

Sprawozdanie DFIR KRYCY

Autorzy:

Paweł Gryka, Michał Wawrzyńczak

Opis sprawy

Pracownik firmy na wysokim stanowisku zaakceptował dużą sumę pieniędzy od konkurencyjnej firmy w zamian za zrobienie poważnego wycieku danych. Otrzymaliśmy używane przez niego urządzenia i nośniki danych i naszym zadaniem jest znalezienie wszystkich dowodów cyfrowych mówiących o wycieku.

Zadanie

Nasze zadanie polegało na przeanalizowaniu sprawy `Data Leakage Case` od NIST i odpowiedzeniu na co najmniej 7 wbranych pytań zawartych na [tej stronie](#).

Wybór pytań

Żeby nie wybrać najprostszych pytań zdecydowaliśmy się na użycie generatora liczb losowych w zakresie 1-60 by to on wybrał nam realizowane zadania. Generator wybrał liczby:

[1,7,10,19,22,25,39,41]

Więc zadania o właśnie tych numerach zrealizowaliśmy.

Gdy na liście znajdowały się zadania powiązane z tymi wylosowanymi to także je wykonywaliśmy.

Wykorzystane narzędzia

Do wykonania zadania używaliśmy obu zaproponowanych narzędzi (`AUTOPSY 4.19.3`, `AXIOM v5.8.0.27495` oraz `FTKImager 4.7.1.2`) oraz innych, które potrzebne były do wykonania specyficznych zadań (np. `Thumbnail database viewer`). Zadania realizowaliśmy oddzielnie na dwóch różnych komputerach. Oba posiadały system operacyjny Windows 10, oraz odpowiednio procesory I7-9750H oraz R7-4800H.

Case Details

Case

Case Name: KRYCY_DFIR_LAB
Case Number: 2022_01_26__1__
Created Date: 2022/01/26 20:33:43 (CET)
Case Directory: D:\OneDrive - Politechnika Warszawska\PW\Semestr V\KRYCY\lab3\autopsy\KRYCY_DFIR_LAB
Case Type: Single-user case
Database Name: D:\OneDrive - Politechnika Warszawska\PW\Semestr V\KRYCY\lab3\autopsy\KRYCY_DFIR_LAB\autopsy.db
Case UUID: krycy_dfir_lab_20220126_203343

Examiner

Name: Michał Wawrzyńczak
Phone: 111222333
Email: random@mail.com
Notes: KRYCY DFIR LAB

Organization

Name: Not Specified
Point of Contact:
Phone:
Email:

[Edit Details](#) [Close](#)

1. What are the hash values (MD5 & SHA-1) of all images? Does the acquisition and verification hash value match?

Dokonano sprawdzenia wartości skrótów wszystkich kopii binarnych, wartości wyliczone w trakcie weryfikacji zgadzają się z wartościami zapisanymi w czasie akwizycji.

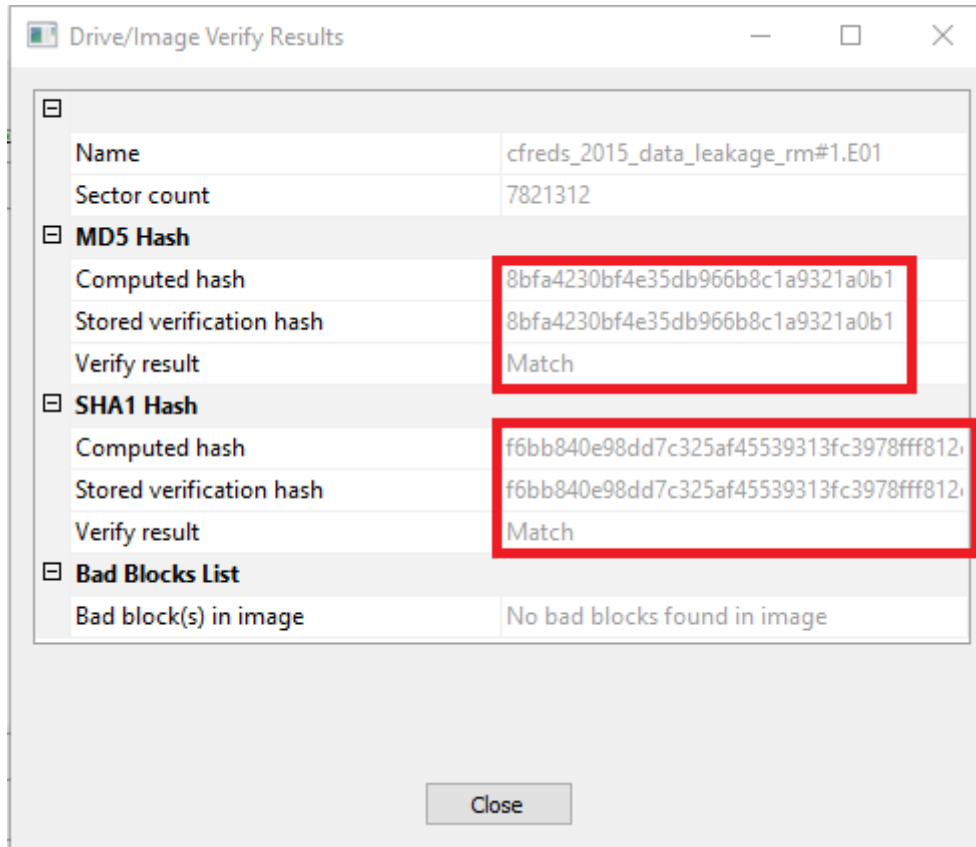
- Komputer

Drive/Image Verify Results

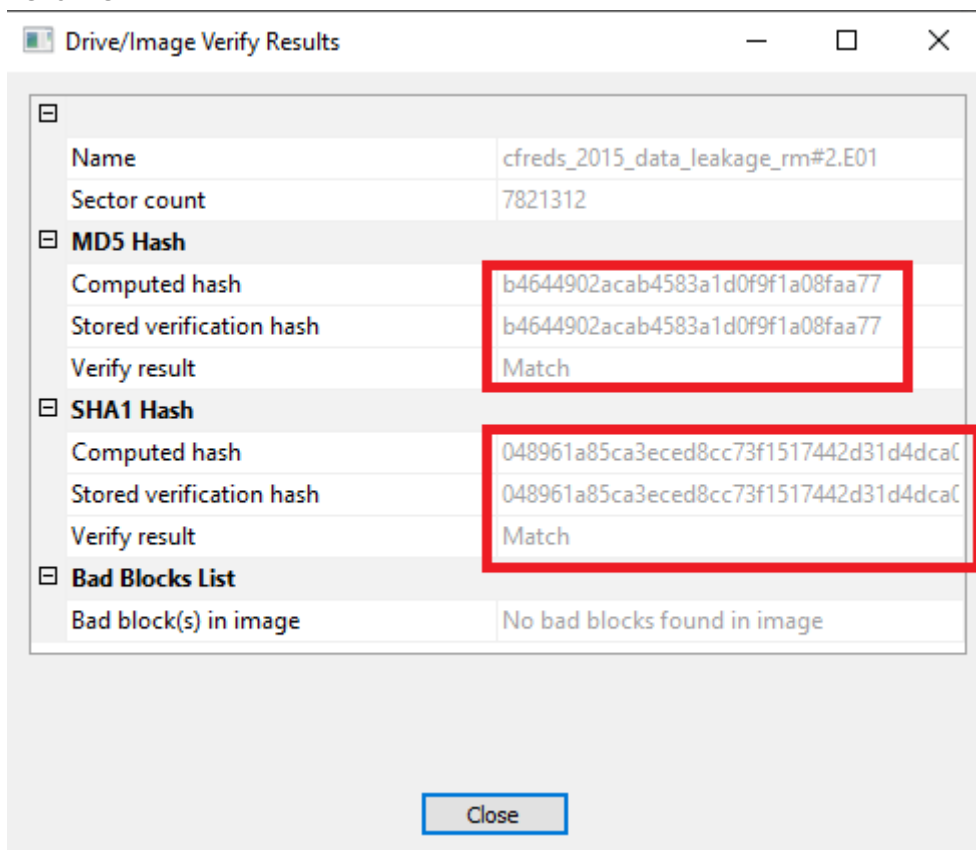
Name	cfreds_2015_data_leakage_pc.E01
Sector count	41943040
MD5 Hash	
Computed hash	a49d1254c873808c58e6f1bcd60b5bde
Stored verification hash	a49d1254c873808c58e6f1bcd60b5bde
Verify result	Match
SHA1 Hash	
Computed hash	afe5c9ab487bd47a8a9856b1371c2384d44fd785
Stored verification hash	afe5c9ab487bd47a8a9856b1371c2384d44fd785
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

[Close](#)

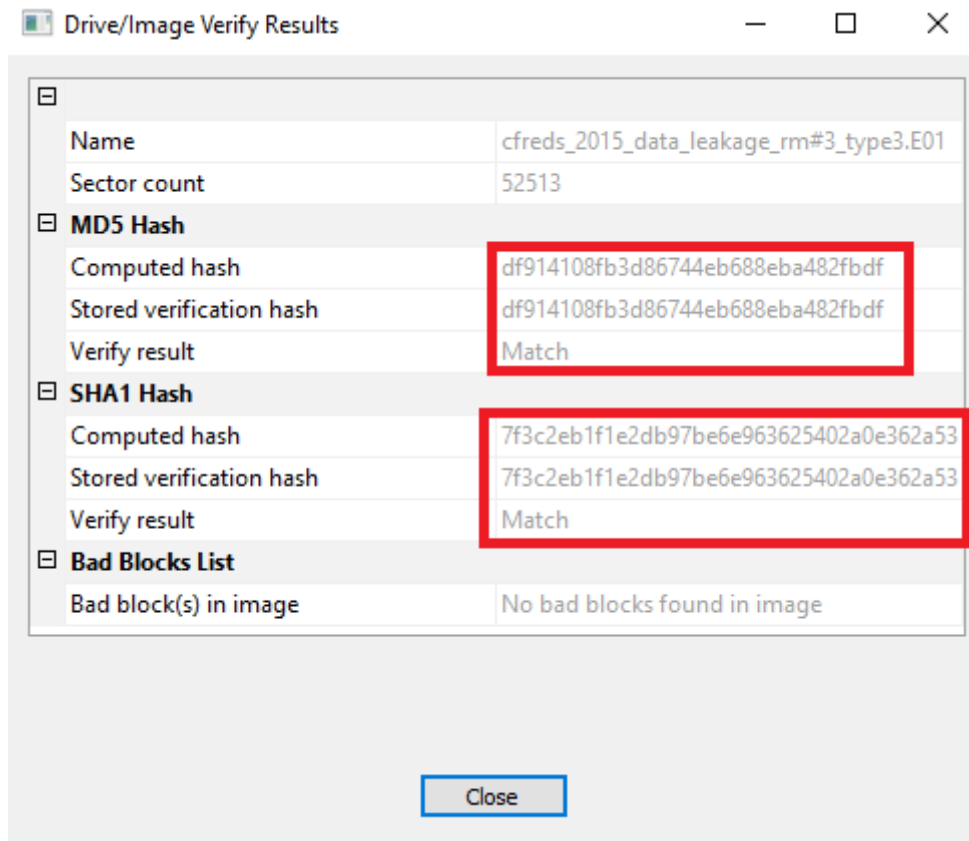
- Pendrive 1



- Pendrive2



- Płyta



7. Who was the last user to logon into PC?

Jako ostani na tym komputerze był uzytkownik o nawie uzytkownika **informant**

- Axiom

User...	Full...	Type...	Security Identifier	Profile Path	Last Login...	Last Password...	Pass...	Pass...
informant		Local User	S-1-5-21-2425377081-312...	C:\Users\informant	25.03.2015 10:45:59	22.03.2015 10:33:54	True	IAMAN
informant		Local User	S-1-5-21-2425377081-312...	C:\Users\informant	25.03.2015 09:06:08	22.03.2015 10:33:54	True	IAMAN
admin11	admin11	Local User	S-1-5-21-2425377081-312...	C:\Users\admin11	22.03.2015 11:57:02	22.03.2015 11:52:10	True	
temporary	temporary	Local User	S-1-5-21-2425377081-312...	C:\Users\temporary	22.03.2015 11:55:57	22.03.2015 11:53:11	True	
Administrator		Local User	500		20.11.2010 22:47:20	20.11.2010 22:57:24	False	
		Built-in	S-1-5-18	%systemroot%\syste...				

- Autopsy

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				systemprofile	cfreds_201...	Local		
S-1-5-19				LocalService	cfreds_201...	Local		
S-1-5-20				NetworkService	cfreds_201...	Local		
S-1-5-21-2425377081-3129163575-2985601102-1000			0	informant	cfreds_201...	Local		2015-03-22 10:33:54 EDT

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

Basic Properties

Login: informant
 Full Name:
 Address: S-1-5-21-2425377081-3129163575-2985601102-1000
 Type:
 Creation Date: 2015-03-22 10:33:54 EDT

cfreds 2015 data leakage pc.E01 1 Host Details

Last Login: 2015-03-25 14:06:08 CET
 Login Count: 9
 Administrator: True
 Password Hint: IAMAN
 Password Fail Date: 2015-03-22 16:57:48 CET
 Password Settings: Password does not expire, Password not required
 Flag: Normal user account
 Last Login: 2015-03-25 15:45:59 CET
 Login Count: 10
 Administrator: True
 Password Hint: IAMAN
 Password Fail Date: 2015-03-25 15:45:43 CET
 Password Settings: Password does not expire, Password not required
 Flag: Normal user account
 Home Directory: C:/Users/informant
 Home Directory: C:/Users/informant

Realm Properties

Name: Unknown
 Address: S-1-5-21-2425377081-3129163575-2985601102
 Scope: Local
 Confidence: Inferred

W trakcie realizowania tego zadania zauważyliśmy, przesunięcie w czasie pomiędzy datami prezentowanymi przez Autopsy oraz Axiom. Sprawdziliśmy zgodność ustawionych stref czasowych w obu programach. Pomimo pozornej zgodności przesunięcie czasowe występuje i nie udało nam się tego "naprawić".

AUTOPSY

When displaying times:

☐ Use local time zone

☒ Use another time zone

(GMT-5:00) US/Eastern

(GMT-5:00) US/Michigan

(GMT-4:00) America/Anguilla

AXIOM

DATE AND TIME FORMAT

Date format: DD.MM.YYYY 28.08.2014

☒ Use system date and time format

Time format: 24-hour clock

TIME ZONE

Time zone: (UTC-05:00) Eastern Time (US & Canada)

☐ Use system time zone

☒ Apply daylight saving time (DST)

☐ Set this time zone as the default for all cases

CANCEL
OKAY

Dodatkowo w Axiomie widoczny jest dodatkowy rekord z późniejszą datą zalogowania przez tego samego użytkownika **informant**, rekord ten różni się od pozostałych data source'em. Może to świadczyć o próbie zatarcia jakiś śladów.

Source **cfreds_2015_data_leakage_pc.E01 - Partition 2 (Microsoft NTFS, 19.9 GB)\Windows\System32\config\SAM**

Source **cfreds_2015_data_leakage_pc.E01 - Partition 2 (Microsoft NTFS, 19.9 GB)\Windows\System32\config\RegBack\SAM**

10. What applications were installed by the suspect after installing OS?

Data instalacja systemu operacyjnego:

EVIDENCE (2)

Column view

Operating Sys...	Versi...	Installed/Updated Date/Time	Product Key	Owner
Windows 7 Ultimate ()	6.1	22.03.2015 10:34:26	D4F6K-QK3RD-TMVMJ-BBMRX-3MBMV	informant
Windows 7 Ultimate ()	6.1	22.03.2015 10:34:26	D4F6K-QK3RD-TMVMJ-BBMRX-3MBMV	informant

Programy instalowane przez urzytkownika:

EVIDENCE (14)

Column view

Application Name	Company	Crea...	Key Last Up...	Insta...	Version	Potential Location
Bonjour	Apple Inc.	23.03.2015	23.03.2015 16:00:58	2052	3.0.0.10	
Eraser 6.2.0.2962	The Eraser Project	25.03.2015	25.03.2015 10:57:31	18308	6.2.2962	
Google Chrome	Google Inc.	22.03.2015	22.03.2015 11:11:51		41.0.2272.101	C:\Program Files (x86)\Google\Chrome\Application
Google Update Helper	Google Inc.	22.03.2015	22.03.2015 11:16:03	29	1.3.26.9	
Google Drive	Google, Inc.	23.03.2015	23.03.2015 16:02:46	38784	1.20.8672.3137	
Apple Application Support	Apple Inc.	23.03.2015	23.03.2015 16:00:45	96831	3.0.6	
Apple Software Update	Apple Inc.	23.03.2015	23.03.2015 16:01:01	2441	2.1.3.127	
iCloud	Apple Inc.	23.03.2015	23.03.2015 16:01:54	94234	4.0.6.28	
Bonjour	Apple Inc.	23.03.2015	23.03.2015 16:00:58	2052	3.0.0.10	
Google Chrome	Google Inc.	22.03.2015	22.03.2015 11:11:51		41.0.2272.101	C:\Program Files (x86)\Google\Chrome\Application
Google Update Helper	Google Inc.	22.03.2015	22.03.2015 11:16:03	29	1.3.26.9	
Google Drive	Google, Inc.	23.03.2015	23.03.2015 16:02:46	38784	1.20.8672.3137	
Apple Application Support	Apple Inc.	23.03.2015	23.03.2015 16:00:45	96831	3.0.6	
Apple Software Update	Apple Inc.	23.03.2015	23.03.2015 16:01:01	2441	2.1.3.127	

Program Name	Date/Time
Google Chrome v.41.0.2272.101	2015-03-22 10:11:51 EDT
Google Update Helper v.1.3.26.9	2015-03-22 10:16:03 EDT
Apple Application Support v.3.0.6	2015-03-23 15:00:45 EDT
Bonjour v.3.0.0.10	2015-03-23 15:00:58 EDT
Apple Software Update v.2.1.3.127	2015-03-23 15:01:01 EDT
iCloud v.4.0.6.28	2015-03-23 15:01:54 EDT
Google Drive v.1.20.8672.3137	2015-03-23 15:02:46 EDT
DXM_Runtime	2015-03-25 05:15:21 EDT
MPlayer2	2015-03-25 05:15:21 EDT
Microsoft .NET Framework 4 Client Profile v.4.0.30319	2015-03-25 09:51:39 EDT
Microsoft .NET Framework 4 Client Profile v.4.0.30319	2015-03-25 09:52:06 EDT
Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 09:54:06 EDT
Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 09:54:33 EDT
Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 09:57:31 EDT

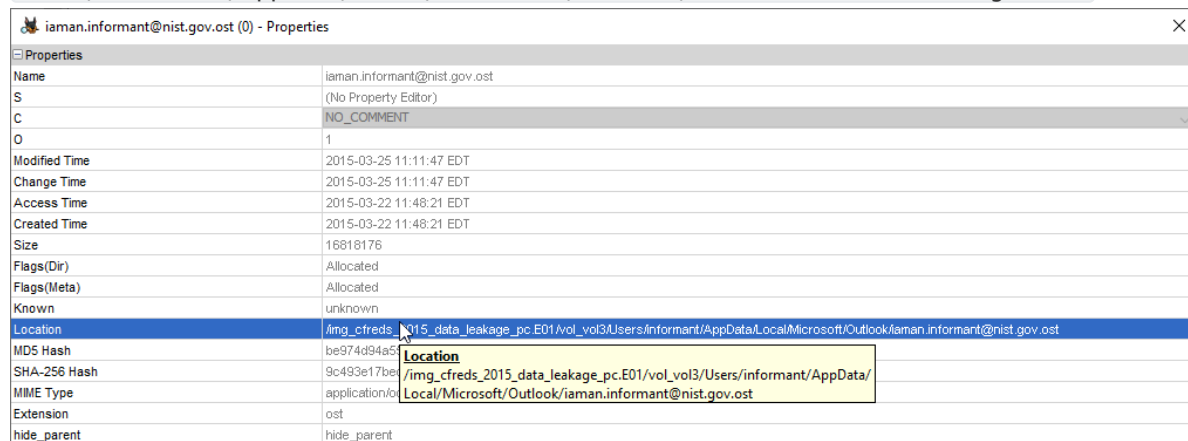
Interesujący jest fak, że na komputerze zainstalowany został program **Eraser**.

Eraser - program przeznaczony do trwałego usuwania plików przez ich zamazanie, pracujący w środowisku Windows, wydany na licencji GPL. Trwale usuwa pliki przez ich wielokrotne nadpisanie wcześniej wybranym wzorcem.

19. Where is the e-mail file located?

Plik zawierający e-mail'e znajduje się w:

Users/informant/AppData/Local/Microsoft/Outlook/iaman.iaman@nist.gov.ost



Properties

Name: iaman.iaman@nist.gov.ost

S: (No Property Editor)

C: NO_COMMENT

O: 1

Modified Time: 2015-03-25 11:11:47 EDT

Change Time: 2015-03-25 11:11:47 EDT

Access Time: 2015-03-22 11:48:21 EDT

Created Time: 2015-03-22 11:48:21 EDT

Size: 16818176

Flags(Dir): Allocated

Flags(Meta): Allocated

Known: unknown

Location: /img_cfreds_2015_data_leakage_pc.E01/vol3/Users/informant/AppData/Local/Microsoft/Outlook/iaman.iaman@nist.gov.ost

MD5 Hash: be974d94a5

SHA-256 Hash: 9c493e17be

MIME Type: application/octet-stream

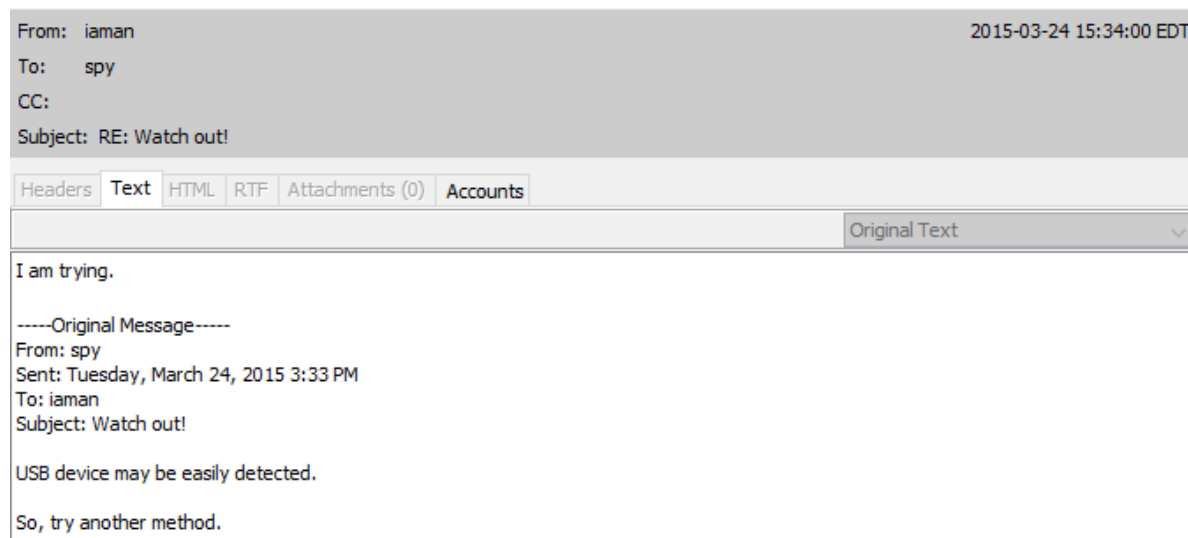
Extension: .ost

hide_parent: hide_parent

W pliku tym znajdują się 14 wiadomości. Część z nich została usunięta.

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plain...	Message ID	Path
iaman.iaman@nist.gov.ost				iaman	spy	RE: Watch out!	2015-03-24 15:34:00 EDT	I am trying,-----O...	2105284	\\Root - Mailbox\IPM_SUBTREE\Deleted Items
iaman.iaman@nist.gov.ost				iaman	spy	RE: Last request	2015-03-24 09:35:00 EDT		2104484	\\Root - Mailbox\IPM_SUBTREE\Deleted Items
iaman.iaman@nist.gov.ost				spy: spy.conspirator@nist.gov		RE: It's me	2015-03-23 16:41:22 EDT		2103300	\\Root - Mailbox\IPM_SUBTREE\Deleted Items
iaman.iaman@nist.gov.ost				iaman	spy	Done	2015-03-24 17:05:00 EDT		2105860	\\Root - Mailbox\IPM_SUBTREE\Deleted Items
iaman.iaman@nist.gov.ost				spy: spy.conspirator@nist.gov		Hello, Iaman	2015-03-23 13:29:29 EDT		2098340	\\Root - Mailbox\IPM_SUBTREE\Inbox
iaman.iaman@nist.gov.ost				spy: spy.conspirator@nist.gov		Good job, buddy.	2015-03-23 15:15:00 EDT		2100772	\\Root - Mailbox\IPM_SUBTREE\Inbox
iaman.iaman@nist.gov.ost				spy: spy.conspirator@nist.gov		RE: Good job, buddy.	2015-03-23 15:20:41 EDT		2101476	\\Root - Mailbox\IPM_SUBTREE\Inbox
iaman.iaman@nist.gov.ost				spy: spy.conspirator@nist.gov		Important request	2015-03-23 15:26:23 EDT		2101700	\\Root - Mailbox\IPM_SUBTREE\Inbox
iaman.iaman@nist.gov.ost				spy: spy.conspirator@nist.gov		Last request	2015-03-24 09:25:59 EDT		2103780	\\Root - Mailbox\IPM_SUBTREE\Inbox
iaman.iaman@nist.gov.ost				iaman	spy	RE: Hello, Iaman	2015-03-23 14:44:00 EDT		2098692	\\Root - Mailbox\IPM_SUBTREE\Sent Items
iaman.iaman@nist.gov.ost				iaman	spy	RE: Important request	2015-03-23 15:27:00 EDT		2101796	\\Root - Mailbox\IPM_SUBTREE\Sent Items
iaman.iaman@nist.gov.ost				iaman	iaman	Synchronization Log:	2015-03-23 15:57:30 EDT		2102468	\\Root - Mailbox\IPM_SUBTREE\Sync Issues
iaman.iaman@nist.gov.ost				iaman	iaman	Synchronization Log:	2015-03-25 11:01:49 EDT		2106724	\\Root - Mailbox\IPM_SUBTREE\Sync Issues
iaman.iaman@nist.gov.ost				iaman	iaman	Synchronization Log:	2015-03-25 11:01:55 EDT		2106820	\\Root - Mailbox\IPM_SUBTREE\Sync Issues

Wśród wiadomości usuniętych znajdują się m.in. następująca konwersacja między "spy" a "iaman".



From: iaman 2015-03-24 15:34:00 EDT

To: spy

CC:

Subject: RE: Watch out!

Headers Text HTML RTF Attachments (0) Accounts

Original Text

I am trying.

-----Original Message-----

From: spy

Sent: Tuesday, March 24, 2015 3:33 PM

To: iaman

Subject: Watch out!

USB device may be easily detected.

So, try another method.

22. List external storage devices attached to PC.

Do komputera podłączone zostały następujące urządzenia usb:

EVIDENCE (9)

Column view

Device Class ID	Serial Number	Friendly...	Asso...	Last...	Last Conne...	First Connected...	First Connect...	Install I
VID_0E0F&PID_0002	68b77da92&0&2				25.03.2015 09:05:36			25.03.20'
VID_0E0F&PID_0003	68b77da92&0&1				25.03.2015 09:05:36			25.03.20'
VID_0E0F&PID_0003&MI_00	782a7d3009&0&0000				25.03.2015 09:05:36			25.03.20'
Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01	4C530012550531106501&0	SanDisk Cruzer...			24.03.2015 15:38:09	2015-03-24 09:58:32	24.03.2015 09:58:33	24.03.20'
ROOT_HUB20	5&299e1c9f&0				25.03.2015 09:05:35			25.03.20'
VID_0E0F&PID_0003&MI_01	782a7d3009&0&0001				25.03.2015 09:05:36			25.03.20'
ROOT_HUB	5&3bb57b&0				25.03.2015 09:05:35			25.03.20'
Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01	4C530012450531101593&0	SanDisk Cruzer...			24.03.2015 09:38:00	2015-03-23 14:31:10	24.03.2015 09:38:00	23.03.20'
Disk&Ven_VMware_8&Prod_VMware_Virtual_S	5&22be343f&0&000000	VMware, VMwa...			25.03.2015 09:05:27			25.03.20'

Wśród nich można wyróżnić następujące urządzenia pamięci masowej. Były to podobne urządzenia różniące się numerem seryjnym

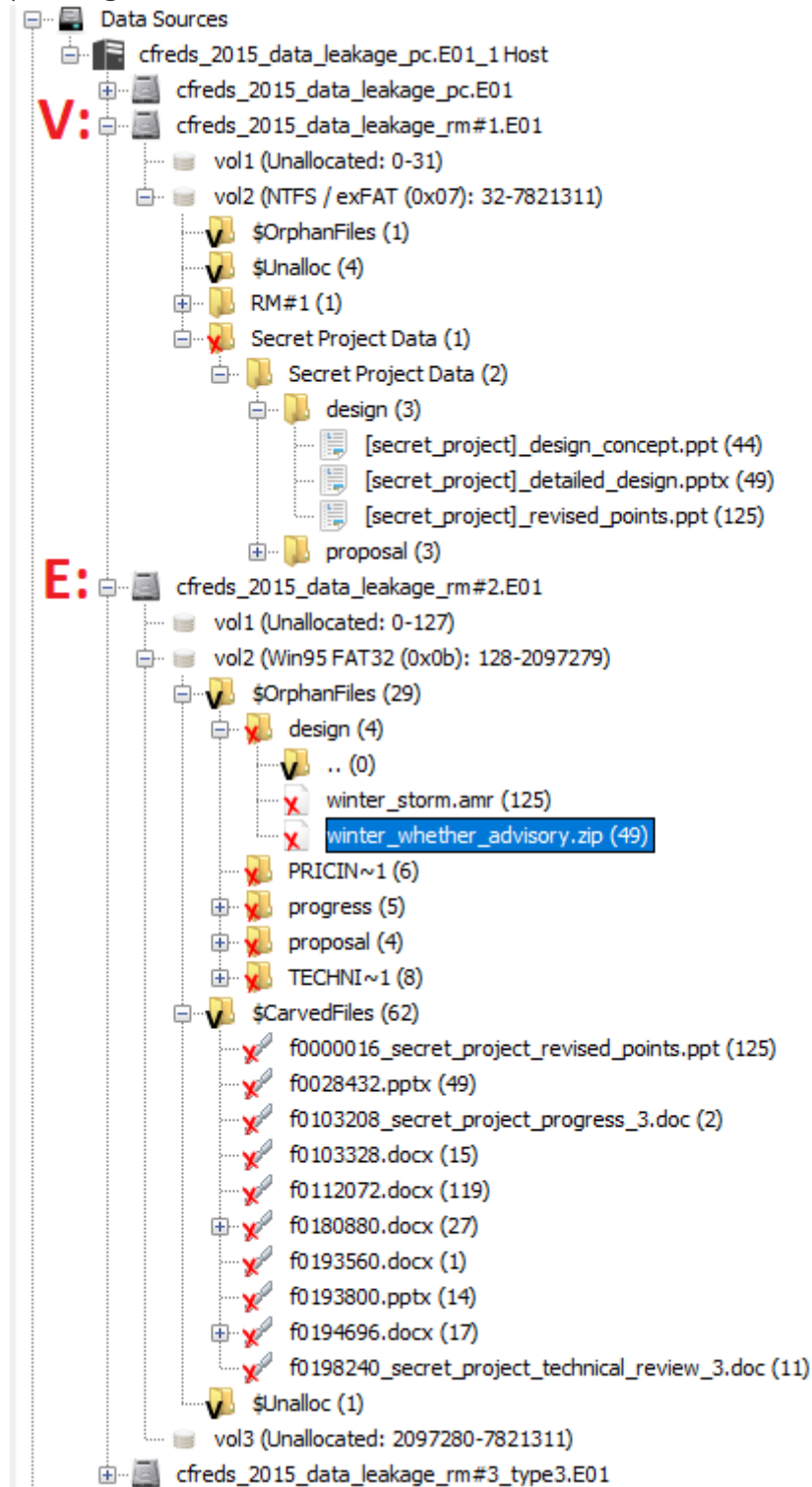
Date/Time	Device Make	Device Model	Serial Number
2015-03-24 09:38:00 EDT	SanDisk Corp.	Cruzer Fit	4C530012450531101593
2015-03-24 15:38:09 EDT	SanDisk Corp.	Cruzer Fit	4C530012550531106501

Dodatkowo podłączone urządzenia pamięci masowej możemy obserwować przy pomocy artefaktów dotyczących shellbagów.

My Computer	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01					2015-03-25 10:30:06 EDT
My Computer\{E}	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01					
My Computer\E\{RM#}	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-02-15 15:51:38 EST	2015-02-15 15:52:10 EST	2015-02-15 15:52:08 EST		
My Computer\E\{RM#}\Secret Project Dat	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-02-15 15:51:38 EST	2015-02-15 15:52:10 EST	2015-02-15 15:52:08 EST	2015-03-24 08:38:31 EDT	
My Computer\E\{RM#}\Secret Project Dat\desig	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-02-15 15:51:38 EST	2015-02-15 15:52:10 EST	2015-02-15 15:52:08 EST	2015-03-24 08:38:52 EDT	
My Computer\E\{RM#}\Secret Project Dat	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-24 08:57:28 EDT	2015-03-24 08:59:28 EDT	2015-03-23 23:00:00 EDT	2015-03-24 09:00:19 EDT	
My Computer\E\{RM#}\Secret Project Dat\technical revie	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-24 08:56:22 EDT	2015-03-24 09:00:14 EDT	2015-03-23 23:00:00 EDT		
My Computer\E\{RM#}\Secret Project Dat\propos	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-24 08:55:18 EDT	2015-03-24 08:59:46 EDT	2015-03-23 23:00:00 EDT		
My Computer\E\{RM#}\Secret Project Dat\progres	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-24 08:54:54 EDT	2015-03-24 08:59:44 EDT	2015-03-23 23:00:00 EDT	2015-03-24 15:54:07 EDT	
My Computer\E\{RM#}\Secret Project Dat\pricing decisio	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-24 08:57:32 EDT	2015-03-24 08:59:40 EDT	2015-03-23 23:00:00 EDT		
My Computer\E\{RM#}\Secret Project Dat\desig	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-24 08:57:14 EDT	2015-03-24 08:59:28 EDT	2015-03-23 23:00:00 EDT		
My Computer\E\{RM#}\Secret Project Dat\desig\winter_wether...	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2014-12-16 10:10:26 EST	2015-03-24 08:59:38 EDT	2015-03-23 23:00:00 EDT	2015-03-24 09:01:29 EDT	
My Computer\E\{RM#}\Secret Project Dat\desig\winter_wether...	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01				2015-03-24 09:01:32 EDT	
My Computer\{W}	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01					
My Computer\{W}\Secret Project Dat	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-22 09:52:24 EDT	2015-03-22 09:52:22 EDT	2015-03-22 09:52:24 EDT	2015-03-23 15:27:24 EDT	
My Computer\{W}\Secret Project Dat\{fina	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01	2015-03-22 09:52:22 EDT	2015-03-22 09:52:22 EDT	2015-03-22 09:52:22 EDT	2015-03-23 15:27:29 EDT	
My Computer\{C}	Local Settings\Soft...	cfreds_2015_data_leakage_pc.E01				2015-03-25 10:30:09 EDT	

W shellbag'ach widoczne są jakie podłączane urządzenia i przeglądane na nich katalogi. Analizując shellbagi oraz zawartość konkretnych nośników możemy ustalić jaką literką podmontowane były

poszczególne nośniki.



Jak widać ostrzerzenie od spiega było jak najbardziej zasadne, podłączane urządzenia usb są łatwe do wykrycia.

From: iaman

To: spy

CC:

Subject: RE: Watch out!

HeadersTextHTMLRTFAttachments (0)Accounts

I am trying.

-----Original Message-----

From: spy

Sent: Tuesday, March 24, 2015 3:33 PM

To: iaman

Subject: Watch out!

USB device may be easily detected.

So, try another method.

iaman choć próbował się nie pozostawiać śladów, starał się zbyt słabo.

25. List all directories that were traversed in 'RM#2'.

Ponieważ już wiedzieliśmy, że urządzenie **RM#2** mapowane jest na dysk **E:** to całkiem prosto było znaleźć listę przetrawiersowanych folderów. Należało wejść w **shellbags** i znaleźć ścieżki odpowiadające temu wolumenowi (chodzi głównie o kolumnę **Path**):

Source Name	Path	Key	Data Source	FIELD5	FIELD6	FIELD7	FIELD8
UsrClass.dat	My Computer\E\	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\	cfreds_2015_data_leakage_pc.E01				
UsrClass.dat	My Computer\E\RM#	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\	2015-02-15 21:51:38 CET	2015-02-15 21:52:10 CET	2015-02-15 21:52:08 CET	cfreds_2015_data_leakage_pc.E01	
UsrClass.dat	My Computer\E\RM#\Secret Project Dat	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\	2015-03-24 13:38:31 CET	2015-02-15 21:51:38 CET	2015-02-15 21:52:10 CET	2015-02-15 21:52:08 CET	cfreds_2015_data_leakage_pc.E01
UsrClass.dat	My Computer\E\RM#\Secret Project Dat\desig	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\	2015-03-24 13:38:52 CET	2015-02-15 21:51:38 CET	2015-02-15 21:52:10 CET	2015-02-15 21:52:08 CET	cfreds_2015_data_leakage_pc.E01
UsrClass.dat	My Computer\E\Secret Project Dat	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\	2015-03-24 14:00:19 CET	2015-03-24 13:57:28 CET	2015-03-24 13:59:28 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01
UsrClass.dat	My Computer\E\Secret Project Dat\technical revie	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\0\	2015-03-24 13:56:22 CET	2015-03-24 14:00:14 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01	
UsrClass.dat	My Computer\E\Secret Project Dat\propos	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\1\	2015-03-24 13:55:18 CET	2015-03-24 13:59:46 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01	
UsrClass.dat	My Computer\E\Secret Project Dat\progres	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\2\	2015-03-24 20:54:07 CET	2015-03-24 13:54:54 CET	2015-03-24 13:59:44 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01
UsrClass.dat	My Computer\E\Secret Project Dat\pricing decisio	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\3\	2015-03-24 13:57:32 CET	2015-03-24 13:59:40 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01	
UsrClass.dat	My Computer\E\Secret Project Dat\desig	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\4\	2015-03-24 13:57:14 CET	2015-03-24 13:59:28 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01	
UsrClass.dat	My Computer\E\Secret Project Dat\desig\winter_wether_advisory.zi	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\4\0\	2015-03-24 14:01:29 CET	2014-12-16 16:10:26 CET	2015-03-24 13:59:38 CET	2015-03-24 04:00:00 CET	cfreds_2015_data_leakage_pc.E01
UsrClass.dat	My Computer\E\Secret Project Dat\desig\winter_wether_advisory.zi\Unknown Type (0x3a)	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\4\0\0\0\2015-03-24 14:01:32 CET	cfreds_2015_data_leakage_pc.E01				

38 i 39. Where are 'Thumbcache' files located. Identify traces related to confidential files stored in Thumbcache. (Include '256' only)

Pliki thumbcache znajdują się pod ścieżką:

Users\informant\AppData\Local\Microsoft\Windows\Explorer

Wyeksportowaliśmy te pliki, a następnie, za pomocą programu `Thumbnail database viewer` odnaleźliśmy następujące artefakty:

[Shared Data]

orientation_part_2.xlsx

This file is one of Gooddocs (<http://digitalcorps.org/corpus/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

b064e178c6fe????

4900b4722444????

[Shared Data]

team_meeting.xls

This file is one of Gooddocs (<http://digitalcorps.org/corpus/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

fbaed14c4b37????

c9fd46746b18????

[Secret Project]

detailed_design.pptx

This file is one of Gooddocs (<http://digitalcorps.org/corpus/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

d2d8254e499e????

df9fcaa6268f????

[Secret Project]

final_meeting.pptx

This file is one of Gooddocs (<http://digitalcorps.org/corpus/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

824aeae6654b????

336f5adfc6b6???? ()

[Secret Project]

technical_review_#3.ppt

This file is one of Goodies (<http://bugtd.com/goodies/secret/secret.ppt>)
The first page is added by NIST-CFRaDS project.
All following pages have no connection with to the scenario.

448006780b63????

408149f765d7????

[Secret Project]

technical_review_#2.ppt

This file is one of Goodies (<http://bugtd.com/goodies/secret/secret.ppt>)
The first page is added by NIST-CFRaDS project.
All following pages have no connection with to the scenario.

8e844d284921????

930997664164????

[Secret Project]

final_meeting.pptx

This file is one of Goodies (<http://bugtd.com/goodies/secret/secret.pptx>)
The first page is added by NIST-CFRaDS project.
All following pages have no connection with to the scenario.

574f482bff40????

17d5da5aa5c5????

[Secret Project]

final_meeting.pptx

This file is one of Goodies (<http://bugtd.com/goodies/secret/secret.pptx>)
The first page is added by NIST-CFRaDS project.
All following pages have no connection with to the scenario.

5122a42617ce????

0310732cc06d????

[Secret Project]

revised_points.ppt

This file is one of Gooddocs (<http://lightboxcorp.com/engpost/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

2feeea985a34????

376a2eabbcf6????

[Secret Project]

technical_review_#2.ppt

This file is one of Gooddocs (<http://lightboxcorp.com/engpost/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

31cb0d486a21????

[Secret Project]

detailed_design.pptx

This file is one of Gooddocs (<http://lightboxcorp.com/engpost/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

dae74f4ce479????

69739da03d9f????

[Secret Project]

technical_review_#1.pptx

This file is one of Gooddocs (<http://lightboxcorp.com/engpost/gooddocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.

b8e9b582c502????

b9c9cbd7e3bb????

40 i 41. Where are Sticky Note files located? Identify notes stored in the Sticky Note file.

Pliki sticky note znajdują się w folderze

Users\informant\AppData\Roaming\Microsoft\Sticky Notes

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2015-03-24 19:30:09 CET	2015-03-24 19:30:09 CET	2015-03-24 19:30:09 CET	2015-03-24 19:30:09 CET	272	Allocated	Allocated	unknown	/img_cfreds_2015_c
[parent folder]				2015-03-24 19:30:09 CET	2015-03-24 19:30:09 CET	2015-03-24 19:30:09 CET	2015-03-22 15:34:41 CET	56	Allocated	Allocated	unknown	/img_cfreds_2015_c
StickyNotes.snt	✓		0	2015-03-24 19:31:59 CET	2015-03-24 19:31:59 CET	2015-03-24 19:30:09 CET	2015-03-24 19:30:09 CET	4096	Allocated	Allocated	unknown	/img_cfreds_2015_c

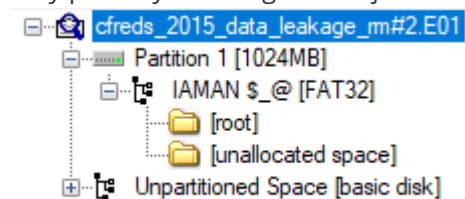
Root Entry
Version
Metafile
ccbb72fb-d253-11e4-b
ccbb72fb-d253-11e4-b
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fa0
rset0\Segoe Print}{\f1\fnil\Segoe Print}}
{\generator Modified 5.4.1.21.2510;}viewkind4\uc1\pard\tx360\tx720\tx1080\tx1440\tx1800\tx2160\tx2520\tx2880\tx3240\tx3600\tx4320\tx4680\tx5040\tx5400\tx5760\tx6120\tx6480\tx6840\tx7200\tx7560\tx7920\tx8280\tx8640\tx9000\tx9360\tx9720\tx10080\tx10440\tx10800\tx11160\tx11520\highlight0\fs22 Tomorrow... \par
 \par
Everything will be OK... \par
 \par
 \par
 \par
Tomorrow...
Everything will be OK...

Ciekawym wydają się tutaj czytelne kawałki tekstu. Wyglądają albo jak uspokajanie kogoś zdenerwowanego.

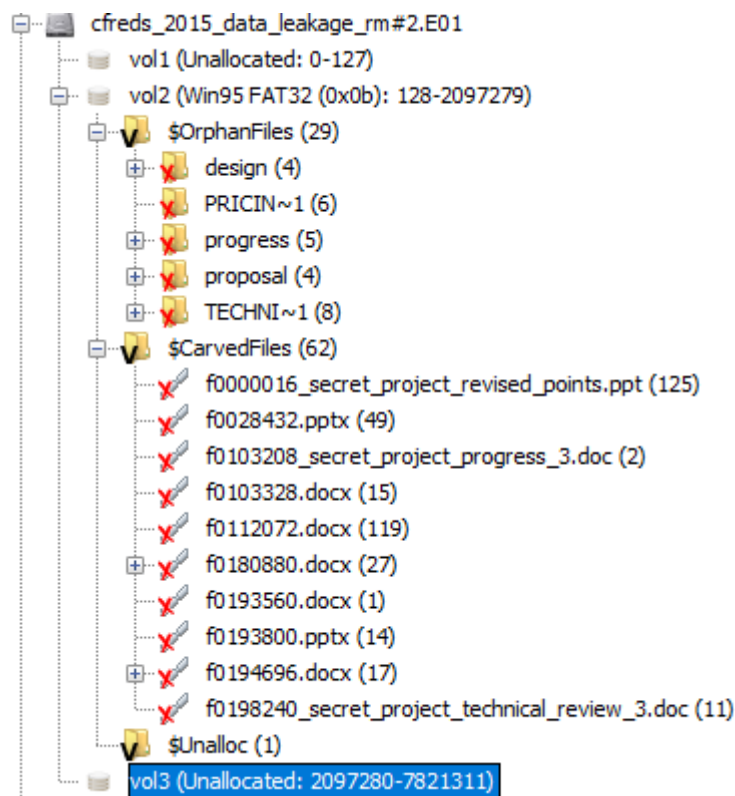
Próbowaliśmy także otworzyć odzyskany plik ale okazało się to bardzo trudne na Windows 10. Format odpowiada plikom z Windows 7 i Vista. Zastanawialiśmy się nad postawieniem maszyny wirtualnej, z którymś z wymienionych systemów ale stwierdziliśmy, że nie jest to warte zachodu.

53. Recover deleted files from USB drive 'RM#2'.

Przy pomocy FTKImager'a nie jest możliwe odczytanie, żadnych plików z USB drive 'RM#2'



Narzędzie Autopsy potrafi już jednak odzyskać część plików która znajdowała się tam przed usunięciem



Przykładowe odzyskane pliki:



[Secret Project]

Technical Review #3.doc

This file is one of Govdocs (<http://digitalcorpora.org/corpora/govdocs>)
The first page is added by NIST CReDS project.
All following pages have no connection with to the scenario.

GRAPHIC MATERIALS

Rules for Describing

Original Items and Historical Collections

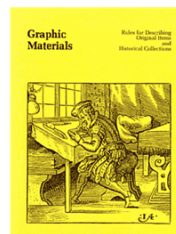
compiled by
Elisabeth W. Betz

Library of Congress, Washington, D.C., 1982

Word 2000 Version
(July 2000; with MARC21 tagging added in March 2002)

With cumulated updates: 1982-1996
and

List of areas to update for second edition: 1997-2000



Cover illustration: "Sculptor: Der *Formschneider*." Woodcut by Jost Amman in Hartmann Schönober's *Panoplia omnium liberalium mechanicarum aut sedentarium artium genera continens*, printed at Frankfurt am Main by S. Feussleben, 1568. Rosenwald Collection, Rare Book and Special Collections Division. (Neg. no. LC-USZ62-44613)

Podsumowanie

Na tym laboratorium wcieliłiśmy się w rolę pracowników działu DFIR i przeanalizowaliśmy wybrane pytania z **Data Leakage Case** i nauczyliśmy się podstaw obsługi narzędzi do autopsji cyfrowej. Oraz obudziliśmy naszego wewnętrznego Sherlocka Holmesa, żeby odkryć tajemnice spowitej ciemnością i grozą zagadki.