Analiza obrazu dysku oraz przedstawienie narzędzi wykorzystywanych w informatyce śledczej

Informatyka Śledcza

Magdalena Ślusarczyk

Wydział Informatyki, Elektroniki i Telekomunikacji
Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

17.01.2022r.

Spis treści

1 Wstęp **2**

2 Przygotowanie obrazu do analizy **2**

3 Analiza obrazu dysku z wykorzystaniem narzędzia Autopsy. **2**
3.1 Podstawowe informacje na temat analizowanego obrazu. 2
3.2 Zainstalowane programy 3
3.3 Znalezione pliki 3
3.3.1 Pulpit 3
3.3.2 Folder 'Normalny folder' 4
3.3.3 Folder 'Pomarańcze' 5
3.3.4 Folder 'Zdjęcie(niepodejrzane)' 5
3.3.5 Folder 'Documents' 6
3.3.6 Usunięte pliki 6
3.4 Historia przeglądarki 8
3.5 Wnioski z przeprowadzonej analizy 8

4 Analiza pamięci operacyjnej **9**
4.1 Zrzut pamięci 9
4.2 Analiza zrzutu 9

5 Kopia binarna nośnika USB **9**
5.1 Pozyskanie kopii 9
5.2 Podstawowe informacje na temat obrazu 10
5.3 Odczytanie zawartości 10

6 Metadane **11**
6.1 Odczyt metadanych z wybranego pliku 11
6.2 Zmiana metadanych 11

1 Wstęp

Celem projektu jest zaznajomienie się z oraz praktyczne wykorzystanie narzędzi służących do analizy śledczej. Niezbędna będzie również znajomość najpopularniejszych systemów operacyjnych, ich systemów plików oraz narzędzi służących do wirtualizacji.

2 Przygotowanie obrazu do analizy

Pierwszym zadaniem w projekcie było przygotowanie obrazu maszyny wirtualnej do analizy przez inną osobę. Została przeprowadzona symulacja działań użytkownika systemu Linux (Debian 11), która obejmowała:

- utworzenie dwóch folderów na pulpicie: /pdf oraz /zdjecia,
- dodanie do folderu /pdf kilku plików tekstowych o tematyce militarnej pobranych z Internetu, a następnie usunięcie folderu z całą zawartością,
- dodanie pięciu zdjęć prywatnych do katalogu /zdjęcia zawierajacych metadane, z których można odczytać np.: lokalizację, nazwę urządzenia, którym zostało wykonane zdjęcie datę utworzenia pliku,
- usunięcie dwóch zdjęć z wyżej wymienionego folderu,
- zmianę formatu czasu na 12-sto godzinny,
- pobranie rozszerzenia AdGuard do przeglądarki Firefox,
- zainstalowanie narzędzi curl, snap oraz programów OpenVPN i Spotify,
- przeglądanie Internetu w poszukiwaniu sklepów z bronią, oglądanie filmów o tematyce militarnej w serwisie YouTube.

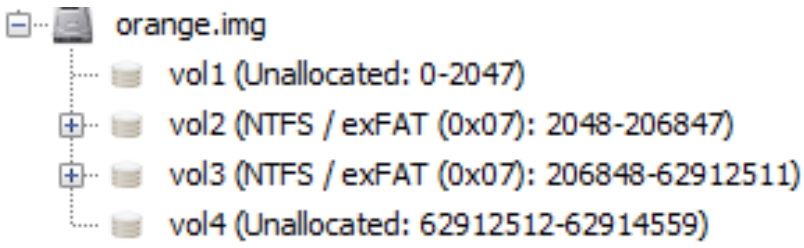
Maszynę utworzono w programie VMware, a następnie przekonwertowano do formatu raw przy pomocy programu FTK Imager.

3 Analiza obrazu dysku z wykorzystaniem narzędzia Autopsy.

3.1 Podstawowe informacje na temat analizowanego obrazu.

Format obrazu: .img (raw)
Wielkość obrazu: 32 313 154 720 B
Rozmiar sektora: 512 B
Woluminy:

1. Przestrzeń niezaalokowana - sektory 0 - 2047
2. Partycja systemowa - sektory 2048 - 206847
3. System plików NTFS - sektory 206848 - 62912511
4. Przestrzeń niezaalokowana - sektory 62912511 - 62914559

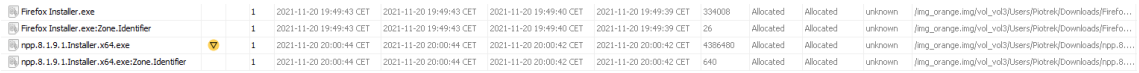


System operacyjny: Windows 7 Home Premium Service Pack 1
Użytkownicy: "Piotrek"

Type	Value	Source(s)
Program Name	Windows 7 Home Premium Service Pack 1	Recent Activity
Date/Time	2021-11-20 19:46:46 CET	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00359-112-0000007-85674	Recent Activity
Owner	Piotrek	Recent Activity
Organization		Recent Activity
Source File Path	/img_orange.img/vol_vol3/Windows/System32/config/RegBack/SOFTWARE	
Artifact ID	-9223372036854775733	

3.2 Zainstalowane programy

Na komputerze zainstalowano przeglądarkę Firefox oraz program Notepad++. Świadczą o tym pozostawione pliki instalacyjne w folderze Piotrek/Downloads oraz pliki tych programów w /Program Files, a także znalezione przez Autopsy artefakty zainstalowanych programów.

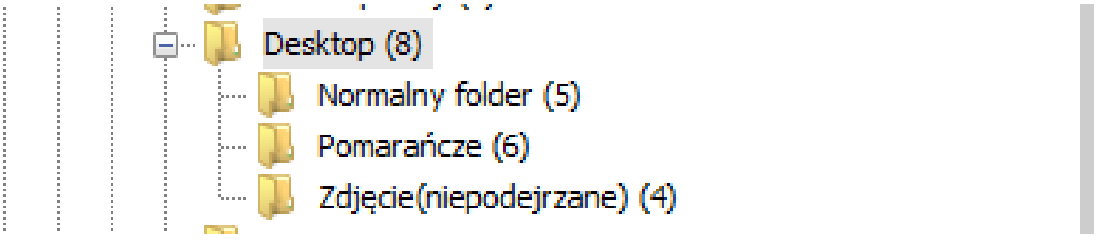


Source File	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			1	Notepad++ (64-bit x64) v.8.1.9.1	2021-11-20 19:01:03 CET	orange.img
SOFTWARE			1	Notepad++ (64-bit x64) v.8.1.9.1	2021-11-20 19:01:03 CET	orange.img
SOFTWARE			1	Mozilla Maintenance Service v.94.0.1	2021-11-20 18:50:15 CET	orange.img
SOFTWARE			1	Mozilla Maintenance Service v.94.0.1	2021-11-20 18:50:15 CET	orange.img
SOFTWARE			1	Mozilla Firefox (x64 pl) v.94.0.1	2021-11-20 18:50:08 CET	orange.img
SOFTWARE			1	Mozilla Firefox (x64 pl) v.94.0.1	2021-11-20 18:50:08 CET	orange.img

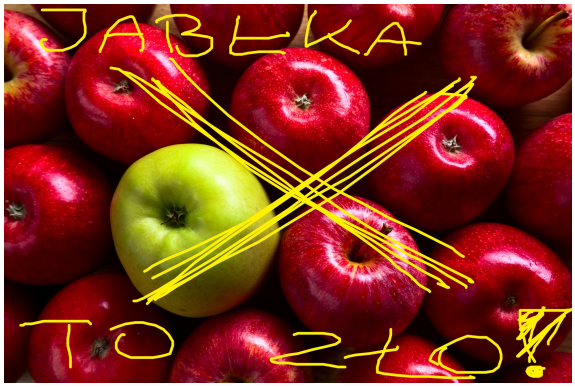
3.3 Znalezione pliki

3.3.1 Pulpit

Na pulpicie użytkownika Piotrek znaleziono 3 utworzone przez niego foldery:



oraz edytowane zdjęcie jabłek (oryginał pobrany z Internetu):



Data utworzenia obrazu: 20.11.2021 godz. 20:37:51
Data modyfikacji obrazu: 20.11.2021 godz. 21:26:51

3.3.2 Folder 'Normalny folder'

W Folderze /Pulpit/Normalny folder znajdują się 2 pliki, zdjęcie zdewastowanego sadu pobrane z Internetu:

Data utworzenia: 20.11.2021 godz. 21:47:14

oraz plik tesktowy z wiadomością wyglądajacą jak zapisana w alfabecie morsa. Po odkodowaniu zawartości pliku otrzymujemy następującą wiadomość:

Tekst w alfabecie polskim do przetłumaczenia na alfabet Morse'a:

wszyscy jabłkoryści (nie używać tej nazwy przy innych!)
sprawa jest poważna, podkomisarz jabłkowiec depcze nam po piętach.
zabezpieczcie swoje maszyny, zniszczcie dowody

↓ tłumacz na alfabet Morse'a ↓

Tekst w alfabecie Morse'a do przetłumaczenia na alfabet polski (rozdzielony spacją):

... .--. .-. .- .-- .- / .--- . ... - / .--. --- .-- .- --.-. -. .- --.-- / .--. --- -.. -.- --- -- .. ... .- .-. --.. / .---
.- -... .-..- -.- --- .-- .. . -.-. / -.. . .--. -.-. --.. . / -. .- -- / .--. --- / .--. .. ..-.. - .- -.-. .... .-.-.-
--.. .- -... . --.. .--. .. . -.-. --.. -.-. .. . / ... .-- --- .--- . / -- .- ... --.. -.-- -. -.-- --..-- / --.. -. .. ... -
-.. -.-. --.. -.-. .. . / -.. --- .-- --- -.. -.--

↑ tłumacz na zwykły alfabet ↑

3.3.3 Folder 'Pomarańcze'

W folderze /Pulpit/Pomarańcze znajdują się dwa pliki .jpg, obydwa pobrane z internetu. Jeden z nich został zmodyfikowany.

Data utworzenia: 20.11.2021 godz. 19:55:40

Data utworzenia: 20.11.2021 godz. 19:58.17
Data modyfikacji: 20.11.2021 godz. 21:53:23

3.3.4 Folder 'Zdjęcie(niepodejrzane)'

Folder /Pulpit/Zdjęcie(niepodejrzane) zawiera jeden plik .jpg:

Z analizy pliku wynika, ze zdjęcie zostało wykonane aparatem NIKON COOLPIX P6000 dnia 20.10.2008 o godz. 17:00:07. Po wyszukaniu obrazu w Google dowiadujemy się, ze zdjęcie przedstawia kościół Santa Maria della Pieve we Włoszech.

3.3.5 Folder 'Documents'

W folderze /Documents poza pustymi folderami stworzonymi przez system znajdują się dwa pliki tekstowe:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Dlaczego nie warto jeść jabłek.txt			1	2021-11-20 20:36:59 CET	2021-11-20 20:36:59 CET	2021-11-20 20:36:59 CET	2021-11-20 20:36:59 CET	200
Dlaczego warto jeść pomarańcze.txt			1	2021-11-20 20:06:43 CET	2021-11-20 20:06:43 CET	2021-11-20 20:06:43 CET	2021-11-20 20:06:43 CET	677

Zawartość pliku 'Dlaczego nie warto jeść jabłek.txt':

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

Strings | Indexed Text | Translation

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset

Dowody że jabłka są niebezpieczne:

PESTKI JABŁEK TO TRUCIZNA????
KTO TO DOPUŚCIŁ DO SPRZEDAŻY?????!?!?!??!
https://zywienie.abczdrowie.pl/pestki-jablek-wyjasniamy-dlaczego-nalezy-na-nie-uwazac

----------METADATA----------

Data utworzenia pliku: 20.11.2021 godz. 20:36:59.

Zawartość pliku 'Dlaczego warto jeść pomarańcze.txt':

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

Strings | Indexed Text | Translation

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset

Dlaczego pomarańcze są najlepsze:

1. Drzewo pomarańczowe jest symbolem płodności - jego liście nie żółkną, na jednym drzewie przez 100 lat rośnie około 800-1000 pomarańcz. (źródło - interia kobiety)

2. Pomarańcze dla lepszej sylwetki - pomarańcza to TYLKO 90 kcal! (źródło - interia kobiety)

3. Pomarańcze: korzyści dla zdrowia - dużo witaminy C, fosforu, cynku itp! (LEPSZE NIŻ TE GŁUPIE JABŁKA, NIE ZNOSZĘ JABŁEK!!!!!) - (źródło - interia kobiety)

4. Pomarańcze czy sok pomarańczowy? - POMARAŃCZE (źródło - interia kobiety)

Źródło - https://kobieta.interia.pl/zdrowie/news-dlaczego-warto-jesc-pomarancze,nId,5632355

----------METADATA----------

Data utworzenia pliku: 20.11.2021 godz. 20:06:43.

3.3.6 Usunięte pliki

W odzyskanych przez Autopsy plikach znaleziono kilka zdjęć jabłek bez istotnych metadanych:

Oraz zdjęcie kościoła w miejscowości Lutynia:

Nie zawiera ono jednak również istotnych metadanych.

3.4 Historia przeglądarki

Użytkownik używał dwóch przeglądarek: FireFox oraz Internet Explorer. Historia wyszukiwania w Internet Explorer:

index.dat				google.pl	Pomarańcze	Internet Explorer	2021-11-20 18:48:11 CET	orange.img
index.dat				google.pl	Firefox	Internet Explorer	2021-11-20 18:48:56 CET	orange.img
index.dat				google.pl	Pomarańcze	Internet Explorer	2021-11-20 18:48:13 CET	orange.img
index.dat				google.pl	Pomarańcze	Internet Explorer	2021-11-20 18:48:11 CET	orange.img
index.dat				google.pl	Pomarańcze	Internet Explorer	2021-11-20 18:48:11 CET	orange.img
index.dat				google.pl	Firefox	Internet Explorer	2021-11-20 18:48:56 CET	orange.img
index.dat				google.pl	Firefox	Internet Explorer	2021-11-20 18:48:56 CET	orange.img
index.dat				google.pl	Pomarańcze	Internet Explorer	2021-11-20 18:48:21 CET	orange.img
index.dat				google.pl	Pomarańcze	Internet Explorer	2021-11-20 18:48:11 CET	orange.img
index.dat				google.pl	Firefox	Internet Explorer	2021-11-20 18:48:56 CET	orange.img

Przeglądarki tej użytkownik użył tylko do pobrania przeglądarki FireFox oraz do wyszukania hasła 'pomarańcze'.

W zapytaniach przeglądarki FireFox możemy znaleźć takie wyszukiwania jak 'tłumacz morse'a', 'Lutynia', 'sady jabłkowe wrocław', 'gospodarstwo sadownicze PIOSAD', 'klub pomarańcza katowice', 'zniszczone sady jabłkowe', 'dlaczego warto jeść pomarańcze' itp. Jeśli chodzi o wyszukiwarkę internetową, to korzystano z wyszukiwarek Google oraz DuckDuckGo.

Source File	S	C	O	Domain	Text	Program Na...	Date Accessed	Data Source
places.sqlite				duckduckgo.com	Dlaczego warto jeść pomarańcze	FireFox	2021-11-20 20:01:35 CET	orange.img
places.sqlite				duckduckgo.com	klub pomarańcza	FireFox	2021-11-20 20:33:53 CET	orange.img
places.sqlite				duckduckgo.com	klub pomarańcza	FireFox	2021-11-20 20:33:57 CET	orange.img
places.sqlite				duckduckgo.com	klub pomarańcza	FireFox	2021-11-20 20:33:57 CET	orange.img
places.sqlite				duckduckgo.com	klub pomarańcza katowice	FireFox	2021-11-20 20:34:04 CET	orange.img
places.sqlite				duckduckgo.com	klub pomarańcza katowice	FireFox	2021-11-20 20:34:04 CET	orange.img
places.sqlite				duckduckgo.com	czy klub pomarańcza w katowicach to klub dla fanów pomar...	FireFox	2021-11-20 20:34:41 CET	orange.img
places.sqlite				duckduckgo.com	czy klub pomarańcza w katowicach to klub dla fanów pomar...	FireFox	2021-11-20 20:34:41 CET	orange.img
places.sqlite				duckduckgo.com	czy klub pomarańcza w katowicach to klub dla fanów pomar...	FireFox	2021-11-20 20:34:44 CET	orange.img
places.sqlite				duckduckgo.com	Dlaczego nie warto jeść jabłek	FireFox	2021-11-20 20:34:52 CET	orange.img
places.sqlite				duckduckgo.com	Dlaczego nie warto jeść jabłek	FireFox	2021-11-20 20:34:54 CET	orange.img
places.sqlite				google.com	jabłka	FireFox	2021-11-20 20:37:16 CET	orange.img
places.sqlite				duckduckgo.com	jabłka	FireFox	2021-11-20 20:37:25 CET	orange.img
places.sqlite				duckduckgo.com	jabłka	FireFox	2021-11-20 20:37:26 CET	orange.img
places.sqlite				duckduckgo.com	jabłka	FireFox	2021-11-20 20:37:30 CET	orange.img
places.sqlite				duckduckgo.com	jabłka	FireFox	2021-11-20 20:37:31 CET	orange.img
places.sqlite				duckduckgo.com	zniszczone sady jabłkowe	FireFox	2021-11-20 21:33:45 CET	orange.img
places.sqlite				duckduckgo.com	zniszczone sady jabłkowe	FireFox	2021-11-20 21:33:46 CET	orange.img
places.sqlite				duckduckgo.com	zniszczone sady jabłkowe	FireFox	2021-11-20 21:33:48 CET	orange.img
places.sqlite				duckduckgo.com	sady jabłkowe wrocław	FireFox	2021-11-20 21:34:55 CET	orange.img
places.sqlite				duckduckgo.com	sady jabłkowe wrocław	FireFox	2021-11-20 21:34:55 CET	orange.img
places.sqlite				duckduckgo.com	sady jabłkowe wrocław	FireFox	2021-11-20 21:34:58 CET	orange.img
places.sqlite				duckduckgo.com	sady jabłkowe w pobliżu wrocławia	FireFox	2021-11-20 21:35:13 CET	orange.img
places.sqlite				duckduckgo.com	sady jabłkowe w pobliżu wrocławia	FireFox	2021-11-20 21:35:14 CET	orange.img
places.sqlite				google.com	Gospodarstwo Sadownicze PIOSAD	FireFox	2021-11-20 21:35:54 CET	orange.img
places.sqlite				duckduckgo.com	Gospodarstwo Sadownicze PIOSAD	FireFox	2021-11-20 21:36:03 CET	orange.img
places.sqlite				duckduckgo.com	Gospodarstwo Sadownicze PIOSAD	FireFox	2021-11-20 21:36:05 CET	orange.img
places.sqlite				duckduckgo.com	Gospodarstwo Sadownicze PIOSAD	FireFox	2021-11-20 21:38:10 CET	orange.img
places.sqlite				duckduckgo.com	Gospodarstwo Sadownicze PIOSAD Lutynia	FireFox	2021-11-20 21:38:24 CET	orange.img
places.sqlite				duckduckgo.com	Gospodarstwo Sadownicze PIOSAD Lutynia	FireFox	2021-11-20 21:38:25 CET	orange.img
places.sqlite				duckduckgo.com	Gospodarstwo Sadownicze PIOSAD Lutynia	FireFox	2021-11-20 21:38:28 CET	orange.img
places.sqlite				duckduckgo.com	Lutynia	FireFox	2021-11-20 21:38:35 CET	orange.img
places.sqlite				duckduckgo.com	Lutynia	FireFox	2021-11-20 21:38:36 CET	orange.img
places.sqlite				duckduckgo.com	Lutynia	FireFox	2021-11-20 21:38:38 CET	orange.img
places.sqlite				duckduckgo.com	Lutynia	FireFox	2021-11-20 21:38:50 CET	orange.img
places.sqlite				google.com	tłumacz morse'a	FireFox	2021-11-20 21:47:45 CET	orange.img

3.5 Wnioski z przeprowadzonej analizy

Komputer należał prawdopodobnie do osoby będącej fanatykiem pomarańczy i jednocześnie przeciwnikiem jabłek. Profil użytkownika wskazuje na to, że imię tej osoby to Piotr. Osoba ta należy do jakiejś zorganizowanej grupy, którą można podejrzewać o niszczenie sadów jabłkowych (wyszukiwanie sadów w Internecie, zdjęcie zniszczonego sadu, komunikat zawarty w pliku tekstowym). Z historii przeglądania wywnioskować można, że osoba ta mieszka w okolicach Wrocławia (wyszukiwania 'Lutynia', 'sady jabłkowe wrocław').

4 Analiza pamięci operacyjnej

4.1 Zrzut pamięci

Wykonany został zrzut pamięci operacyjnej przy użyciu narzędzia avml:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ./avml zrzut.dmp
[sudo] password for kali:
```

4.2 Analiza zrzutu

Przy pomocy polecenia strings oraz grep została wyszukana przykładowo informacja o przechodzeniu do jednego z katalogów w systemie plików:

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# strings ./zrzut.dmp | grep "home/kali/Desktop/sysopy"
cd /home/kali/Desktop/sysopy/lab3
cd /home/kali/Desktop/sysopy/lab
cd /home/kali/Desktop/sysopy/lab3
/home/kali/Desktop/sysopy
/home/kali/Desktop/sysopy
```

5 Kopia binarna nośnika USB

5.1 Pozyskanie kopii

Z wykorzystaniem narzędzia ewfacquire utworzona została kopia nośnika USB:

```
Acquiry completed at: Jan 11, 2022 14:21:45

Written: 1.8 GiB (2002763964 bytes) in 1 minute(s) and 57 second(s) with 16 MiB/s (17117640 bytes/second).
MD5 hash calculated over data:          e31f6e534c9e3f4256b29cd8b83073bb
ewfacquire: SUCCESS
```

5.2 Podstawowe informacje na temat obrazu

Przy pomocy narzędzie ewfinfo odczytane zostały informacje o nośniku:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ewfinfo ./file.E01
ewfinfo 20140807

Acquiry information
        Case number:            1
        Acquisition date:       Tue Jan 11 14:19:48 2022
        System date:            Tue Jan 11 14:19:48 2022
        Operating system used:  Linux
        Software version used:  20140807
        Password:               N/A
        Model:                  Flash Disk

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      3911648
        Media size:             1.8 GiB (2002763776 bytes)

Digest hash information
        MD5:                    e31f6e534c9e3f4256b29cd8b83073bb
```

Data pozyskania obrazu: Tue Jan 11 14:19:48 2022
Użyty system: Linux
Model urządzenia: Flash disk
Format pliku: EnCase 6
Typ urządzenia: removable disk
Wielkość sektora: 512B
Ilość sektorów: 3911648
Wielkość obrazu: 2 002 763 776 B

5.3 Odczytanie zawartości

Przy pomocy polecenia fls odczytana została zawartość obrazu nośnika:

```
Informatyka sledcza_LAB7.pdf
IMG_20211025_135031.jpg
Informatyka sledcza_LAB4.pdf
Informatyka sledcza_LAB6.pdf
_olla.jpg
jolla.jpg.opdownload
jolla.jpg
Kodak_CX7530.jpg
Kodak_CX7530.jpg.opdownload
Kodak_CX7530.jpg
Canon_PowerShot_S40.jpg
Canon_PowerShot_S40.jpg.opdownload
Canon_PowerShot_S40.jpg
iphone_hdr_NO.jpg
iphone_hdr_NO.jpg.opdownload
iphone_hdr_NO.jpg
cpuz_x64.exe
$MBR
$FAT1
$FAT2
$OrphanFiles
```

6 Metadane

6.1 Odczyt metadanych z wybranego pliku

Przy pomocy narzędzia ExifTool zostały odczytane metadane z poniższego obrazu:

Nazwa pliku: Canon_PowerShot_S40.jpg
Typ pliku: JPEG
Model kamery: Canon PowerShot S40
Wersja firmware kamery: Firmware Version 1.10
Obiektyw fotograficzny: 7.1 - 21.3 mm
Pole widzenia: 19.7 stopni
Orientacja: pozioma
Data utworzenia: 2003:12:14 12:01:44
Flash: Auto, nie uruchomił się
Właściciel pliku: Andreas Huggel

6.2 Zmiana metadanych

Zmieniony został właściciel pliku na 'Magda' oraz data utworzenia na 2022:01:11 20:00:00:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool ./Canon_PowerShot_S40.jpg -OwnerName=Magda  -CreateDate='2022:01:11 20:00:00'
    1 image files updated

┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool ./Canon_PowerShot_S40.jpg -OwnerName  -CreateDate
Owner Name                      : Magda
Create Date                     : 2022:01:11 20:00:00
```