# Raport 9: Pozyskiwanie dowodów cyfrowych

## Wstęp

To laboratorium ma na celu zapoznanie się z formatem EWF (E01) oraz opanowanie komend zaprezentowanych na wykładzie

Konfiguracja środowiska:

Wszystkie zadania (chyba, że zaznaczono inaczej) muszą być wykonywane na maszynie wirtualnej SIFT lub skonfigurowanej równoważnie maszynie wirtualnej z Linuksem, lub równoważnie skonfigurowanym hoście z Linuksem.

Upewnij się, że posiadasz w systemie następujące komendy w odpowiednich wersjach:

• **ewfinfo** w dowolnej wersji. Jeżeli jej nie posiadasz to zainstaluj pakiet ewf-tools (Debian/Ubuntu), ewftools (Fedora/CentOS).

• **img_stat** w dowolnej wersji, ale musisz mieć następujący wynik po jej wykonaniu z parametrem -i list:

```
$ img_stat -i list
Supported image format types:
        raw (Single or split raw file (dd))
        aff (Advanced Forensic Format)
        afd (AFF Multiple File)
        afm (AFF with external metadata)
        afflib (All AFFLIB image formats (including beta ones))
        ewf (Expert Witness Format (EnCase))
        vmdk (Virtual Machine Disk (VmWare, Virtual Box))
        vhd (Virtual Hard Drive (Microsoft))
```

Na maszynie SIFT wystarczy mieć zainstalowany pakiet sleuthkit. Pakiet w Fedorze i CentOS-ie nazywa się tak samo.

# 1. Praca z plikiem E01

Pobierz plik File item-08x1.E01.

Używając komend zaprezentowanych na wykładzie i analizując ich wyjście odpowiedz na pytania:

1. Jaki jest format (typ) obrazu?

Typ: ewf

Komenda: img_stat item-08x01.E01

Zrzut ekranu:

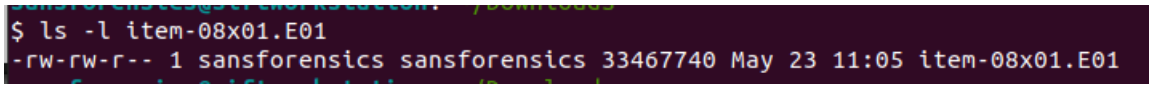
```
$ img_stat item-08x01.E01
IMAGE FILE INFORMATION
--------------------------------------------
Image Type:             ewf

Size of data in bytes:  15728640000
Sector size:    512
MD5 hash of data:       e44d0988d1d49a96d40c99b00fd80673
```

2. Jaki jest rozmiar pliku? (W bajtach.)

Rozmiar: 33467740

Komenda: ls -l item-08x01.E01

Zrzut ekranu:

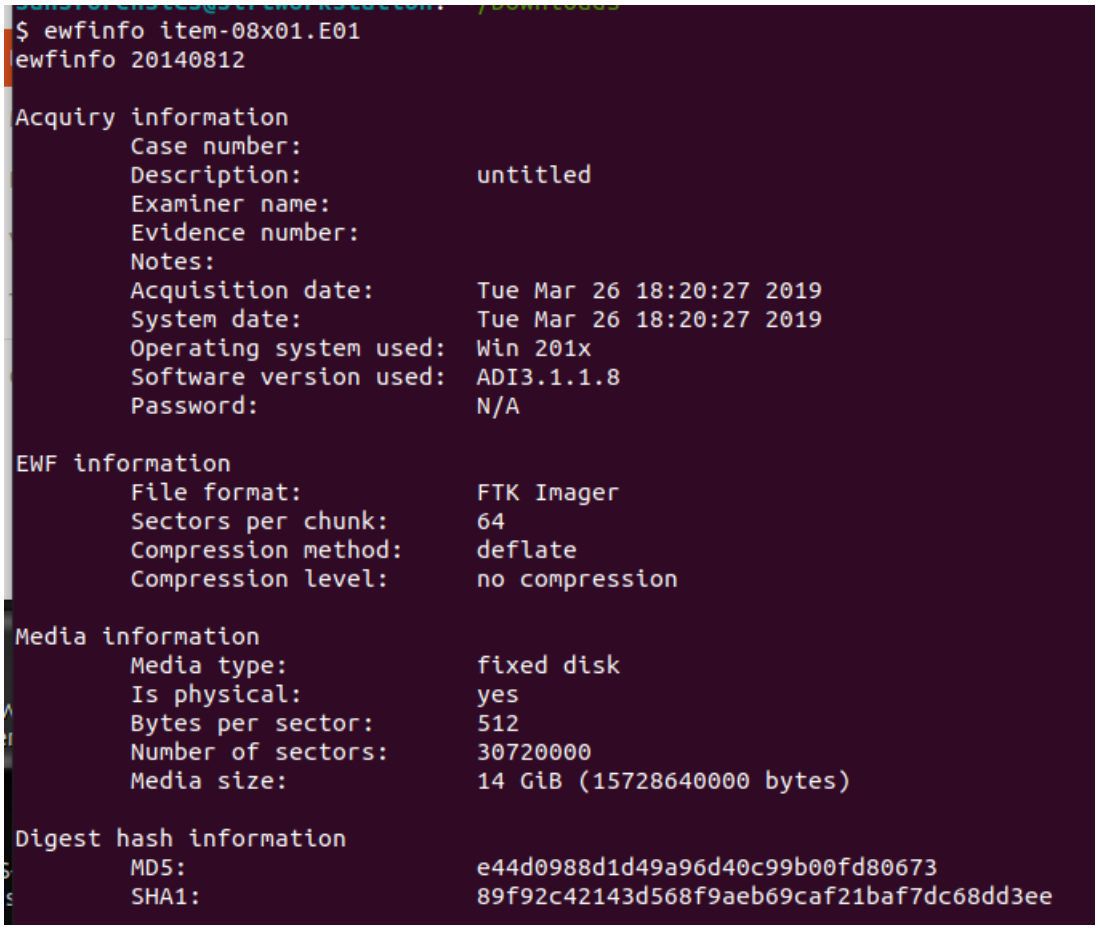



3. Jaka jest liczba sektorów w oryginalnym dysku?

Liczba sektorów: 30720000

Komenda: ewfinfo item-08x01.E01

Zrzut ekranu:

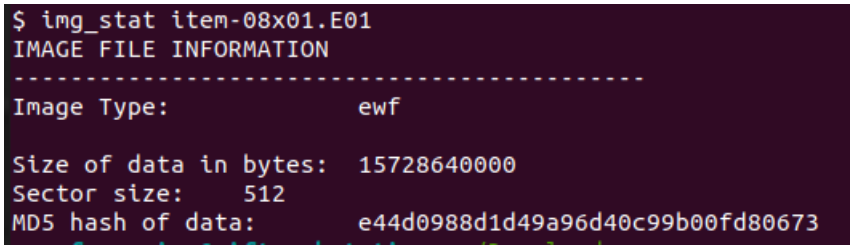



4. Jaki jest oryginalny rozmiar obrazu? (W bajtach.)

Rozmiar obrazu: 15728640000 B

Komenda: img_stat item-08x01.E01

Zrzut ekranu:



5. Jaki jest hash MD5 i SHA1 oryginalnego obrazu?

MD5: e44d0988d1d49a96d40c99b00fd80673

SHA1: 89f92c42143d568f9aeb69caf21baf7dc68dd3ee

Komenda: ewfinfo item-08x01.E01

Zrzut ekranu(pokazano tylko fragment z hashami):

```
Digest hash information
        MD5:                    e44d0988d1d49a96d40c99b00fd80673
        SHA1:                   89f92c42143d568f9aeb69caf21baf7dc68dd3ee
```

6. Kiedy został wykonany obraz?

Data wykonania: wtorek 26 marca 18:20:27 2019
Komenda: ewfinfo item-08x01.E01
Zrzut ekranu:

```
sansforensics@siftworkstation: ~/Downloads
$ ewfinfo item-08x01.E01
ewfinfo 20140812

Acquiry information
        Case number:
        Description:            untitled
        Examiner name:
        Evidence number:
        Notes:
        Acquisition date:       Tue Mar 26 18:20:27 2019
        System date:            Tue Mar 26 18:20:27 2019
        Operating system used:  Win 201x
        Software version used:  ADI3.1.1.8
        Password:               N/A
```

7. Jaka kompresja została użyta?

Kompresja: deflate bez drugiego etapu

Komenda: ewfinfo item-08x01.E01

Zrzut ekranu:

```
EWF information
        File format:            FTK Imager
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression
```

# 2. Pozyskanie obrazu za pomocą ewfacquire

Zamontuj plik E01 w taki sposób, aby mieć dostęp do formatu raw:

```
sansforensics@siftworkstation: ~/Downloads
$ sudo ewfmount item-08x01.E01 /mnt/ewf/
ewfmount 20140812
```

Ta komenda stworzy w katalogu FOLDER /mnt/ewf plik File ewf1, który będzie reprezentował oryginalny obraz dysku znajdujący się w pliku E01. Jeżeli katalog FOLDER /mnt/ewf nie istnieje (taka sytuacja będzie miała miejsce, gdy nie korzystasz z maszyny SIFT), to go stwórz.

1. Zweryfikuj, że powyższa komenda zadziałała:

```
sansforensics@siftworkstation: ~/Downloads
$ sudo ls -l /mnt/ewf
total 0
-r--r--r-- 1 root root 15728640000 May 23 12:18 ewf1
```

2. Utwórz urządzenie typu loop, które umożliwi dostęp do dysku:

```
sansforensics@siftworkstation: ~/Downloads
$ sudo losetup --find --show /mnt/ewf/ewf1
/dev/loop0
```

Komenda ta zwróci ścieżkę do urządzenia blokowego będącego dyskiem.

3. Za pomocą ewfacquire wykonaj obraz z dysku File /dev/loop0). Komenda zapyta Cię o wiele parametrów i metadanych – możesz wybrać dowolne i pobawić się konfiguracją.

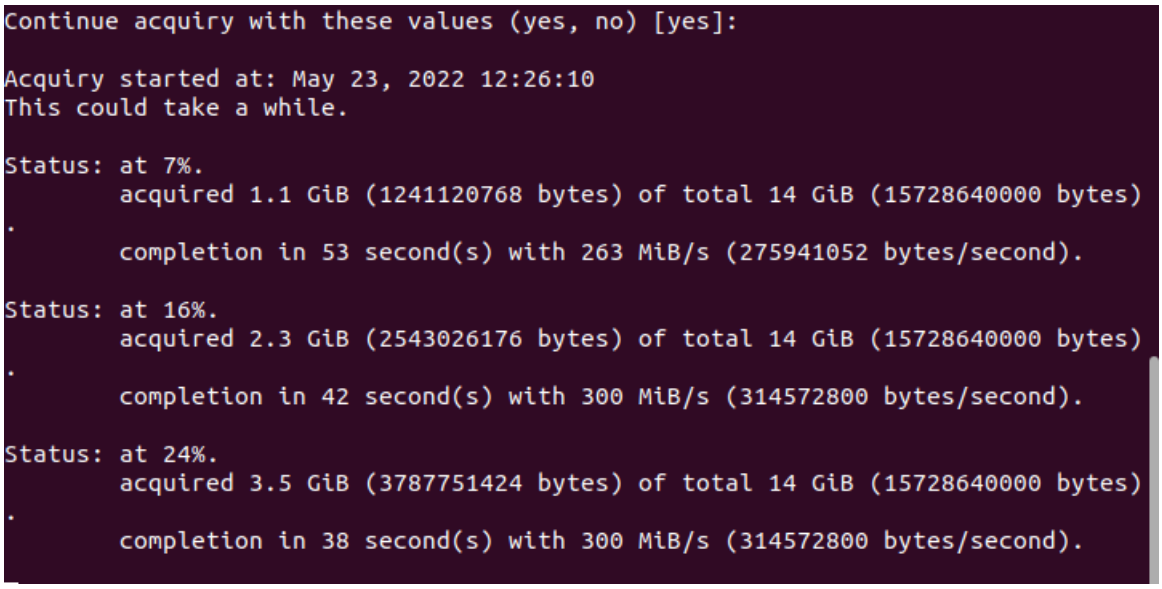
```
$ sudo ewfacquire -c -best -t ./item08x01-new /dev/loop0
ewfacquire 20140812

Device information:
Bus type:
Vendor:
Model:
Serial:

Storage media information:
Type:                                   Device
Media type:                             Fixed
Media size:                             15 GB (15728640000 bytes)
Bytes per sector:                       512

Unsupported compression values defaulting to method: deflate with level: none.
Acquiry parameters required, please provide the necessary input
Case number: 2
Description: obraz item-08x01-new
Evidence number: 1
Examiner name: PR
Notes: 2
Media type (fixed, removable, optical, memory) [fixed]:
Media characteristics (logical, physical) [physical]:
Use EWF file format (ewf, smart, ftk, encase1, encase2, encase3, encase4, encas
e5, encase6, linen5, linen6, ewfx) [encase6]:
```

```
The following acquiry parameters were provided:
Image path and filename:                ./item08x01-new.E01
Case number:                            2
Description:                            obraz item-08x01-new
Evidence number:                        1
Examiner name:                          PR
Notes:                                  2
Media type:                             fixed disk
Is physical:                            yes
EWF file format:                        EnCase 6 (.E01)
Compression method:                     deflate
Compression level:                      none
Acquiry start offset:                   0
Number of bytes to acquire:             14 GiB (15728640000 bytes)
Evidence segment file size:             1.4 GiB (1572864000 bytes)
Bytes per sector:                       512
Block size:                             64 sectors
Error granularity:                      64 sectors
Retries on read error:                  2
Zero sectors on read error:             no
```

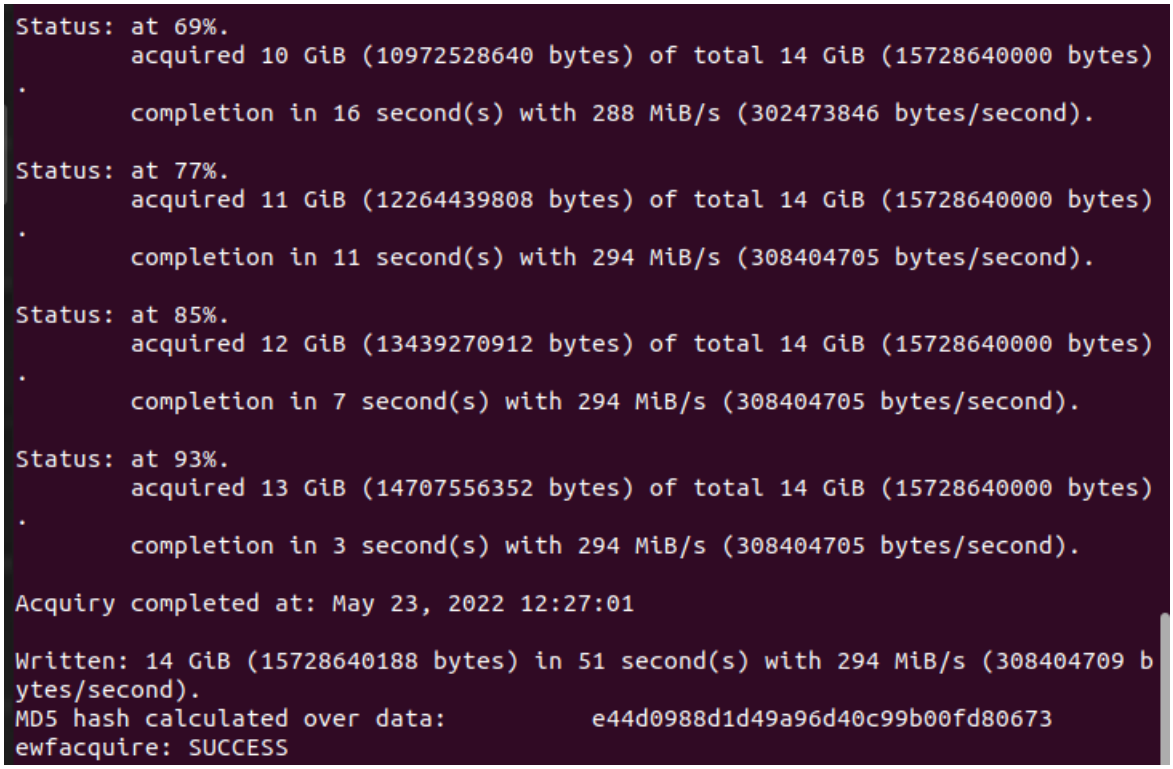
Wywołanie komendy powoduje wypisanie parametrów urządzenia ;.

Następnie prosi o nas o uzupełnienie kilku elementów takich jak numer sprawy, opis, numer dowodu, imię sprawdzającego. Następnie ukazują nam się parametry przetwarzania np. zakres pozyskiwanych danych. Po wykonaniu tych działań ukazuje nam się podsumowanie wprowadzonych parametrów.

Początek przetwarzania:




Koniec przetwarzania:




Zakończono sukcesem.

Sprawdzamy czy istnieją różnice między pierwotnym a nowoutworzonym obrazem.

Pierwotny obraz:

```
sansforensics@siftworkstation: ~/Downloads
$ ewfinfo item-08x01.E01
ewfinfo 20140812

Acquiry information
        Case number:
        Description:            untitled
        Examiner name:
        Evidence number:
        Notes:
        Acquisition date:       Tue Mar 26 18:20:27 2019
        System date:            Tue Mar 26 18:20:27 2019
        Operating system used:  Win 201x
        Software version used:  ADI3.1.1.8
        Password:               N/A

EWF information
        File format:            FTK Imager
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      30720000
        Media size:             14 GiB (15728640000 bytes)

Digest hash information
        MD5:                    e44d0988d1d49a96d40c99b00fd80673
        SHA1:                   89f92c42143d568f9aeb69caf21baf7dc68dd3ee
```

Nowy obraz:

```
$ ewfinfo item08x01-new.E01
ewfinfo 20140812

Acquiry information
        Case number:            2
        Description:            obraz item-08x01-new
        Examiner name:          PR
        Evidence number:        1
        Notes:                  2
        Acquisition date:       Mon May 23 12:26:10 2022
        System date:            Mon May 23 12:26:10 2022
        Operating system used:  Linux
        Software version used:  20140812
        Password:               N/A

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      no compression
        Set identifier:         49585270-7ffd-0000-3196-54b4a5550000

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      30720000
        Media size:             14 GiB (15728640000 bytes)

Digest hash information
        MD5:                    e44d0988d1d49a96d40c99b00fd80673
```

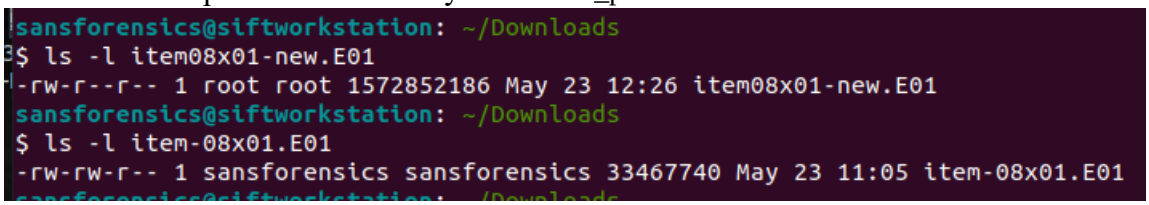
Parametry w sekcji Acquiry information, a także EWF information różnią się, ale wynika to z wprowadzonych zmian parametrów i konfiguracji. Natomiast parametry z sekcji Media Information takie jak liczba sektorów oraz wygenerowany hash MD5 są identyczne.

Porównanie na podstawie komendy img_stat:

```
sansforensics@siftworkstation: ~/Downloads
$ img_stat item-08x01.E01
IMAGE FILE INFORMATION
--------------------------------------------
Image Type:             ewf

Size of data in bytes:  15728640000
Sector size:    512
MD5 hash of data:       e44d0988d1d49a96d40c99b00fd80673
sansforensics@siftworkstation: ~/Downloads
$ img_stat item08x01-new.E01
IMAGE FILE INFORMATION
--------------------------------------------
Image Type:             ewf

Size of data in bytes:  15728640000
Sector size:    512
MD5 hash of data:       e44d0988d1d49a96d40c99b00fd80673
```

Wywołane parametry niczym się od siebie nie różnią.

Porównanie na podstawie komendy ls -l nazwa_pliku.E01




Pliki różnią się rozmiarem.

# 3 TRIM

Poszukaj informacji o tym, czym jest mechanizm TRIM w dyskach SSD. Znajdź przynajmniej jeden whitepaper lub opis techniczny (Wikipedia się nie liczy).

TRIM jest poleceniem, przy użyciu którego system operacyjny może poinformować dysk półprzewodnikowy (SSD), które bloki danych nie są już potrzebne i można je usunąć lub oznaczyć jako wolne do przepisania. Mówiąc inaczej, TRIM to polecenie, które pomaga systemowi operacyjnemu dokładnie wiedzieć, gdzie są przechowywane dane, które chce się przenieść lub usunąć. W ten sposób dysk SSD może uzyskać dostęp tylko do bloków zawierających dane. Ponadto za każdym razem, gdy użytkownik lub system operacyjny wyda polecenie usunięcia, polecenie TRIM natychmiastowo usuwa dane strony lub bloki. Oznacza to, że następnym razem, gdy system operacyjny spróbuje zapisać nowe dane w tym obszarze, nie będzie musiał najpierw czekać na ich usunięcie.

Gdyby polecenie TRIM nie istniało (jak miało to miejsce przed Windows 7), dysk SSD nie wiedziałby, że określone sektory na dysku zawierają nieprawidłowe informacje, dopóki nie wypłynie od komputera do napędu komunikat, aby zapisał nowe informacje w tej lokalizacji. Dysk musiałby usunąć istniejące informacje, a następnie zapisać nowe. Zajmuje to nieco więcej czasu niż tylko zapisywanie nowych informacji, więc korzystanie z funkcji TRIM i Active Garbage Collection pomaga dyskowi SSD w szybszym wykonywaniu poleceń zapisu.

TRIM wpływa również na żywotność dysku SSD. Jeśli dane są zapisywane i usuwane przez cały czas z tych samych komórek NAND, te komórki zaczną się zużywać - utracą integralność. Aby zapewnić optymalną żywotność, każda komórka powinna być wykorzystywana mniej więcej w takim samym tempie, jak inne komórki. Nazywa się to wyrównaniem zużycia. Polecenie TRIM informuje dysk SSD, które komórki można wymazać w czasie bezczynności, co umożliwia również dyskowi uporządkowanie pozostałych komórek wypełnionych danymi i pustych komórek do zapisu, aby uniknąć niepotrzebnego wymazywania i przepisywania.

Największą zaletą TRIM jest oszczędność czasu dzięki możliwości usuwania danych z dysku SSD, gdy komputer jest bezczynny, zamiast poświęcania dodatkowego czasu podczas procesu zapisu na usunięcie danych, które nie są już ważne. Ponieważ usługa Active Garbage Collection przenosi powiązane segmenty danych obok siebie, dynamiczne równoważenie zużycia działa wydajniej. Wyrzucanie elementów bezużytecznych i przycinanie działają z wyrównywaniem zużycia, algorytmem zapewniającym, że każda komórka jest zapisywana i usuwana mniej więcej tyle samo razy, co wszystkie inne komórki. Wydłuża to żywotność dysku SSD.

TRIM a systemy operacyjne:

Komenda TRIM jest wysyłana do kontrolera dysku SSD automatycznie przez system operacyjny za każdym razem kiedy usuwa plik (oczywiście jeśli funkcjonalność jest włączona w OS-ie i jest wspierana – Windows 7 i wyższe wspierają TRIM natywnie, natomiast Mac OS wspiera TRIM jedynie dla Apple's OEM SSDs, czyli dysków przeznaczonych dla komputerów Mac).

Dyski SSD jako dowody cyfrowe:

W wyniku powyżej opisanego powiązania między dyskiem SSD a systemami operacyjnymi, tworzą się dość spore i nowe problemy w przypadku analizy dowodów cyfrowych. Usunięte dane, które podejrzany próbował zniszczyć np. poprzez formatowanie dysku, mogą zostać utracone na zawsze w przeciągu kilku minut. Nawet wyłączenie komputera, którego dotyczy problem, natychmiast po wydaniu polecenia, nie jest w stanie zatrzymać niszczenia. Po ponownym uruchomieniu urządzenie dysk SSD będzie wciąż sam czyścił całą zawartość, nawet w przypadku użycia blokera (urządzenie, które uniemożliwia zapisanie pliku, czyli wprowadzenie w nim zmian). Jeżeli proces samozniszczenia już się rozpoczął, nie ma możliwości jego zatrzymania, chyba że mamy do czynienia z niezwykle ważnymi dowodami, w którym to przypadku dysk wraz z nakazem sądowym może zostać przesłany do producenta w celu odzyskania danych. Jednak ze względu na ochronę danych osobowych uzyskanie sądowego nakazu bywa bardzo trudne.

**Z pracy Piotra Karaska: Odzyskiwanie usuniętych dowodów cyfrowych w postępowaniu karnym**

Tę właściwość dysków SSD zbadali B. B. Bell i R. Boddington, którzy w 2010 r. przeprowadzili serię eksperymentów mających na celu sprawdzenie, jaki jest wpływ *garbage collection* na zabezpieczanie cyfrowego materiału dowodowego i poszukiwanie danych usuniętych z dysków SSD. Rezultaty ich pracy potwierdziły wcześniejsze obawy, że skasowane przez użytkownika dowody cyfrowe podlegają ciągłemu, automatycznemu procesowi trwałego usuwania danych. Ujawniony został również inny, bardzo poważny problem: ponieważ wspomniane zmiany w strukturze danych są wprowadzane w pełni niezależnie od pracy systemu operacyjnego, usuwanie „niepotrzebnych" plików trwa zawsze wtedy, gdy dysk SSD jest podłączony do zasilania, a więc również podczas wykonywania dowodowej kopii danych. Może się więc zdarzyć, że dane ulegną modyfikacji zanim ich kopia zostanie uwierzytelniona przez biegłego czy specjalistę za pomocą sumy kontrolnej, a w efekcie standardowa weryfikacja integralności danych nie będzie możliwa. Co więcej, procesom tym nie zapobiega stosowanie sprzętowych blokerów zapisu. Autorzy sugerują, że byłoby to możliwe poprzez fizyczne wymontowanie sterownika dysku przed podjęciem próby zabezpieczenia danych. Jednocześnie jednak słusznie dodają, że stanowiłoby to duże wyzwanie techniczne.

Źródła:

https://www.crucial.com/articles/about-ssd/what-is-trim

https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1051&context=m sia_etds

https://www.digitalcitizen.life/simple-questions-what-trim-ssds-why-it-useful/

https://belkasoft.com/download/info/SSD%20Forensics%202012.pd