

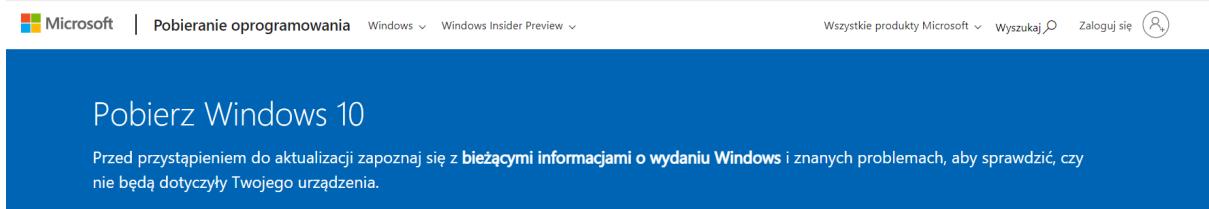
Szymon Kozioł

# PROJEKT

## Część I

1)

Zdecydowałem się na użycie VirtualBoxa, a system na który postawiłem to Windows 10 Pro.



The screenshot shows the Microsoft download page for Windows 10. At the top, there are navigation links for Microsoft products, search, and sign-in. Below that, a large blue button labeled "Pobierz Windows 10" is prominently displayed. A subtext below the button reads: "Przed przystąpieniem do aktualizacji zapoznaj się z **bieżącyimi informacjami o wydaniu Windows** i znanych problemach, aby sprawdzić, czy nie będą dotyczyć Twojego urządzenia." To the right of the main content area, there is a small image of a laptop displaying the Windows 10 desktop interface.

Chcesz zainstalować system Windows 10 na swoim komputerze?

Aby rozpocząć, przede wszystkim musisz mieć licencję na zainstalowanie systemu Windows 10. Następnie możesz pobrać i uruchomić narzędzie do tworzenia multimedialów. Jeśli chcesz się dowiedzieć, jak korzystać z narzędzia, zobacz poniższe instrukcje.

[Pobierz narzędzie](#)



Prywatność

 [Korzystanie z narzędzia w celu uaktualnienia tego komputera do systemu Windows 10 \(kliknij, aby wyświetlić mniej lub więcej informacji\)](#)

 [Tworzenie za pomocą tego narzędzia nośnika instalacyjnego \(dysku flash USB, DVD lub pliku ISO\) w celu zainstalowania systemu Windows 10 na innym komputerze \(kliknij, aby wyświetlić więcej lub mniej informacji\)](#)

Instalacja przebiegła pomyślnie. Zdecydowałem się wydzielić 8GB pamięci RAM oraz 20GB dysku.

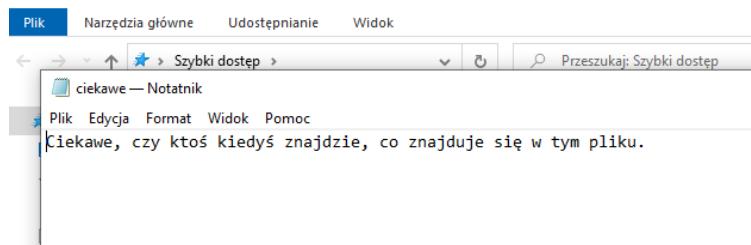
The screenshot shows the Oracle VM VirtualBox Manager interface. At the top, there are four icons: 'Nowa' (New), 'Ustawienia' (Settings), 'Odrzuć' (Reject), and 'Uruchom' (Start). Below these are two main sections: 'Ogólne' (General) and 'Podgląd' (Preview). The 'Ogólne' section displays the VM name as 'Windows 10' and the operating system as 'Windows 10 (64-bit)'. The 'System' section provides details about RAM (8192 MB), processors (2), boot order (Floppy, Optical drive, Hard disk), acceleration (VT-x/AMD-V, Nested Paging, Paravirtualization, Hyper-V), and network适配器 (VBoxNetAdp). The 'Ekran' section shows video memory (128 MB) and graphics controller (VBoxSVGA). The 'Pamięć' section lists the memory controller (SATA) and two drives: Port SATA 0 (Windows 10.vhd, 20,00 GB) and Port SATA 1 (Optical drive Win10\_22H2\_Polish\_x64v1.iso, 5,62 GB). On the right, a preview window shows a dark Windows desktop environment.

2)

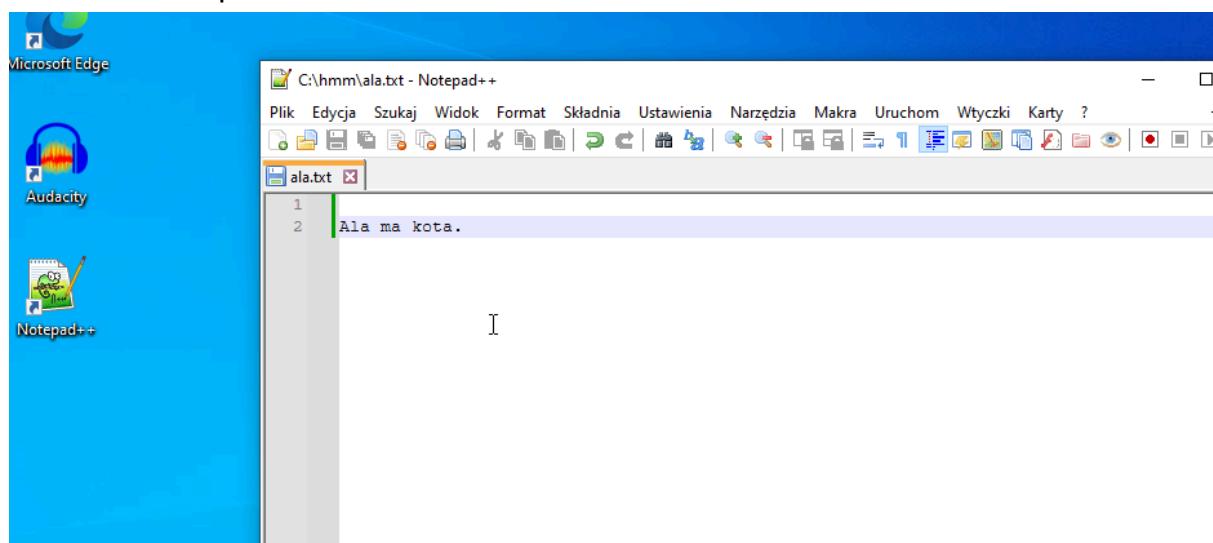
Pobrałem program Audacity:



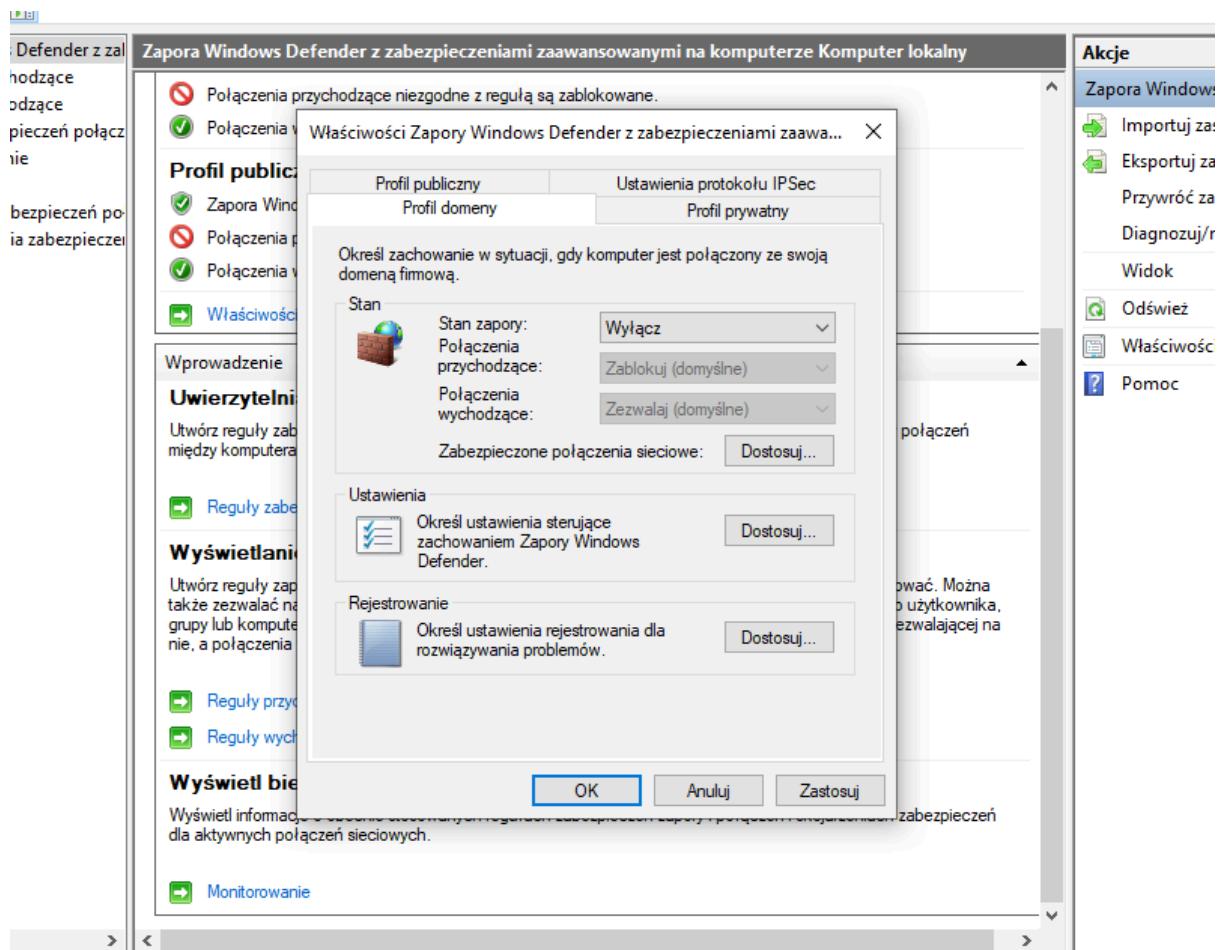
Stworzyłem kilka plików .txt, które poukrywałem w systemie w ramach "easter egg'ów":



Pobrałem Notepad++:



Zmieniłem ustawienia firewall'a:



łaczenia przychodzące niezgodne z regułą są zablokowane.

### Właściwości Zapory Windows Defender z zabezpieczeniami zaawansowanymi

publiczny

porta Windo

łaczenia p

łaczenia v

aściwości

dzenie

zycieli

eguły zab

omputera

guły zabe

ietlani

eguły zap

zwalać na

komputer

łaczenia

guły przy

guły wych

ietl bie

l informac

vnych połączeni

Właściwości Zapory Windows Defender z zabezpieczeniami zaawansowanymi

Profil publiczny      Ustawienia protokołu IPSec

Profil domeny      Profil prywatny

Określ zachowanie w sytuacji, gdy komputer jest połączony z lokalizacją w sieci prywatnej.

Stan

Stan zapory: Wyłącz  
Połączenia przychodzące: Zablokuj (domyślne)  
Połączenia wychodzące: Zezwalaj (domyślne)  
Zabezpieczone połączenia sieciowe: Dostosuj...

Ustawienia

Określ ustawienia sterujące zachowaniem Zapory Windows Defender. Dostosuj...

Rejestrowanie

Określ ustawienia rejestrowania dla rozwiązywania problemów. Dostosuj...

OK

Anuluj

Zastosuj



Zapora Windows Defender z zabezpieczeniami zaawansowanymi zapewnia zabezpieczenia sieciowe komputerom z systemem Windows.

#### Przegląd

##### Profil domeny

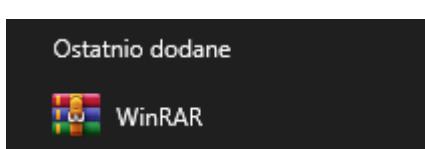
Zapora Windows Defender jest wyłączona.

##### Profil prywatny

Zapora Windows Defender jest wyłączona.

Wchodziłem na strony, które mogą świadczyć o tym, że użytkownik interesuje się sportem.

Pobrałem zdjęcie z przeglądarki i ustawiłem je jako tło pulpitu.



Zainstalowałem WinRAR, tworząc przy tym folder “Tajne dane”, do którego mam zamiar umieścić część zdjęć i pdf’ów, a następnie utworzyć jego kopię i spakować go do archiwum z ciekawym rozszerzeniem.

# Windows Update



## Wymagane ponowne uruchomienie

Twoje urządzenie zostanie uruchomione ponownie poza godzinami aktywnego użytkowania.

Na Twoim urządzeniu brakuje ważnych poprawek związanych zabezpieczeniami i jakością.

Narzędzie Windows do usuwania złośliwego oprogramowania dla komputerów z procesorem x64 — v5.120 (KB890830)

**Stan:** Oczekiwanie na pobranie

2024-01 Aktualizacja zbiorcza dotycząca środowiska .NET Framework 3.5, 4.8 i 4.8.1 dla systemu Windows 10 Version 22H2 opartego na architekturze x64 (KB5034275)

**Stan:** Oczekiwanie na pobranie

2024-01 Aktualizacja zbiorcza dla systemu Windows 10 Version 22H2 dla systemów opartych na architekturze x64 (KB5034122)

**Stan:** Oczekiwanie na pobranie

Program Microsoft .NET Framework 4.8.1 dla systemu Windows 10 Version 22H2 dla systemów opartych na procesorze x64 (KB5011048)

**Stan:** Oczekiwanie na ponowne uruchomienie

Aktualizacja platformy ochrony przez złośliwym kodem Windows Defender Antivirus — KB4052623 (wersja 4.18.2001.10)

**Stan:** Oczekiwanie na pobranie

Po jakimś czasie pojawiły się dostępne aktualizacje. Zaktualizowałem system.



Pobrałem archiwum z dodatkowymi plikami.

Tajne dane

Narzędzia główne Udstępianie Widok

Przeszukaj: Tajne dane

	Nazwa	Data modyfikacji	Typ	Rozmiar
Symbol dostępu	<a href="#">Prawo_indukcji_elektromagnetycznej_Far...</a>	27.11.2023 17:59	Microsoft Edge P...	812 KB
Pulpit	<a href="#">README</a>	11.01.2019 07:35	Dokument tekstowy	1 KB
Pobrane	<a href="#">Zestaw_3.doc</a>	23.10.2023 16:05	Plik DOC	32 KB
Dokumenty				
Obrazy				

Przeniosłem je do różnych lokalizacji.

główne Udstępianie Widok

Przeszukaj: nauka

	Nazwa	Data modyfikacji	Typ	Rozmiar
Symbol dostępu	<a href="#">ekstremaschemat</a>	23.04.2023 13:27	Archiwum WinRA...	205 KB
Pulpit	<a href="#">hesjany</a>	23.04.2023 13:27	Archiwum WinRA...	77 KB
Pobrane	<a href="#">01_badanie_zjawiska_halla</a>	30.10.2023 18:56	Microsoft Edge P...	403 KB
Dokumenty	<a href="#">4 Szyfry asymetryczne</a>	30.08.2023 11:36	Microsoft Edge P...	927 KB
Obrazy				

glaszne główne Udstępianie Widok Narzędzia obrazów

Przeszukaj: Moje zdjęcia

	Nazwa	Data modyfikacji	Typ	Rozmiar
Symbol dostępu		IMG_20230922_18	Microsoft Edge P...	4112
Pulpit		IMG_20230924_13	Microsoft Edge P...	2043
Pobrane		IMG_20220812_14	Microsoft Edge P...	0021
Dokumenty		IMG_20220813_14	Microsoft Edge P...	0733
Obrazy		IMG_20230222_13	Microsoft Edge P...	4010
Symbol dostępu		IMG_20231019_15	Microsoft Edge P...	1641
Pulpit		IMG_20230925_09	Microsoft Edge P...	1420
Pobrane				
Dokumenty				
Obrazy				

3D

Pousuwałem parę plików, przykładowo:

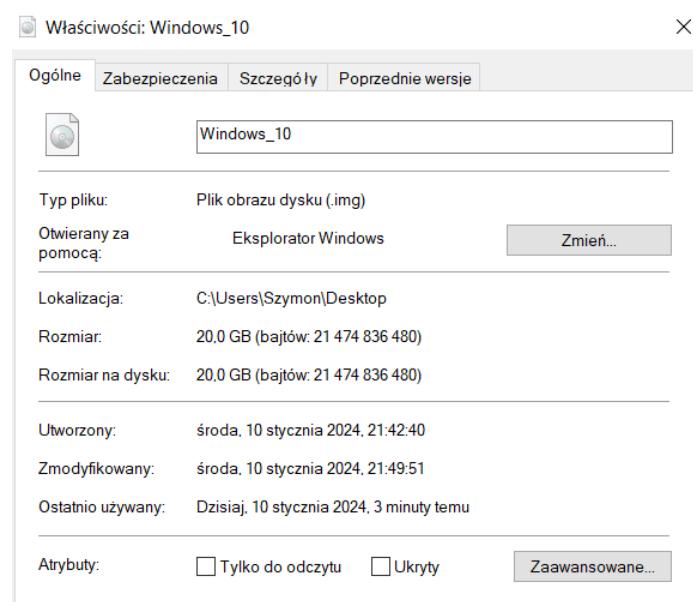
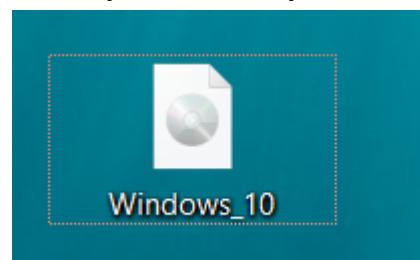
	Nazwa	Lokalizacja oryginalna	Data usunięcia
stęp	ok	C:\Users\Projekt\Documents	10.01.2024 21:16
entv	reducta	C:\Users\Projekt\Downloads	10.01.2024 21:18

Wszystko działało się na przestrzeni ok. miesiąca. Pobrane pliki, historia przeglądarki, pliki użytkownika świadczą o jego zainteresowaniach i w pewnym stopniu o sytuacji życiowej.

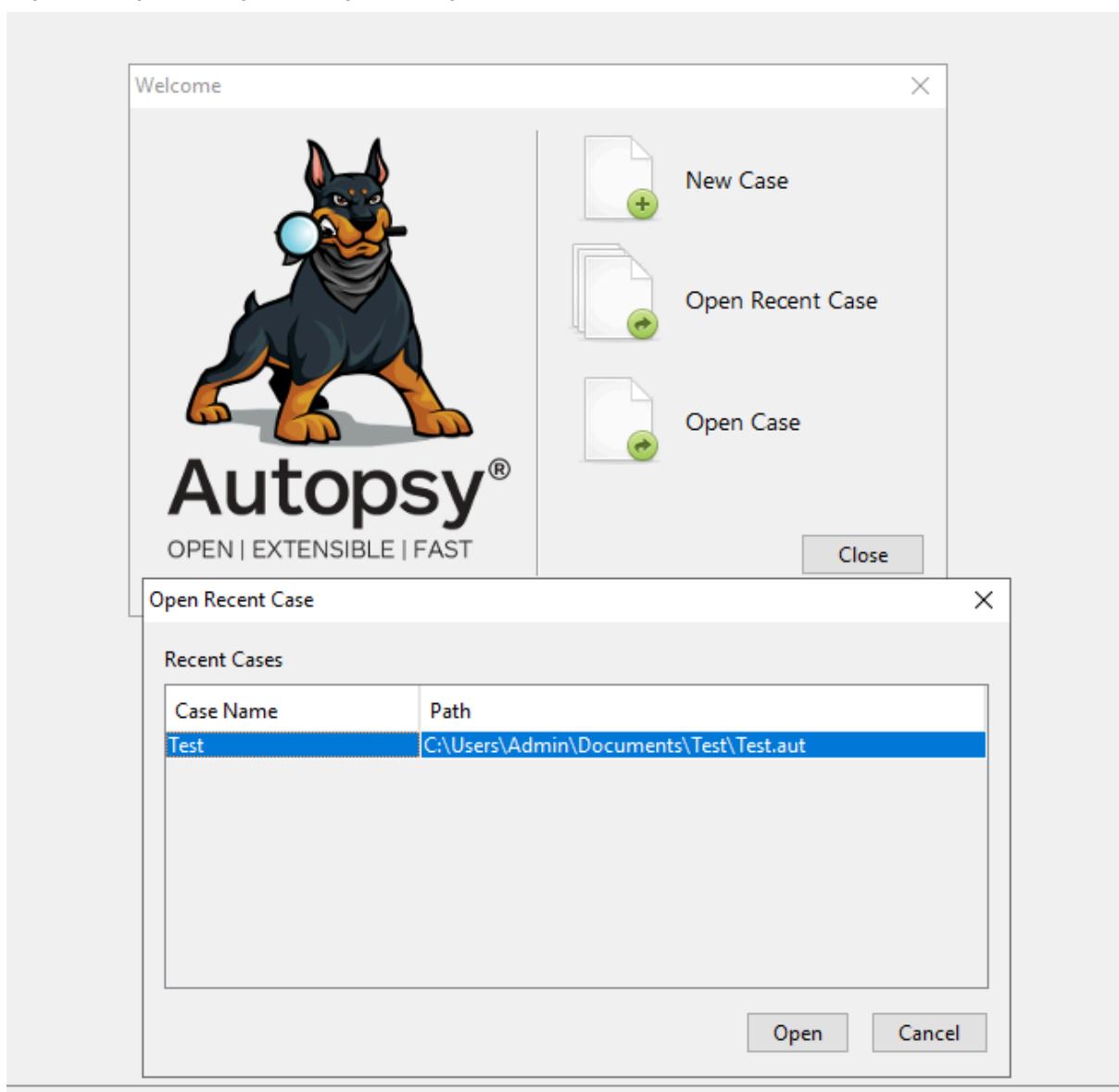
### 3)

```
C:\Program Files\Oracle\VirtualBox>VBoxManage.exe clonehd "c:\Users\Szymon\VirtualBox VMs\Windows 10\Windows 10.vhd" "C:\Users\Szymon\Desktop\Windows_10.img" --format raw
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'raw'. UUID: 066e618a-7589-43a9-9c67-fe4405b4b371
```

Stworzyłem obraz systemu.



4) & 5) & 6) & 7) & 8)



W ramach testu wrzuciłem swój obraz do Autopsy.

Screenshot of the Autopsy 4.21.0 forensic analysis tool interface. The left sidebar shows a tree view of 'Data Sources' under 'Windows\_10img.1 Host'. The main pane displays a table titled 'my\_windows\_10img\you\your\users\projekt\pictures\moje zdjęcia' with columns: Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. The table lists several image files (e.g., IMG\_20220812\_140021.jpg, IMG\_20230924\_13043.jpg) with their respective details. Below the table is a preview area showing a photograph of a canal scene in Venice.

Znalazłem swoje, zdjęcia, historie przeglądarki, pobrane pliki, czy zainstalowane programy. W dużym skrócie - znajduje się tam wszystko co powinno. Obraz został zgrany poprawnie.

Screenshot of the Autopsy 4.21.0 forensic analysis tool interface. The left sidebar shows a tree view of 'Data Sources' under 'Windows\_10img.1 Host'. The main pane displays a table titled 'Listing' with columns: Source Name, S, C, O, URL, Date Accessed, Referrer URL, and Title. The table lists numerous browser history entries for Microsoft Edge, including search queries like 'audacity - Wyszukaj' and 'audacity | Free Audio editor, recorder, mixer'. Below the table is a preview area showing a photograph of a canal scene in Venice.

Teraz zimportuje obraz systemu kolegi:

Welcome

X



**Autopsy®**

OPEN | EXTENSIBLE | FAST



New Case



Open Recent Case



Open Case

Close



New Case Information

X

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type:  Single-User  Multi-User

Case data will be stored in the following directory:

< Back

Next >

Finish

Cancel

Help

 New Case Information X

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number:

Examiner

Name: Sz

Phone:

Email:

Notes: Projekt

Organization

Organization analysis is being done for: Not Specified

 Add Data Source X

**Steps**

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

**Select Data Source**

Path:

Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Po wykonaniu wszystkich kroków mogę zacząć analizę obrazu.

# ANALIZA OBRAZU:

Jeżeli chodzi o historię przeglądarki to łatwo wywnioskować następujące informacje:

History	1	<a href="https://dev.to/gamegods3/how-to-install-gcc-in-win...">https://dev.to/gamegods3/how-to-install-gcc-in-win...</a>	2023-12-27 17:39:17 CET	<a href="https://dev.to/gamegods3/how-to-install-gcc-in-win...">https://dev.to/gamegods3/how-to-install-gcc-in-win...</a>	GCC for Windows: How to install gcc in Wi...
History	1	<a href="https://sourceforge.net/projects/mingw/files/Installer...">https://sourceforge.net/projects/mingw/files/Installer...</a>	2023-12-27 17:39:02 CET	<a href="https://sourceforge.net/projects/mingw/files/Installer...">https://sourceforge.net/projects/mingw/files/Installer...</a>	Download mingw-get-setup.exe (MinGW -
History	1	<a href="https://sourceforge.net/projects/mingw/postdownload">https://sourceforge.net/projects/mingw/postdownload</a>	2023-12-27 17:38:59 CET	<a href="https://sourceforge.net/projects/mingw/postdownload">https://sourceforge.net/projects/mingw/postdownload</a>	Find out more about MinGW - Minimalist (
History	2	<a href="https://www.google.com/search?q=cpp+programming...">https://www.google.com/search?q=cpp+programming...</a>	2023-12-27 17:51:30 CET	<a href="https://www.google.com/search?q=cpp+programing...">https://www.google.com/search?q=cpp+programing...</a>	cpp programing wxmaps - Szukaj w Goog
History	2	<a href="https://www.google.com/search?q=cpp+programming...">https://www.google.com/search?q=cpp+programming...</a>	2023-12-27 17:51:39 CET	<a href="https://www.google.com/search?q=cpp+programing...">https://www.google.com/search?q=cpp+programing...</a>	cpp programing examples - Szukaj w Goog
History	1	<a href="https://www.programiz.com/cpp-programming/exa...">https://www.programiz.com/cpp-programming/exa...</a>	2023-12-27 17:51:42 CET	<a href="https://www.programiz.com/cpp-programming/exa...">https://www.programiz.com/cpp-programming/exa...</a>	C++ Examples   Programiz
History	1	<a href="https://www.programiz.com/cpp-programming/exa...">https://www.programiz.com/cpp-programming/exa...</a>	2023-12-27 17:51:50 CET	<a href="https://www.programiz.com/cpp-programming/exa...">https://www.programiz.com/cpp-programming/exa...</a>	C++ Programs To Print Triangle, Pyramid, I
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://www.programiz.com/cpp-programming/exa...">https://www.programiz.com/cpp-programming/exa...</a>	2023-12-28 13:00:48 CET	<a href="https://www.programiz.com/cpp-programming/exa...">https://www.programiz.com/cpp-programming/exa...</a>	C++ Program to Add Two Numbers
History	2	<a href="https://www.google.com/search?q=yt&amp;oq=yt&amp;gs_icr...">https://www.google.com/search?q=yt&amp;oq=yt&amp;gs_icr...</a>	2023-12-28 13:04:49 CET	<a href="https://www.google.com/search?q=yt&amp;oq=yt&amp;gs_icr...">https://www.google.com/search?q=yt&amp;oq=yt&amp;gs_icr...</a>	yt - Szukaj w Google
History	1	<a href="https://www.youtube.com/?hl=pl&amp;gl=PL">https://www.youtube.com/?hl=pl&amp;gl=PL</a>	2023-12-28 13:04:51 CET	<a href="https://www.youtube.com/?hl=pl&amp;gl=PL">https://www.youtube.com/?hl=pl&amp;gl=PL</a>	YouTube
History	1	<a href="https://www.youtube.com/">https://www.youtube.com/</a>	2023-12-28 13:05:02 CET	<a href="https://www.youtube.com/">https://www.youtube.com/</a>	YouTube
History	1	<a href="https://www.programiz.com/cpp-programming/onlin...">https://www.programiz.com/cpp-programming/onlin...</a>	2023-12-28 13:05:50 CET	<a href="https://www.programiz.com/cpp-programming/onlin...">https://www.programiz.com/cpp-programming/onlin...</a>	Online C++ Compiler
History	2	<a href="https://www.google.com/search?q=unsplash&amp;oq=un...">https://www.google.com/search?q=unsplash&amp;oq=un...</a>	2023-12-28 13:06:45 CET	<a href="https://www.google.com/search?q=unsplash&amp;oq=un...">https://www.google.com/search?q=unsplash&amp;oq=un...</a>	unsplash - Szukaj w Google
History	1	<a href="https://unsplash.com/photos/a-bottle-of-soap-next-t...">https://unsplash.com/photos/a-bottle-of-soap-next-t...</a>	2023-12-28 13:06:51 CET	<a href="https://unsplash.com/photos/a-bottle-of-soap-next-t...">https://unsplash.com/photos/a-bottle-of-soap-next-t...</a>	A bottle of soap next to a dish of soap on a
History	1	<a href="https://unsplash.com/photos/cwbP8HqGkU0">https://unsplash.com/photos/cwbP8HqGkU0</a>	2023-12-28 13:07:02 CET	<a href="https://unsplash.com/photos/cwbP8HqGkU0">https://unsplash.com/photos/cwbP8HqGkU0</a>	Beautiful Free Images & Pictures   Unsplash

Użytkownik interesuje się programowaniem (Język C++), pobrał edytor tekstu VisualStudioCode.

History	2	<a href="https://www.google.com/search?q=snapdrop&amp;oq=sn...">https://www.google.com/search?q=snapdrop&amp;oq=sn...</a>	2024-01-06 18:25:56 CET	<a href="https://www.google.com/search?q=snapdrop&amp;oq=sn...">https://www.google.com/search?q=snapdrop&amp;oq=sn...</a>	snapdrop - Szukaj w Google
History	2	<a href="https://snapdrop.net/">https://snapdrop.net/</a>	2024-01-06 18:14:45 CET	<a href="https://snapdrop.net/">https://snapdrop.net/</a>	Snapdrop
History	2	<a href="https://www.google.com/search?q=windows+how+to...">https://www.google.com/search?q=windows+how+to...</a>	2024-01-06 18:57:17 CET	<a href="https://www.google.com/search?q=windows+how+to...">https://www.google.com/search?q=windows+how+to...</a>	windows how to checksu - Szukaj w Google
History	2	<a href="https://www.google.com/search?q=windows+how+to...">https://www.google.com/search?q=windows+how+to...</a>	2024-01-06 18:57:17 CET	<a href="https://www.google.com/search?q=windows+how+to...">https://www.google.com/search?q=windows+how+to...</a>	windows how to chekcsu - Szukaj w Google

Prawdopodobnie udostępniał pliki za pomocą snapdropa.

History	2	<a href="https://www.google.com/search?q=unsplash&amp;oq=un...">https://www.google.com/search?q=unsplash&amp;oq=un...</a>	2023-12-25 20:00:50 CET	<a href="https://www.google.com/search?q=unsplash&amp;oq=un...">https://www.google.com/search?q=unsplash&amp;oq=un...</a>	unsplash - Szukaj w Google
History	2	<a href="https://www.google.com/search?q=unsplash&amp;oq=un...">https://www.google.com/search?q=unsplash&amp;oq=un...</a>	2023-12-25 20:00:50 CET	<a href="https://www.google.com/search?q=unsplash&amp;oq=un...">https://www.google.com/search?q=unsplash&amp;oq=un...</a>	unsplash - Szukaj w Google
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/photos/a-large-fire-at-night-H...">https://unsplash.com/photos/a-large-fire-at-night-H...</a>	2023-12-25 20:00:59 CET	<a href="https://unsplash.com/photos/a-large-fire-at-night-H...">https://unsplash.com/photos/a-large-fire-at-night-H...</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/photos/a-man-standing-in-a-c...">https://unsplash.com/photos/a-man-standing-in-a-c...</a>	2023-12-25 20:01:04 CET	<a href="https://unsplash.com/photos/a-man-standing-in-a-c...">https://unsplash.com/photos/a-man-standing-in-a-c...</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/photos/a-small-dog-wearing-a...">https://unsplash.com/photos/a-small-dog-wearing-a...</a>	2023-12-25 20:01:10 CET	<a href="https://unsplash.com/photos/a-small-dog-wearing-a...">https://unsplash.com/photos/a-small-dog-wearing-a...</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/modal=%5B%22Login%22%2C%22...">https://unsplash.com/modal=%5B%22Login%22%2C%22%2C..."&gt;https://unsplash.com/modal=%5B%22Login%22%2C%22%2C...</a>	2023-12-25 20:01:17 CET	<a href="https://unsplash.com/modal=%5B%22Login%22%2C%22%2C...">https://unsplash.com/modal=%5B%22Login%22%2C%22%2C...</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/">https://unsplash.com/</a>	2023-12-28 13:07:09 CET	<a href="https://unsplash.com/">https://unsplash.com/</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/photos/a-snowy-landscape-wit...">https://unsplash.com/photos/a-snowy-landscape-wit...</a>	2023-12-25 20:01:25 CET	<a href="https://unsplash.com/photos/a-snowy-landscape-wit...">https://unsplash.com/photos/a-snowy-landscape-wit...</a>	A snowy landscape with christmas trees and
History	1	<a href="https://unsplash.com/photos/a-snow-covered-path-i...">https://unsplash.com/photos/a-snow-covered-path-i...</a>	2023-12-25 20:01:24 CET	<a href="https://unsplash.com/photos/a-snow-covered-path-i...">https://unsplash.com/photos/a-snow-covered-path-i...</a>	Beautiful Free Images & Pictures   Unsplash
History	1	<a href="https://unsplash.com/photos/a-snowy-landscape-wit...">https://unsplash.com/photos/a-snowy-landscape-wit...</a>	2023-12-25 20:01:25 CET	<a href="https://unsplash.com/photos/a-snowy-landscape-wit...">https://unsplash.com/photos/a-snowy-landscape-wit...</a>	A snowy landscape with christmas trees and

Szukał ciekawych zdjęć na unsplash.com

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
⌚ History				google.com	windows 10sss	Google Chrome	2023-12-27 17:37:23 CET	Windows_10.img
⌚ History				google.com	installing gcc windows 10	Google Chrome	2023-12-27 17:37:44 CET	Windows_10.img
⌚ History				google.com	installing gcc windows 10	Google Chrome	2023-12-27 17:37:44 CET	Windows_10.img
⌚ History				google.com	cpp programing wxmaplw	Google Chrome	2023-12-27 17:51:30 CET	Windows_10.img
⌚ History				google.com	cpp programing wxmaplw	Google Chrome	2023-12-27 17:51:30 CET	Windows_10.img
⌚ History				google.com	cpp programing examples	Google Chrome	2023-12-27 17:51:30 CET	Windows_10.img
⌚ History				google.com	cpp programing examples	Google Chrome	2023-12-27 17:51:39 CET	Windows_10.img
⌚ History				google.com	cpp programing examples	Google Chrome	2023-12-28 13:00:32 CET	Windows_10.img
⌚ History				google.com	cpp programing examples	Google Chrome	2023-12-28 13:00:32 CET	Windows_10.img
⌚ History				google.com	yt	Google Chrome	2023-12-28 13:04:49 CET	Windows_10.img
⌚ History				google.com	yt	Google Chrome	2023-12-28 13:04:49 CET	Windows_10.img
⌚ History				google.com	unsplash	Google Chrome	2023-12-28 13:06:45 CET	Windows_10.img
⌚ History				google.com	unsplash	Google Chrome	2023-12-28 13:06:45 CET	Windows_10.img
⌚ History				google.com	wireshark	Google Chrome	2024-01-06 17:46:56 CET	Windows_10.img
⌚ History				google.com	wireshark	Google Chrome	2024-01-06 17:46:56 CET	Windows_10.img
⌚ History				google.com	snapdrop	Google Chrome	2024-01-06 18:25:56 CET	Windows_10.img
⌚ History				google.com	snapdrop	Google Chrome	2024-01-06 18:25:56 CET	Windows_10.img
⌚ History				google.com	windows how to checksu	Google Chrome	2024-01-06 18:57:17 CET	Windows_10.img
⌚ History				google.com	windows how to checksu	Google Chrome	2024-01-06 18:57:17 CET	Windows_10.img
⌚ History				ooale.com	virustotal	Goole Chrome	2024-01-06 18:58:32 CET	Windows_10.img

Wyszukiwania zdają się potwierdzać te wnioski.

⌚ Cookies	2	.google.com	2024-01-08 18:14:30 CET	AEC	Google Chrome	google.com	Default
⌚ Cookies	2	.google.com	2024-01-08 18:14:34 CET	SNID	Google Chrome	google.com	Default
⌚ Cookies	2	.notepad-plus-plus.org	2024-01-08 18:13:30 CET	_ga	Google Chrome	notepad-plus-plus.org	Default
⌚ Cookies	2	.notepad-plus-plus.org	2024-01-08 18:13:52 CET	_ga_06CVYXZPHS	Google Chrome	notepad-plus-plus.org	Default
⌚ Cookies	2	www.google.com	2024-01-08 18:14:37 CET	DV	Google Chrome	www.google.com	Default
⌚ Cookies	2	.google.com	2024-01-08 18:14:35 CET	NID	Google Chrome	google.com	Default
⌚ Cookies	2	.msn.com	2023-12-25 20:05:23 CET	MUID	Microsoft Edge	msn.com	Default
⌚ Cookies	2	assets.msn.com	2023-12-25 20:05:24 CET	MUIDB	Microsoft Edge	assets.msn.com	Default
⌚ Cookies	2	ntp.msn.com	2023-12-25 20:05:23 CET	MUIDB	Microsoft Edge	ntp.msn.com	Default
⌚ Cookies	2	.msn.com	2023-12-25 20:05:23 CET	_EDGE_V	Microsoft Edge	msn.com	Default
⌚ Cookies	2	.msn.com	2023-12-25 20:05:23 CET	_SS	Microsoft Edge	msn.com	Default
⌚ Cookies	2	.bing.com	2024-01-08 18:13:26 CET	MUID	Microsoft Edge	bing.com	Default
⌚ Cookies	2	www2.bing.com	2023-12-22 15:30:24 CET	MUIDB	Microsoft Edge	www2.bing.com	Default
⌚ Cookies	2	.bing.com	2024-01-08 18:13:26 CET	SRCHD	Microsoft Edge	bing.com	Default
⌚ Cookies	2	.bing.com	2024-01-08 18:13:26 CET	SRCHUID	Microsoft Edge	bing.com	Default
⌚ Cookies	2	.bing.com	2024-01-08 18:13:26 CET	SRCHUSR	Microsoft Edge	bing.com	Default

Użytkownik korzystał z dwóch przeglądarek: Google Chrome oraz Microsoft Edge.

Listing  
USB Device Attached

Table | Thumbnail | Summary | Save Table as CSV

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM		0		2024-01-08 19:12:25 CET		ROOT_HUB30	4&24054718&0&0	Windows_10.img
SYSTEM		0		2024-01-08 19:12:25 CET	VirtualBox	USB Tablet	5&12c8f4c08&0&1	Windows_10.img

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 2 of 2 Result ↶ ↷ USB Device Attached

Type	Value	Source(s)
Date/Time	2024-01-08 19:12:25 CET	Recent Activity
Device Make	VirtualBox	Recent Activity
Device Model	USB Tablet	Recent Activity
Device ID	5&12c8f4c08&0&1	Recent Activity
Source File Path	/img_Windows_10.img/vol_vo13/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775701	

System został postawiony za pomocą VirtualBox'a.

Source Name	S	C	O	Name	Program Name	Processor Architecture
Windows_10.img				DESKTOP-NJH985J	Windows 10 Pro	AMD64

Był to system Windows 10 Pro, komputer posiadał procesor AMD64.

Jeżeli chodzi o zainstalowane programy to system posiadał m. in. najnowszą na tamten moment wersję programu Wireshark.

SOFTWARE	1	WIC	2019-12-07 09:17:28 CET	Windows_10.img
SOFTWARE	0	Google Chrome v.120.0.6099.199	2024-01-06 17:10:01 CET	Windows_10.img
SOFTWARE	0	Wireshark 4.2.2 x64 v.4.2.2	2024-01-06 16:52:05 CET	Windows_10.img
SOFTWARE	0	Npcap v.1.78	2024-01-06 16:50:15 CET	Windows_10.img
SOFTWARE	0	Microsoft Visual C++ 2015-2022 Redistributable (x64) - ...	2024-01-06 16:47:58 CET	Windows_10.img

Ostatnią zainstalowaną aplikacją był Notepad++

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE		0		Notepad++ (64-bit x64) v.8.6.1	2024-01-08 17:13:52 CET	Windows_10.img
SOFTWARE		0		USBPcap 1.5.4.0 v.1.5.4.0	2024-01-06 16:51:10 CET	Windows_10.img

Source Name	S	C	O	Path	User ID	Domain	Short Cut	Name	Username	Program Name	Data Source
Local State				Default				Profile 1	Profile 1	Microsoft Edge	Windows_10.img
Local State				Default				Osoba 1	Osoba 1	Google Chrome	Windows_10.img

Utworzone zostały dwa profile dla przeglądarek.

Profile 1 - dla Microsoft Edge

Osoba 1 - dla Google Chrome

Pliki o rozmiarze 50-200MB:

Listing 50 - 200MB											
Table <a href="#">Thumbnail</a> <a href="#">Summary</a>											
Page: 1 of 1 Pages: < > Go to Page: <input type="text"/>				Save Table as CSV							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met)	
Edge.wim				2023-05-05 14:24:37 CEST	2024-01-06 17:57:34 CET	2024-01-06 19:14:42 CET	2023-05-05 14:24:37 CEST	115133979	Allocated	Allocated	
Edge.wim				2023-05-05 14:24:37 CEST	2024-01-06 17:57:34 CET	2024-01-06 19:14:42 CET	2023-05-05 14:24:37 CEST	115133979	Allocated	Allocated	
mpasbase.vdm			1	2023-12-25 19:59:26 CET	2024-01-06 17:52:50 CET	2024-01-08 18:15:52 CET	2023-12-25 19:59:32 CET	72321624	Allocated	Allocated	
I2057.ngr				2019-10-15 15:47:00 CET	2023-12-22 16:13:06 CET	2019-12-07 15:47:29 CET	2019-12-07 15:47:29 CET	57343084	Allocated	Allocated	
I2057.ngr				2019-10-15 15:47:00 CET	2023-12-22 16:13:06 CET	2019-12-07 15:47:29 CET	2019-12-07 15:47:29 CET	57343084	Allocated	Allocated	
MicrosoftEdge_X64_120.0.2210.91.exe				2023-12-25 20:00:02 CET	2023-12-25 20:00:02 CET	2023-12-25 20:00:02 CET	2023-12-25 19:59:37 CET	171516472	Allocated	Allocated	
OneDriveSetup.exe				2023-12-25 19:59:06 CET	2023-12-25 19:59:24 CET	2024-01-06 19:17:22 CET	2023-12-25 19:59:24 CET	65858576	Allocated	Allocated	
Wireshark-4.2.2-x64.exe				2024-01-06 17:47:11 CET	2024-01-06 17:47:16 CET	2024-01-08 18:16:05 CET	2024-01-06 17:46:56 CET	86375712	Allocated	Allocated	
ServiceHub.Host.Node.x86.exe				2023-12-26 13:02:07 CET	2023-12-26 13:02:07 CET	2024-01-06 19:11:19 CET	2023-12-26 13:02:06 CET	57554040	Allocated	Allocated	
node.exe				2023-12-19 01:35:58 CET	2023-12-19 01:35:58 CET	2023-12-28 13:03:25 CET	2023-12-19 01:35:58 CET	71239832	Allocated	Allocated	
MicrosoftEdge_X64_120.0.2210.91.exe				2023-12-22 15:20:20 CET	2023-12-22 15:21:53 CET	2023-12-28 13:03:25 CET	2023-12-22 15:20:11 CET	171516472	Allocated	Allocated	
MicrosoftEdge_X64_120.0.2210.91.exe				2023-12-25 20:00:34 CET	2023-12-25 20:00:31 CET	2024-01-06 19:12:33 CET	2023-12-25 20:00:04 CET	171516472	Allocated	Allocated	
MRT.exe				2023-12-28 13:00:19 CET	2023-12-28 13:00:19 CET	2024-01-08 18:13:32 CET	2023-12-28 13:00:19 CET	182871392	Allocated	Allocated	
libwireshark.dll				2024-01-05 01:37:20 CET	2024-01-06 17:47:49 CET	2024-01-06 19:12:07 CET	2024-01-05 01:37:20 CET	88709872	Allocated	Allocated	
mpcache-AEE6192CCD9E65CB96012BAA1A82D9C4				2024-01-06 17:52:44 CET	2024-01-08 18:12:49 CET	2024-01-08 18:21:43 CET	2024-01-06 17:52:42 CET	63438848	Allocated	Allocated	
\$BadClus:\$Bad				2023-12-22 16:11:49 CET	2023-12-22 16:11:49 CET	2023-12-22 16:11:49 CET	2023-12-22 16:11:49 CET	52424704	Allocated	Allocated	
SOFTWARE				2024-01-08 18:21:44 CET	2023-12-22 16:14:53 CET	2024-01-08 18:21:44 CET	2019-12-07 10:03:44 CET	75235328	Allocated	Allocated	

Widzimy tu bardzo dużo plików .exe, które służą do instalowania aplikacji.

Pliki o rozmiarze 200MB-1GB:

Listing 200MB - 1GB											
Table <a href="#">Thumbnail</a> <a href="#">Summary</a>											
Page: 1 of 1 Pages: < > Go to Page: <input type="text"/>				Save Table as CSV							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
Winre.wim				2023-05-05 14:11:22 CEST	2023-12-22 16:18:26 CET	2024-01-06 19:10:06 CET	2023-12-22 16:18:25 CET	448962094	Allocated	Allocated	unknc
swapfile.sys				2024-01-08 19:12:29 CET	2024-01-08 19:12:29 CET	2024-01-08 19:12:29 CET	2023-12-22 16:16:06 CET	268435456	Allocated	Allocated	unknc
chrome.dll				2024-01-03 01:08:39 CET	2024-01-06 18:10:01 CET	2024-01-08 18:15:10 CET	2024-01-06 18:09:48 CET	230748960	Allocated	Allocated	unknc
msedge.dll				2023-12-21 05:07:26 CET	2023-12-25 20:06:02 CET	2024-01-08 18:12:55 CET	2023-12-22 15:20:39 CET	268004904	Allocated	Allocated	unknc
msedge.dll				2023-12-21 05:07:26 CET	2023-12-25 20:06:02 CET	2024-01-08 18:12:55 CET	2023-12-22 15:20:39 CET	268004904	Allocated	Allocated	unknc
msedge.dll				2023-12-21 05:07:26 CET	2024-01-08 18:12:55 CET	2024-01-08 18:12:55 CET	2023-12-22 15:20:39 CET	268004904	Allocated	Allocated	unknc
Cab_1_for_KB503372_PSFX.cab				2023-12-03 14:41:20 CET	2024-01-08 18:14:08 CET	2024-01-08 18:14:56 CET	2024-01-08 18:14:02 CET	693567940	Unallocated	Unallocated	unknc
Windows10-KB503372-x64.cab				2023-12-26 12:58:16 CET	2024-01-08 18:14:08 CET	2023-12-26 12:57:16 CET	2024-01-08 18:07:55 CET	788469818	Allocated	Allocated	unknc
chrome.7z				2024-01-06 18:07:55 CET	2024-01-06 18:10:01 CET	2024-01-06 19:17:02 CET	2024-01-06 18:07:55 CET	363641875	Allocated	Allocated	unknc
\$UsnJnl:\$J				2023-12-22 16:16:03 CET	2023-12-22 16:16:03 CET	2023-12-22 16:16:03 CET	2023-12-22 16:16:03 CET	304514896	Allocated	Allocated	unknc
SMFT				2023-12-22 16:11:50 CET	2023-12-22 16:11:50 CET	2023-12-22 16:11:50 CET	2023-12-22 16:11:50 CET	305397760	Allocated	Allocated	unknc
\$BadClus:\$Bad				2023-12-22 16:18:24 CET	2023-12-22 16:18:24 CET	2023-12-22 16:18:24 CET	2023-12-22 16:18:24 CET	555741184	Allocated	Allocated	unknc

Widzimy tu archiwa i trochę plików DLL\*.

\*DLL (z ang. Dynamic-Link Library – biblioteka łączona dynamicznie) – biblioteka współdzielona (z ang. shared library) w środowisku Microsoft Windows, przechowująca implementacje różnych podprogramów programu lub zasoby programu.

## Pliki o rozmiarze 1GB+:

Listing									
1GB+									
Table   Thumbnail   Summary									
Page: 1 of 1		Pages: < >		Go to Page: <input type="text"/>					
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	
pagefile.sys				2024-01-08 19:12:29 CET	2024-01-08 19:12:29 CET	2024-01-08 19:12:29 CET	2023-12-22 16:16:06 CET	1170	
\$BadClus:\$Bad				2023-12-22 16:11:50 CET	2023-12-22 16:11:50 CET	2023-12-22 16:11:50 CET	2023-12-22 16:11:50 CET	2086	

Dwa pliki systemowe.

Listing									
Images									
Table   Thumbnail   Summary									
Page: 1 of 2		Pages: < >		Go to Page: <input type="text"/>					
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir) Flags(M)
WelcomeFax.tif				2019-10-15 15:48:00 CEST	2024-01-06 17:57:34 CET	2024-01-06 19:14:44 CET	2019-12-07 15:46:49 CET	89534	Allocated Allocated
128.png				2023-12-22 15:27:10 CET	2023-12-22 15:27:10 CET	2024-01-06 19:17:19 CET	2023-12-22 15:27:10 CET	4942	Allocated Allocated
alertIcon.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	718	Allocated Allocated
alertIconWhite.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	408	Allocated Allocated
Camera_Upload_Upsell_Light_728x360.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	40390	Allocated Allocated
ElevatedAppBlue.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	4694	Allocated Allocated
HeroImage_FirstUploadLowCostSKUToast.png				2023-12-25 19:59:17 CET	2023-12-25 19:59:17 CET	2023-12-25 19:59:17 CET	2023-12-25 19:59:17 CET	170356	Allocated Allocated
AppBlue.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-28 13:06:12 CET	2023-12-25 19:59:16 CET	10242	Allocated Allocated
AppErrorBlue.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	6028	Allocated Allocated
AppErrorWhite.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	5460	Allocated Allocated
AppWhite.png				2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	2023-12-25 19:59:16 CET	3824	Allocated Allocated
Square4x44Logo.altform-unplated_targetsize-16.p				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	637	Allocated Allocated
Square44x44Logo.altform-lightunplated_targetsize-				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	637	Allocated Allocated
Square44x44Logo.altform-lightunplated_targetsize-				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	1000	Allocated Allocated
Square44x44Logo.altform-lightunplated_targetsize-				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	18878	Allocated Allocated
Square44x44Logo.altform-lightunplated_targetsize-				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	1407	Allocated Allocated
Square44x44Logo.altform-lightunplated_targetsize-				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2349	Allocated Allocated
Square44x44Logo.altform-unplated_targetsize-24.p				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	1000	Allocated Allocated
Square44x44Logo.altform-unplated_targetsize-256.				2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	2023-12-25 19:59:19 CET	18878	Allocated Allocated

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

0%  78%   Reset Tags Me



Każda przeglądarka pobrała wiele plików w formacie .png.

**Data Sources**

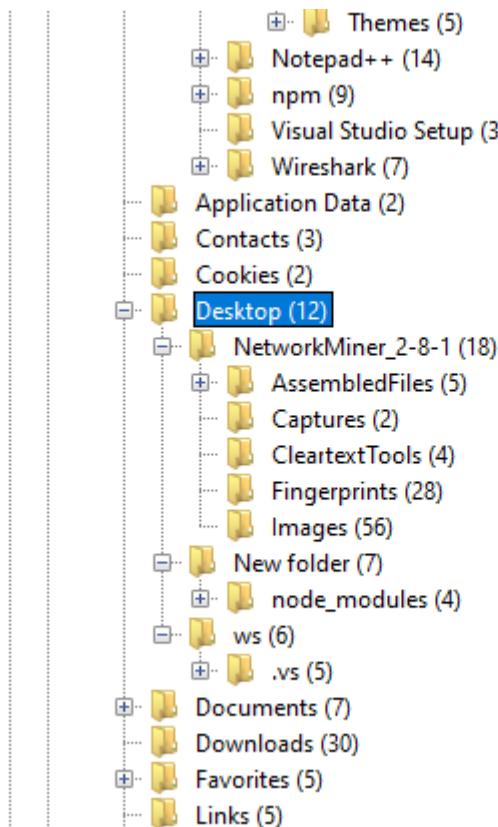
- Windows\_10.img\_1 Host
  - Windows\_10.img
    - vol1 (Unallocated: 0-2047)
    - vol2 (NTFS / exFAT (0x07): 2048-104447)
      - \$OrphanFiles (0)
      - \$Extend (7)
        - \$Deleted (2)
        - \$RmMetadata (6)
      - \$Unalloc (1)
      - Boot (49)
      - System Volume Information (3)
    - vol3 (NTFS / exFAT (0x07): 104448-40853168)
      - \$OrphanFiles (61556)
      - \$Extend (9)
      - \$Recycle.Bin (4)
      - \$Unalloc (2)
      - \$WinREAgent (3)
        - Scratch (2)
      - Documents and Settings (2)
      - MinGW (9)
      - PerfLogs (2)
      - Program Files (30)
        - Common Files (6)
        - Google (3)
        - Internet Explorer (14)
        - Microsoft Update Health Tools (8)
        - Microsoft Visual Studio (3)
        - ModifiableWindowsApps (2)
        - nodejs (12)
        - Notepad++ (19)
        - Npcap (15)

Name	S	C	O	Modified time	Change time	Access time	Created time	Size	Flags(Dir)	Flags(Mem)
desktop.ini				2019-12-07 10:12:42 CET	2023-12-22 16:12:18 CET	2024-01-08 18:17:08 CET	2019-12-07 10:14:54 CET	174	Allocated	Allocated
[current folder]				2024-01-08 18:13:44 CET	2024-01-08 18:13:44 CET	2024-01-08 18:17:49 CET	2019-12-07 10:14:52 CET	168	Allocated	Allocated
[parent folder]				2024-01-08 18:13:27 CET	2024-01-08 18:13:27 CET	2024-01-08 18:21:42 CET	2019-12-07 10:03:44 CET	56	Allocated	Allocated
Common Files				2023-12-26 13:02:44 CET	2023-12-26 13:02:44 CET	2024-01-08 19:12:31 CET	2019-12-07 10:14:52 CET	56	Allocated	Allocated
Google				2023-12-22 15:33:03 CET	2023-12-22 15:33:03 CET	2024-01-08 18:17:49 CET	2023-12-22 15:33:03 CET	144	Allocated	Allocated
Internet Explorer				2023-05-05 14:31:50 CEST	2023-12-22 16:14:53 CET	2024-01-06 19:16:21 CET	2019-12-07 10:14:52 CET	56	Allocated	Allocated
Microsoft Update Health Tools				2024-01-06 17:46:30 CET	2024-01-06 17:46:30 CET	2024-01-06 19:10:24 CET	2024-01-06 17:46:30 CET	56	Allocated	Allocated
Microsoft Visual Studio				2023-12-26 13:01:09 CET	2023-12-26 13:01:09 CET	2024-01-06 19:11:37 CET	2023-12-26 13:01:09 CET	144	Allocated	Allocated
ModifiableWindowsApps				2019-12-07 10:14:52 CET	2023-12-22 16:14:53 CET	2024-01-06 19:11:41 CET	2019-12-07 10:14:52 CET	48	Allocated	Allocated
nodejs				2023-12-25 20:00:00 CET	2023-12-25 20:00:00 CET	2024-01-08 18:12:51 CET	2023-12-25 19:59:59 CET	56	Allocated	Allocated
Notepad++				2024-01-08 18:13:48 CET	2024-01-08 18:13:48 CET	2024-01-08 18:13:56 CET	2024-01-08 18:13:44 CET	56	Allocated	Allocated
Npcap				2024-01-06 17:50:15 CET	2024-01-06 17:50:15 CET	2024-01-08 18:12:34 CET	2024-01-06 17:49:05 CET	56	Allocated	Allocated
Oracle				2023-12-22 15:27:46 CET	2023-12-22 15:27:46 CET	2024-01-06 19:11:54 CET	2023-12-22 15:27:46 CET	288	Allocated	Allocated
RUXIM				2023-12-28 13:00:12 CET	2023-12-28 13:00:12 CET	2024-01-06 19:11:55 CET	2023-12-28 13:00:12 CET	56	Allocated	Allocated
Uninstall Information				2023-12-22 16:16:32 CET	2023-12-22 16:16:32 CET	2024-01-06 19:11:55 CET	2023-12-22 16:16:32 CET	48	Allocated	Allocated
USBPcap				2024-01-06 17:51:13 CET	2024-01-06 17:51:13 CET	2024-01-06 19:11:55 CET	2024-01-06 17:51:10 CET	56	Allocated	Allocated
VideoLAN				2023-12-22 15:39:23 CET	2023-12-22 15:39:23 CET	2024-01-06 19:12:00 CET	2023-12-22 15:39:23 CET	136	Allocated	Allocated
Windows Defender				2023-12-25 20:09:08 CET	2023-12-25 20:09:08 CET	2024-01-08 18:12:35 CET	2019-12-07 10:14:52 CET	56	Allocated	Allocated
Windows Defender Advanced Threat Protection				2023-05-05 14:31:50 CEST	2023-12-22 16:14:53 CET	2024-01-06 19:16:21 CET	2019-12-07 15:49:02 CET	56	Allocated	Allocated

Folder "Program Files" na systemie Windows jest standardowym katalogiem, w którym przechowywane są zainstalowane aplikacje programowe. W zależności od tego, co jest zainstalowane na systemie, zawartość tego folderu może się różnić.

Analizując ten obraz można zauważać raczej dość standardowe programy w tym folderze.

Użytkownik posiadał domyślne programy dla Windowsa 10, ale w folderze znajdują się również foldery z plikami aplikacji, które zdecydował się manualnie zainstalować. Node JS, Visual Studio Code, Notepad++ i ogólny folder Oracle dają do zrozumienia, że w głównej mierze użytkownik z biegiem czasu kompletował swoje środowisko do programowania.



Ciekawsze rzeczy znajdowały się głównie na pulpicie, w profilu użytkownika ZM.

File List - Windows 10 Image Analysis									
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	
123.txt				2023-12-22 15:45:40 CET	2023-12-22 15:45:40 CET	2024-01-06 19:17:18 CET	2023-12-22 15:45:31 CET	17	
Microsoft Edge.Ink				2023-12-22 15:27:05 CET	2023-12-22 15:27:05 CET	2024-01-08 18:15:51 CET	2023-12-22 15:25:37 CET	2348	
MinGW Installer.Ink				2023-12-27 17:39:50 CET	2023-12-27 17:39:50 CET	2024-01-08 18:15:51 CET	2023-12-27 17:39:50 CET	879	
neom-wTmGtmGQCjQ-unplash.jpg				2023-12-25 20:01:14 CET	2023-12-25 20:03:03 CET	2024-01-08 18:15:53 CET	2023-12-25 20:01:11 CET	7514645	
neom-wTmGtmGQCjQ-unplash.jpg.Zone.Identifier				2023-12-25 20:01:14 CET	2023-12-25 20:03:03 CET	2024-01-08 18:15:53 CET	2023-12-25 20:01:11 CET	212	
desktop.ini				2023-12-22 15:25:36 CET	2023-12-22 15:25:36 CET	2024-01-08 18:16:15 CET	2023-12-22 15:25:36 CET	282	
WEWE.bmp				2023-12-22 15:45:51 CET	2023-12-22 15:45:52 CET	2024-01-08 18:15:55 CET	2023-12-22 15:45:51 CET	0	
[current folder]				2024-01-06 19:24:47 CET	2024-01-06 19:24:47 CET	2024-01-08 18:15:51 CET	2023-12-22 15:24:43 CET	56	
[parent folder]				2023-12-26 13:04:21 CET	2023-12-26 13:04:21 CET	2024-01-08 18:16:55 CET	2023-12-22 15:24:43 CET	256	
NetworkMiner_2-8-1				2024-01-06 19:24:50 CET	2024-01-06 19:24:50 CET	2024-01-06 19:25:29 CET	2024-01-06 19:24:47 CET	56	
New folder				2023-12-26 12:57:36 CET	2023-12-26 12:57:36 CET	2024-01-06 18:55:59 CET	2023-12-25 20:03:56 CET	56	
ws				2023-12-28 13:04:28 CET	2023-12-28 13:04:28 CET	2024-01-03 13:10:15 CET	2023-12-27 17:45:20 CET	56	

## Zawartość pliku 123.txt:

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of - Page ⏪ ⏩ Matches on page: - of - Match ⏪ ⏩ 100% ⏴ ⏵ Reset

FYUADHKJGHAJKSHJD

-----METADATA-----

## Obraz:



W folderze o nazwie ws znajdowały się programy napisane w języku C++ oraz C:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
sssss.txt.txt				2023-12-27 17:47:22 CET	2023-12-27 17:47:22 CET	2023-12-27 17:52:44 CET	2023-12-27 17:46:58 CET	5	Allocated	Allocated
pyramid.cpp				2023-12-27 17:52:44 CET	2023-12-27 17:53:01 CET	2023-12-27 17:53:27 CET	2023-12-27 17:52:44 CET	686	Allocated	Allocated
add.c				2023-12-28 13:01:43 CET	2023-12-28 13:04:28 CET	2024-01-03 13:10:15 CET	2023-12-28 13:01:42 CET	397	Allocated	Allocated
[current folder]				2023-12-28 13:04:28 CET	2023-12-28 13:04:28 CET	2024-01-03 13:10:15 CET	2023-12-27 17:45:20 CET	56	Allocated	Allocated
[parent folder]				2024-01-06 19:24:47 CET	2024-01-06 19:24:47 CET	2024-01-08 18:15:51 CET	2023-12-22 15:24:43 CET	56	Allocated	Allocated
.vs				2023-12-27 17:46:44 CET	2023-12-27 17:46:44 CET	2023-12-27 17:46:48 CET	2023-12-27 17:45:45 CET	56	Allocated	Allocated

Strings Extracted Text Translation

Page: 1 of - Page < > Matches on page: - of - Match < > 100% ⌂ ⌃ Reset Text Source

Hacks

-----METADATA-----

W folderze New Folder znajdowały się biblioteki przydatne do programowania w języku Javascript:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loc
index.js.txt				2023-12-25 20:04:45 CET	2023-12-25 20:04:45 CET	2023-12-25 20:05:12 CET	2023-12-25 20:04:45 CET	0	Allocated	Allocated	unknown	/im
yarn.lock				2023-12-26 12:57:36 CET	2023-12-26 12:57:36 CET	2023-12-26 12:57:37 CET	2023-12-26 12:57:36 CET	356	Allocated	Allocated	unknown	/im
package-lock.json				2023-12-26 12:57:21 CET	2023-12-26 12:57:21 CET	2023-12-26 12:57:37 CET	2023-12-26 12:57:21 CET	590	Allocated	Allocated	unknown	/im
package.json				2023-12-26 12:57:21 CET	2023-12-26 12:57:21 CET	2023-12-26 12:57:36 CET	2023-12-25 20:04:28 CET	258	Allocated	Allocated	unknown	/im
[current folder]				2023-12-26 12:57:36 CET	2023-12-26 12:57:36 CET	2024-01-06 18:55:59 CET	2023-12-25 20:03:56 CET	56	Allocated	Allocated	unknown	/im
[parent folder]				2024-01-06 19:24:47 CET	2024-01-06 19:24:47 CET	2024-01-08 18:15:51 CET	2023-12-22 15:24:43 CET	56	Allocated	Allocated	unknown	/im
node_modules				2023-12-26 12:57:36 CET	2023-12-26 12:57:36 CET	2024-01-06 18:55:59 CET	2023-12-26 12:57:21 CET	472	Allocated	Allocated	unknown	/im

Użytkownik posiadał również program Network Miner:

[parent folder]				2023-12-20 15:04:21 CET	2023-12-20 15:04:21 CET	2024-01-08 18:10:55 CET	2023-12-22 15:24:45 CET	250	Allocated	Allocated
NetworkMiner_2-8-1				2024-01-06 19:24:50 CET	2024-01-06 19:24:50 CET	2024-01-06 19:25:29 CET	2024-01-06 19:24:47 CET	56	Allocated	Allocated

Użytkownik posiadał również folder visual studio 2022 w sekcji Dokumenty:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
desktop.ini				2023-12-22 15:25:37 CET	2023-12-22 15:25:37 CET	2024-01-08 18:16:15 CET	2023-12-22 15:25:36 CET	402	Allocated
[current folder]				2023-12-26 13:02:29 CET	2023-12-26 13:02:29 CET	2024-01-06 19:25:29 CET	2023-12-22 15:24:43 CET	56	Allocated
[parent folder]				2023-12-26 13:04:21 CET	2023-12-26 13:04:21 CET	2024-01-08 18:16:55 CET	2023-12-22 15:24:43 CET	256	Allocated
My Music				2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	48	Allocated
My Pictures				2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	48	Allocated
My Videos				2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	2023-12-22 15:24:44 CET	48	Allocated
Visual Studio 2022				2023-12-26 13:04:21 CET	2023-12-26 13:04:21 CET	2023-12-27 17:46:23 CET	2023-12-26 13:02:29 CET	256	Allocated

A w sekcji Pobrane trochę “instalek” i zdjęć:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met)
IMG_4459.jpeg				2024-01-08 18:15:11 CET	2024-01-08 18:15:33 CET	2024-01-08 18:16:55 CET	2024-01-08 18:15:10 CET	823792	Allocated	Allocated

W folderach, z którymi przeciętny użytkownik ma do czynienia na co dzień to by było raczej tyle.

Przeszukałem wszystko i w żadnym innym miejscu nie zauważylem nic nieregularnego, czy godnego uwagi.

Teraz skupię się na plikach, które nie są powszechnie, a znajdują się w obrazie przetworzonym przez Autopsy.

## Wszystkie aktualizacje systemu przeprowadzone przez użytkownika:

Listing /img_Windows_10.img/vol_vo13/Windows/Logs/WindowsUpdate											14 Results
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	
WindowsUpdate.20240108.171237.720.10.etl				2024-01-08 18:17:46 CET	2024-01-08 18:17:46 CET	2024-01-08 18:17:34 CET	2024-01-08 18:17:34 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.11.etl				2024-01-08 18:17:56 CET	2024-01-08 18:17:56 CET	2024-01-08 18:17:56 CET	2024-01-08 18:17:46 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.12.etl				2024-01-08 18:18:07 CET	2024-01-08 18:18:07 CET	2024-01-08 18:18:07 CET	2024-01-08 18:17:56 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.13.etl				2024-01-08 18:18:18 CET	2024-01-08 18:18:18 CET	2024-01-08 18:18:18 CET	2024-01-08 18:18:07 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.14.etl				2024-01-08 18:18:34 CET	2024-01-08 18:18:34 CET	2024-01-08 18:18:34 CET	2024-01-08 18:18:18 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.15.etl				2024-01-08 18:18:55 CET	2024-01-08 18:18:55 CET	2024-01-08 18:18:55 CET	2024-01-08 18:18:34 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.16.etl				2024-01-08 18:20:56 CET	2024-01-08 18:20:56 CET	2024-01-08 18:20:56 CET	2024-01-08 18:18:55 CET	65536	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.5.etl				2024-01-08 18:15:59 CET	2024-01-08 18:15:59 CET	2024-01-08 18:15:59 CET	2024-01-08 18:14:58 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.6.etl				2024-01-08 18:16:41 CET	2024-01-08 18:16:41 CET	2024-01-08 18:16:41 CET	2024-01-08 18:15:59 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.7.etl				2024-01-08 18:17:07 CET	2024-01-08 18:17:07 CET	2024-01-08 18:17:07 CET	2024-01-08 18:16:41 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.8.etl				2024-01-08 18:17:22 CET	2024-01-08 18:17:22 CET	2024-01-08 18:17:22 CET	2024-01-08 18:17:07 CET	139264	Allocated	Allocated	
WindowsUpdate.20240108.171237.720.9.etl				2024-01-08 18:17:34 CET	2024-01-08 18:17:34 CET	2024-01-08 18:17:34 CET	2024-01-08 18:17:22 CET	139264	Allocated	Allocated	
[current folder]				2024-01-08 18:18:55 CET	2024-01-08 18:18:55 CET	2024-01-08 18:18:58 CET	2024-01-06 18:06:28 CET	56	Allocated	Allocated	
[parent folder]				2024-01-08 18:20:56 CET	2024-01-08 18:20:56 CET	2024-01-08 18:20:56 CET	2019-12-07 10:14:52 CET	56	Allocated	Allocated	

## Podłączono urządzenie do drukarki:

Listing /img_Windows_10.img/vol_vo13/Windows/PrintDialog											13 Results
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kno
appxblockmap.xml				2023-05-05 14:25:54 CEST	2023-12-22 16:12:52 CET	2023-05-05 14:25:54 CEST	2023-05-05 14:25:54 CEST	319	Allocated	Allocated	unkr
appxmanifest.xml				2023-05-05 14:25:54 CEST	2023-12-22 16:12:52 CET	2024-01-08 18:16:07 CET	2023-05-05 14:25:54 CEST	2810	Allocated	Allocated	unkr
resources.pri				2023-05-05 14:25:54 CEST	2024-01-06 17:57:49 CET	2024-01-06 19:12:59 CET	2023-05-05 14:25:54 CEST	2200	Allocated	Allocated	unkr
SmallLogo.png				2023-05-05 14:25:54 CEST	2024-01-06 17:57:49 CET	2024-01-06 19:12:59 CET	2023-05-05 14:25:54 CEST	741	Allocated	Allocated	unkr
appxsignature.p7x				2023-05-05 14:25:54 CEST	2023-12-22 16:12:52 CET	2023-12-22 15:29:23 CET	2023-05-05 14:25:54 CEST	8596	Allocated	Allocated	unkr
PrintDialog.exe				2023-05-05 14:25:54 CEST	2023-12-22 16:12:52 CET	2024-01-08 18:16:07 CET	2023-05-05 14:25:54 CEST	122920	Allocated	Allocated	unkr
PrintDialog.dll				2023-05-05 14:25:54 CEST	2023-12-22 16:12:52 CET	2023-05-05 14:25:54 CEST	2023-05-05 14:25:54 CEST	1754112	Allocated	Allocated	unkr
[current folder]				2023-12-22 15:29:23 CET	2023-12-22 15:29:23 CET	2024-01-08 18:16:07 CET	2019-12-07 10:14:52 CET	56	Allocated	Allocated	unkr
[parent folder]				2023-12-25 20:58:23 CET	2023-01-08 18:21:42 CET	2024-01-08 18:21:42 CET	2019-12-07 10:03:44 CET	432	Allocated	Allocated	unkr
Assets				2019-12-07 10:14:55 CET	2023-12-22 16:14:54 CET	2024-01-08 18:16:04 CET	2019-12-07 10:14:52 CET	456	Allocated	Allocated	unkr
en-US				2019-12-07 15:45:25 CET	2023-12-22 16:14:54 CET	2024-01-08 18:16:04 CET	2019-12-07 15:45:25 CET	168	Allocated	Allocated	unkr
microsoft.system.package.metadata				2023-12-22 15:29:23 CET	2023-12-22 15:29:23 CET	2024-01-08 18:16:05 CET	2023-12-22 16:16:46 CET	144	Allocated	Allocated	unkr
pris				2023-05-05 14:31:50 CEST	2023-12-22 16:14:54 CET	2024-01-08 18:16:07 CET	2019-12-07 10:14:52 CET	168	Allocated	Allocated	unkr



Tak wyglądała tapeta:

The screenshot shows a digital forensic analysis interface. At the top, there's a navigation bar with 'Listing' and a path '/img\_Windows\_10.img/vol\_vol3/Windows/Web/4K/Wallpaper/Windows'. Below it is a table titled 'Table | Thumbnail | Summary' with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table lists several JPEG files with their details. Below the table is a preview window showing a Windows desktop background. At the bottom, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences, along with zoom controls (0%, 25%, 50%, 100%, Reset) and a Tags Menu.

Usunięto kilka folderów:

X [current folder]		2024-01-08 18:21:37 CET	2024-01-08 18:21:37 CET	2024-01-08 18:21:37 CET	2024-01-08 18:14:10 CET	48	Unallocated
X [parent folder]		2024-01-08 18:21:40 CET	2024-01-08 18:21:40 CET	2024-01-08 18:21:40 CET	2024-01-08 18:13:53 CET	48	Unallocated

Użytkownik na pewno łączył się do różnych sieci Wi Fi i prawdopodobnie zmieniał ustawienia Firewall'a:

\IPv6 Control Message	Local System	2024-01-06 19:06:00 CET	4074	0
System	Local System	2024-01-06 19:06:00 CET	35088	5833

Ostatniego dnia użytkowania próbowało pobrać program VLC, ale ostatecznie nie było go nigdzie, nawet w odinstalowanych zasobach:



Obraz był rozmiaru 20GB z czego większość miejsca zajmowały pliki systemowe. Użytkownik działał głównie na pulpicie i nie pobierał wielu zasobów. System prawdopodobnie postawił, aby zrealizować projekt dotyczący programowania.

Przeszukałem wszystkie możliwe miejsca i wszystkie znalezione rzeczy udokumentowałem.

# Część II

3)

Postanowiłem przeprowadzić analizę dla 2 zdjęć. Chcę sprawdzić, czy mój telefon prawidłowo przypisze lokalizacje.

Zdjęcie nr 1:



```
[szmpns@kali:~/InformatykaSledcza/projekt_partII]
$ exiftool IMG_20220812_140021.jpg
ExifTool Version Number : 12.67
File Name : IMG_20220812_140021.jpg
Directory : .
File Size : 4.1 MB
File Modification Date/Time : 2022:08:12 14:00:22+02:00
File Access Date/Time : 2024:01:27 13:13:09+01:00
File Inode Change Date/Time : 2024:01:27 13:13:09+01:00
File Permissions : -rwxr-xr-x
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
Exif Byte Order : Big-endian (Motorola, MM)
Y Resolution : 72
```

Rozmiar: 4.1 MB

Czas utworzenia: 2022:08:12 14:00:22+02:00

Urządzenie: OnePlus 7T

ISO: 125

Ustawienie światła: 9.3

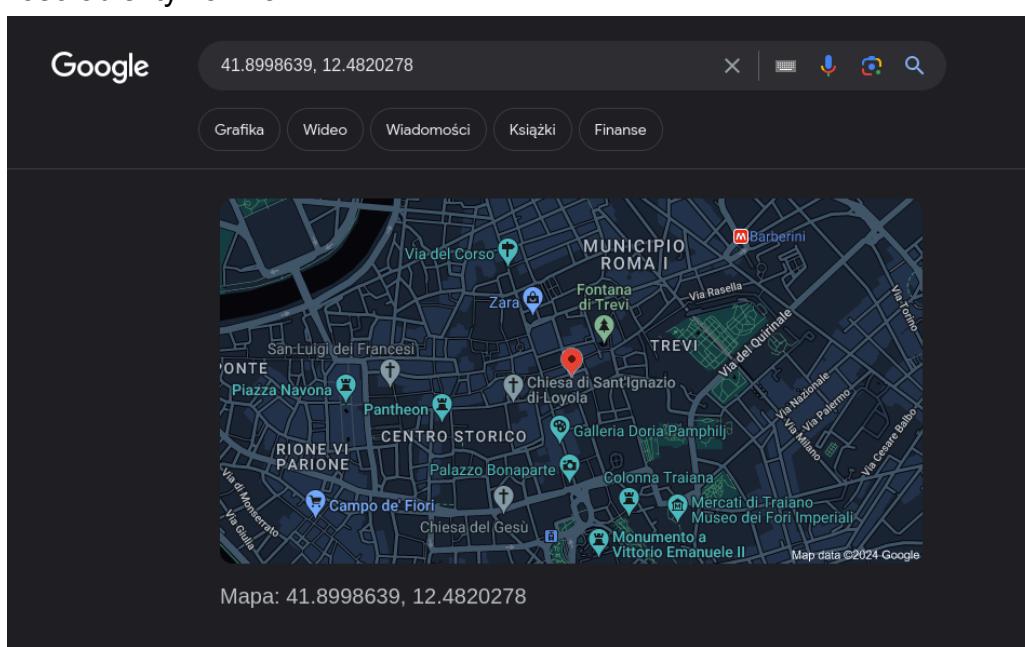
Flash: Auto, Did not fire

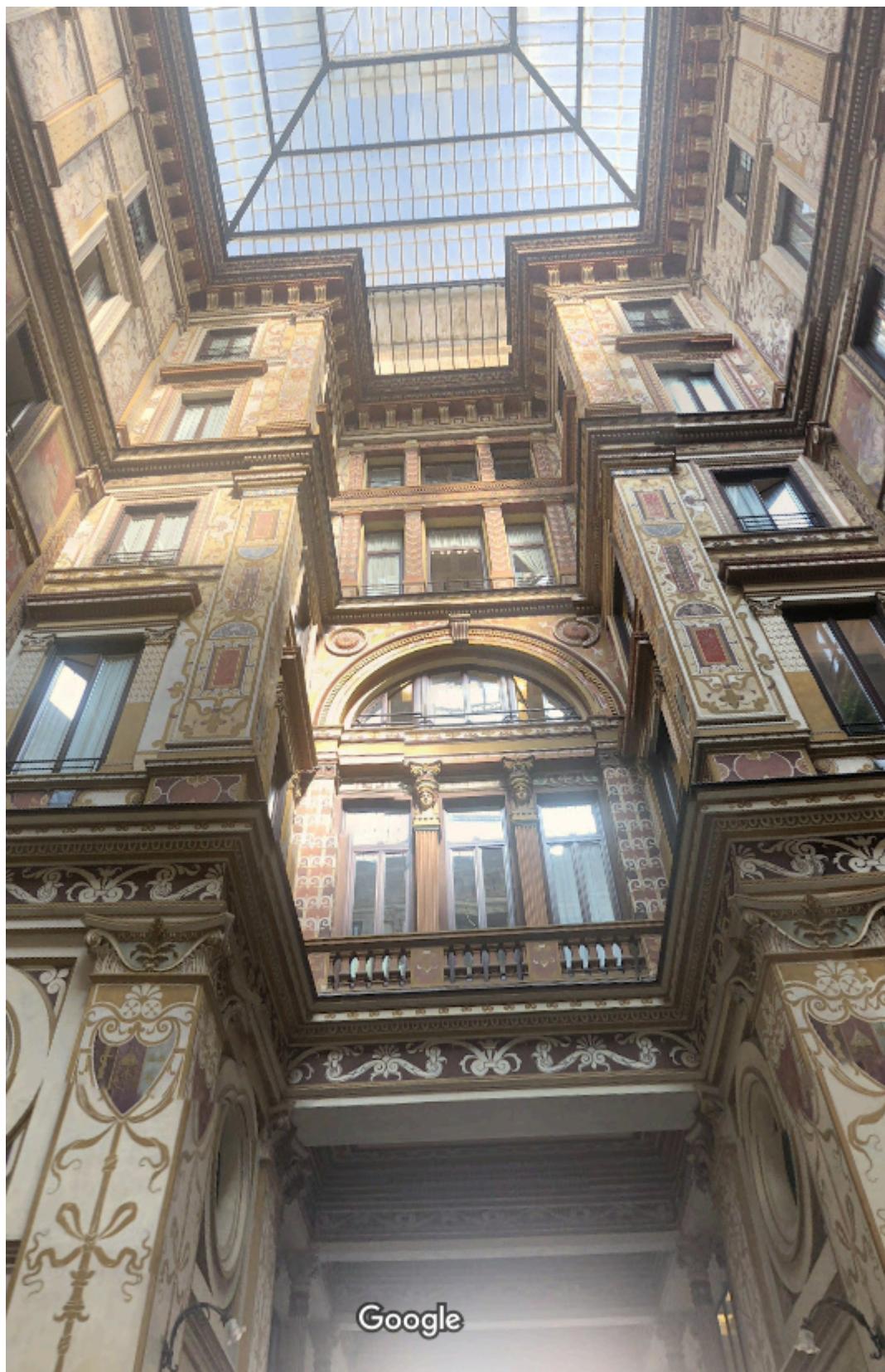
Rozdzielcość: 4000x3000

Przesłona: 1/100

Lokalizacja: 41 deg 53' 59.51" N, 12 deg 28' 55.30" E

Ilość obiektywów: 3





Jest to dokładnie to miejsce.

Zdjęcie nr 2:



```
(szmpns@kali)-[~/InformatykaSledcza/projekt_partII]
$ exiftool IMG_20230925_091420.jpg
ExifTool Version Number : 12.67
File Name : IMG_20230925_091420.jpg
Directory :
File Size : 6.5 MB
Rozmiar: 6.5 MB
Czas utworzenia: 2023:09:25 09:14:22+02:00
Urządzenie: OnePlus 7T
ISO: 125
Ustawienia: 1/100
Flash: Off, Did not fire
Rozdzielcość: 4000x3000
Rozdzielcość: 4000x3000
Przesłona: 1/100
Lokalizacja: 45 deg 26' 5.10" N, 12 deg 20' 6.87" E
Ilość obiektywów: 3
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
```

Rozmiar: 6.5 MB

Czas utworzenia: 2023:09:25 09:14:22+02:00

Urządzenie: OnePlus 7T

ISO: 125

Ustawienie światła: 9.3

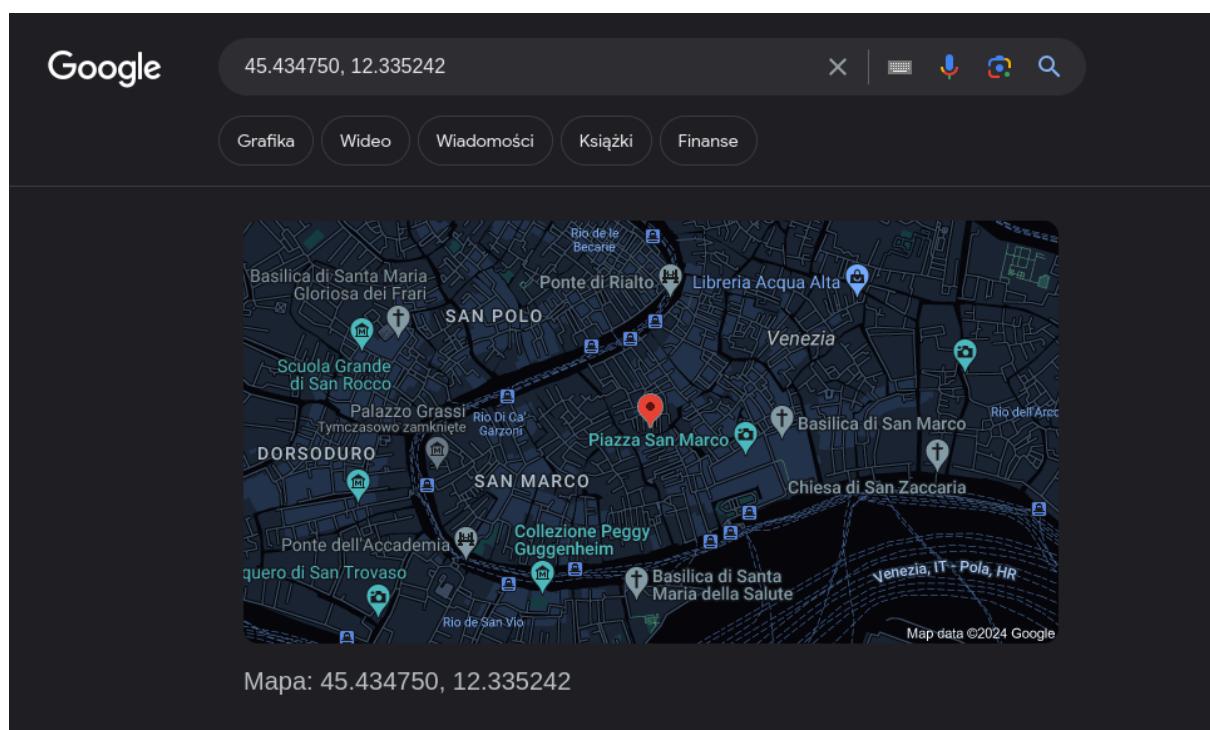
Flash: Off, Did not fire

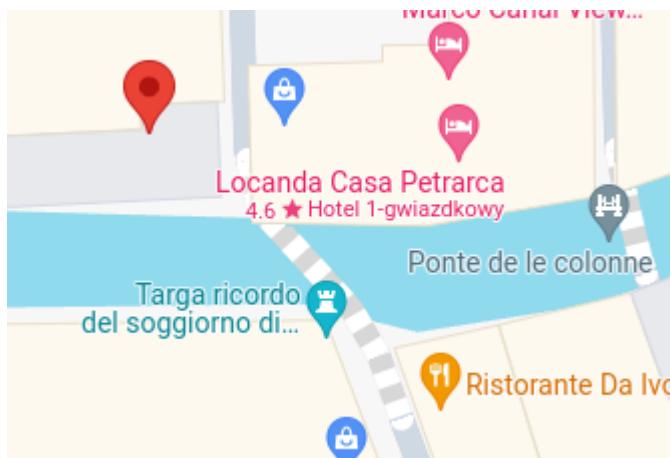
Rozdzielcość: 4000x3000

Przesłona: 1/100

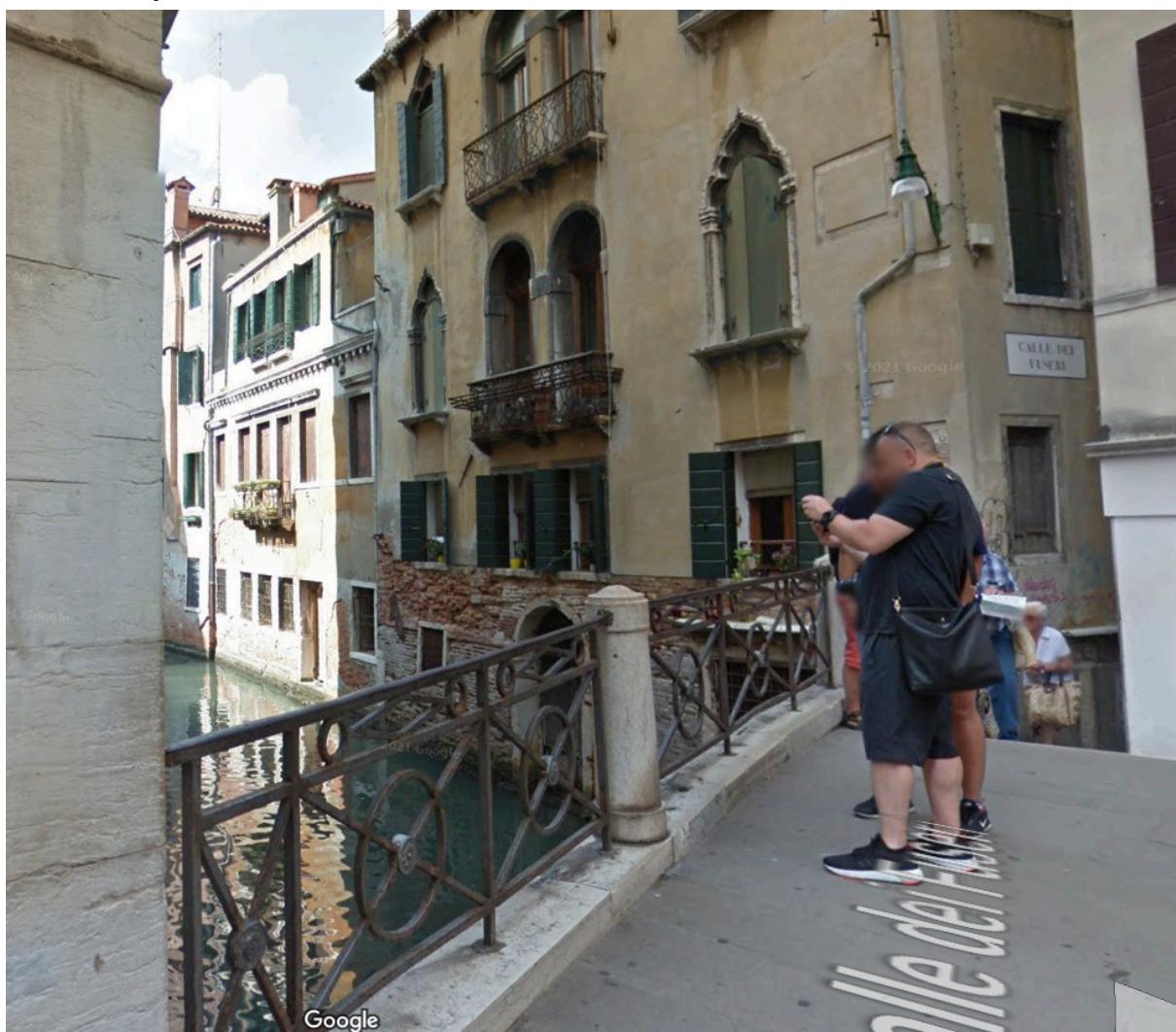
Lokalizacja: 45 deg 26' 5.10" N, 12 deg 20' 6.87" E

Ilość obiektywów: 3





Zdjęcie zostało wykonane na moście, zatem odczyt lokalizacji jest trochę niedokładny.



Jest to natomiast dokładnie to miejsce.

Do odzyskania plików wykorzystam narzędzie foremost. Zapamiętałem, że było ono najbardziej skuteczne i pracowało mi się z nim najwygodniej.

Odzyskam dane z pendrive'a:

```
└──(szmpns㉿kali)-[~] $ sudo foremost -i /dev/sda -o ~/InformatykaSledcza/InfSI_LAB04/description_pendrive
[sudo] password for szmpns:
Processing: /dev/sda Obraz: ZADANIE 2:
|*****|  
  
└──(root㉿kali)-[/home/szmpns/InformatykaSledcza/InfSI_LAB04/description_pendrive]
└─# ls -R
.:  
audit.txt jpg ole pdf rar  
  
.jpg:  
00033730.jpg 00034670.jpg 00035616.jpg 00058432.jpg 00081908.jpg  
00033849.jpg 00034757.jpg 00049040.jpg 00071184.jpg 00082530.jpg  
  
.ole:  
00083392.ole  
  
.pdf:  
00032880.pdf 00033728.pdf 00081680.pdf  
  
.rar:  
00083616.rar 00084064.rar
```

Pliki zostały odzyskane, a ich metadane zachowały się w oryginalnym stanie.

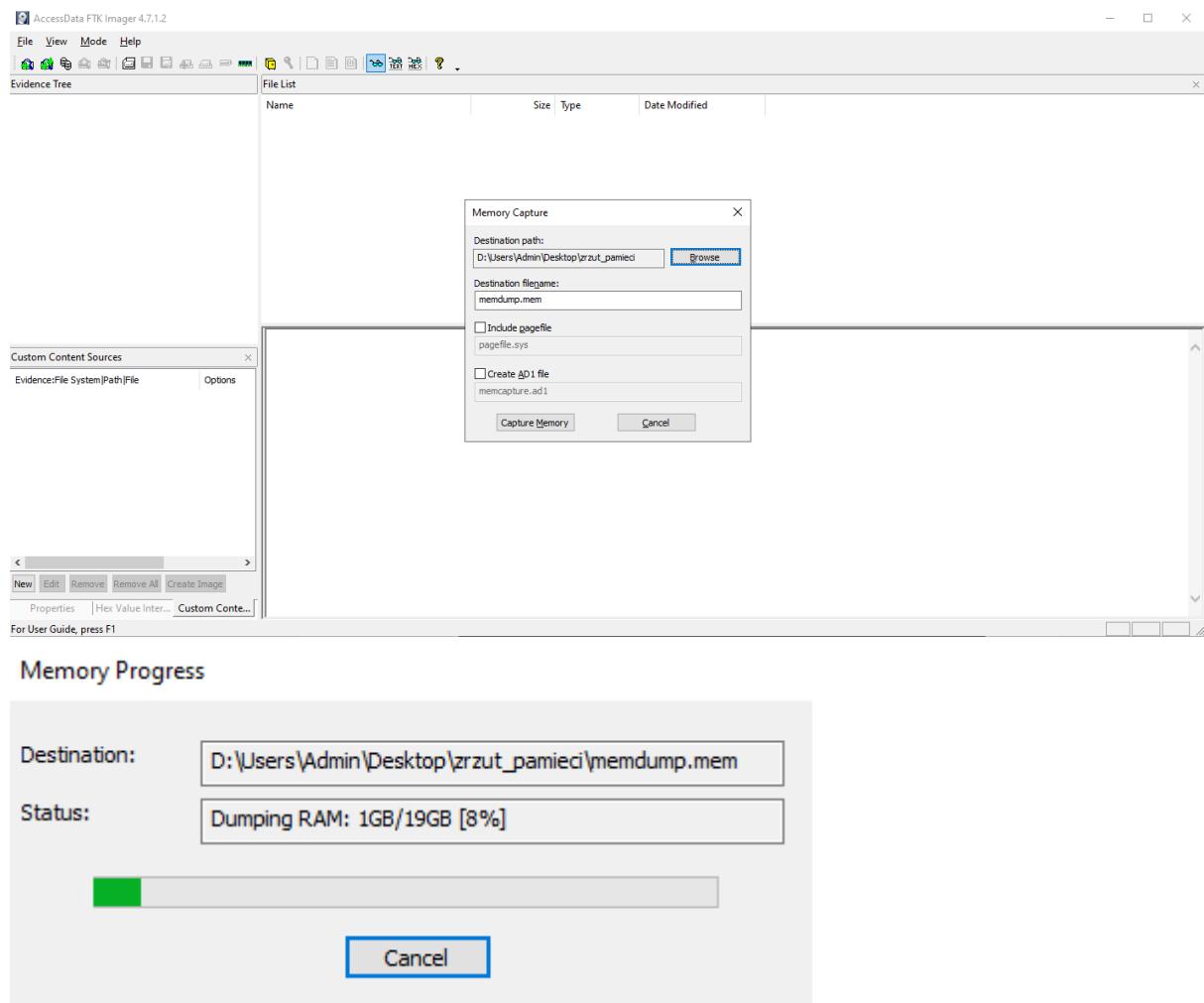
Program wygenerował również audit.

Dlaczego foremost jest tak solidny?

Działa na zasadzie carvingu: Narzędzie to opiera się na technice zwanej "carvingiem", która polega na analizie zawartości dysku w poszukiwaniu nagłówków i stóp plików, a następnie rekonstrukcji tych plików na podstawie ich struktury. Dzięki temu Foremost jest w stanie odzyskiwać pliki nawet w sytuacjach, gdy struktura systemu plików jest uszkodzona.

1)

Przykładowy zrzut Windows:



Na linuxie(za pomocą avml):

```
[szmpns㉿kali)-[~/Informaty
$ sudo ./avml kali_mem.dmp
```

Całość można przeszukać za pomocą polecenia strings + grep

```
$ sudo strings kali_mem.dmp | grep wikipedia
english_wikipedia.txt
# see http://en.wikipedia.org/wiki/GUID_Part
Homepage: https://en.wikipedia.org/wiki/Tnftp
Homepage: https://en.wikipedia.org/wiki/Tnftp
* From https://en.wikipedia.org/wiki/IEEE
```

