie operacyjnym.	
Plik wsadowy systemu Windows	Jest to plik skryptowy, który pozwala na grupowanie zestawu poleceń, linia po linii. Pozwala na stosowanie struktur repetytorium, struktur warunkowych, stosowanie zmiennych, typowych dla języka skryptowego.	
Powershell	PowerShell jest obecnie językiem skryptowym, początkowo opracowanym dla systemów MS Windows, przy czym jego otwarty kod źródłowy i wsparcie dla wielu platform zostały udostępnione w 2016 roku. Posiadając własną powłokę, PowerShell został opracowany w celu umożliwienia wykonywania cmdletów, umożliwiając również wykonywanie innych powłok.	

4.1.2. Narzędzia zewnętrzne

W przypadku korzystania z narzędzi zewnętrznych należy zadbać o dokładne przetestowanie każdego z nich, aby wiedzieć, co dokładnie robią w systemie. W przypadku korzystania z narzędzi zewnętrznych należy odnotować datę/godzinę ich użycia, a także opisać zamiar ich użycia.

Sysinternals Windows	Windows Sysinternals reprezentuje zestaw narzędzi pierwotnie stworzonych przez Marka Russinovicha, przeznaczonych do pomocy administratorom systemów w zarządzaniu i monitorowaniu systemów Windows. https://docs.microsoft.com/en-us/sysinternals/	Windows Sysinternals
Nirsoft	NirSoft reprezentuje zestaw narzędzi stworzonych przez Nira Sofera, z których wyróżniamy te, które sklasyfikował jako forensic. http://www.nirsoft.net/	NirSoft Tools and Utilities
Mitec	Mitec to również strona oferująca zestaw ciekawych narzędzi do zbierania i analizy informacji, takich jak jej MiTeC System Information X i Windows Registry Recovery. https://www.mitec.cz/	MITEC
Zimmerman	Eric Zimmerman opracował zestaw bezpłatnych narzędzi przeznaczonych do pomocy w reagowaniu na incydenty i analizie kryminalistycznej.	**Eric Zimmerman Narzędzia**

4.1.3. Data, czas i inne informacje o systemie

Ten element powinien być zbierany jako pierwszy podczas prowadzenia badania. Data systemowa umożliwia kontekstualizację zebranych później informacji oraz pozwala badaczowi na zbudowanie osi czasu zdarzeń, które miały miejsce nie tylko w analizowanym systemie, ale poprzez korelację pomiędzy informacjami z innych systemów. Kolejnym ważnym elementem danych jest czas, jaki upłynął od ostatniego uruchomienia systemu (uptime).

Niektóre narzędzia mogą pomóc badaczom w tych zadaniach, np. MiTeC - System Information X[1] i WinAudit[2] .

Zbieranie daty/czasu serwisowanego systemu (Rysunek 32).

```
C:\>echo "the current time is: %date% - %time%" > currentTime.log

C:\>type currentTime.log
"the current time is: 21/03/2019 - 18:38:39,76"
```

Rysunek 32 - Uzyskiwanie daty i czasu systemu.

Zbieranie daty/czasu ostatniego uruchomienia systemu (Rysunek 33).

```
C:\>dir /a c:\pagefile.sys
 Volume in drive C is Windows
 Volume Serial Number is 822C-E9A2

 Directory of c:\

04/08/2022  15:55    10 907 262 976 pagefile.sys
```

Rysunek 33 - Uzyskiwanie daty i godziny ostatniego uruchomienia systemu

Polecenia przydatne do uzyskania danych z systemu:

- Wersja dla systemu Windows: **ver**

- Zmienne środowiskowe: **set**
- Informacje o systemie: **systeminfo /fo list >> C:™mpinfo.txt**
- Sprawdź rejestr: **zapytanie reg "HKLM Microsoft NT CurrentVersion" /v ProductName**
- Konsultacja z WMI: **wmic os get name, version**
- Uruchamianie i zamykanie systemu: **TurnedOnTimesView.exe** (Fonte: Nirsoft.net)

Polecenia przydatne do uzyskania danych o użytkownikach systemu

- Użytkownicy:

o **Net User** [username]

o **Userprofilesview.exe /shtml "f:™profiles.html" /sort "User Name"** (Źródło: Nirsoft.net)

- Zalogowani użytkownicy:

o **PSLoggedOn.exe** (Źródło: SysInternals)

o **LogonSessions.exe** (Źródło: SysInternals)

4.1.4. Procesy i zastosowania

Kluczowe jest wyliczenie procesów działających w potencjalnie zagrożonym systemie. Proces to część lub instancja aplikacji, która jest uruchomiona. Przeglądanie uruchomionych procesów w Menedżerze zadań daje pewne informacje, jednak można uzyskać o wiele więcej informacji, niż można tam zobaczyć.

Niektóre z rodzajów informacji o uruchomionych procesach, które można uzyskać:

- Absolutna ścieżka do pliku wykonywalnego
- Polecenie użyte do uruchomienia procesu
- Czas trwania procesu
- Jaki użytkownik rozpoczął proces i jaki ma poziom uprawnień w systemie
- Moduły, które proces załadował
- Zawartość pamięci przydzielonej procesowi

Przykłady programów i poleceń do pozyskiwania informacji o **procesach działających w** systemie:

- **Psinfo.exe -h -s -d /accepteula** (Źródło: SysInternals)
- ***PsList.exe*** (Źródło: sysinternals)
- ***CurrProcess.exe*** (Źródło: Nirsoft.net)
- ***tasklist /v***
- ***Wmic process get name, processid, priority, threadcount, privatepagecount***

Przykłady programów i poleceń do pozyskiwania informacji o usługach, zaplanowanych zadaniach i zdarzeniach systemowych:

- [Services] **PsService.exe** (SysInternals)
- **net start** [Services]
- [zaplanowane zadania] **schtasks**
- [zdarzenia] **PsLogList.exe** (SysInternals)
- [events] **EventLogSourcesView.exe** (Nirsoft)
- [wydarzenia] **wevtutil**

4.1.5. Pamięć

Schowek to obszar w pamięci, w którym dane mogą być przechowywane do przyszłego użytku. Większość aplikacji systemu Windows udostępnia tę funkcję poprzez menu Edycja i opcje Kopiuj, Wklej lub Wytnij. Funkcja ta jest przydatna do przenoszenia danych między aplikacjami lub dokumentami. Często dane pozostają w Schowku przez wiele dni, a użytkownik nie zdaje sobie z tego sprawy.

Do zbierania danych zapisanych w tym obszarze pamięci można wykorzystać następującą aplikację **InsideClipboard.exe** (Nirsoft.net).

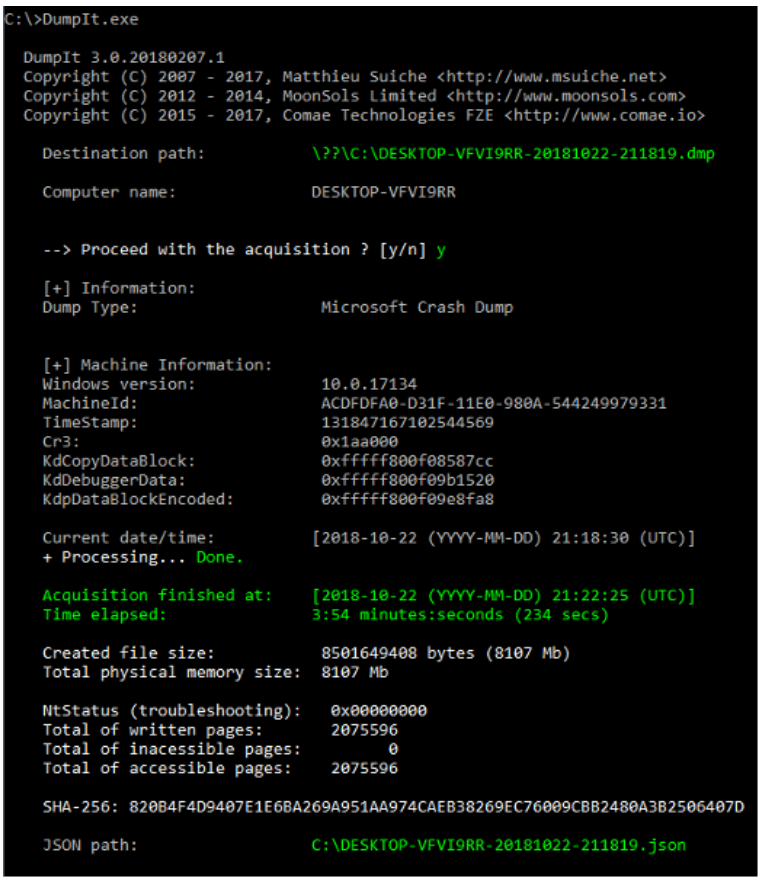
Analitycy złośliwego oprogramowania szukają w pamięci, gdy mają do czynienia z obfuskowanym złośliwym oprogramowaniem, ponieważ gdy jest ono wykonywane, jest rozszyfrowywane w tej samej pamięci. Ponadto Rootkity ukrywają procesy, pliki, klucze rejestru, a nawet połączenia sieciowe. Możliwe jest sprawdzenie, co jest ukryte przed wzrokiem użytkownika, poprzez analizę pamięci RAM. Dane te są bardzo przydatne do kontekstualizacji zidentyfikowanych danych w przyszłych analizach.

4.1.6. Pozyskiwanie pamięci

Proces Memory Dump (Rysunek 34) jest również szeroko stosowany do diagnozowania błędów w programach, ponieważ zrzuty te są zwykle tworzone, gdy wystąpi błąd i programy nieoczekiwanie przestają działać.

Te zrzuty pamięci wykonywane są w formacie binarnym, ósemkowym lub szesnastkowym. Dochodzenie można przeprowadzić za pomocą programów, takich jak:

- DumpIT (moonsols)
- AccessData FTK Imager
- Belkasoft Live RAM Capturer



Rysunek 34 - Przykład działania DumpIT

Istnieją inne pliki[3] , do obsługi pamięci głównej, które muszą być gromadzone, takie jak **pagefile.sys,** używane przez Windows jako "pamięć wirtualna". Zawsze, gdy system potrzebuje użyć więcej pamięci niż jest dostępne w pamięci RAM. Albo **hiberfil.sys** służy do przechowywania danych z pamięci, gdy komputer przechodzi w stan hibernacji.

Do zbierania pamięci w środowisku linuksowym *można wykorzystać programy dcfldd* lub *insmod*.

- dcfldd if=/dev/fmem of=memory.dump
- insmod lime-XX.ko "path="memory.dump" format=raw"

4.1.7. Informacje o sieci

Zbieranie zmiennych informacji o stanie sieci komputera: aktywne połączenia, otwarte porty, informacje i konfiguracja routingu, cache, ARP....

Natychmiast po zgłoszeniu incydentu osoba prowadząca badanie musi zebrać informacje o stanie połączeń sieciowych z systemem dotkniętym incydentem.

Te połączenia mogą wygasnąć, a informacje mogą zniknąć z czasem. Spojrzenie na te dane może pomóc w określeniu, czy atakujący jest nadal zalogowany do systemu, czy istnieją połączenia związane ze złośliwym oprogramowaniem, czy istnieje proces próbujący znaleźć inne maszyny w sieci w celu propagacji tego złośliwego oprogramowania lub wysłania informacji z dziennika do złośliwego serwera.

Zbieranie tych informacji może dostarczyć ważnych wskazówek i dodać kontekst do innych zebranych informacji.

Przykłady poleceń do zbierania informacji o sieci:

- Informacje o karcie sieciowej: **ipconfig /all**
- DNS cache: **ipconfig /displaydns**
- Aktywne połączenia sieciowe: **Netstat -a**
- ARP cache: **Arp -a**
- **Netsh int ipv6 show neigh**
- Wydarzenia wifi: **Netsh wlan show all**
- Sieci bezprzewodowe: **WifiInfoView.exe** (Źródło: Nirsoft.net)
- Tablica routingu: **Wydruk trasy.**
- Połączenia w pamięci podręcznej: **Netstat -c**
- Lista sesji Cache: **Netstat -s**
- **Rachunki netto**
- Udostępnianie zasobów: **Udział netto**
- Zapytaj serwer o DNS: **Nslookup -d**
- Lista aktualnych połączeń: **Rasdial**
- Lista profili: **Netsh wlan show profiles**

---

[1] www.mitec.cz/msi.html

[2] www.parmavex.co.uk

[3] https://www.hackingarticles.in/forensics-analysis-of-pagefile-and-hibersys-file-in-physical-memory/

4.2. Analiza pozyskiwania pamięci

Istnieją pewne narzędzia do analizy zrzutu pamięci, które opierają się tylko na zawartości pamięci RAM. Zawartość ta może być niekompletna, ponieważ części pamięci są przechowywane na dysku, gdy nie wystarcza do przechowywania wszystkich danych. Aby przezwyciężyć ten problem, Nicholas Paul Maclean opublikował swoją pracę dyplomową "Acquisition and Analysis of Windows Memory", jak działa zarządzanie pamięcią w systemach Windows i udostępnił narzędzie open-source o nazwie vtop, aby w pełni zrekonstruować przestrzeń pamięci wirtualnej procesu.

Do analizy Memory Dump możemy wykorzystać program Volatility, w którym możliwe jest wykonanie takich zadań jak uzyskanie wysokopoziomowych informacji o obrazie, gdzie wydedukowano identyfikację systemu operacyjnego (Rysunek 35), service pack, sprzęt, architektura, adres pamięci oraz wydedukowany jest czas wykonania Dump'u.

```
C:\DumpIt>volatility_2.6_win64_standalone.exe -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_10586, Win10x64_14393, Win10x64, Win2016x64_14393
                     AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\DumpIt\memdump.mem)
                      PAE type : No PAE
                           DTB : 0x1ab002L
                          KDBG : 0xf8002b7e04d0L
          Number of Processors : 8
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80029e4e000L
                KPCR for CPU 1 : 0xffffa98079180000L
                KPCR for CPU 2 : 0xffffa98079214000L
                KPCR for CPU 3 : 0xffffa980792b9000L
                KPCR for CPU 4 : 0xffffa98079346000L
                KPCR for CPU 5 : 0xffffa98079680000L
                KPCR for CPU 6 : 0xffffa98079714000L
                KPCR for CPU 7 : 0xffffa980797ab000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-04-03 16:00:13 UTC+0000
     Image local date and time : 2019-04-03 17:00:13 +0100
```

Rysunek 35 - Uzyskiwanie informacji o zrzucie pamięci

Polecenia przydatne do wykonania zrzutu rekordów:

Eksport do tekstu:

C:Regdmp.exe > e:registryDump.txt

Znajdź wyrażenia w wyeksportowanym pliku:

C:\"URL\" registryDump.txt

Kopia plików rejestru w użyciu:

C:\NRawCopy.exe C:\NWINDOWS \NKonfiguracja E:\Noutput -AllAttr

Inne przydatne polecenia:

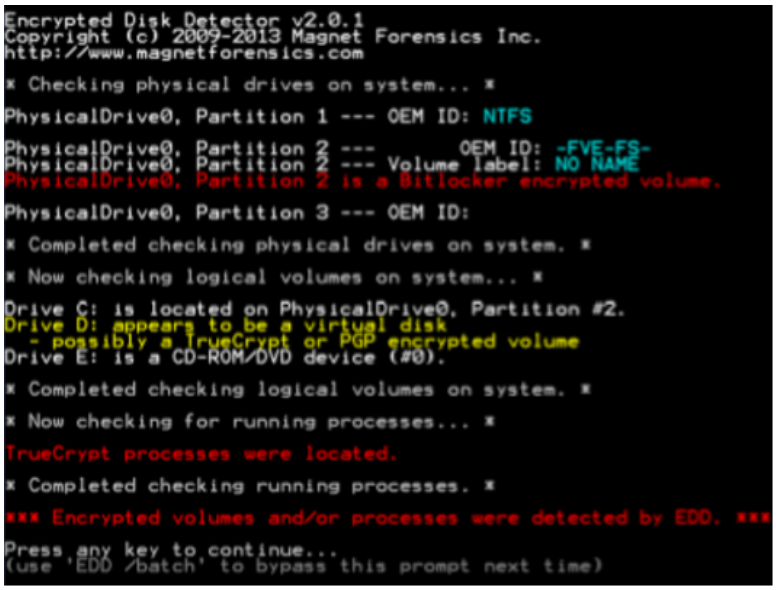
Uzyskaj zrzut ekranu pulpitu:

C:nircmd.exe savescreenshot screen1.png (Nirsoft.net)

Sprawdzenie, czy dysk jest chroniony za pomocą funkcji Encryption (Rysunek 36)

C:EDD.exe /accepteula /Batch > e:\NEncryptedDiskDetector.txt

C:-zarządzanie-bde -protektory c: -get



Rysunek 36 - Identyfikacja dysku zaszyfrowanego

4.2.1. Sintax programu Volatility

Pierwsza wersja Volatility Framework została ujawniona na konferencji Black Hat. Oprogramowanie opiera się na latach badań akademickich w zakresie zaawansowanej analizy pamięci i kryminalistyki. Volatility pozwala teraz badaczom analizować, w jakim stanie znajdowała się maszyna w momencie dokonywania przejęcia, na podstawie danych zebranych z pamięci lotnej.

Volatility Framework bazuje na języku programowania Python, będąc rozwijanym w Pythonie 2 w jego najbardziej dojrzałej wersji, czyli tej, którą zajmiemy się w tym temacie. Wraz z pojawieniem się Pythona 3 zaistniała również potrzeba aktualizacji wersji Volatility, wykorzystując nową wersję Pythona i zapewniając mu większą automatyzację. W wersji 2 Volatility Framework pierwszym krokiem do wykonania analizy pamięci jest określenie rodzaju Systemu Operacyjnego. W tym celu możemy skorzystać z polecenia imageinfo programu Volatility (Rysunek 37). Polecenie to jest przydatne do uzyskania wysokopoziomowych informacji o obrazie, wskazuje prawdopodobną identyfikację systemu operacyjnego (profil), Service Pack, architekturę sprzętową, adres pamięci i czas zrzutu.

```
C:\DumpIt>volatility_2.6_win64_standalone.exe -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_10586, Win10x64_14393, Win10x64, Win2016x64_14393
                     AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\DumpIt\memdump.mem)
                      PAE type : No PAE
                           DTB : 0x1ab002L
                          KDBG : 0xf8002b7e04d0L
          Number of Processors : 8
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80029e4e000L
                KPCR for CPU 1 : 0xffffa98079180000L
                KPCR for CPU 2 : 0xffffa98079214000L
                KPCR for CPU 3 : 0xffffa980792b9000L
                KPCR for CPU 4 : 0xffffa98079346000L
                KPCR for CPU 5 : 0xffffa98079680000L
                KPCR for CPU 6 : 0xffffa98079714000L
                KPCR for CPU 7 : 0xffffa980797ab000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-04-03 16:00:13 UTC+0000
     Image local date and time : 2019-04-03 17:00:13 +0100
```

Rysunek 37 - Przykładowy rezultat polecenia imageinfo

Później musimy przekazać zawartość pamięci do plików tekstowych, aby możliwa była analiza jej zawartości. Volatility dostarcza do tego celu szeregu wtyczek.

Sintax: **volatility -f <nome_da_imagem> -profile=< tipo_de_OS> <plugin> > <output>.**

- **-f:** Plik wynikający z przejęcia systemu
- **-profile:** *instrukcja użycia profilu systemu operacyjnego (wcześniej zidentyfikowanego)*
- **plugin:** plugin, który ma zostać wykonany

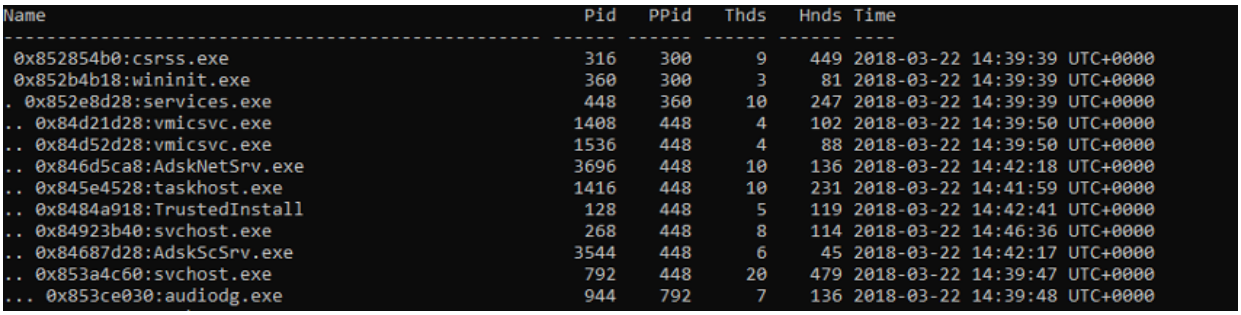
- **output:** plik do eksportu wyników

4.2.2. Pluginy Volatility - Ekstrakcja

Wtyczki, których używa volatility, są specyficzne dla identyfikacji odpowiednich informacji w zawartości RAM dump. Niektóre z tych pluginów omówimy tutaj.

Pslist Lista uruchomionych procesów

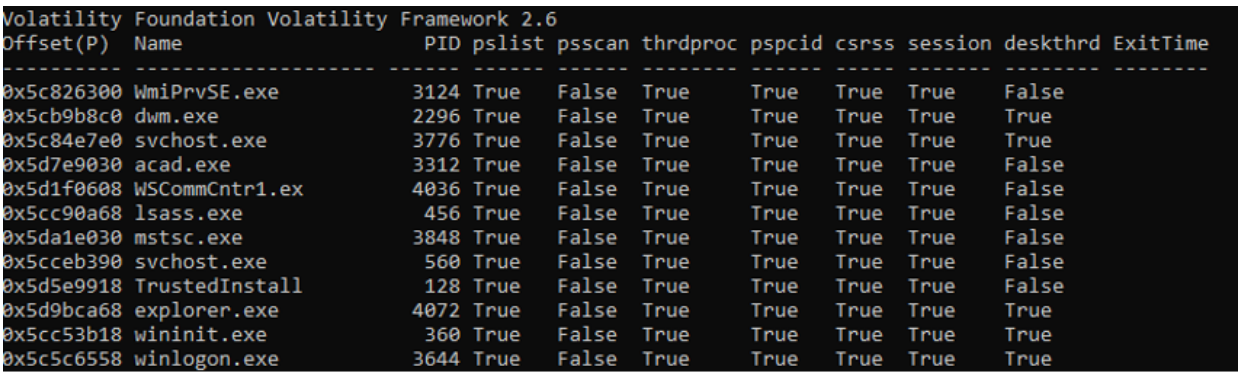
Pstree Wyświetl procesy, rozróżniając je pod względem pochodzenia (Rysunek 38)



```
Name                                               Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x852854b0:csrss.exe                               316    300      9    449 2018-03-22 14:39:39 UTC+0000
 0x852b4b18:wininit.exe                             360    300      3     81 2018-03-22 14:39:39 UTC+0000
. 0x852e8d28:services.exe                           448    360     10    247 2018-03-22 14:39:39 UTC+0000
.. 0x84d21d28:vmicsvc.exe                          1408    448      4    102 2018-03-22 14:39:50 UTC+0000
.. 0x84d52d28:vmicsvc.exe                          1536    448      4     88 2018-03-22 14:39:50 UTC+0000
.. 0x846d5ca8:AdskNetSrv.exe                       3696    448     10    136 2018-03-22 14:42:18 UTC+0000
.. 0x845e4528:taskhost.exe                         1416    448     10    231 2018-03-22 14:41:59 UTC+0000
.. 0x8484a918:TrustedInstall                        128    448      5    119 2018-03-22 14:42:41 UTC+0000
.. 0x84923b40:svchost.exe                           268    448      8    114 2018-03-22 14:46:36 UTC+0000
.. 0x84687d28:AdskScSrv.exe                        3544    448      6     45 2018-03-22 14:42:17 UTC+0000
.. 0x853a4c60:svchost.exe                           792    448     20    479 2018-03-22 14:39:47 UTC+0000
... 0x853ce030:audiodg.exe                          944    792      7    136 2018-03-22 14:39:48 UTC+0000
```

Rysunek 38 - Wtyczka pstree

Psxview Porównaj procesy (Rysunek 39)



```
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x5c826300 WmiPrvSE.exe           3124 True   False  True     True   True  True    False
0x5cb9b8c0 dwm.exe                2296 True   False  True     True   True  True    True
0x5c84e7e0 svchost.exe            3776 True   False  True     True   True  True    True
0x5d7e9030 acad.exe               3312 True   False  True     True   True  True    False
0x5d1f0608 WSCommCntr1.ex         4036 True   False  True     True   True  True    False
0x5cc90a68 lsass.exe               456 True   False  True     True   True  True    False
0x5da1e030 mstsc.exe              3848 True   False  True     True   True  True    False
0x5cceb390 svchost.exe             560 True   False  True     True   True  True    False
0x5d5e9918 TrustedInstall          128 True   False  True     True   True  True    False
0x5d9bca68 explorer.exe           4072 True   False  True     True   True  True    True
0x5cc53b18 wininit.exe             360 True   False  True     True   True  True    True
0x5c5c6558 winlogon.exe           3644 True   False  True     True   True  True    True
```

Rysunek 39 - Plugin Volatility psxview

Netscan Wyświetlanie połączeń sieciowych

Cmdline Cmdline Porównaj procesy (Rysunek 40)

```
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
************************************************************************
smss.exe pid:    240
Command line : \SystemRoot\System32\smss.exe
************************************************************************
csrss.exe pid:    316
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows S
erServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
************************************************************************
csrss.exe pid:    352
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows S
erServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
************************************************************************
wininit.exe pid:    360
Command line : wininit.exe
************************************************************************
winlogon.exe pid:    400
Command line : winlogon.exe
************************************************************************
services.exe pid:    448
Command line : C:\Windows\system32\services.exe
************************************************************************
```

Rysunek 40 - Plugin cmdline Volatility

Cmdscan Porównaj procesy (Rysunek 41)

```
C:\DumpIt>volatility_2.6_win64_standalone -f IE8WIN7.dmp --profile=Win7SP1x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 3624
CommandHistory: 0x229a98 Application: java.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xc
**************************************************
CommandProcess: conhost.exe Pid: 4056
CommandHistory: 0x2cd448 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #22 @ 0xff818488: ??3?
Cmd #25 @ 0xff818488: ??3?
Cmd #36 @ 0x2800c4: ,?,?(???(
Cmd #37 @ 0x2cb3b0: ,?(????
```

Rysunek 41 - Wtyczka cmdscan Volatility

Konsole. Porównaj procesy (Rysunek 42)

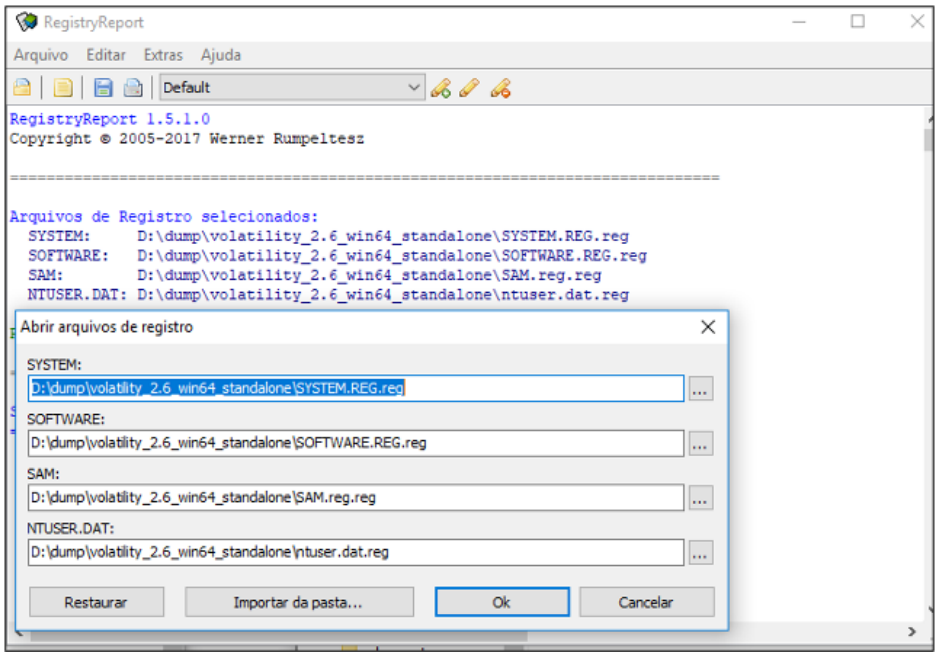
```
C:\DumpIt>volatility_2.6_win64_standalone -f IE8WIN7.dmp --profile=Win7SP1x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 3624
Console: 0x1681c0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Program Files\Autopsy-4.4.0\jre\bin\java.exe
Title: C:\Program Files\Autopsy-4.4.0\jre\bin\java.exe
AttachedProcess: java.exe Pid: 3916 Handle: 0xc
----
CommandHistory: 0x229a98 Application: java.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xc
----
Screen 0x22d160 X:80 Y:300
Dump:
```

Rysunek 42 - Plugin konsoli Volatility

Zrzut rejestru Wyciągnij pliki dziennika

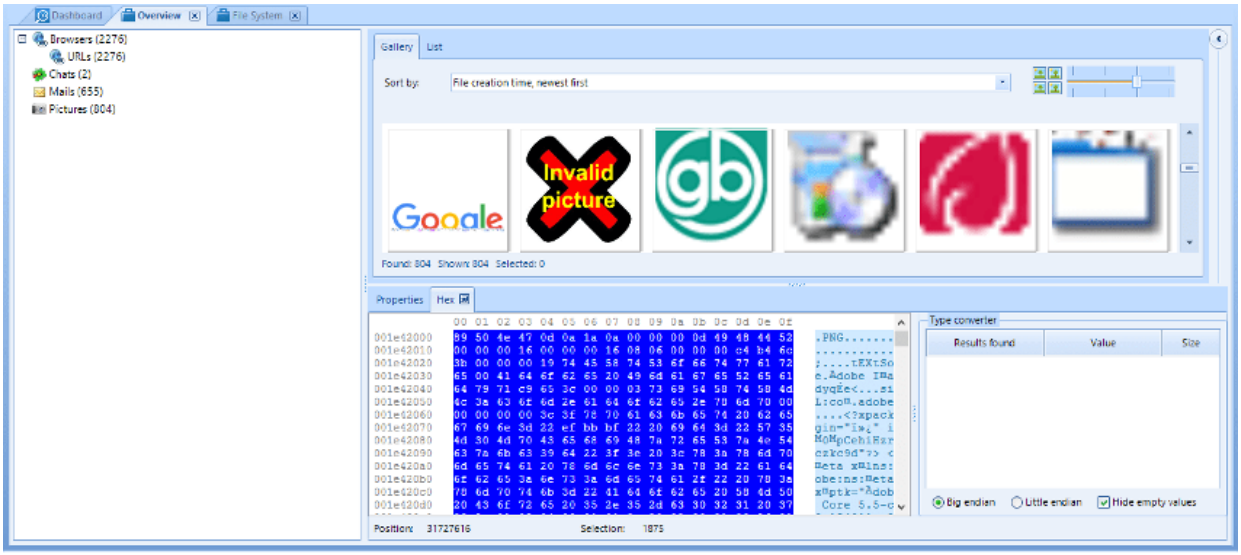
4.2.3. Zmienność wtyczek - analiza

Mając wyodrębnione z pamięci pliki dziennika, można je analizować za pomocą tych samych narzędzi, co pliki dziennika wyodrębnione z systemu operacyjnego. Przykładem może być RegRipper, sama zmienność, czy RegistryReport, pokazany w. Rysunek 43.



Rysunek 43 - Analiza pliku RegistryReport

W analizie pamięci możliwe jest również uzyskanie plików, które zostały przetworzone. Istnieją programy z możliwością identyfikacji i wyodrębniania plików z pamięci, jak na poniższym rysunku z oprogramowaniem Belkasoft, gdzie można sprawdzić, że zidentyfikował on adresy przeglądania w przeglądarkach, dane rozmów na czacie, pliki poczty elektronicznej oraz pliki graficzne (Rysunek 44).



Rysunek 44 - Analiza plików za pomocą programu Belkasoft

SANS opublikował plakat (Rysunek 45) nawiązujący do analizy pamięci przy użyciu Volatility, który podsumowuje wiele wtyczek przydatnych w tego typu analizach.

Rysunek 45 - SANS Poster - Memory Forensics Cheat Sheet v2.0

Utwórz linię czasową zdarzeń w pamięci

Mając dane wydobyte z pamięci lotnej warto stworzyć Oś czasu, aby umożliwić datowanie i sortowanie wskazań w systemie. Jest to proces obejmujący opisane poniżej procedury:

Timeliner utworzyć oś czasu

C:™> volatility_2.6_win64_standalone.exe -f IE8WIN7.dmp --profile=Win7SP1x86_23418 timeliner -- output=body > timeliner.body

Czytaj więcej: https://volatility-labs.blogspot.com/2013/05/movp-ii-23-creating-timelines-with.html

Mftparser Obt (Master File Table).

C:™> volatility_2.6_win64_standalone.exe -f IE8WIN7.dmp --profile=Win7SP1x86_23418 mftparser -- output=body > mftparser.body

Połącz pliki dotyczące wtyczki **timeliner** i **mftparser.**

cat timeliner.body mftparser.body >> timeline.log

Mactime[1] Generowanie osi czasu z połączenia plików

mactime -d -b timeline.log > timeline.csv

Końcowy wynik działania procedur TimeLine (Rysunek 46)

Date	Size	Type	Mode	UID	GID	Meta	File Name
Fri Jan 25 2008 00:02:43	0	...b	---a-------|---	0	0	68267	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\CONTEN~1.CUI (Offset: 0xf352c00)
Fri Jan 25 2008 00:02:43	0	...b	---a-------|---	0	0	68267	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\contentsearch.cui (Offset: 0xf352c00)
Fri Jan 25 2008 00:02:43	0	m..b	---a-------|---	0	0	68267	[MFT STD_INFO] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\CONTEN~1.CUI (Offset: 0xf352c00)
Fri Jan 25 2008 00:57:05	0	...b	---a-------|---	0	0	68199	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\ACIMPR~1.CUI (Offset: 0xe84ec00)
Fri Jan 25 2008 00:57:05	0	...b	---a-------|---	0	0	68199	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\AcImpression.cui (Offset: 0xe84ec00)
Fri Jan 25 2008 00:57:05	0	m..b	---a-------|---	0	0	68199	[MFT STD_INFO] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\ACIMPR~1.CUI (Offset: 0xe84ec00)
Sat Jan 26 2008 16:24:32	0	m..b	---a----------	0	0	18486	[MFT STD_INFO] PROGRA~1\AUTOCA~1\PPCLIE~1.MAN (Offset: 0x4a15d800)

Rysunek 46 - Zawartość pliku timeline.csv

Dzięki tej tabeli można łatwo zidentyfikować akcje przekazywane w pamięci urządzenia, a te uzupełnią informacje uzyskane podczas analizy urządzenia w dead-box forensics.

Przykład identyfikacji dostępu do sieci TOR

Jako przykład analizy danych pamięciowych mamy wykorzystanie przeglądarki Tor, ponieważ nie przechowuje ona informacji nawigacyjnych na dysku twardym, choć możliwa jest ich identyfikacja i analiza poprzez pamięć.

Zaczynamy od potwierdzenia **profilu systemu** (Rysunek 47).

```
     Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                AS Layer2 : FileAddressSpace (D:\dump\tor\memdump.mem)
                 PAE type : PAE
                      DTB : 0x185000L
                     KDBG : 0x8293ac30L
     Number of Processors : 2
Image Type (Service Pack) : 1
           KPCR for CPU 0 : 0x8293bc00L
           KPCR for CPU 1 : 0x807c1000L
       KUSER_SHARED_DATA : 0xffdf0000L
     Image date and time : 2019-04-04 20:24:26 UTC+0000
Image local date and time : 2019-04-04 13:24:26 -0700
```

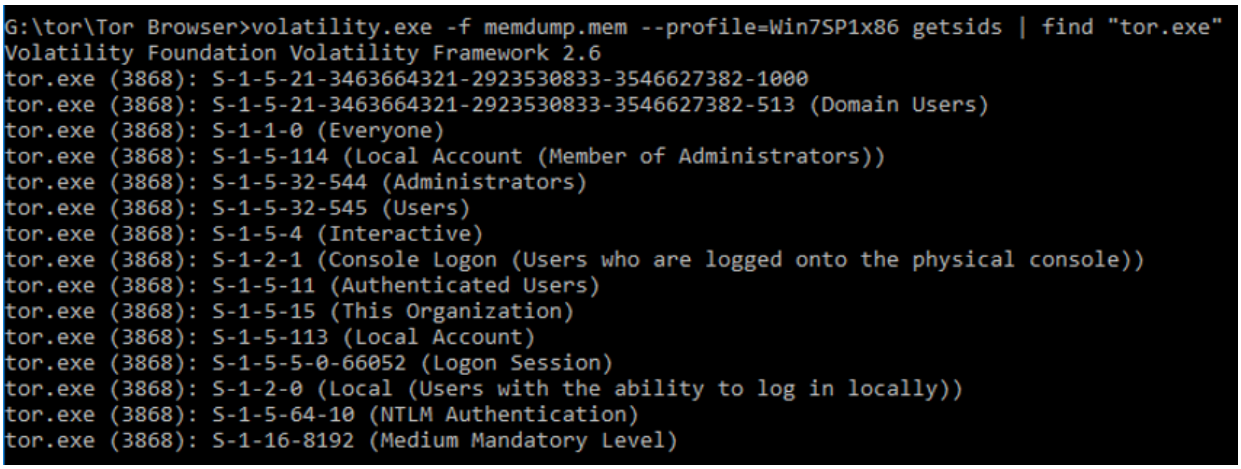
Rysunek 47 - Wtyczka Volatility imageinfo

Użyliśmy wtyczki **pstree** do sprawdzenia uruchomionych procesów, filtrując procesy według nazwy "firefox.exe" (Rysunek 48), ponieważ Tor Browser używa tego procesu, lub bezpośrednio po nazwie "tor.exe". Aby uzyskać więcej informacji o procesach w analizowanym urządzeniu, mamy jeszcze możliwość skorzystania z wtyczek **pslist**, **psscan**.

```
D:\dump\tor>volatility_2.6_win64.exe -f memdump.mem --profile=Win7SP1x86_23418 pstree | find "firefox.exe"
Volatility Foundation Volatility Framework 2.6
. 0x84cd67c8:firefox.exe                          1736   1604     45    715 2019-04-04 20:58:21 UTC+0000
.. 0x85f484c8:firefox.exe                         2428   1736     21    340 2019-04-04 20:59:08 UTC+0000
.. 0x844d8b20:firefox.exe                         2484   1736     19    328 2019-04-04 20:59:47 UTC+0000

D:\dump\tor>volatility_2.6_win64.exe -f memdump.mem --profile=Win7SP1x86_23418 pstree | find "tor.exe"
Volatility Foundation Volatility Framework 2.6
.. 0x85c15380:tor.exe                             2064   1736      4     65 2019-04-04 20:58:49 UTC+0000
```

Rysunek 48 - Wykorzystanie zmienności w badaniach procesowych

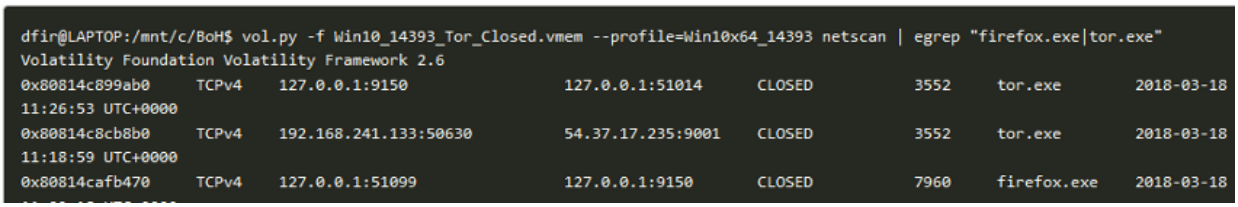
Getsids Informacja o rozpoczęciu procesu, odnosząca proces do użytkownika (Rysunek 49).



Rysunek 49 - Wykorzystanie zmienności w identyfikacji procesu

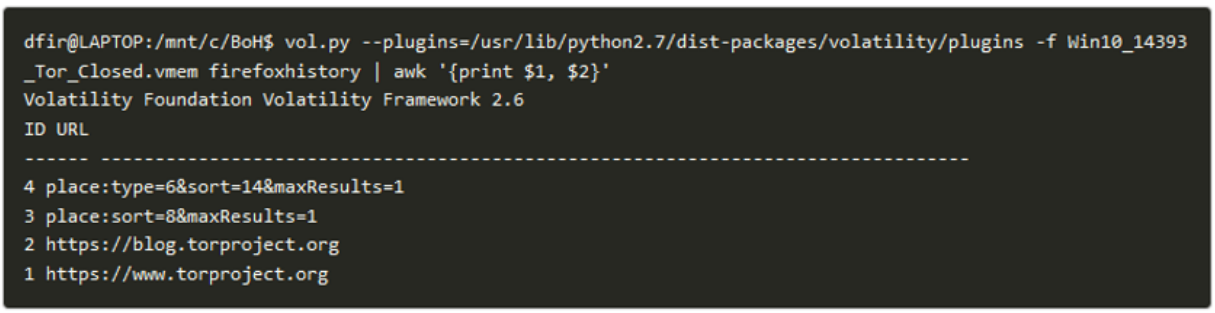
netscan wyświetlanie połączeń sieciowych

W tym przypadku proces "tor.exe" wskazuje na zakończone połączenie z docelowym IP "54.37.17.235" na porcie 9001 (Rysunek 50).



Rysunek 50 - Użycie Volatility w identyfikacji sieci

Firefoxhistory Lista zapytanych adresów (URL) (Rysunek 51).



Rysunek 51 - Wykorzystanie zmienności do pobierania adresów URL z pamięci

Źródło: https://blog.superponible.com/2014/08/31/volatility-plugin-firefox-history/

---

[1] https://wiki.sleuthkit.org/index.php?title=Mactime

5. Identyfikacja i analiza informacji w systemach operacyjnych

Według "https://gs.statcounter.com/os-market-share/desktop/worldwide" system operacyjny Microsoft Windows ma udział w rynku na poziomie około 75 procent, na drugim miejscu jest Apple OS X z 14,5 procentami. Analityk kryminalistyczny znajdzie znacznie więcej urządzeń z systemem operacyjnym Micrososft niż jakimkolwiek innym. Uzasadnia to większą uwagę poświęconą analizie tego systemu operacyjnego.

SANS prowadzi znakomitą pracę badawczą i edukacyjną w zakresie informatyki śledczej, a jednym z czynników zainteresowania jest regularne publikowanie tzw. Posterów, pod adresem: https://www.sans.org/posters/, z wynikami tych badań. Postery te są również ważnym źródłem informacji dotyczących lokalizacji artefaktów będących przedmiotem zainteresowania kryminalistyki, gdyż systemy operacyjne MS Windows przechowują liczne artefakty w codziennych działaniach swoich użytkowników.

5.1. Rejestr MS Windows

"*Centralna hierarchiczna baza danych w systemie Windows ... używana do przechowywania informacji niezbędnych do skonfigurowania systemu dla jednego lub więcej użytkowników, aplikacji i urządzeń sprzętowych. Rejestr zawiera informacje, do których Windows nieustannie odwołuje się podczas pracy, takie jak profile każdego użytkownika, aplikacje zainstalowane na komputerze i typy dokumentów, które każda z nich może tworzyć, ustawienia arkusza właściwości dla folderów i ikon aplikacji, jaki sprzęt istnieje w systemie i jakie porty są używane.* "

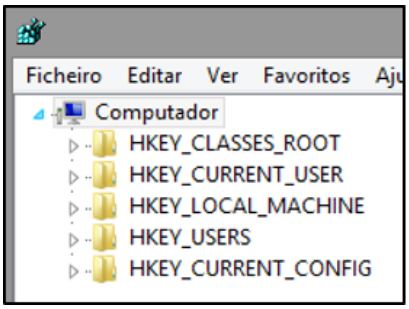
Źródło: *Microsoft Computer Dictionary.--5th ed.* , Redmond, Washington, Microsoft Press, 2002, s. 445

Można zatem stwierdzić, że rejestr systemu Windows, mimo plików strukturalnych, zawiera strukturę logiczną w ciągłym użyciu przez system operacyjny, przechowującą zestaw informacji niezbędnych do jego działania.

Struktura logiczna rejestru systemu Windows zawiera:

1. **Klucze rejestru**, klucze o nazwie "Software" i "System", należące do *roju* "HKEY_CURRENT_CONFIG".
2. **Podklucze rejestru**, gdzie przechowywane są informacje rejestru (np.: podklucz "Fonts").
3. **Wartości rejestru,** które zawierają informacje poprzez określenie ich typu w odpowiedniej kolumnie (np.: REG_DWORD - 32-bitowa wartość binarna, REG_QWORD - 64-bitowa wartość binarna).

Pięć głównych Hives w strukturze logicznej systemu operacyjnego MS Windows można zobaczyć na. Rysunek 52.



Rysunek 52 - UI główny

Ule rejestru (Root Keys) charakteryzują się przedrostkiem "HKEY_", skrótem od "Handle to a KEY".

Istnieje 5 głównych ulów, przechowywanych w różnych plikach tworzących rejestr, chociaż tylko HKEY_USERS i HKEY_LOCAL_MACHINE są uważane za prawdziwe ule, reszta to skróty lub aliasy dla gałęzi w nich zawartych.

UI	Skrót	Opis	*Link*
HKEY_CURRENT_USER	**HKCU**	Wskazuje na profil użytkownika aktualnie zalogowanego użytkownika	Podklucz w HKEY_USERS odpowiadający aktualnie zalogowanemu użytkownikowi
HKEY_USERS	**HKU**	Zawiera podklucze dla wszystkich załadowanych profili użytkowników	Nie link
HKEY_CLASSES_ROOT	**HKCR**	Zawiera informacje o skojarzeniach plików i rejestracji COM	Nie jest to bezpośredni link; raczej połączony widok HKLMSOFTWARE Classes i HKEY_CURRENT_USERSOFTWARE Classes.
HKEY_LOCAL_MACHINE	**HKLM**	Ustawienia globalne dla urządzenia.	Nie link

HKEY_CURRENT_CONFIG	**HKCC**	Aktualny profil sprzętowy	HKLMSYSTEMU Sterownik - Profile sprzętowe - HKLMSYSTEMSetet - Profile sprzętowe
HKEY_PERFORMANCE_DATAHKPD		Liczniki wydajności	Nie link

Źródło: *Windows Internals.--6th ed., Part 1*,

Redmond, Washington, Microsoft Press, 2012, s. 281

Pliki dziennika znajdują się w następujących folderach:

Pliki dziennika systemu operacyjnego

C:\NWindows \System32 \NKonfiguracja

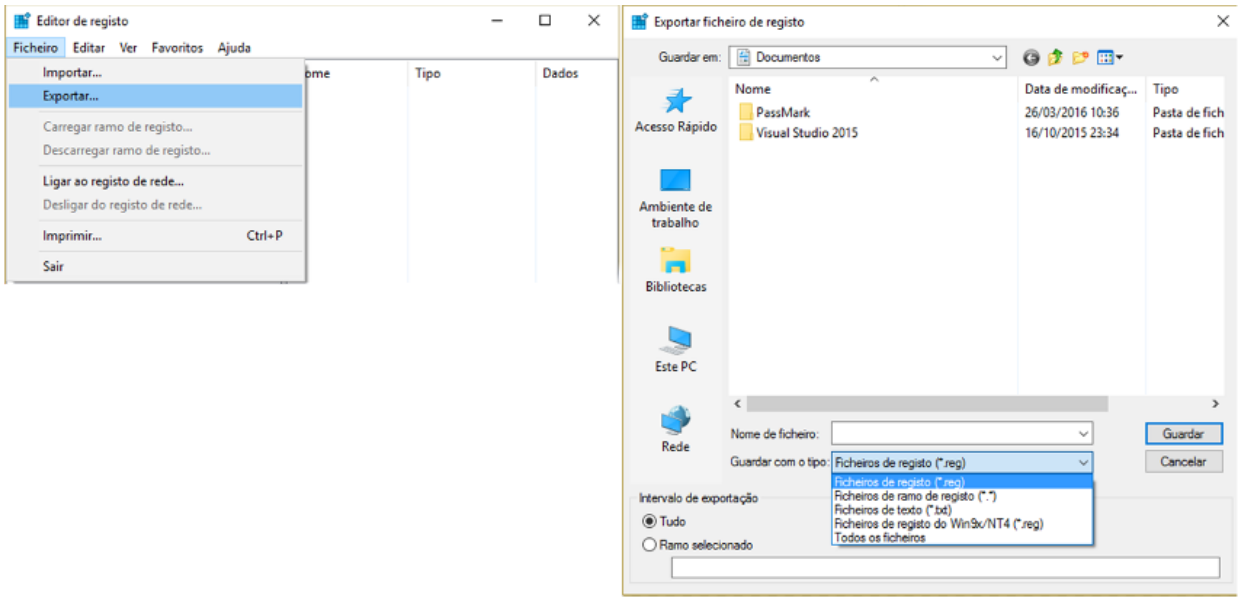
Pliki rejestru dla każdego użytkownika

C:{\i0}C:{\i1}Niezależnie od tego, czy jest to użytkownik, czy nie.{\i0}

5.1.1. Edytor rejestru (RegEdit)

Edytor rejestru, w wersji graficznej, umożliwia eksport jednego lub kilku kluczy rejestru (Rysunek 53).

RegEdit, Plik > Eksport



Rysunek 53 - Eksport rejestru przez RegEdit

Przez wiersz poleceń:

regedit /e c:output.reg "HKEY_LOCAL_MACHINE "System..."

5.1.2. ERUNTgui

Aplikacja ERUNTgui (Rysunek 54), pozwala na tworzenie kopii zapasowych, przywracanie i optymalizację rejestru, będąc w kręgu zainteresowań kryminalistyki możliwość wykonania kopii zapasowej rejestru, co umożliwia jego późniejszą analizę.

Rysunek 54 - eksport rejestru przez ERUNTgui

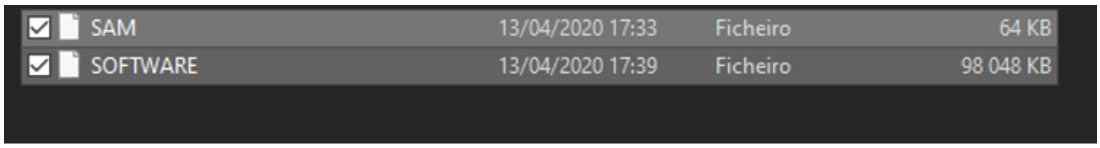
1.1.3. RAWCopy

Aplikacja RAWCopy (.Rysunek 55), umożliwia kopiowanie sektorów dysku, w których znajdują się używane pliki, pokonując w ten sposób ograniczenie kopiowania plików otwieranych przez system.

```
C:\ForensicsSoftware\VArios\RawCopy>RawCopy64.exe C:\WINDOWS\system32\config\SAM C:\
RawCopy v1.0.0.9

Error: NtOpenFile returned: 0xC0000043
Opening target file failed, now re-trying with INDX method from parent folder
Record number: 128277 found at disk offset: 3352581120 -> 0x41E8FA8A80000000
Record number: 219734 found at disk offset: 63105103872 -> 0x422D62B6F0000000
Writing: SAM

Job took 1.07 seconds

C:\ForensicsSoftware\VArios\RawCopy>RawCopy64.exe C:\WINDOWS\system32\config\SOFTWARE C:\
RawCopy v1.0.0.9

Error: NtOpenFile returned: 0xC0000043
Opening target file failed, now re-trying with INDX method from parent folder
Record number: 128277 found at disk offset: 3352581120 -> 0x41E8FA8A80000000
Record number: 220159 found at disk offset: 63105539072 -> 0x422D62C438000000
Writing: SOFTWARE

Job took 1.31 seconds

C:\ForensicsSoftware\VArios\RawCopy>
```

Rysunek 55 - Eksport rejestru przez RAWCopy

Poprzez RAWCopy możliwe było uzyskanie kopii pliku SAM i SOFTWARE z uruchomionym systemem (Rysunek 56).



Rysunek 56 - Pliki wyeksportowane przez RAWCopy

Źródło: https://github.com/jschicht/RawCopy

5.2. Analiza rejestru systemu Windows

Analizę rejestru systemu Windows można przeprowadzić za pomocą oprogramowania kryminalistycznego, takiego jak AccessData Registry Viewer, narzędzia Erica Zimmermana, RegRipper lub nawet innego oprogramowania zdolnego do wyodrębnienia danych z tych plików rejestru.

Ze względu na złożoność rejestru systemu Windows, identyfikacja lokalizacji każdego istotnego fragmentu informacji może być zniechęcającym zadaniem, jednak skorzystaliśmy z pomocy SANS FOR500 (https://digital-forensics.sans.org/docs/DFPS_FOR500_v4.11_0121.pdf), identyfikując wiele ważnych lokalizacji, w których można znaleźć istotne informacje.

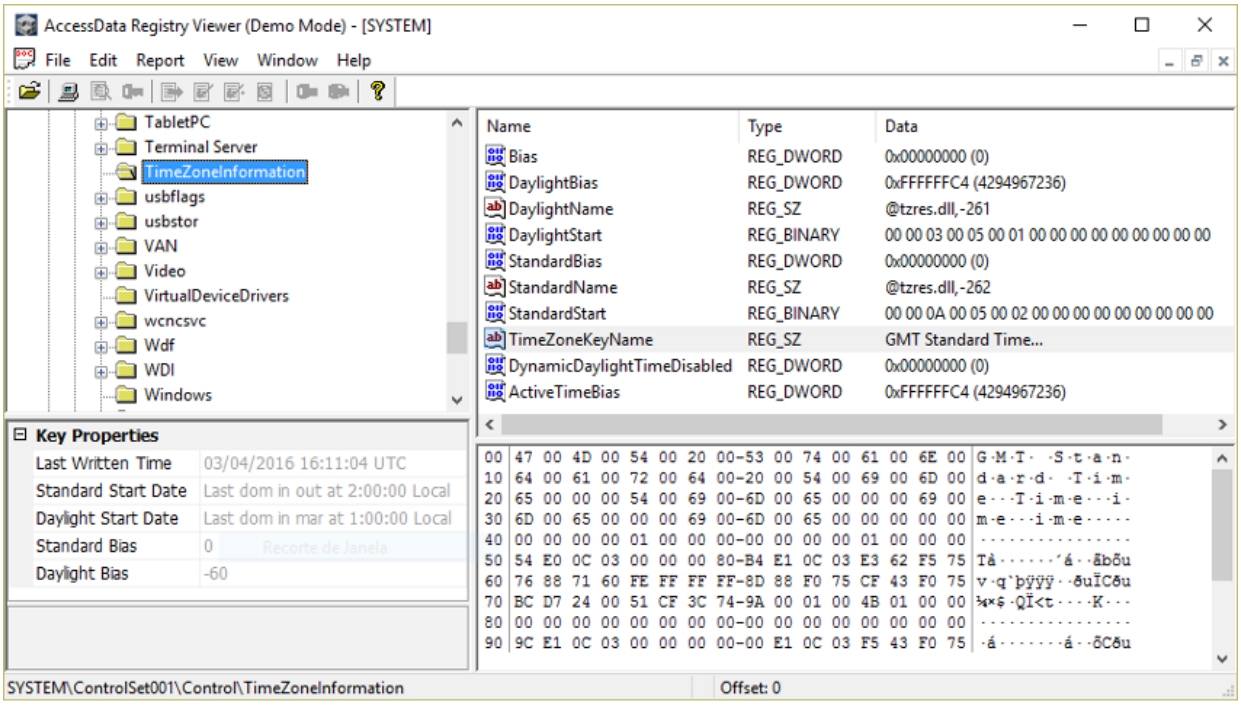
Może zaistnieć potrzeba wyodrębnienia dziennika z podłączonego komputera, dziennik jest ogromnym źródłem informacji istotnych z punktu widzenia kryminalistyki, konieczne będzie uzyskanie wszystkich tych informacji. (Czytaj: https://resources.infosecinstitute.com/windows-registry-analysis-regripper-hands-case-study-2/). Istnieje kilka sposobów na wykonanie zrzutu rejestru, tutaj skupimy się na kilku różnych sposobach.

5.2.1. Strefa czasowa

Pierwszą informacją, którą należy przeanalizować, powinna być Strefa czasowa (Rysunek 57), gdyż może ona doprowadzić nas do błędów w obliczu działań prezentujących datę/godzinę inną niż prawdziwa, tylko dlatego, że system jest skonfigurowany z inną strefą czasową niż ta, z której korzysta analityk kryminalistyczny.

Informacje te można zidentyfikować w SYSTEMIE *ULA*, w następującym miejscu :

SYSTEMY STREFY CZASU



Rysunek 57 - Strefa czasowa w widoku rejestru AccessData

5.2.2. Urządzenia USB

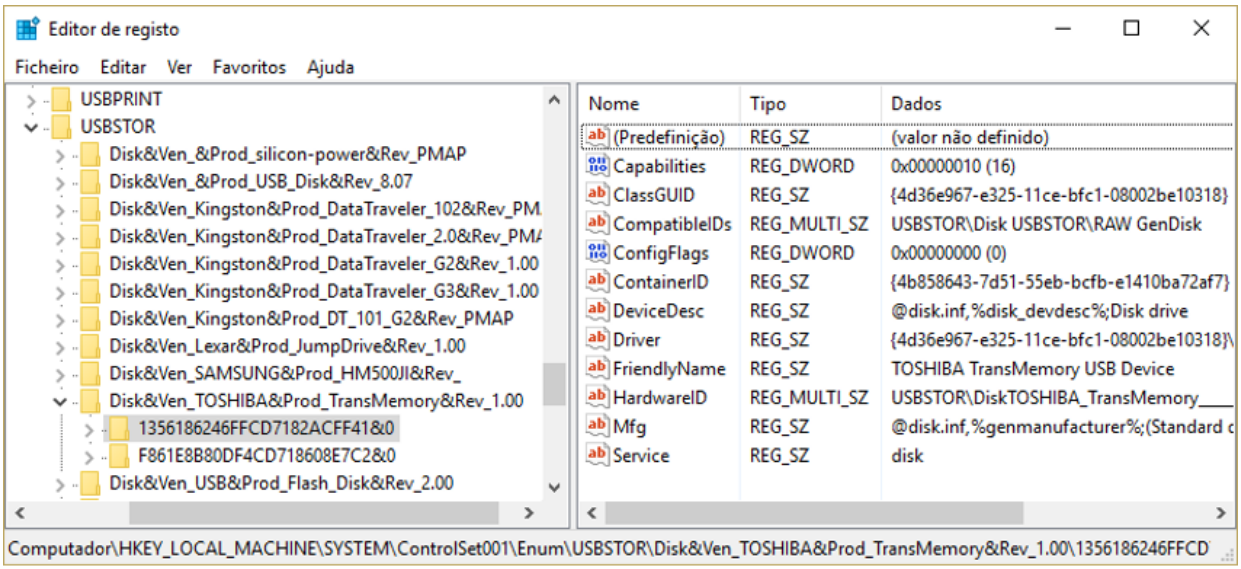
W rejestrze możliwe jest również uzyskanie informacji z urządzeń USB, które podłączyły się do systemu w *ulu* SYSTEM:

Do uzyskania: Producent / Marka / nr seryjny. / data / godzina pierwszego i ostatniego podłączenia do systemu

HKLM SYSTEMY BIEŻĄCE SetupEnum.

HKLM SYSTEM Bieżąca kontrola - Setum USB

Przeglądając (Rysunek 58).



Rysunek 58 - Przeglądanie urządzeń USB w Edytorze Rejestru

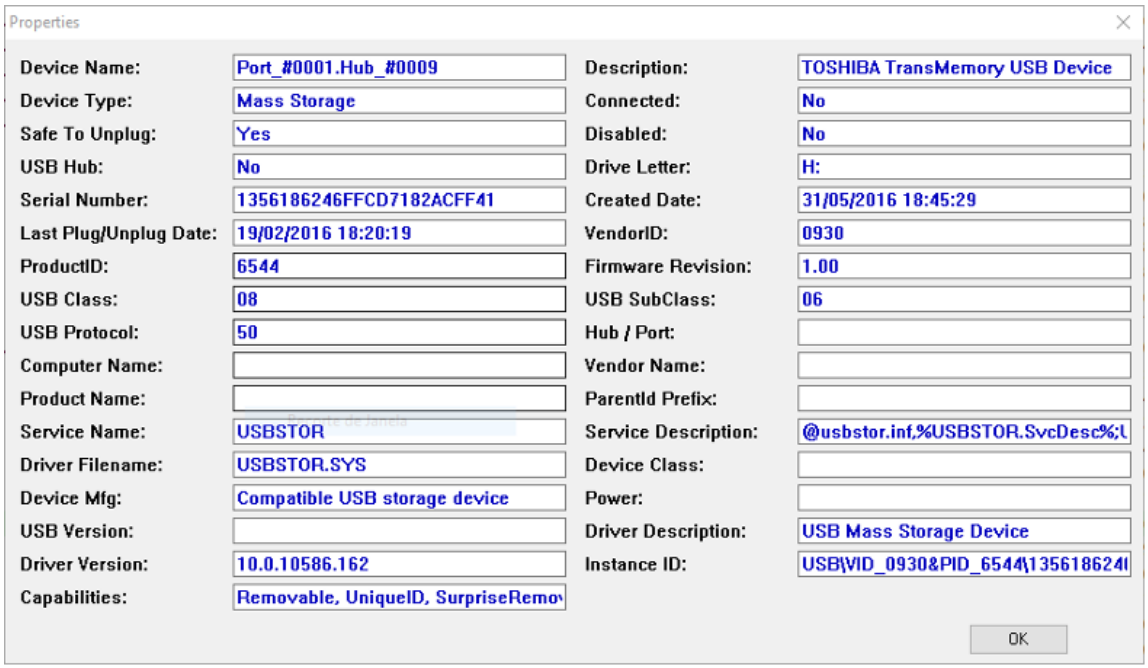
Aby uzyskać literę przypisaną do urządzenia USB

HKLM SYSTEM - urządzenia zamontowane

Aby uzyskać użytkownika, który podłączył urządzenie do systemu

NTUSER.dat Oprogramowanie Microsoft Windows, bieżąca wersja, eksplorator, punkty montowania.

Te same informacje można uzyskać za pomocą specjalnych narzędzi do uzyskiwania informacji z urządzeń USB, takich jak narzędzia 4Discovery lub USBDeview(Figura 59).



Rysunek 59 - Przeglądanie urządzeń USB w USBDeview

Czytaj:https://www.researchgate.net/publication/318514858_USB_Storage_Device_Forensics_for_Windows_10

5.2.3. Użytkownicy

Informacje o użytkownikach systemu są przechowywane w rejestrze Windows w ulu SAM, ale dla każdego użytkownika istnieje również plik rejestru NTUSER.DAT, który przechowuje dane specyficzne dla tego użytkownika:

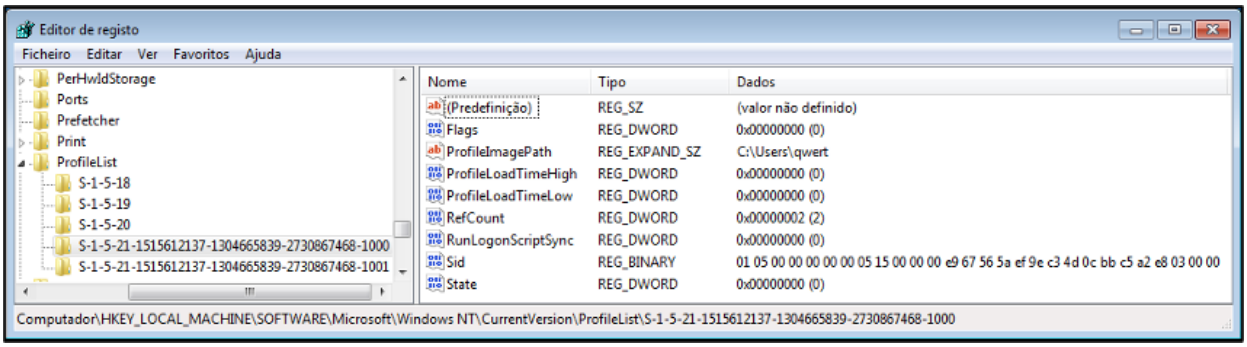
Lista lokalnych profili użytkowników

W rejestrze: HKLM Oprogramowanie Windows NT "CurrentVersion

Użytkownicy systemu

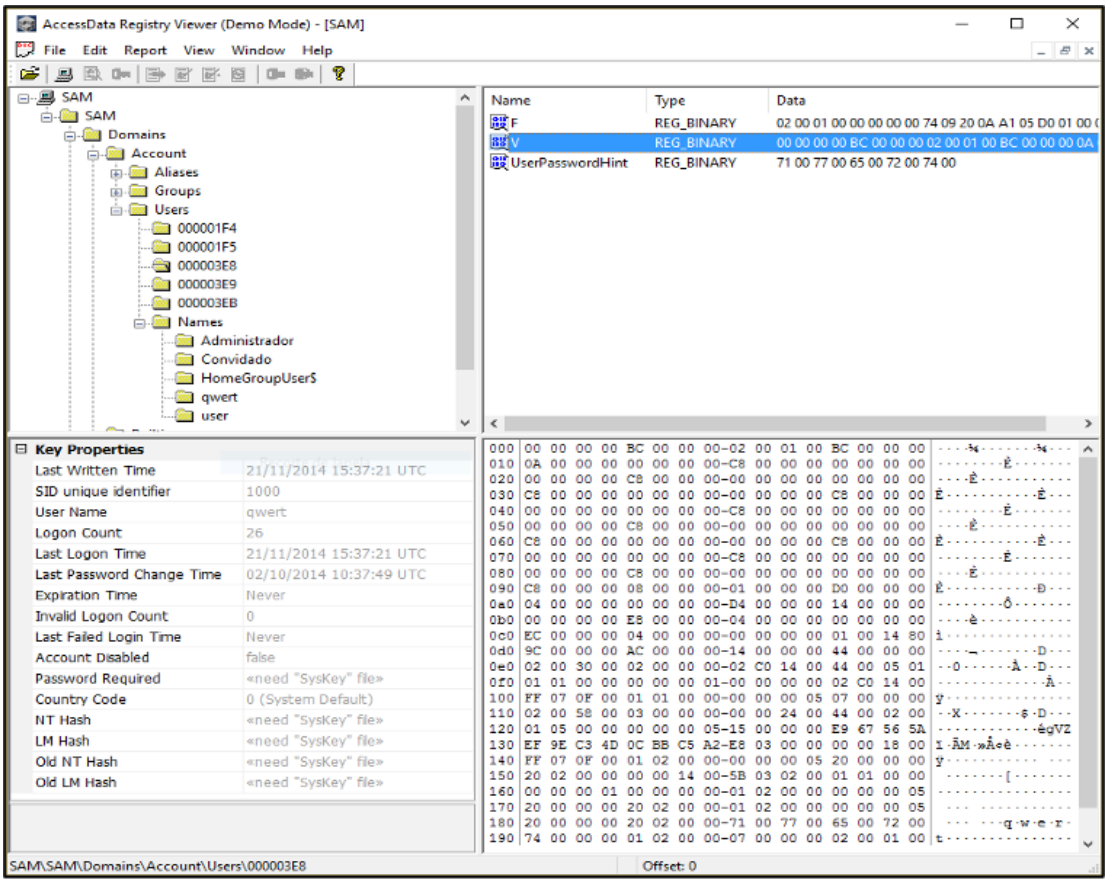
W pliku: SAM domeny, konta, użytkowników.

Przeglądając ten klucz rejestru poprzez Edytor rejestru, można zobaczyć, jak wyświetlane są te informacje (Rysunek 60).



Rysunek 60 - Przeglądanie użytkowników w edytorze rejestru

Te same informacje można uzyskać za pomocą specjalnych narzędzi do uzyskiwania informacji o użytkownikach, takich jak AccessData Registry Viewer (Rysunek 61).



Rysunek 61 - Wyświetlanie użytkowników w programie AccessData Registry Viewer

5.2.4. Sieć

Dziennik zawiera również różne informacje o sieci, takie jak sieci bezprzewodowe, z którymi połączył się system:

HKLM Oprogramowanie Microsoft NT CurrentVersion NetworkList.

W tej lokalizacji możliwa jest identyfikacja:

- Nazwa sieci (SSID)
- Nazwa domeny / intranetu
- Data/czas ostatniego połączenia (poprzez datę/czas zapisania odpowiedniego klucza)

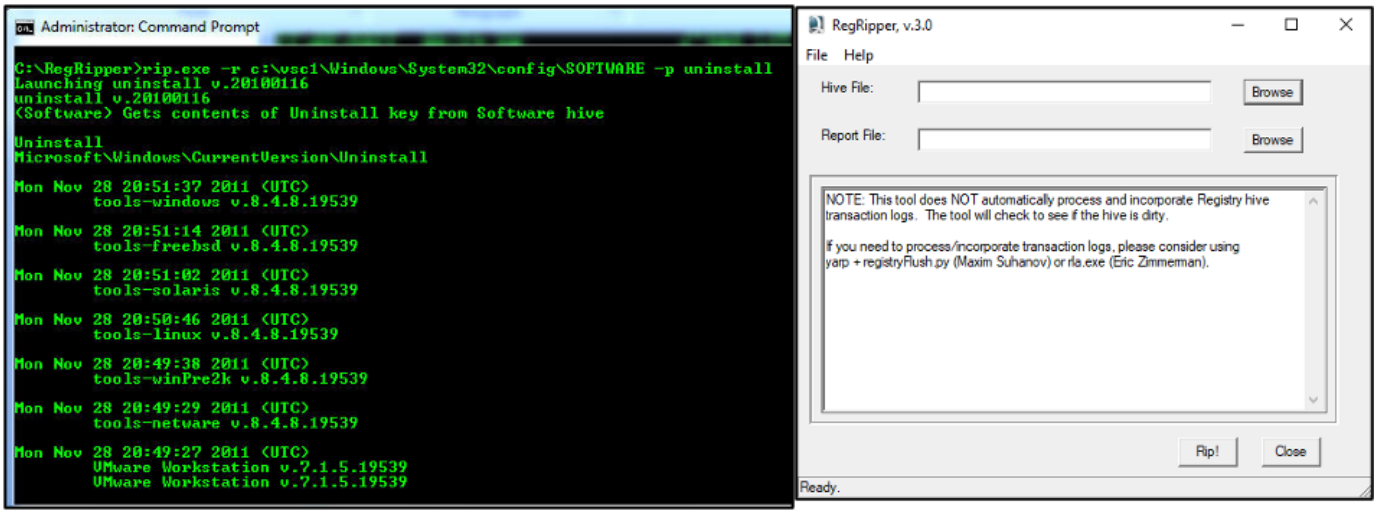
- Adres MAC bramy

5.2.5. Analiza rejestru systemu Windows - RegRipper

Jeśli chodzi o analizę rejestru Windows, istnieje wiele narzędzi kryminalistycznych, które możemy wykorzystać w celu ułatwienia analizy informacji zawartych w rejestrze Windows. Skupiamy się tutaj na niektórych darmowych narzędziach, takich jak RegRipper, RegistryReport i Windows Registry Recovery.

RegRipper (http://github.com/keydet89) to aplikacja Open Source Forensic, opracowana przez Harlana Carvey'a i napisana w języku PERL, której celem jest wydobywanie informacji z plików rejestru systemu Windows w czytelny sposób.

Program RegRipper (Rysunek 62) może być używany poprzez wiersz poleceń oraz interfejs graficzny do wyodrębniania określonych informacji z każdego pliku rejestru. Podczas korzystania z wiersza poleceń możliwe jest wybranie wtyczki, która ma być zastosowana do każdego roju rejestru, natomiast w przypadku wiersza poleceń stosowane są wszystkie wtyczki dostępne dla wybranego roju. Wynik wyodrębnionych informacji może być wyświetlony na ekranie lub zapisany w pliku tekstowym, w przypadku użycia linii poleceń. Poprzez swój interfejs graficzny konieczne będzie wskazanie lokalizacji wyjściowej, zwanej Report File, aby utworzyć plik tekstowy z wynikiem wszystkich wtyczek zastosowanych do danego ula rejestru....

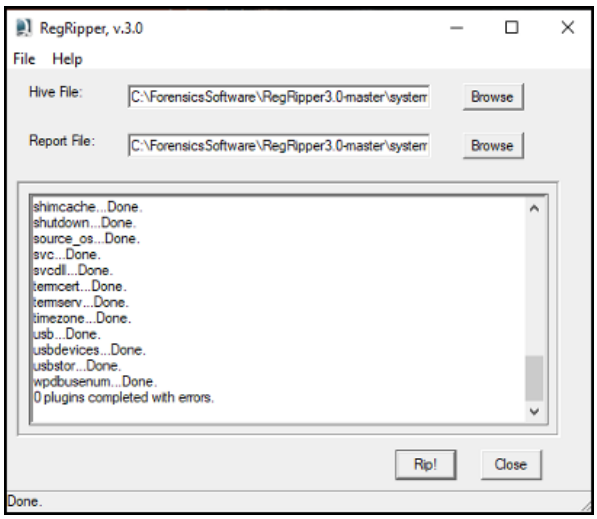


Rysunek 62 - Użycie RegRippera

Poprzez linię poleceń można sprawdzić dostępne wtyczki do zastosowania poprzez argument "-l -c".

C:RegRipper3.0-master>rip -l -c > c:list.csv

W trybie GUI (.Rysunek 63), nie ma możliwości wybrania przez nas pojedynczego pluginu, lecz Ula, którego chcemy analizować.



Rysunek 63 - Używanie GUI RegRippera

Plik wyjściowy (Rysunek 64)

```
----------------------------------------
winver v.20200525
(Software) Get Windows version & build info

ProductName              Microsoft Windows XP
CSDVersion               Service Pack 3
BuildLab                 2600.xpsp.080413-2111
RegisteredOrganization   ubinet
RegisteredOwner          ubinet
InstallDate              2000-01-01 17:45:17Z
----------------------------------------
```

Rysunek 64 - Plik wyjściowy programu RegRipper

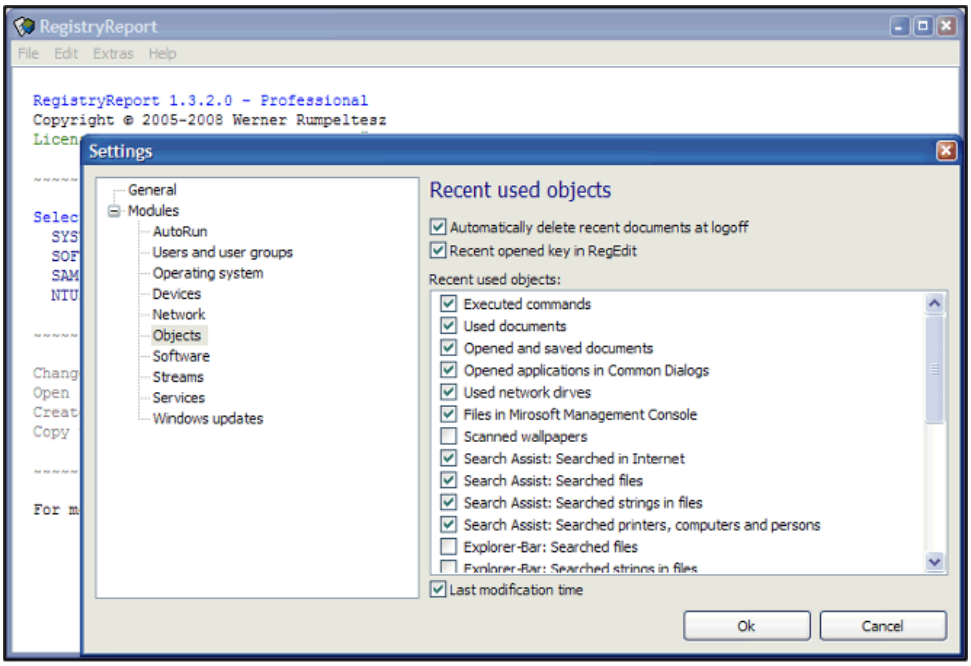
Istnieją inne aplikacje kryminalistyczne o tym samym celu interpretacji zawartości plików rejestru, takie jak Registry Report i Windows Registry Recovery.

RegistryReport

Podobnie jak RegRipper, Gaijin Registry Repport również prezentuje informacje z rejestru w sposób łatwy do odczytania i przeszukiwania. Działa w prosty sposób, pozwalając wybrać informacje, które chcesz pobrać z rejestru poprzez pola wyboru, jak pokazano w Rysunek 65.

Źródło: https://gaijin.at/en/files?dir=old-software registryreport

https://github.com/jschicht?tab=repositories

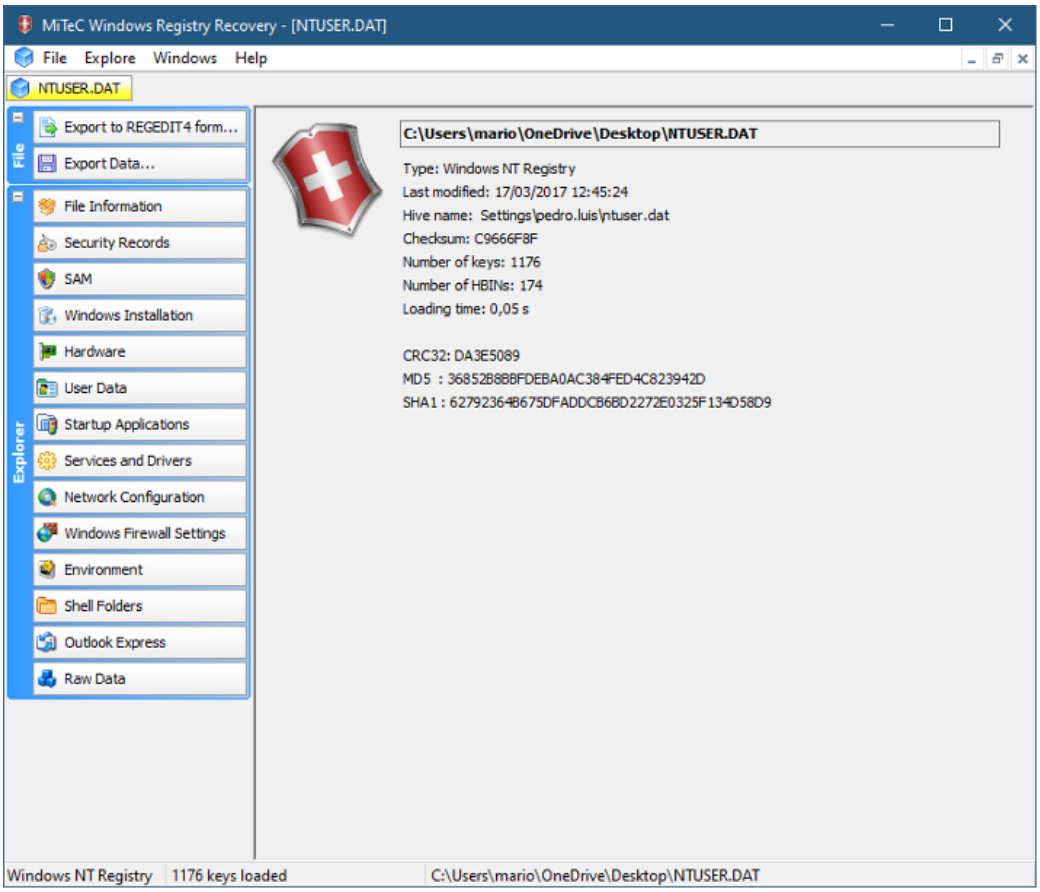


Rysunek 65 - Użycie RegistryReport

Źródło: https://www.gaijin.at/en/files?dir=old-software&sort=N&order=A registryreport

Odzyskiwanie rejestru systemu Windows

WRR (Rysunek 66) jest jedną z aplikacji, którą możemy wykorzystać do analizy rejestru Windows



Rysunek 66 - Używanie MiTeC Windows Registry Recovery

Źródło: http://www.mitec.cz/wrr.html

5.3. Analiza systemów opartych na systemie Linux

Cyfrowa kryminalistyka w systemach operacyjnych MS Windows, jest szeroko rozpowszechniona, zarówno poprzez kursy i artykuły naukowe, jak i poprzez nowe media, takie jak filmy. Cyfrowa kryminalistyka w systemach operacyjnych Linux, nie jest tak rozpowszechniona, głównie dlatego, że analiza tychże jest również znacznie mniejsza.

Systemy plików

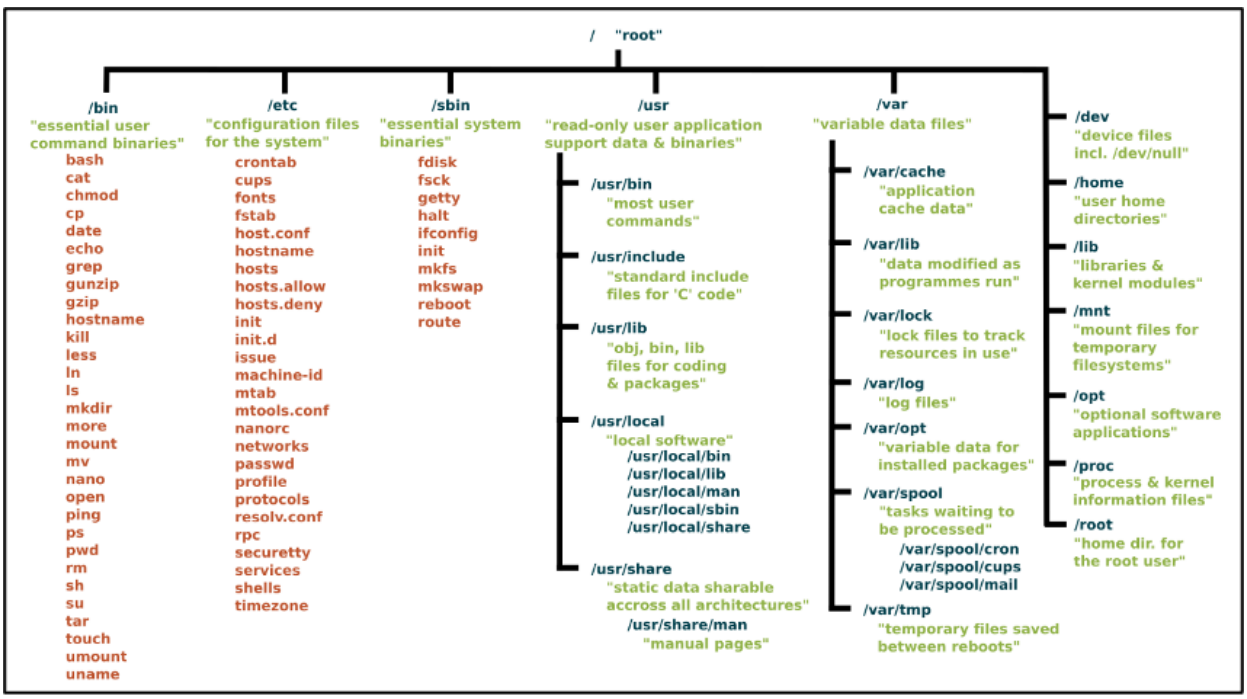
Standardowym systemem plików w Linuksie jest obecnie Ext4, chociaż obsługuje on różne typy systemów plików

System plików Linux	Dane	
Ext	1992	Oznacza "Extended file system", był to pierwszy system plików stworzony dla linuxa w 1992 roku
Ext2	1993	Obsługiwał dyski do 2 TB i nie obsługiwał journalingu. Ponieważ nie używa journalingu, może być używany na pamięciach USB.
Ext3	1999	To samo co Ext2, ale z przewagą journalingu.
Ext4	2006	Obecna wersja Ext. typy ma kilka korzystnych cech w porównaniu do swoich poprzedników, takich jak zmniejszenie fragmentacji systemu, pracuje z dużymi plikami i więcej. EXT4 obsługuje 1EB (1 Exabyte) maksymalny rozmiar systemu plików i 16TB maksymalny rozmiar pliku. Możliwe jest posiadanie nieograniczonej liczby podkatalogów

Uwagi ogólne

1. Nie ma plików dziennika jak w systemie operacyjnym Windows
2. Informacje powinny być zbierane w rozproszonych miejscach
3. Różne struktury plików systemowych w różnych dystrybucjach

Strukturę plików i folderów w systemie Linux można podsumować w sposób przedstawiony na rysunku Rysunek 67.

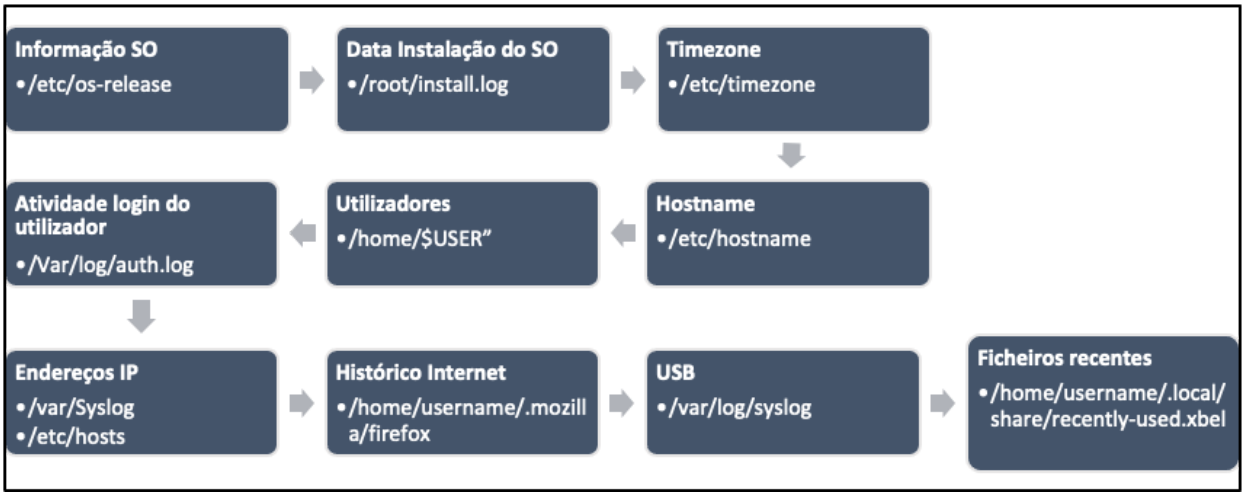


Rysunek 67 - Struktura plików systemu Linux

Źródło: The Linux Foundation - https://linuxfoundation.org/blog/classic-sysadmin-the-linux-filesystem-explained/

5.3.1. Punkty zainteresowania w systemach Linux

Analiza aktywności użytkowników w systemach Ubuntu Linux powinna przebiegać zgodnie z sekwencją walidacji i zbierania informacji, przedstawioną np. Rysunek 68.



Rysunek 68 - Propozycja gromadzenia informacji o systemie Linux

Autorun programów działających w systemie :

Należy pamiętać, że wiele programów jest skonfigurowanych do automatycznego uruchamiania przy starcie systemu. Informacje o programach, które powinny być uruchamiane przy starcie znajdują się w katalogu "**/etc/rc.local**".

Udostępnione dokumenty :

Egzaminator może wiedzieć, do których dokumentów miał ostatnio dostęp. Plik zawierający te informacje znajduje się w katalogu **/home/user/.local/share/recently-used.xbel.** Do przeglądania zawartości tego pliku można użyć polecenia **cat.** Plik .xbel zawiera szczegółowe informacje o plikach, do których użytkownik miał dostęp, takie jak czas dostępu i modyfikacji...

Zainstalowane aplikacje :

Informacje o aplikacjach znajdują się w folderze **/usr/bin** biblioteki potrzebne dla aplikacji znajdują się w folderze **/usr/lib.** Listę aplikacji można uzyskać za pomocą polecenia **ls -l /usr/bin/.** Można zrozumieć datę instalacji, uprawnienia, rozmiar itp.

Informacje o sieci:

Ubuntu przechowuje listę sieci podłączonych do systemu w: **/etc/NetworkManager/system-connections**

Plik **/var/log/syslog** podaje datę i godzinę nawiązania połączenia sieciowego.

Sprzęt **podłączony:**

Katalog /dev dostarcza informacji o sprzęcie podłączonym do systemu.

W pliku **/var/log/syslog** znajdują się również informacje o urządzeniach, które zostały podłączone do systemu.

Ostatnie logowanie i aktywność Użytkownika::

Informacje o ostatnim **logowaniu** można uzyskać w **/var/log/lastlog**

Aktywność w przeglądaniu Internetu:

Przedstawiamy lokalizację folderów wraz z informacjami nawigacyjnymi, w dwóch głównych przeglądarkach używanych w systemie operacyjnym Linux (Rysunek 69 oraz Rysunek 70). Po wyodrębnieniu tych treści, możliwa staje się ich analiza w taki sam sposób jak w systemie Windows .

Przeglądarka Firefox

OS	Localização Profile
Linux	/home/$username/.mozilla/firefox/Profiles

OS	Localização da Cache
Linux	/home/$username/.mozilla/firefox/Profiles

Rysunek 69 - Lokalizacja informacji o przeglądarce Firefox

Google Chrome

OS	Localização
Linux	/home/$USER/.config/google-chrome/Default/Preferences

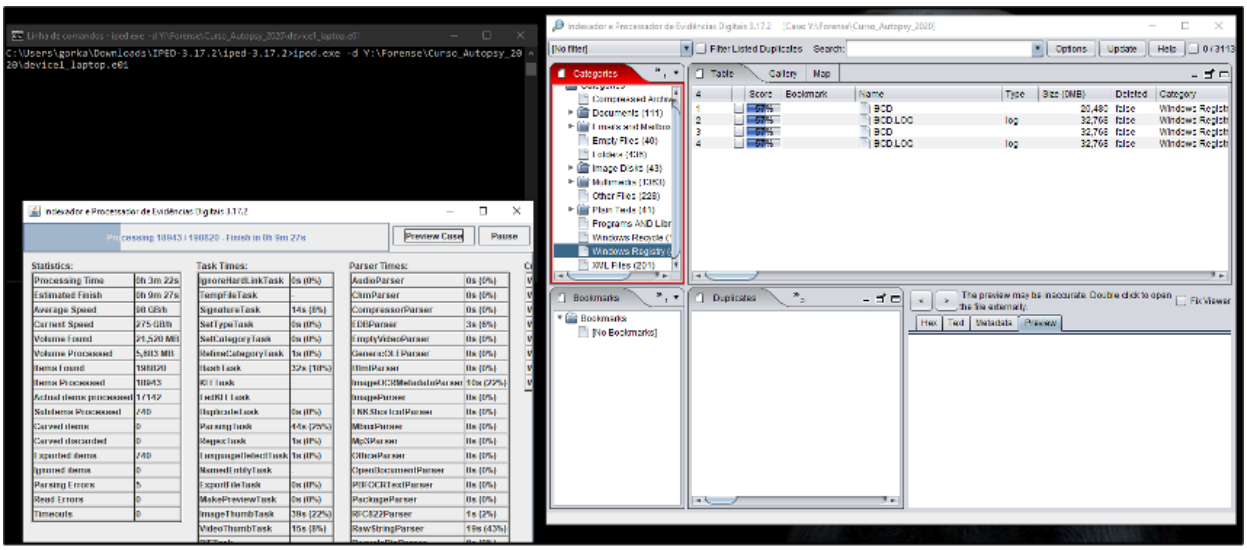
Rysunek 70 - Lokalizacja informacji o przeglądarce Google Chrome

6. Analiza kryminalistyczna z bezpłatnymi pakietami

Analiza kryminalistyczna wymaga znajomości konkretnych narzędzi, które potrafią uzyskać i przetworzyć pożądane przez nas informacje. Wiele z nich to narzędzia komercyjne, takie jak między innymi OpenText EnCase, AccessData FTK, Magnet Axiom. W przypadku narzędzi darmowych sytuacja jest zgoła odmienna, gdyż dostępnych do użytku jest bardzo niewiele pakietów analitycznych. W ten sposób skupimy się na 2 takich pakietach, IPED i Autopsy The Sleuth Kit.

6.1. IPED

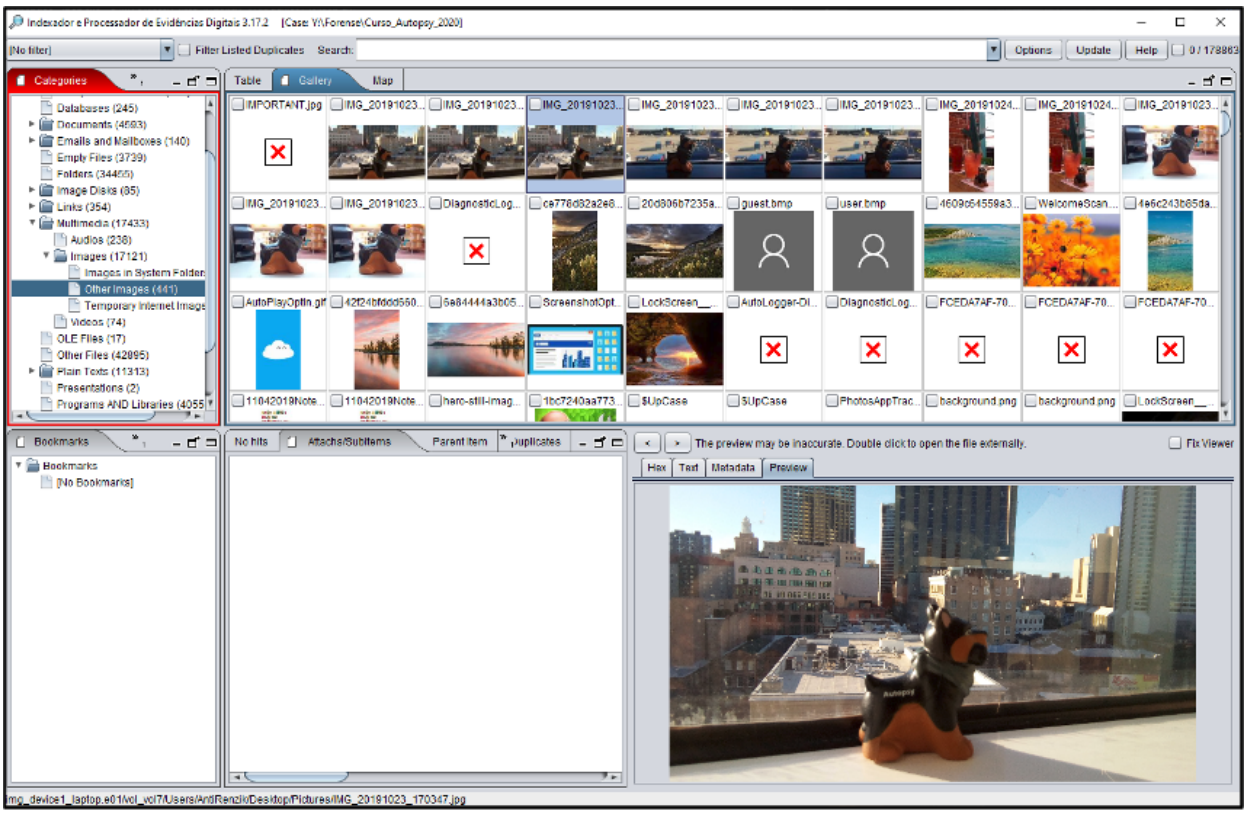
IPED - Indexer and Digital Evidence Processor to narzędzie open source, opracowane w Javie przez brazylijską policję federalną zajmującą się kryminalistyką śledczą, znane z dobrej wydajności przetwarzania (Rysunek 71. Zostało ono opracowane w celu umożliwienia analizy dużych ilości danych przez dużą liczbę osób, gdyż celowo zostało stworzone na potrzeby śledztwa w sprawie operacji Lava Jato w Brazylii. Wysoka wydajność wielowątkowa do 400GB/h prędkości przetwarzania umożliwia wsparcie dla dużych spraw z dużą ilością danych do przetworzenia.



Rysunek 71 - Przetwarzanie za pomocą IPED

https://github.com/sepinf-inc/IPED

Jest to oprogramowanie, które mimo prostego i intuicyjnego wyglądu wymaga pewnej wiedzy w jego obsłudze, co widać na Rysunku 72.



Rysunek 72 - Analiza z IPED

Źródło: https://github.com/sepinf-inc/IPED/wiki/Beginner's-Start-Guide

https://servicos.dpf.gov.br/ferramentas/IPED/

6.2. Zestaw The Sleuth

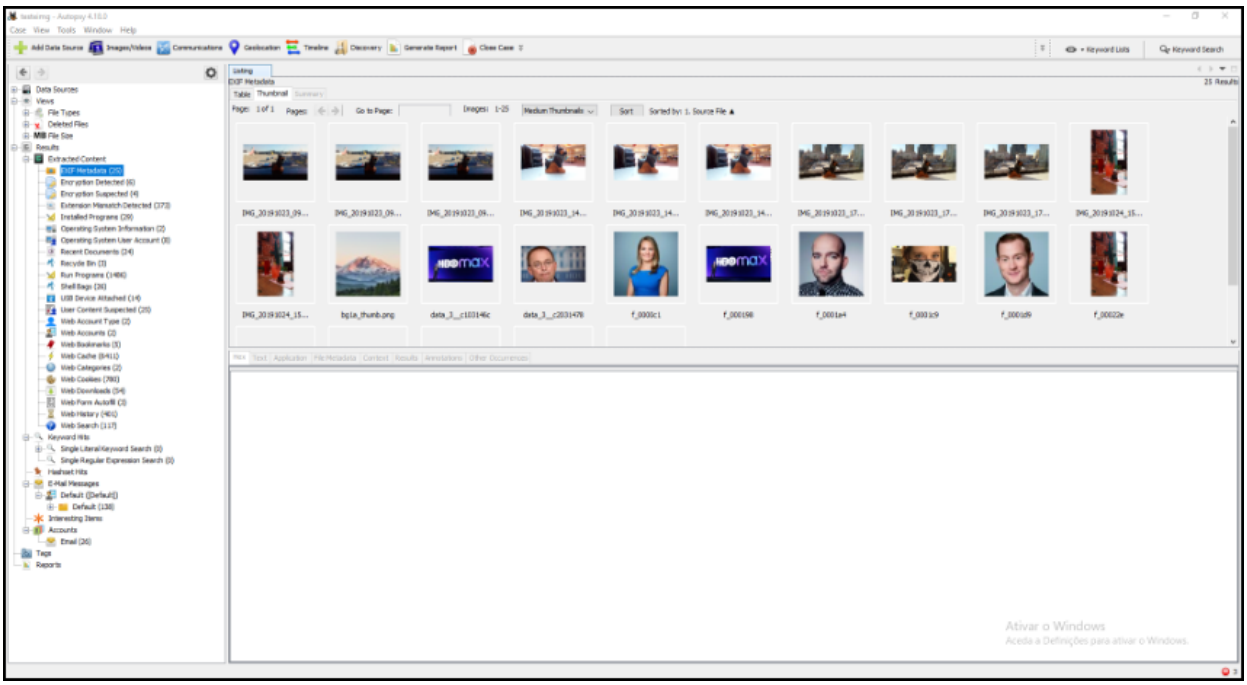
Sleuth Kit® to biblioteka, a także zestaw narzędzi, które pozwalają na analizę systemów plików FAT, NTFS, Ext2/3/4 i UFS, w tym powszechnie wykorzystywanych przez system operacyjny Linux, pozwala także na analizę plików i folderów, odzyskiwanie usuniętych plików, tworzenie *osi czasu* aktywności plików, wykonywanie wyszukiwań ekspresyjnych oraz korzystanie z baz *haseł*.

https://github.com/sleuthkit/sleuthkit/blob/develop/NEWS.txt

Autopsy - Autopsy to graficzny interfejs użytkownika (GUI) programu The Sleuth Kit. Jest to jedna z platform open source, opracowana w celu wykorzystania możliwości The Sleuth Kit do przeprowadzania analizy kryminalistycznej na urządzeniach takich jak m.in. dyski twarde, karty multimedialne, smartfony. Integruje również inne narzędzia kryminalistyczne, zarówno open source i/lub komercyjne, poprzez wtyczki lub komplementarne moduły w języku Java lub Python....

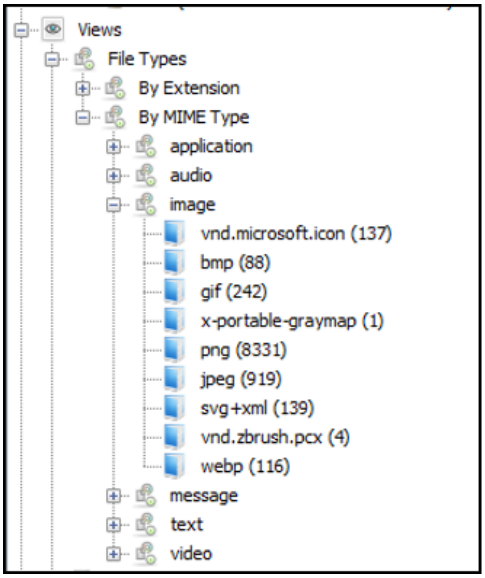
https://github.com/sleuthkit/autopsy/blob/develop/NEWS.txt

Prezentowany jest prosty interfejs graficzny programu Autopsy (Rysunek 73).



Rysunek 73 - Analiza z Autopsy

Zawiera lewe menu ze skategoryzowanymi informacjami, identyfikującymi pliki według typu rozszerzenia i typu MIME, ale także wszystkich kategorii, do których należą (- Categorisation of files in Autopsy Rysunek 74).



Rysunek 74- Kategoryzacja plików w Autopsy

Wersje

https://github.com/sleuthkit/autopsy/releases/

Kod źródłowy

https://github.com/sleuthkit/autopsy

Zadania i wnioski

https://github.com/sleuthkit/autopsy/issues