

iu-cf-lab-02-Iskander_Nafikov

- **Name:** Iskander Nafikov
- **E-mail:** i.nafikov@innopolis.university
- **GitHub:** <https://github.com/iskanred>

CCF Lab 2 - Forensic file system analysis

Task description

In this lab, you will learn how to investigate a forensic analysis of a compromised file system. This is one of the basic and at the same time relevant and actual areas in forensic science.

Task 1 - Download the evidence file

Task description

You are offered to investigate the image of compromised system

- Since my student number is 15 which means odd I used [case-1](#) system

14 Нуралла Ахмед Шаабан Абдельрэзак	Ahmed Shaaban Abdelrazzak	Nouralla	nginx-st14
15 Нафиков Искандер Маратович	Iskander	Nafikov	nginx-st15
16 Окоре Джоэль Чидике	Joel Chidike	Okore	nginx-st16

Task 2 - Black box Forensics analysis

Task description

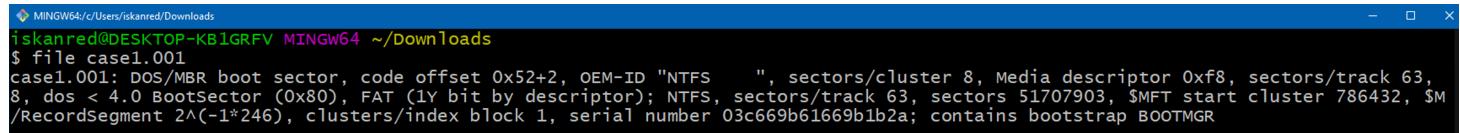
Use any forensics tools that you want. Different forensics tools can help you to analyze:

- Figure out the platform, system and file system type
- Perform a malware search
- Create and analyze a timeline
- Find artifacts in Windows components:
 - Windows Registry
 - Logs
 - Personal data of users
 - Network

- Mail
- Browser
- Messengers
- Windows libraries and configuration files
- Other assets found in the compromised system

Image file investigation

- First, I ran `file` command on my Windows machine using MinGW to investigate what type of file I received



```
MINGW64/c/Users/iskanred/Downloads
iskanred@DESKTOP-KB1GRFV MINGW64 ~/Downloads
$ file case1.001
case1.001: DOS/MBR boot sector, code offset 0x52+2, OEM-ID "NTFS      ", sectors/cluster 8, Media descriptor 0xf8, sectors/track 63,
8, dos < 4.0 BootSector (0x80), FAT (1Y bit by descriptor); NTFS, sectors/track 63, sectors 51707903, $MFT start cluster 786432, $M
/RecordSegment 2^(1*246), clusters/index block 1, serial number 03c669b61669b1b2a; contains bootstrap BOOTMGR
```

- Here we can see that this is actually some Windows OS image because it contains:
 - NTFS filesystem
 - DOS/MBR boot sector with 1.5Gb of size
 - [BOOTMGR](#) which used starting from Windows Vista or Windows Server 2008

AutoPsy configuration

- I decided to use it **AutoPsy** since it is a very powerful tool that brings simplicity in working with registry, files, logs, events, browser, databases, network and etc.
- I added the image to investigate as a new AutoPsy case with all the modules enabled (including [Plaso](#) which we used manually in the previous lab to generate timeline from logs - `log2timeline`)

Add Data Source

Steps

- Select Host
- Select Data Source Type
- Select Data Source
- Configure Ingest**
- Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

Recent Activity
 Hash Lookup
 File Type Identification
 Extension Mismatch Detector
 Embedded File Extractor
 Picture Analyzer
 Keyword Search
 Email Parser
 Encryption Detection
 Interesting Files Identifier
 Central Repository
 PhotoRec Carver
 Virtual Machine Extractor
 Data Source Integrity
 Android Analyzer (aLEAPP)
 Cyber Triage Malware Scanner
 DJI Drone Analyzer
 Plaso
 YARA Analyzer
 iOS Analyzer (iLEAPP)
 GPX Parser
 Android Analyzer

NOTE: This module can take a long time to run.
All modules except chrome_cache* and the below are enabled. Enabling these will cause Plaso to run slow.

winreg: Parser for Windows NT Registry (REGF) files
 pe: Parser for Portable Executable (PE) files

* Disabled because it duplicates existing Autopsy modules

Runs Plaso against a Data Source.

Global Settings

< Back **Next >** Finish Cancel Help

- Ingesting all the modules for this case took **a lot of time**: ≈ 3 days (that's why I submitted it much later than I supposed 😊)
- Finally, it ended and I got the following picture:

iu-cf-lab-02 - Autopsy 4.22.0

Case View Tools Window Help

Add Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Data Sources **case1.001_1 Host**

File Views File Types By Extension By MIME Type Deleted files File System (7854) All (8708)

MB File Size

Data Artifacts Communication Accounts (24) Email (24) E-Mail Messages (147) Default [Default] Default (147) Installed Programs (92) Metadata (145) Operating System Information (1) Recent Documents (30) Run Programs (1898) Shell Bags (63) USB Device Attached (5) Web Bookmarks (1) Web Cookies (13) Web Downloads (54) Web History (5)

Analysis Results Encryption Suspected (4) EXIF Metadata (9) Extension Mismatch Detected (161) Interesting Items (5) Cloud Storage (3) Encryption Programs (1) Privacy Programs (1) User Content Suspected (9) Web Categories (3)

OS Accounts Tags Score Bad Items (0) Suspicious Items (170)

Reports

case1.001_1 Host

Table: Thumbnail Summary

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
case1.001	Image	26474446848	512	Europe/Moscow	a11ea660-14f2-429e-9bb-ba87fec84191

Save Table as CSV

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

Strings Extracted Text Translation

Page: 1 of Page Go to Page: Script: Latin - Basic

Investigation

Basic system information & Timeline

Let's begin with figuring some standard system info such as username, hostname, IP address, and etc.

- From the section Operating System Information we can extract a lot of useful information

The screenshot shows the Autopsy 4.22.0 interface. The left sidebar displays a file tree with various file types like Images, Videos, Audio, Archives, Databases, Documents (HTML, Office, PDF, Plain Text, Rich Text), Executable (.exe, .dll, .bat, .cmd, .com), and Data Artifacts (Communication Accounts, E-Mail Messages, Installed Programs, Metadata, Operating System Information, Recent Documents, Run Programs, Shell Bags, USB Device Attached, Web Bookmarks, Web Cookies, Web Downloads, Web History). The main pane shows the "Operating System Information" table with one result:

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Data Source
case1.001				4ORENSICS	Windows 8.1 Enterprise	AMD64	%SystemRoot%\TEMP	C:\Windows	00261-30000-00000-AA825	Hunter	case1.001

Below the table, there is a detailed view of the operating system information:

Type	Value	Source(s)
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Artifact ID	-9223372036854775590	
Source File Path	/img_case1.001	
Product ID	00261-30000-00000-AA825	Recent Activity
Name	4ORENSICS	Recent Activity
Processor Architecture	AMD64	Recent Activity
Path	C:\Windows	Recent Activity
Owner	Hunter	Recent Activity
Program Name	Windows 8.1 Enterprise	Recent Activity

- OS version = Windows 8.1 Enterprise

Detailed view of the OS information table:

Type	Value	Source(s)
Name	4ORENSICS	Recent Activity
Program Name	Windows 8.1 Enterprise	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00261-30000-00000-AA825	Recent Activity
Owner	Hunter	Recent Activity
Source File Path	/img_case1.001	
Artifact ID	-9223372036854775590	

- Hostname = 4ORENSICS

Detailed view of the Hostname table:

Type	Value	Source(s)
Name	4ORENSICS	Recent Activity
Program Name	Windows 8.1 Enterprise	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00261-30000-00000-AA825	Recent Activity
Owner	Hunter	Recent Activity
Source File Path	/img_case1.001	
Artifact ID	-9223372036854775590	

- Owner's username = hunter

Type	Value	Source(s)
Name	4ORENSICS	Recent Activity
Program Name	Windows 8.1 Enterprise	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00261-30000-00000-AA825	Recent Activity
Owner	Hunter	Recent Activity
Source File Path	/img_case1.001	
Artifact ID	9223372036854775590	

- IP address = 10.0.2.15/24 . To figure it out I went to the Windows Registry hive:

HKEY_LOCAL_MACHINE\SYSTEM (C:/Windows/System32/config/SYSTEM). Below we can also see DHCP server information such as its address, lease time, and etc.

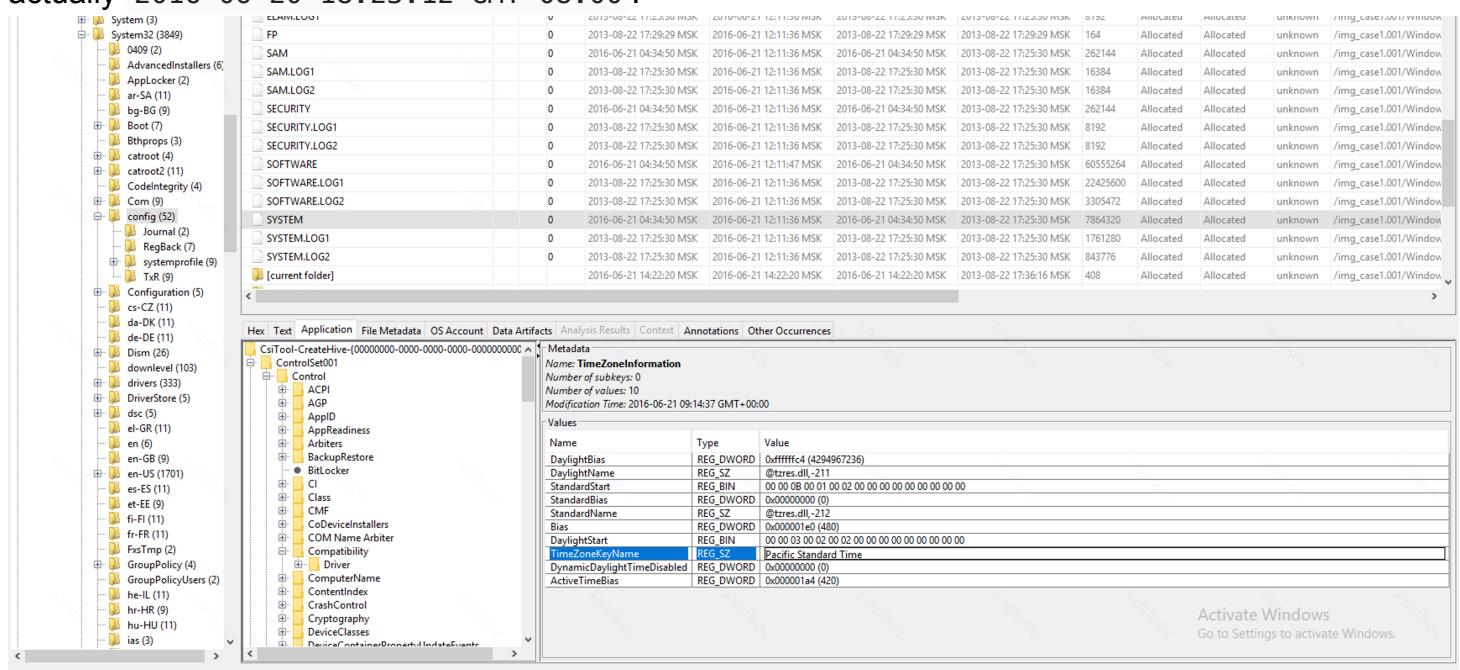
Name	Type	Value
EnableDHCP	REG_DWORD	0x00000001 (1)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
DhcpIpAddress	REG_SZ	10.0.2.15
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	(value not set)
Lease	REG_DWORD	0x000001180 (86400)
LeaseObtainedTime	REG_DWORD	0x5769454c (1466475852)
T1	REG_DWORD	0x57694e0c (1466519052)
T2	REG_DWORD	0x57694e0c (1466551452)
LeaseTerminatesTime	REG_DWORD	0x57694e0c (1466562352)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)

- In addition, using this metadata section we see this registry part modification time from which we can infer that the last time the the IP address was assigned to this interface using DHCP was 2016-06-21 02:23:12 GMT+00:00 or 2016-06-20 04:23:12 GMT+03:00 which is quite late, so let's try to determine the user's timezone. Also checking registry option LeaseObtainedTime we can also prove that since 1466475852 in UNIX is exactly the timestamp we inferred.

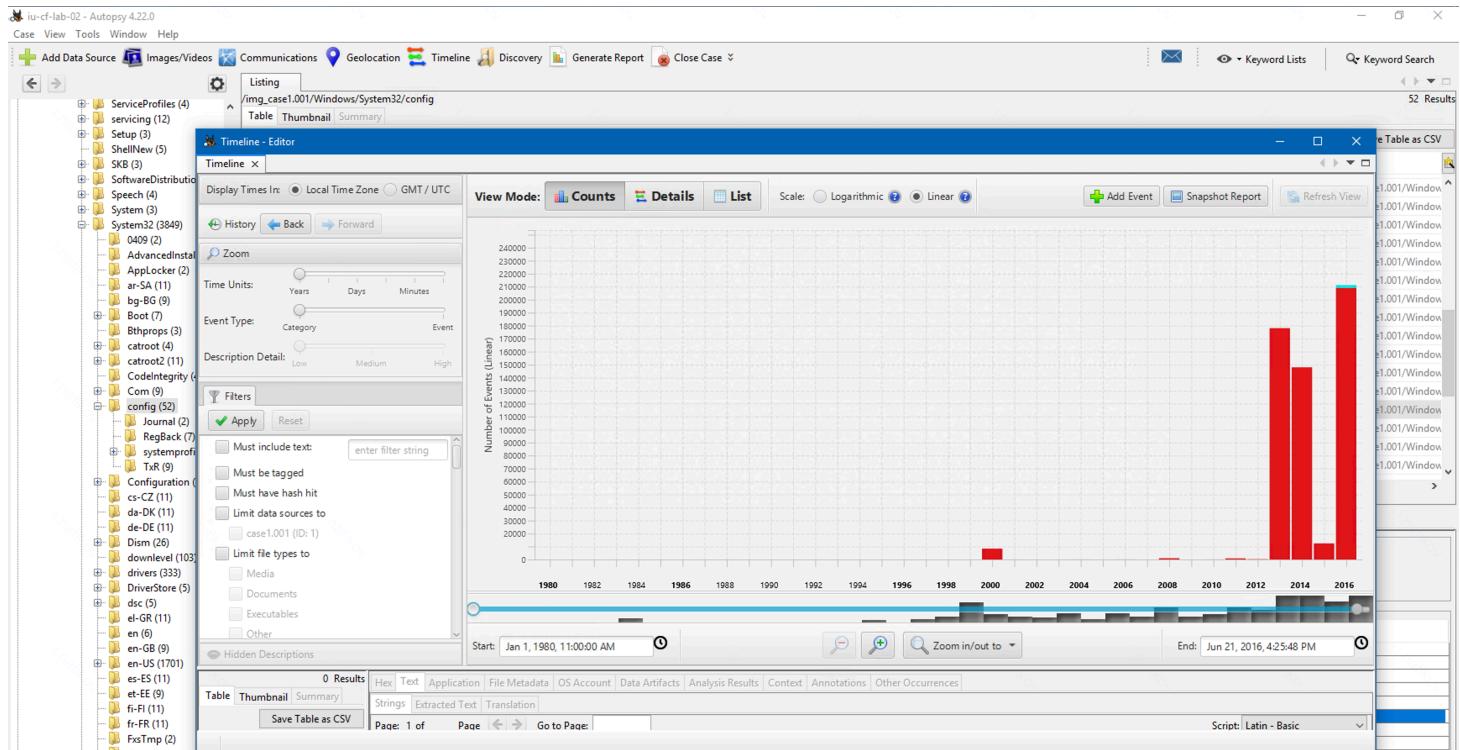
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences

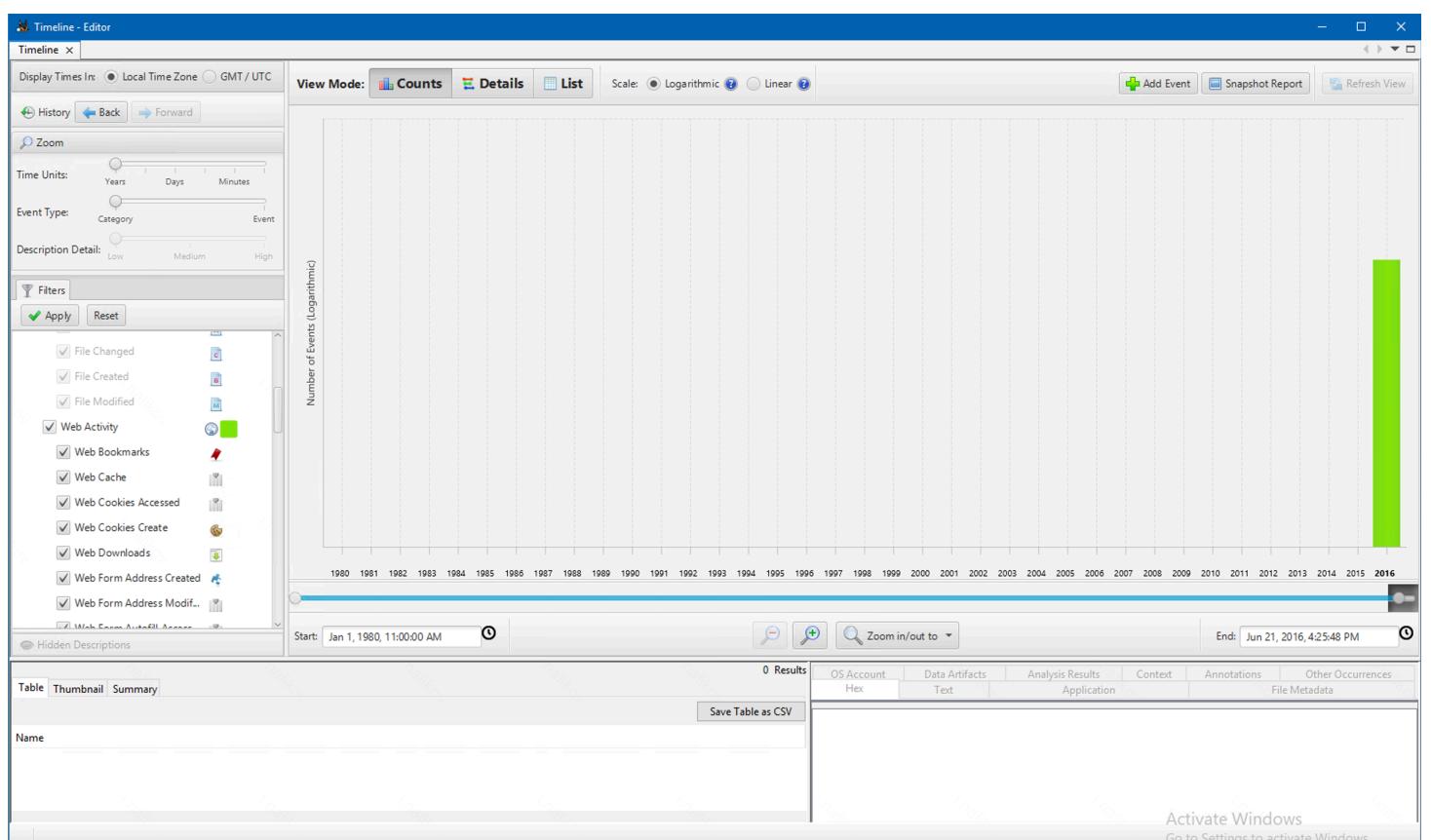
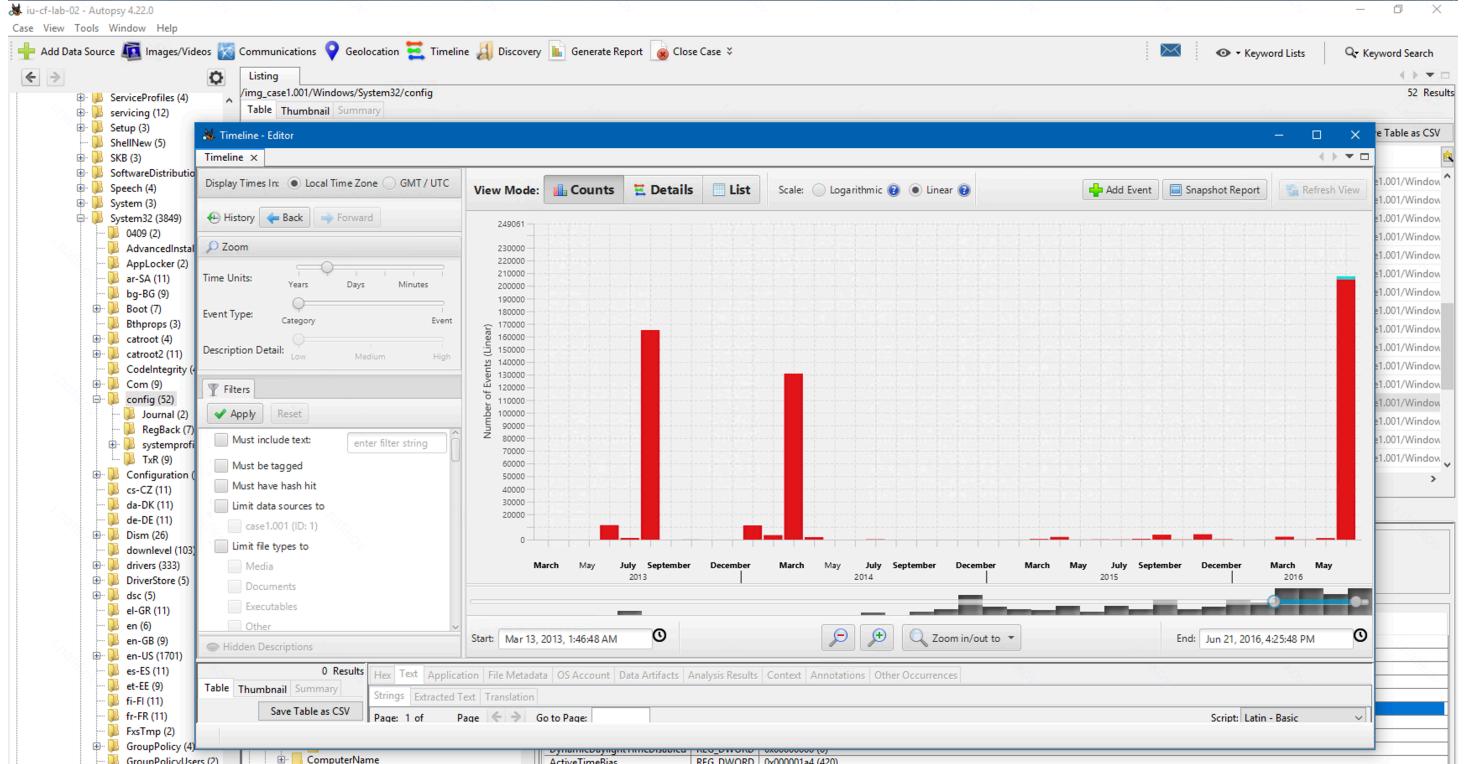
- Timezone & location = UTC-8:00 which is the same as Pacific Standard Time. I also found it inside the registry hive HKEY_LOCAL_MACHINE\SYSTEM . This means that the last DHCP lease obtain time was

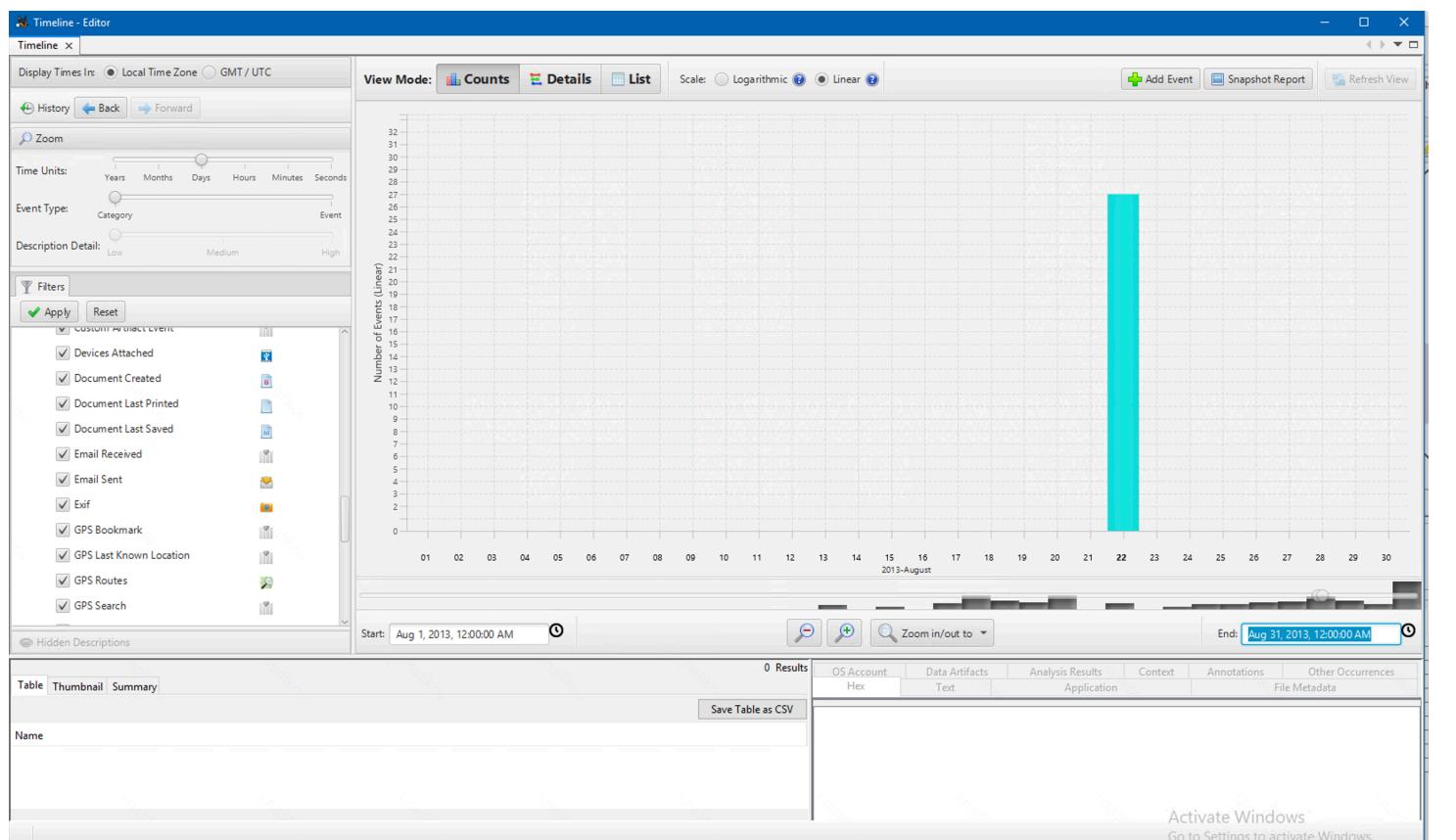
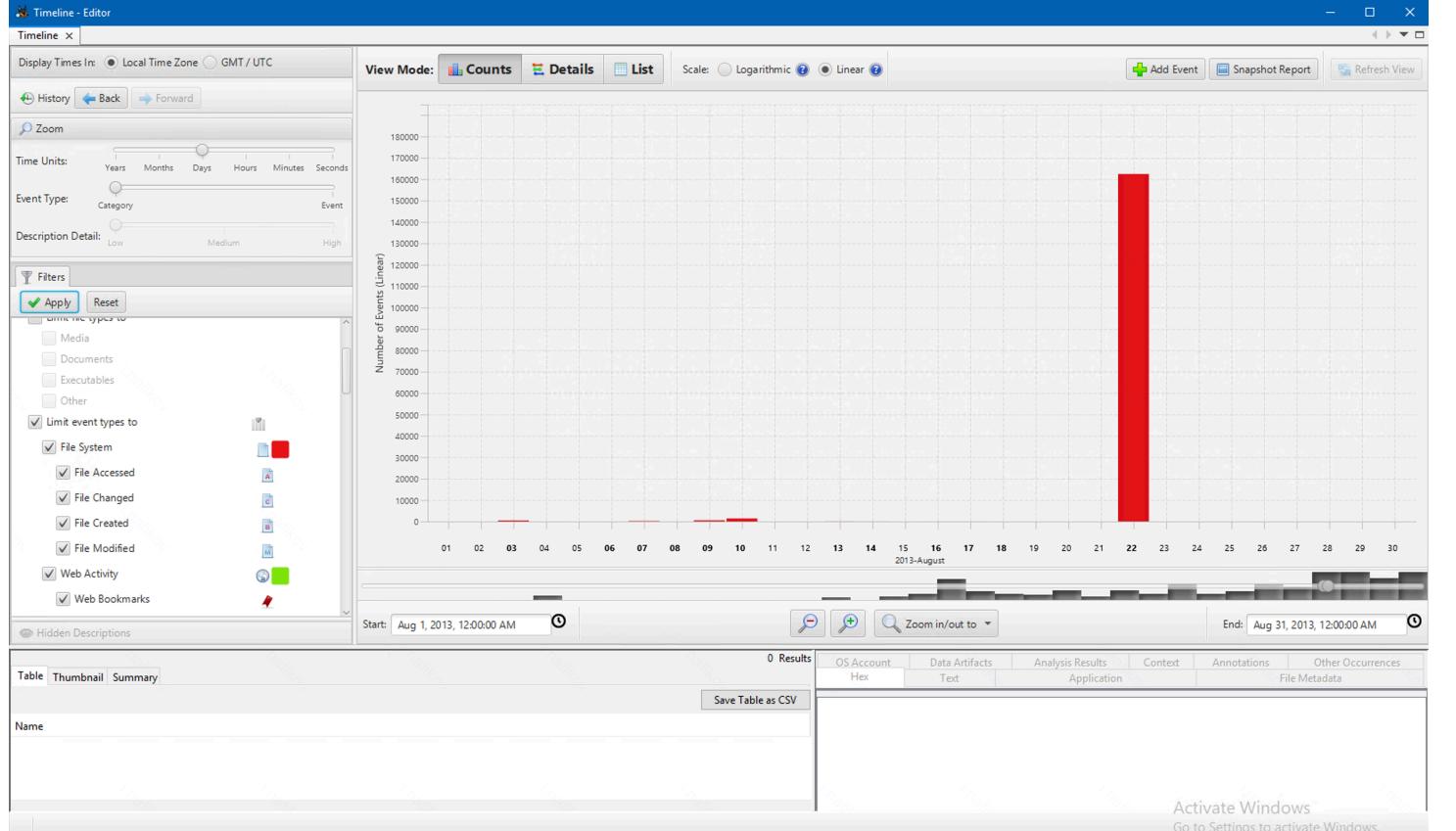
actually 2016-06-20 18:23:12 GMT-08:00 .

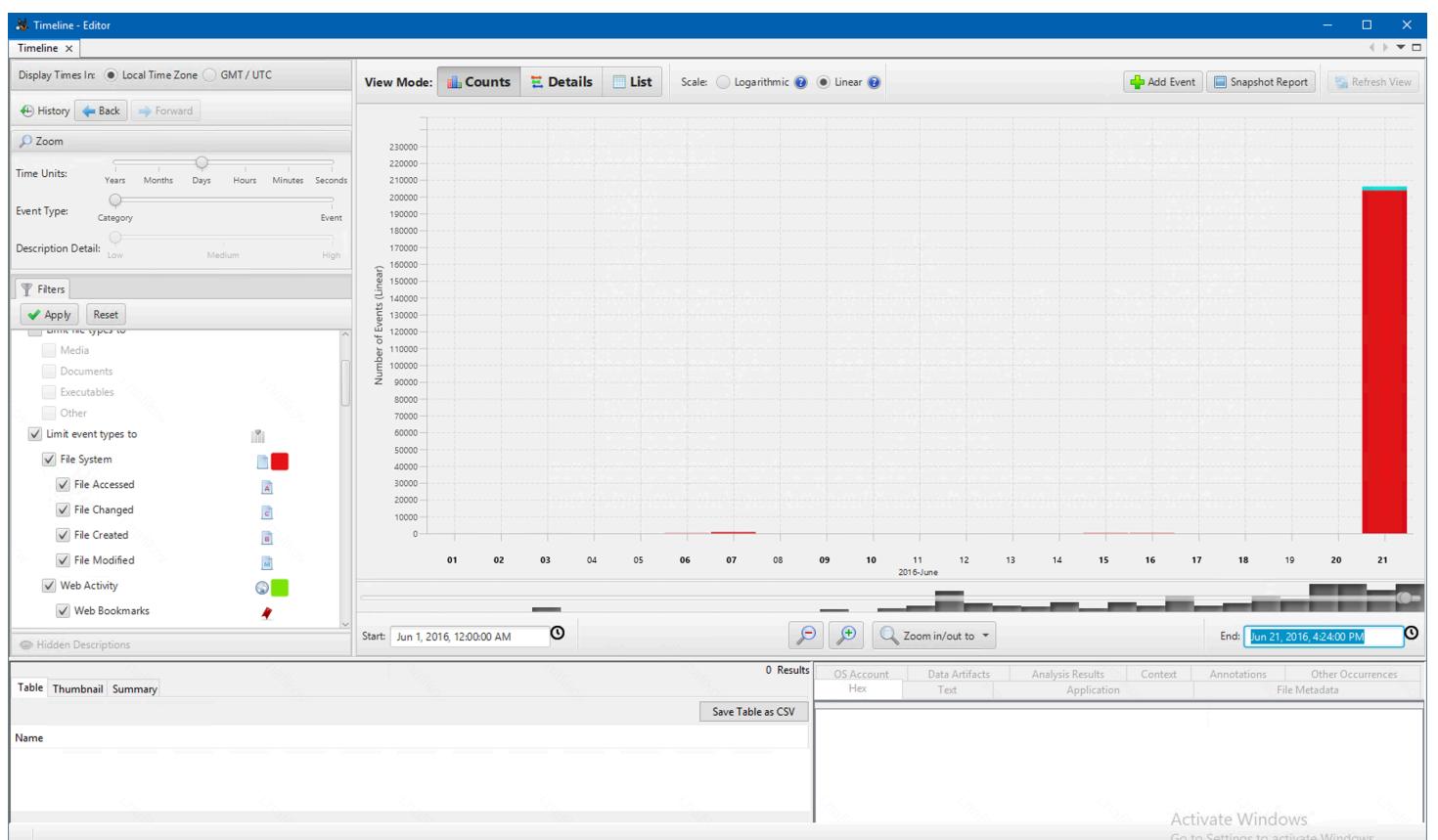
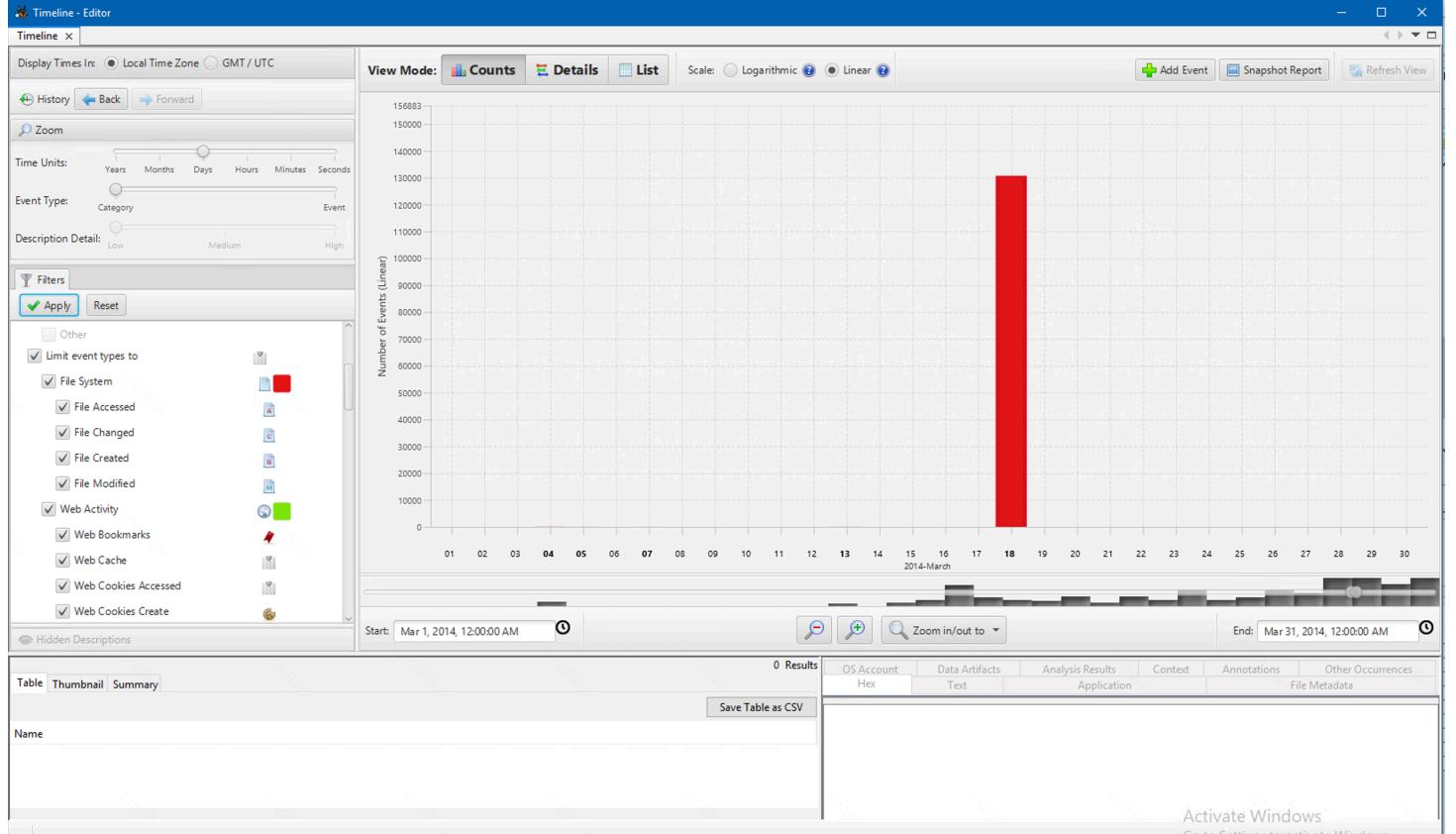


- **OS usage**, by my first assumption, is ≈ 3 years (Jun 2013 - Jun 2016) since the absolute majority of events happened in this time period which I obtained using AutoPsy timeline. An interesting part is that the device was most actively used periodically (22nd of August 2013, 18th of March 2014, 21st June 2016) and the most active usage happened right before the end of the interval in a last month which looks suspicious. Moreover, the web activity also happened only in Jun 2016. That's why I decided to explore some user's logging in information.









- But before moving to the login information I decided to check the **system installation timestamp** which is `2013-08-22 17:25:41 GMT+03:00`. I took it from the creation date of `system.ini` file. Also,

we see that it was changed exactly at the 2016-06-21 .

File Metadata details for system.ini:

Name	Value
Name	/img_case1.001/Windows/system.ini
Type	File System
MIME Type	text/x-ini
Size	219
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2013-08-22 17:25:41 MSK
Accessed	2013-08-22 17:25:41 MSK
Created	2013-08-22 17:25:43 MSK
Changed	2016-06-21 12:09:48 MSK
MDS	286a9edb379dc3423a528b0864a0f111
SHA-256	6f533ccc79227e38f18bf63bfc961ef4d3ee0e2bf3dd097ccf3548a12b743b
Hash Lookup Results	UNKNOWN
Internal ID	235380

Activate Windows
Go to Settings to activate Windows.

- Also, I decided to check **Installation date** inside the SOFTWARE registry hive and found that it was 2016-06-21 11:37:45 GMT+03:00 . This most probably means that the system update was installed on this date.

Autopsy 4.2.0 - Case: /iu-cf-lab-02 - Autopsy 4.2.0

Software registry key details:

Name	Type	Value
SystemRoot	REG_SZ	C:\Windows
SoftwareType	REG_SZ	System
RegisteredOwner	REG_SZ	Hunter
InstallDate	REG_DWORD	0x769fc49 (1466498265)
CurrentVersion	REG_SZ	6.3
CurrentBuild	REG_SZ	9600
RegisteredOrganization	REG_SZ	(value not set)
CurrentType	REG_SZ	Multiprocessor Free
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Enterprise
ProductName	REG_SZ	Windows 8.1 Enterprise
Productid	REG_SZ	00261-30000-0000-AA825
DigitalProductid	REG_BIN	A4 00 00 00 00 00 00 00 30 32 36 31 2D 33 30...
DigitalProductId4	REG_BIN	F8 04 00 00 04 00 00 00 30 30 30 30 00 30 00 30 00...
CurrentBuildNumber	REG_SZ	9600
BuildLab	REG_SZ	9600.winblue_gdr.140221-1952
BuildLabEx	REG_SZ	9600.1703.1.mdf&re.winblue_gdr.140221-1952
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
PathName	REG_SZ	C:\Windows

Activate Windows
Go to Settings to activate Windows.

Convert epoch to human-readable date and vice versa

1466498265 [Timestamp to Human date](#) [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Tuesday, June 21, 2016 8:37:45 AM

Your time zone : Tuesday, June 21, 2016 11:37:45 AM **GMT+03:00**

Relative : 9 years ago

- Login information

- From the AutoPsy OS Accounts section I got that the user's **login count** is just 3

case1.001_1 Host Details

Last Login:	2016-06-21 04:42:40 MSK
Login Count:	3
Administrator:	True
Password Hint:	What do you do?
Password Fail Date:	2016-06-21 15:53:04 MSK
Password Settings:	Password does not expire, Password not required
Flag:	Normal user account
Home Directory:	C:/Users/Hunter

Activate Windows

Basic Properties

Login:	hunter
Full Name:	
Address:	S-1-5-21-2489440558-2754304563-710705792-1001
Type:	
Creation Date:	2016-06-21 11:37:43 MSK
Object ID:	6

- Summary:**

- There is a basic system timeline:
 - 2013-08-22 17:25:41 GMT+03:00** : The system was created. ! However, Windows 8.1 was not released at this moment.
 - 2016-06-20 04:23:12 GMT+03:00** : The system obtained the IPv4 address by DHCP.
 - 2016-06-21 04:42:40 GMT+03:00** : The user Hunter logged in the system last time
 - 2016-06-21 11:37:43 GMT+03:00** : The account was created
 - 2016-06-21 11:37:45 GMT+03:00** : The system was installed ! or updated
 - 2016-06-21 15:53:04 GMT+03:00** : The password fail date
- The user logged in 3 times at all.
- The system logged most number of events at these dates: 22nd of August 2013, 18th of March 2014, 21st of June 2016
- However, the web activity was only detected at the 21st of June 2016.

- Conclusion:**

- From all above I can conclude that there are several possible options why everything looks so strange:
 - The system may be installed first in 2013 on Windows 7 or Windows 8, then updated in 2014 by some administrator, finally updated in 2016 and used by Hunter.
 - Someone changed the proper date information trying to hide the actual timeline.
 - If this is a study case and not a real one, then probably the creators just did everything at once in the system, turned it off and created an image from this meaning that the "timeline" part is not important for investigation.
- Whatever it was, we had a strong fact:
 - The system was used by Hunter user actively on Jun 21 and everything we should investigate seems to happen on this date.

Applications

- Afterwards, I started analysing user's installed programs and their usage

- First, I found **USBPcap** which is a USB sniffer and 7-zip

SOFTWARE	0	USBPcap 1.1.0-g794bf26-3.v1.1.0-g794bf26-3	2016-06-21 09:23:09 MSK	case1.001
SOFTWARE	0	Microsoft Visual C++ 2013 x64 Additional Runtime - 1...	2016-06-21 09:22:48 MSK	case1.001
SOFTWARE	0	Microsoft Visual C++ 2013 x64 Minimum Runtime - 12...	2016-06-21 09:22:48 MSK	case1.001
SOFTWARE	0	7-Zip 16.02 (x64) v.16.02	2016-06-21 09:18:13 MSK	case1.001

- I found that he had a **VirtualBox** installed which means he's not a usual user of PC but some IT guy

The screenshot shows the Autopsy 4.2.0 interface. On the left, there is a file tree view showing various folders like File Views, File Types, By Extension, Documents, Executable, and Data Artifacts. The main pane displays a table titled "Installed Programs" with 92 results. The table has columns for Source Name, S, C, O, Program Name, Date/Time, and Data Source. One row is highlighted in blue, corresponding to the details shown in the bottom right pane. The details pane shows the following information:

Type	Value	Source(s)
Program Name	Oracle VM VirtualBox Guest Additions 5.0.22 v.5.0.22.0	Recent Activity
Date/Time	2016-06-21 09:47:39 MSK	Recent Activity
Source File Path	/img_case1.001/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775680	

Buttons in the bottom right include "Activate Windows", "Go to Settings", and "Go to activate Windows".

- Also, I found **Wireshark**, so the owner is definitely some IT guys who is related to Network and probably even Security

The screenshot shows the Autopsy 4.2.0 interface. The file tree on the left is partially visible. The main pane displays a table titled "Installed Programs" with 92 results. The table has columns for Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. One row is highlighted in blue, corresponding to the details shown in the bottom right pane. The details pane shows the following information:

Type	Value	Source(s)
Program Name	Wireshark 2.0.4 (64-bit) v.2.0.4	Recent Activity
Date/Time	2016-06-21 09:23:19 MSK	Recent Activity
Source File Path	/img_case1.001/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775616	

Buttons in the bottom right include "Activate Windows", "Go to Settings", and "Go to activate Windows".

- Btw, he has an antivirus **McAfee** installed

The screenshot shows the Autopsy 4.2.0 interface. The file tree on the left is partially visible. The main pane displays a table titled "Installed Programs" with 92 results. The table has columns for Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. One row is highlighted in blue, corresponding to the details shown in the bottom right pane. The details pane shows the following information:

Type	Value	Source(s)
Program Name	McAfee Security Scan Plus v.3.11.266.3	Recent Activity
Date/Time	2016-06-21 09:20:51 MSK	Recent Activity
Source File Path	/img_case1.001/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775613	

Buttons in the bottom right include "Activate Windows", "Go to Settings", and "Go to activate Windows".

- Also, the user has **Notepad++**, **Skype**, **Dropbox**, **Google Drive**, and **TeamViewer** installed which is not something suspicious but it can be used by attackers easily.

SOFTWARE	0	Notepad++ v.6.9.2	2016-06-21 09:18:35 MSK	case1.001
SOFTWARE	0	Skype™ 7.25 v.7.25.103	2016-06-21 08:59:08 MSK	case1.001
SOFTWARE	0	Google Update Helper v.1.3.30.3	2016-06-21 08:51:04 MSK	case1.001
SOFTWARE	0	Google Chrome v.51.0.2704.103	2016-06-21 08:43:03 MSK	case1.001
SOFTWARE	0	Dropbox v.4.4.29	2016-06-21 01:47:08 MSK	case1.001
SOFTWARE	0	Dropbox Update Helper v.1.3.43.1	2016-06-21 01:45:12 MSK	case1.001
SOFTWARE	0	Google Drive v.1.30.2170.0459	2016-06-21 01:44:38 MSK	case1.001
SOFTWARE	0	TeamViewer 11 v.11.0.59518	2016-06-21 00:57:44 MSK	case1.001

- Finally, I got something really interesting. The user had **BCWipe** software which is necessary for complete wiping data with no ability to recover it after. It might mean the user wanted to hide some data from the possible investigators

SOFTWARE | 0 | BCWipe 6.0 v.6.08.6 | 2016-06-21 11:44:53 MSK | case1.001

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 49 of 92 Result ← →									
Type	Value								Source(s)
Program Name	BCWipe 6.0 v.6.08.6								Recent Activity
Date/Time	2016-06-21 11:44:53 MSK								Recent Activity
Source File Path	/img_case1.001/Windows/System32/config/SOFTWARE								Activate Windows
Artifact ID	-9223372036854775634								Go to Settings Go to activate Windows



- Another one bingo! **Nmap** is used for port scanning, but why Hunter needed it? For penetration testing or performing real attacks?

SOFTWARE | 0 | Nmap 7.12 v.7.12 | 2016-06-21 11:02:00 MSK | case1.001

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 63 of 92 Result ← →									
Type	Value								Source(s)
Program Name	Nmap 7.12 v.7.12								Recent Activity
Date/Time	2016-06-21 11:02:00 MSK								Recent Activity
Source File Path	/img_case1.001/Windows/System32/config/SOFTWARE								Activate Windows
Artifact ID	-9223372036854775620								Go to Settings Go to activate Windows

- The VirtualBox was used on Jun 21

Source Name	S	C	O	Program Name	Username	△ Date/Time	Bytes Sent	Bytes Received	Comment	Data
SRUDB.dat				\Program Files\Intel\BCA\pabe\vcb4.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files\TrueKey\McAfee.TrueKey.ServiceHelp...	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files\TrueKey\McAfee.TrueKey.ServiceHelp...	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files\TrueKey\McAfee.TrueKey.Service.exe	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files\TrueKey\McAfee.TrueKey.Service.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files\TrueKey\McTkSchedulerService.exe	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files\TrueKey\McTkSchedulerService.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\McAfee Security Scan\3.11.266\Scanner.exe	Hunter	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\ThumbnailExtractionHost.exe	Hunter	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\VBoxService.exe	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\VBoxService.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\SysWOW64\msiexec.exe	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\SysWOW64\msiexec.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\svchost.exe [WerSvcGroup]	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\svchost.exe [WerSvcGroup]	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\VBoxTray.exe	Hunter	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\Common Files\Adobe\ARM\1.0...	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\Common Files\Adobe\ARM\1.0...	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\TeamViewer_Service...	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\TeamViewer_Service...	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas

- Also, TeamViewer was used at the same time with the Skype

Source Name	S	C	O	Program Name	Username	△ Date/Time	Bytes Sent	Bytes Received	Comment	Data
SRUDB.dat				\Windows\System32\svchost.exe [WerSvcGroup]	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Windows\System32\VBoxTray.exe	Hunter	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\Common Files\Adobe\ARM\1.0...	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\Common Files\Adobe\ARM\1.0...	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\TeamViewer_Service...	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\TeamViewer_Service...	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewertv_w32.exe	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewertv_w32.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\tv_x64.exe	'Local System'	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\tv_x64.exe	systemprofile	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat				\Program Files(x86)\TeamViewer\TeamViewer.exe	Hunter	2016-06-21 04:00:00 MSK			System Resource Usage - Application Usage	cas
SRUDB.dat						2016-06-21 04:34:43 MSK	2407079	2766195	System Resource Usage - Network Usage	cas
SRUDB.dat				System	'Local System'	2016-06-21 04:34:43 MSK	92	271	System Resource Usage - Network Usage	cas
SRUDB.dat					systemprofile	2016-06-21 04:34:43 MSK	92	271	System Resource Usage - Network Usage	cas
SRUDB.dat				\program files(x86)\google\chrome\application\chrom...	Hunter	2016-06-21 04:34:43 MSK	2341303	2726356	System Resource Usage - Network Usage	cas
SRUDB.dat				\program files(x86)\skype\phone\skype.exe	Hunter	2016-06-21 04:34:43 MSK	25012	22115	System Resource Usage - Network Usage	cas
SRUDB.dat				\program files(x86)\teamviewer\teamviewer.exe	Hunter	2016-06-21 04:34:43 MSK	108	120	System Resource Usage - Network Usage	cas
SRUDB.dat				\program files(x86)\teamviewer\teamviewer_service.exe	'Local System'	2016-06-21 04:34:43 MSK	9771	8060	System Resource Usage - Network Usage	cas
SRUDB.dat				\program files(x86)\teamviewer\teamviewer_service.exe	systemprofile	2016-06-21 04:34:43 MSK	9771	8060	System Resource Usage - Network Usage	cas
SRUDB.dat				System	'Local System'	2016-06-21 04:34:43 MSK			System Resource Usage - Application Usage	cas

- Wireshark was also used

SRUDB.dat				\Users\Hunter\Downloads\Wireshark-win64-2.0.4.exe	Hunter	2016-06-21 12:47:50 MSK			System Resource Usage	
-----------	--	--	--	---	--------	-------------------------	--	--	-----------------------	--

- Tor Browser was used

SRUDB.dat				\Users\Hunter\Desktop\Tor Browser\Browser\firefox.exe	Hunter	2016-06-21 14:59:00 MSK			System Resource Usage	
SRUDB.dat				\Users\Hunter\Desktop\Tor Browser\Browser\Tor\tor.exe	Hunter	2016-06-21 14:59:00 MSK			System Resource Usage	

- Yeah, Nmap too

			\Program Files(x86)\Nmap\nmap-vcredist_x86.exe	Hunter	2016-06-21 14:59:00 MSK			System Resource Usage - Application Usage	
--	--	--	--	--------	-------------------------	--	--	---	--

- 7-zip, CCleaner and BSWipe were used at the same time after Nmap

		\Program Files\7-Zip\7zG.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\Downloads\python-3.5.1.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\AppData\Local\Temp\{c39d559b-aa83-4476-ba20-988a35a1199a}\...	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\AppData\Local\Programs\Python\Python3-32\python.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\Downloads\jre-8u91-windows-x64.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\AppData\Local\Temp\jds5059234.tmp\jre-8u91-windows-x64.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Program Files\Java\jre1.8.0_91\bin\javaw.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Program Files\CCleaner\CCleaner64.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Windows\System32\wbem\unsecapp.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\Downloads\bCWipeSetup.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Users\Hunter\AppData\Local\Temp\~bcwipeSetup.TMP\Setup.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage
		\Program Files (x86)\Jetico\BCWipe\BCResident.exe	Hunter	2016-06-21 14:59:00 MSK				System Resource Usage - Application Usage

- Skype, TeamViewer, Google Drive, DropBox, Tor Browser, Nmap were actively used actually

➤ SRUDB.dat		\program files (x86)\skype\phone\skype.exe	Hunter	2016-06-21 16:00:00 MSK	136732	235513	System Resource Usag
➤ SRUDB.dat		\program files (x86)\teamviewer\teamviewer.exe	Hunter	2016-06-21 16:00:00 MSK	1447	5641	System Resource Usag
➤ SRUDB.dat		\program files (x86)\teamviewer\teamviewer_service.exe	'Local System'	2016-06-21 16:00:00 MSK	9834265	2245017	System Resource Usag
➤ SRUDB.dat		\program files (x86)\teamviewer\teamviewer_service.exe	systemprofile	2016-06-21 16:00:00 MSK	9834265	2245017	System Resource Usag
➤ SRUDB.dat		\program files (x86)\google\drive\googledrivesync.exe	Hunter	2016-06-21 16:00:00 MSK	31217	39111	System Resource Usag
➤ SRUDB.dat		\program files (x86)\dropbox\client\dropbox.exe	Hunter	2016-06-21 16:00:00 MSK	384438	118914	System Resource Usag
➤ SRUDB.dat		\program files\microsoft office\office15\winword.exe	Hunter	2016-06-21 16:00:00 MSK	1696	43777	System Resource Usag
➤ SRUDB.dat		\users\hunter\desktop\tor browser\browser\torbrowser\tor\tor.exe	Hunter	2016-06-21 16:00:00 MSK	672648	5613506	System Resource Usag
➤ SRUDB.dat		\program files (x86)\nmap\nmap.exe	Hunter	2016-06-21 16:00:00 MSK	41795	169917	System Resource Usag

- FTK Imager together with already mentioned

➤ SRUDB.dat		\Users\Hunter\Downloads\FTK-Imager\FTK Imager.exe	Hunter	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Users\Hunter\Desktop\Tor Browser\Browser\firefox.exe	Hunter	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Users\Hunter\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe	Hunter	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Program Files (x86)\Jetico\BCWipe\BCWipeSvc.exe	'Local System'	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Program Files (x86)\Jetico\BCWipe\BCWipeSvc.exe	systemprofile	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Program Files (x86)\Jetico\BCWipe\BCWipeTM.exe	'Local System'	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Program Files (x86)\Jetico\BCWipe\BCWipeTM.exe	systemprofile	2016-06-21 16:00:00 MSK			System Resource Usag

- What is more, I found Zenmap which is a powerful GUI tool for port scanning based on Nmap

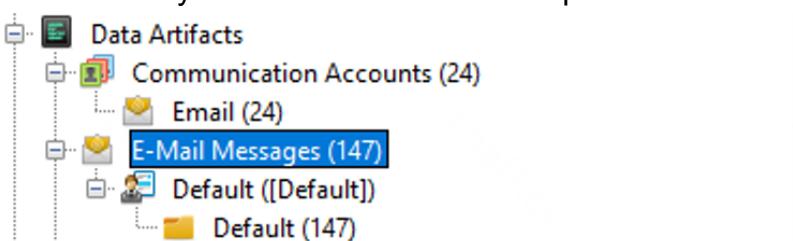
➤ SRUDB.dat		\Program Files (x86)\Nmap\zenmap.exe	Hunter	2016-06-21 16:00:00 MSK			System Resource Usag
➤ SRUDB.dat		\Program Files (x86)\Nmap\nmap.exe	Hunter	2016-06-21 16:00:00 MSK			System Resource Usag

• Conclusion:

- From all above, I can conclude that the owner used: Tor Browser for something probably not legal, port scanning using Zenmap, BCWipe and CCleaner for wiping data, TeamViewer for remote access (maybe someone worked instead of him), Skype for communications, DropBox, Google Drive, 7-zip, FTK-Imager for compressing and stealing some data, Wireshark for capturing Network/USB data, and VBox for some other purposes.
- I may be wrong with my assumption further, but let's see

Communications: Email

- Well, we saw active Skype usage in the date of using Tor, Zenmap, Wireshark, BCWipe. Therefore, I decided to carefully explore user's communications in Skype and other places.
- Since AutoPsy provides an ability to check e-mails from scratch using default ingesting modules I decided firstly to check e-mails and it explored that it not for nothing 😊



- First, I discovered all the E-Mail accounts participated in communications on this device including skype

Source Name	S	C	O	Account Type	ID	Data Source
backup.pst			1	EMAIL	hello@email skype.com	case1.001
backup.pst			1	EMAIL	ehptmsgs@gmail.com	case1.001
backup.pst			1	EMAIL	linux-rul3z@hotmail.com	case1.001
backup.pst			1	EMAIL	no-reply@accounts.google.com	case1.001
backup.pst			1	EMAIL	linux4rulez@gmail.com	case1.001
backup.pst			1	EMAIL	aafrafs@accessdata.com	case1.001
backup.pst			1	EMAIL	hello@email skype.com	case1.001
backup.pst			1	EMAIL	ehptmsgs@gmail.com	case1.001
backup.pst			1	EMAIL	linux-rul3z@hotmail.com	case1.001
backup.pst			1	EMAIL	no-reply@accounts.google.com	case1.001
backup.pst			1	EMAIL	linux4rulez@gmail.com	case1.001
backup.pst			1	EMAIL	aafrafs@accessdata.com	case1.001
ehptmsgs@gmail.com.ost			1	EMAIL	hello@email skype.com	case1.001
ehptmsgs@gmail.com.ost			1	EMAIL	ehptmsgs@gmail.com	case1.001
ehptmsgs@gmail.com.ost			1	EMAIL	linux-rul3z@hotmail.com	case1.001
ehptmsgs@gmail.com.ost			1	EMAIL	no-reply@accounts.google.com	case1.001
ehptmsgs@gmail.com.ost			1	EMAIL	linux4rulez@gmail.com	case1.001
ehptmsgs@gmail.com.ost			1	EMAIL	aafrafs@accessdata.com	case1.001
msg_25.txt			1	EMAIL	mailer-daemon@zinfandel.lacita.com	case1.001
msg_25.txt			1	EMAIL	linuxuser-admin@www.linux.org.uk	case1.001
msg_43.txt			1	EMAIL	webmaster@python.org	case1.001
msg_25.txt			1	EMAIL	mailer-daemon@zinfandel.lacita.com	case1.001
msg_25.txt			1	EMAIL	linuxuser-admin@www.linux.org.uk	case1.001
msg_43.txt			1	EMAIL	webmaster@python.org	case1.001

- It seems that the PC owners' e-mail is ehptmsgs@gmail.com since this email was participated in each communication either as a receiver or a sender. What I found is that this email can be related to the EH Techniques organization which is **Energy Harvesting** or **EHPT** which is the either **Ericsson Hewlett Packard Telecom** or **Ethical Hacker & Penetration Tester**. However, it still can be a personal account, but it looks more as an account of organization.

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	▲ Date Received	Message (Plain)
backup.pst				Google <no-reply@accounts.google.com>	enptmsgs@gmail.com	New sign-in from Chrome on Windows	2016-06-21 02:09:34 MSK	<https://www.
ehptmsgs@gmail.com.ost				Google <no-reply@accounts.google.com>	ehptmsgs@gmail.com	New sign-in from Chrome on Windows	2016-06-21 02:09:34 MSK	
backup.pst				Skype <hello@email skype.com>	ehptmsgs@gmail.com	إيلك كفيفه إضافة جواد انتصال ويندوز التواصل على	2016-06-21 02:16:38 MSK	<http://click.er
backup.pst				Skype <hello@email skype.com>	ehptmsgs@gmail.com	إيلك كفيفه إضافة جواد انتصال ويندوز التواصل على	2016-06-21 02:16:38 MSK	<http://click.er
ehptmsgs@gmail.com.ost				Skype <hello@email skype.com>	ehptmsgs@gmail.com	إيلك كفيفه إضافة جواد انتصال ويندوز التواصل على	2016-06-21 02:16:38 MSK	
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there,lju:
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there,lju:
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there,lju:
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there,lju:
ehptmsgs@gmail.com.ost				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	
ehptmsgs@gmail.com.ost				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,lju:
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,lju:
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,lju:
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,lju:

- I found an e-mail from a representer of [AccessData](#) company which was a software development company that developed [Forensic Toolkit \(FTK\)](#) and FTK Imager until it was acquired by Exterro. This e-mail contains information about some data privacy education event. This could mean that the owner of this e-mail somehow related to the world of Cyber Security.

From: Abdes Afras <aafrafs@accessdata.com>
 To: ehptmsgs@gmail.com
 CC:
 Subject: Don't forget to register for privacy event & reception

2016-06-03 20:47:22 MSK

Headers Text HTML RTF Attachments (0) Accounts Original Text

Hello,

We are less than three weeks away from a data privacy education series that AccessData is hosting, at no cost to you. The event will focus on compliance with data privacy regulations in the UK and throughout Europe. Some of the world's leading experts are serving as panelists.

We will be in three cities for the 75 minute panel discussion, followed immediately by a cocktail reception:

London: 20 June, 2016
 Amsterdam: 22 June, 2016
 Frankfurt: 23 June, 2016

We ask that you kindly arrive by 15:00.

Seats are limited! For more information, including location details for each city, and to reserve your spot, please click to <http://marketing.accessdata.com/e/46432/CrossBorderQuandary/3r324f/859213774>

Activate Windows
[Go to Settings to activate Windows.](#)

- Then I found New sign-in from Chrome Linx which means that this person has some Linux account (but currently we're observing Linux) somewhere and could be hacked at 2016-06-21

02:01:29+03:00 . What is more, I found the next e-mail with the similar content Your recovery email address changed and New sign-in from Chrome on Windows . And everything happened around the same time.

✉ backup.pst		Google <no-reply@accounts.google.com>	ehptmsgs@gmail.com	New sign-in from Chrome on Linux	2016-06-21 02:01:05 MSK	<https://www.
✉ backup.pst		Google <no-reply@accounts.google.com>	ehptmsgs@gmail.com	New sign-in from Chrome on Linux	2016-06-21 02:01:05 MSK	<https://www.
✉ ehptmsgs@gmail.com.ost		Google <no-reply@accounts.google.com>	ehptmsgs@gmail.com	New sign-in from Chrome on Linux	2016-06-21 02:01:05 MSK	<https://www.
✉ backup.pst		Google <no-reply@accounts.google.com>	ehptmsgs@gmail.com	Your recovery email address changed	2016-06-21 02:01:29 MSK	<https://www.

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

Result: 22 of 53 Result ↶ ↷ E-Mail Messages

From: Google <no-reply@accounts.google.com> 2016-06-21 02:01:05 MSK
To: ehptmsgs@gmail.com
CC:
Subject: New sign-in from Chrome on Linux

Headers Text HTML RTF Attachments (0) Accounts
Download Images

The screenshot shows an email message from Google accounts. The subject is "New sign-in from Chrome on Linux". The message body says: "Hi EH, Your Google Account ehptmsgs@gmail.com was just used to sign in from Chrome on Linux." At the bottom, it shows "EH Techniques" and an email address "ehptmsgs@gmail.com". There is also a link to "Activate Windows" with the text "Go to Settings to activate Windows." The interface includes tabs for Hex, Text, Application, etc., and a navigation bar at the top.

backup.pst | Google <no-reply@accounts.google.com> | ehptmsgs@gmail.com | Your recovery email address changed | 2016-06-21 02:01:29 MSK | <https://www. >

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

Result: 21 of 53 Result ← → E-Mail Messages

From: Google <no-reply@accounts.google.com> 2016-06-21 02:01:29 MSK
To: ehptmsgs@gmail.com
CC:
Subject: Your recovery email address changed

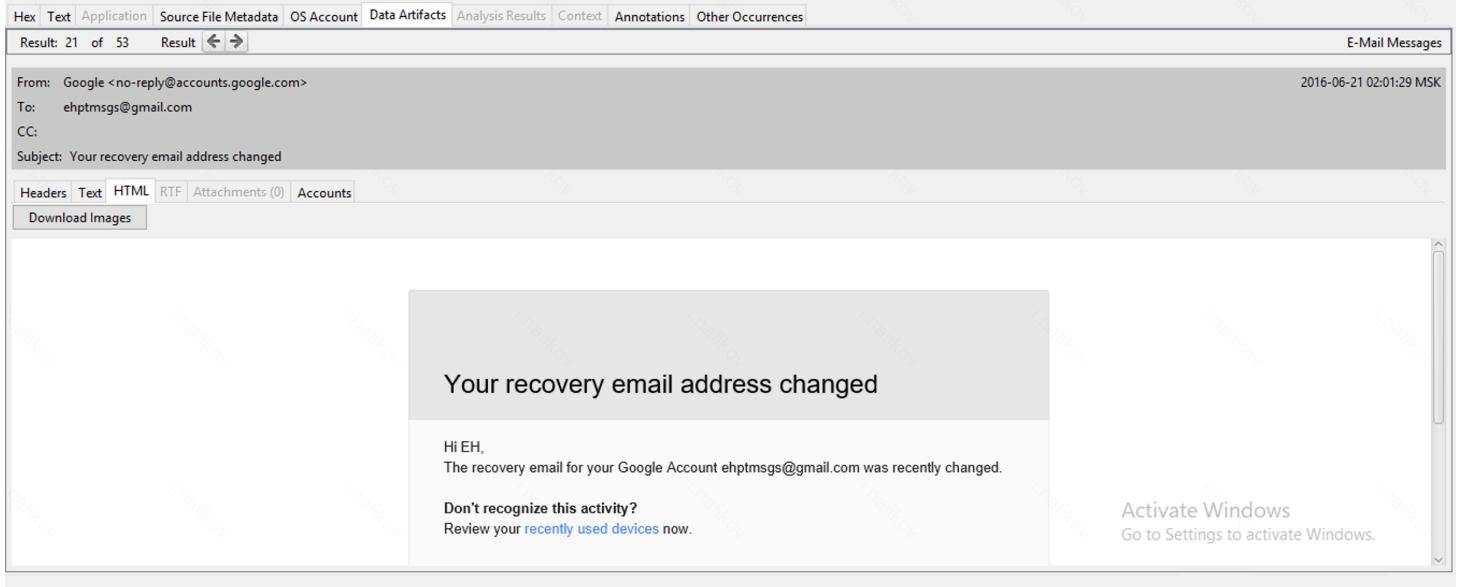
Headers Text HTML RTF Attachments (0) Accounts Download Images

Your recovery email address changed

Hi EH,
The recovery email for your Google Account ehptmsgs@gmail.com was recently changed.

Don't recognize this activity?
Review your [recently used devices](#) now.

Activate Windows
Go to Settings to activate Windows.



backup.pst | Google <no-reply@accounts.google.com> | ehptmsgs@gmail.com | New sign-in from Chrome on Windows | 2016-06-21 02:09:34 MSK | <https://www. >

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

Result: 20 of 53 Result ← → E-Mail Messages

From: Google <no-reply@accounts.google.com> 2016-06-21 02:09:34 MSK
To: ehptmsgs@gmail.com
CC:
Subject: New sign-in from Chrome on Windows

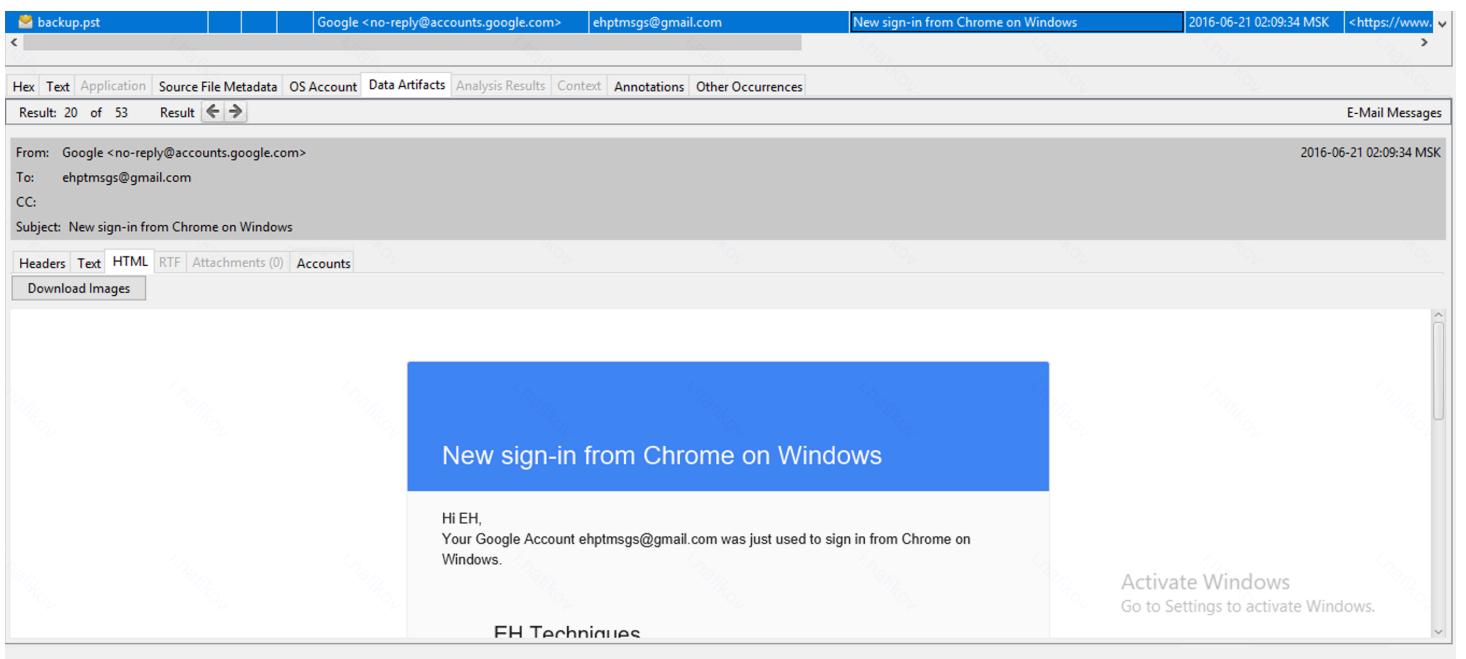
Headers Text HTML RTF Attachments (0) Accounts Download Images

New sign-in from Chrome on Windows

Hi EH,
Your Google Account ehptmsgs@gmail.com was just used to sign in from Chrome on Windows.

Activate Windows
Go to Settings to activate Windows.

FH Techniques



- Also, I found a strange e-mail from Skype in Arabic language which is basically just an invitation to install Skype and find your friends there

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	△ Date Received	Message (Plain)
backup.pst				Skype <hello@email.skype.com>	ehptmsgs@gmail.com	إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype	2016-06-21 02:16:38 MSK	<http://click.er...
backup.pst				Skype <hello@email.skype.com>	ehptmsgs@gmail.com	إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype	2016-06-21 02:16:38 MSK	<http://click.er...
ehptmsgs@gmail.com.ost				Skype <hello@email.skype.com>	ehptmsgs@gmail.com	إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype	2016-06-21 02:16:38 MSK	
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
ehptmsgs@gmail.com.ost				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	
ehptmsgs@gmail.com.ost				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...

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

Result: 3 of 53 Result ← → E-Mail Messages

From: Skype <hello@email.skype.com> 2016-06-21 02:16:38 MSK
 To: ehptmsgs@gmail.com
 CC:
 Subject: إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype

Headers Text HTML RTF Attachments (0) Accounts Download Images



ألا يمكنك أن ترى هذا البريد الإلكتروني جيداً؟
 هل نسيت كلمة المرور الخاصة بك؟

شكراً لك على الانضمام إلى Skype

بعد التسجيل، حان وقت إضافة الأصدقاء، والخبر السار هو أن العثور عليهم وإضافتهم لا يتطلب سوى بضع ثوان. وهكذا يمكنك البدء بالاستفادة من

Activate Windows Go to Settings to activate Windows.

- And further there is a long conversation between the ehptmsgs@gmail.com and linux-rul3z@hotmail.com which I described shortly below:

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	△ Date Received	Message (Plain)
backup.pst				Skype <hello@email.skype.com>	ehptmsgs@gmail.com	إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype	2016-06-21 02:16:38 MSK	<http://click.er...
backup.pst				Skype <hello@email.skype.com>	ehptmsgs@gmail.com	إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype	2016-06-21 02:16:38 MSK	<http://click.er...
ehptmsgs@gmail.com.ost				Skype <hello@email.skype.com>	ehptmsgs@gmail.com	إليك كيفية إضافة جهات اتصال وبدء التواصل على Skype	2016-06-21 02:16:38 MSK	
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
ehptmsgs@gmail.com.ost				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
ehptmsgs@gmail.com.ost				EH Techniques <ehptmsgs@gmail.com>	linux-rul3z@hotmail.com	TeamViewer	2016-06-21 03:53:13 MSK	Hello there, I ju...
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
ehptmsgs@gmail.com.ost				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
ehptmsgs@gmail.com.ost				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter, I ju...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	Linux rul3z	Re: TeamViewer	2016-06-21 03:57:50 MSK	Okay, looking f...
backup.pst				EH Techniques <ehptmsgs@gmail.com>	Linux rul3z	Re: TeamViewer	2016-06-21 03:57:50 MSK	Okay, looking f...
ehntmscas@gmail.com.ost				FH Techniques <ehntmscas@gmail.com>	Linux rul3z	Re: TeamViewer	2016-06-21 03:57:50 MSK	

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

Result: 29 of 53 Result ← → E-Mail Messages

From: EH Techniques <ehptmsgs@gmail.com> 2016-06-21 03:53:13 MSK
 To: linux-rul3z@hotmail.com
 CC:
 Subject: TeamViewer

Headers Text HTML RTF Attachments (0) Accounts Download Images

Hello there,
 I just wanted to confirm the installation of Team Viewer as requested.
 When can we continue our discussion?
 Regards,
 Hunter

Activate Windows Go to Settings to activate Windows.

- So, the content of this E-mail conversation is the following
 - Hunter connected with some guy who seems to understand something in attacks / penetration testing to teach him and help him to attack or pentest some network (probably of their organization but I am not sure yet).
 - Their dialogue established with a Hunter's message about TeamViewer which I suppose lets the other guy to access his device remotely.
 - They converse via E-mail and Skype.
 - In Skype there is some password that can help to unarchive some 7-zip attachments from Hunter with pictures.
 - The other guy sent to Hunter links on YouTube videos about **Data Exfiltration !** and advices Hunter to disguise file using changing their extensions. So, Hunter uses this method and send him a PDF document with the JPG extension

From: EH Techniques <ehptmsgs@gmail.com>

To:

CC:

Subject: Attachment

Headers Text HTML RTF Attachments (1) Accounts

Table Thumbnail Summary

Location	Size	Mime type	Known
/img_case1.001/Users/Hunter/AppData/Local/Micr	338662	application/pdf	unknown

Confidential Document

1 PRIVATE

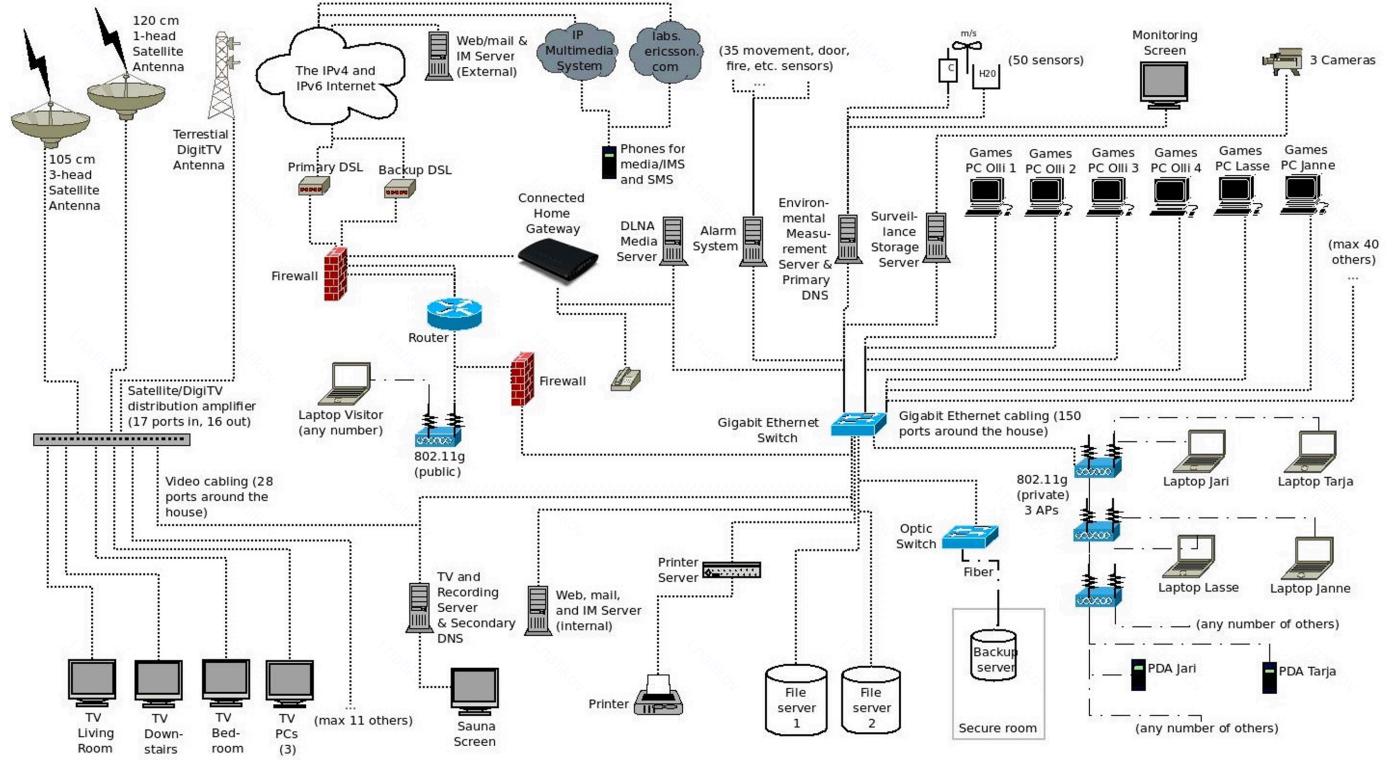
To take advantage of this template's design, use the Styles gallery on the Home tab. You can format your headings by using heading styles, or highlight important text using other styles, like Emphasis and Intense Quote. These styles come in formatted to look great and work together to help communicate your ideas.

Go ahead and get started.

Best regards,

Hunter

- Furthermore, Hunter tried to save this YouTube video links but the other guy told him to remove it, so Hunter wiped them (probably using the BSWipe)
- Also, Hunter suggested to use Hangouts for communication but received no answer
- Hunter sent the other guy a network design sample but got responded that the original print for the network is required to investigate what systems, apps, tools, appliances are used.



- Finally, Hunter asked the other guy to finish the project ASAP and told him that his Outlook setup is working correctly.

Communications: Skype

- So, after this conversation I became even more convinced that I need to check their Skype conversation and find out more useful information and the mentioned password to check pictures sent via e-mail.
- Using the web I easily found where the Skype messages are stored locally. So I accessed the SQLite DB file and was able to explore the data right from AutoPsy. I selected `Messages` table and now I can easily see all the messages of the `huntereprh` which is a Hunter's username in Skype with the

The screenshot shows a digital forensics tool interface with a sidebar navigation menu and a main content area. The sidebar includes options like Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, Keyword Lists, and Keyword Search. The main content area has tabs for Listing, Thumbnail, and Summary. A table titled 'Listing' shows file details for 'img_case1.001/Users/Hunter/AppData/Roaming/Skype/huntereht'. The table columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. Below this is another table titled 'Messages' with 46 entries, showing columns for type, sending..., option_b..., consum..., edited_by, edited_t..., param_k..., param_v..., body_xml, identities, reason, leaverea..., participa..., and err. The interface also includes tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

- From their conversation I got that Hunter asking linux-rul3z to help him to transfer some pictures and documents outside an organization's network since it is monitored. This guys agreed to help him and asks if he is able to access Hunter's device remotely via TeamViewer. Hunter downloaded TeamViewer and then their conversation goes to e-mail which we already saw.
- Also, I got a Hunter's birthday which does not look like a real and a city which seems to be real since the mail from Skype were in Arabic: 1990-01-01 , Amman, Jordan

The screenshot shows a digital forensics tool interface with a sidebar navigation menu and a main content area. The sidebar includes options like Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, Keyword Lists, and Keyword Search. The main content area has tabs for Listing, Thumbnail, and Summary. A table titled 'Listing' shows file details for 'img_case1.001/Users/Hunter/'. The table columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. Below this is another table titled 'Messages' with 7 entries, showing columns for type, sending..., option_b..., consum..., edited_by, edited_t..., param_k..., param_v..., body_xml, identities, reason, leaverea..., participa..., and err. The interface also includes tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

- Unfortunately, I couldn't find any password Hunter told about in mails to unarchive Pics.7z or fakeporn.7z neither in Skype databases, nor in Skype journals. It seems that Hunter quickly removed this message.

Result: 31 of 53 Result ← →

E-Mail Messages

From: EH Techniques <ehptmsgs@gmail.com>

2016-06-21 04:00:31 MSK

To: Linux rul3z

CC:

Subject: Pics

Headers Text HTML RTF Attachments (1) Accounts

Hide Images

Hello,

Attached is a 7z archive of some of the pictures I told you about.

The password will be given to you using Skype :D

Regards,

HunterActivate Windows
Go to Settings to activate Windows.

Result: 35 of 53 Result ← →

E-Mail Messages

From: EH Techniques <ehptmsgs@gmail.com>

2016-06-21 14:50:24 MSK

To: Linux rul3z; linux4rulez@gmail.com

CC:

Subject: Nice Pics

Headers Text HTML RTF Attachments (1) Accounts

Hide Images

Hello,

Just wanted to share these nice pics with you.

Let me know if you liked them :D

--

Regards,
HunterActivate Windows
Go to Settings to activate Windows.

Files

- After figuring out what's probably happened I finally need to investigate Hunter's files and check for a suspicious things
- In Downloads I found a lot of interesting installers. Besides the programs I've mentioned in Applications section I also found out the following:

- Ollydbg** which is a 32-bit assembler level analysing debugger for Windows.

 Ollydbg			2016-06-21 14:07:58 MSK	2016-06-21 14:07:58 MSK	2016-06-21 14:07:58 MSK	2016-06-21 14:07:54 MSK	56	Allocated	Allocated
---	--	--	-------------------------	-------------------------	-------------------------	-------------------------	----	-----------	-----------

- Hash Suite Free** which is a Windows program to test security of password hashes.

 Hash_Suite_Free			2016-06-21 14:43:46 MSK	2016-06-21 14:43:46 MSK	2016-06-21 14:43:46 MSK	2015-04-29 07:16:16 MSK	56	Allocated	Allocated
---	--	--	-------------------------	-------------------------	-------------------------	-------------------------	----	-----------	-----------

- BurpSuite** which is a proprietary software tool for security assessment and penetration testing of web applications.

 burpsuite_free_v1.7.03.jar		0	2016-06-21 14:02:14 MSK	2016-06-21 14:17:44 MSK	2016-06-21 14:00:58 MSK	2016-06-21 14:00:58 MSK	12397221	Allocated	Allocated
--	--	---	-------------------------	-------------------------	-------------------------	-------------------------	----------	-----------	-----------

- Eraser** which is a secure data removal tool for Windows.

 Eraser6.2.0.2971-NoRuntimes.exe		0	2016-06-21 13:57:20 MSK	2016-06-21 13:57:20 MSK	2016-06-21 13:57:17 MSK	2016-06-21 13:57:17 MSK	2274280	Allocated	Allocated
---	--	---	-------------------------	-------------------------	-------------------------	-------------------------	---------	-----------	-----------

- Putty** which is a PuTTY is an SSH and telnet client

 putty.exe		0	2016-06-21 02:57:41 MSK	2016-06-21 14:55:37 MSK	2016-06-21 02:57:34 MSK	2016-06-21 02:57:34 MSK	531368	Allocated	Allocated
---	--	---	-------------------------	-------------------------	-------------------------	-------------------------	--------	-----------	-----------

- **PSCP** which is a PSCP, the PuTTY Secure Copy client, is a tool for transferring files securely between computers using an SSH connection

	0	2016-06-21 02:57:42 MSK	2016-06-21 14:08:15 MSK	2016-06-21 02:57:41 MSK	2016-06-21 02:57:41 MSK	359336	Allocated	Allocated
--	---	-------------------------	-------------------------	-------------------------	-------------------------	--------	-----------	-----------

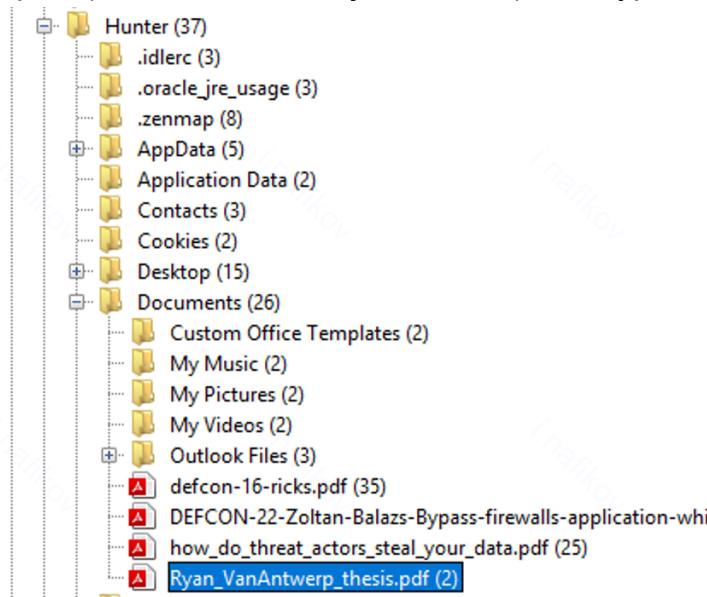
- **SetupSSH** which is a OpenSSH client.

	0	2016-06-21 02:59:06 MSK	2016-06-21 02:59:06 MSK	2016-06-21 02:58:45 MSK	2016-06-21 02:58:45 MSK	2410307	Allocated	Allocated
--	---	-------------------------	-------------------------	-------------------------	-------------------------	---------	-----------	-----------

- **SysinternalSuite** which are technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Windows environment.

	0	2016-06-21 14:02:36 MSK	2016-06-21 14:02:36 MSK	2016-06-21 14:01:24 MSK	2016-06-21 14:01:24 MSK	16127164	Allocated	Allocated
--	---	-------------------------	-------------------------	-------------------------	-------------------------	----------	-----------	-----------

- In **Documents** folder I found 4 documents related to performing Data Exfiltration using different techniques (DNS, FTP, SQL Injection, etc.) and Bypassing Firewall.



- Inside the **Google Drive** folder I found a proposal for Hunter to buy Forensics courses which are quite expensive and some other interesting documents

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M)
[current folder]				2016-06-21 05:04:49 MSK	2016-06-21 05:04:49 MSK	2016-06-21 04:54:20 MSK	2016-06-21 04:54:20 MSK	56	Allocated	Allocated
[parent folder]				2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	0000-00-00 00:00:00		256	Allocated	Allocated
.tmp.driivedownload				2016-06-21 05:04:49 MSK	2016-06-21 05:04:49 MSK	2016-06-21 04:54:25 MSK	2016-06-21 04:54:25 MSK	48	Allocated	Allocated
Accounts.txt	1			2016-06-21 04:46:16 MSK	2016-06-21 04:46:16 MSK	2016-06-21 04:56:29 MSK	2016-06-21 04:56:29 MSK	98	Allocated	Allocated
desktop.ini	0			2016-06-21 04:54:21 MSK	2016-06-21 04:54:21 MSK	2016-06-21 04:54:20 MSK	2016-06-21 04:54:20 MSK	180	Allocated	Allocated
FTK-Imager.zip	1			2016-06-21 05:04:49 MSK	2016-06-21 05:04:49 MSK	2016-06-21 05:04:42 MSK	2016-06-21 05:04:42 MSK	24983628	Allocated	Allocated
Getting started	0			2016-02-24 18:46:39 MSK	2016-06-21 04:54:27 MSK	2016-02-24 18:46:39 MSK	2016-06-21 04:54:25 MSK	1560010	Allocated	Allocated
proposal.pdf	0			2016-06-21 05:03:42 MSK	2016-06-21 05:03:42 MSK	2016-06-21 05:03:45 MSK	2016-06-21 05:03:45 MSK	310382	Allocated	Allocated
Python and the Army Knife (Recovered).gslides	0			2016-02-24 18:47:30 MSK	2016-06-21 04:54:25 MSK	2016-02-24 18:47:30 MSK	2016-06-21 04:54:25 MSK	248	Allocated	Allocated
tools.txt	1			2016-06-21 12:21:53 MSK	2016-06-21 05:05:32 MSK	2016-06-21 04:56:29 MSK	2016-06-21 04:56:29 MSK	166	Allocated	Allocated

- Some tools list

The screenshot shows a software interface for analyzing files. At the top, there's a header bar with tabs for 'Hex', 'Text' (which is selected), 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. Below the header, there are search and filter controls: 'Page: 1 of 1 Page', 'Matches on page: - of - Match', zoom level '100%', and buttons for 'Reset' and 'Text Source: File Text'. The main content area is titled 'Tools to be installed:' and lists the following items:

- 1. Chrome
- 2. Skype
- 3. Outlook / MS Office
- 4. Notepad++
- 5. 7zip
- 6. Wireshark
- 7. Adobe Reader + Other misc stuff come with the offer
- 8.

- And accounts list, unfortunately without passwords 😢

The screenshot shows a software interface for analyzing files. At the top, there's a header bar with tabs for 'Hex', 'Text' (selected), 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. Below the header, there are search and filter controls: 'Page: 1 of 1 Page', 'Matches on page: - of - Match', zoom level '100%', and buttons for 'Reset' and 'Text Source: File Text'. The main content area is titled 'Accounts:' and lists the following information:

- Email: ptehmsg @ gmail
- Skype: HunterPTEH
- Teamviewer:
- Google Drive:
- Dropbox:

- Inside the Pictures I found a folder named `Exfil` which also contained some information about Exfiltration techniques

Table Thumbnail Summary

Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]			2016-06-21 15:01:42 MSK	2016-06-21 15:01:42 MSK	2016-06-21 15:01:42 MSK	2000-00-00 00:00:00	56	Allocated	Allocated	unknown	/img_c...
[parent folder]			2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	2000-00-00 00:00:00	256	Allocated	Allocated	unknown	/img_c...
backgrounds			2016-06-21 02:52:11 MSK	2016-06-21 02:52:11 MSK	2016-06-21 02:52:11 MSK	2016-06-21 12:35:15 MSK	56	Allocated	Allocated	unknown	/img_c...
Exfil			2016-06-21 12:38:13 MSK	2016-06-21 12:38:13 MSK	2016-06-21 12:38:13 MSK	2016-06-21 12:37:36 MSK	680	Allocated	Allocated	unknown	/img_c...
Private			2016-06-21 15:04:15 MSK	2016-06-21 15:04:15 MSK	2016-06-21 15:04:15 MSK	2016-06-21 12:43:16 MSK	56	Allocated	Allocated	unknown	/img_c...
desktop.ini	1		2016-06-21 11:37:53 MSK	2016-06-21 11:37:53 MSK	2016-06-21 11:37:53 MSK	2016-06-21 11:37:53 MSK	504	Allocated	Allocated	unknown	/img_c...
mofygdvh.mcp			1986-04-30 15:43:13 MSD	2016-06-21 15:01:07 MSK	1986-04-30 15:43:13 MSD	1986-04-30 15:43:13 MSD	0	Unallocated	Unallocated	unknown	/img_c...
Thumbs.db	0		2016-06-21 12:37:34 MSK	2016-06-21 12:37:34 MSK	2016-06-21 12:29:58 MSK	2016-06-21 12:29:58 MSK	163328	Allocated	Allocated	unknown	/img_c...
Thumbs.db:encryptable			2016-06-21 12:37:34 MSK	2016-06-21 12:37:34 MSK	2016-06-21 12:29:58 MSK	2016-06-21 12:29:58 MSK	0	Allocated	Allocated	unknown	/img_c...
Thumbs.db			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/img_c...

< >

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

Result: 1 of 1 Result Associated Object

Type	Value	Source(s)
Associated Artifact	-9223372036854775783	Recent Activity
Source File Path	/img_case1.001/Users/Hunter/Pictures/Exfil	
Artifact ID	-9223372036854775782	

Listing /img_case1.001/Users/Hunter/Pictures/Exfil 8 Results

Table Thumbnail Summary

Save Table as CSV

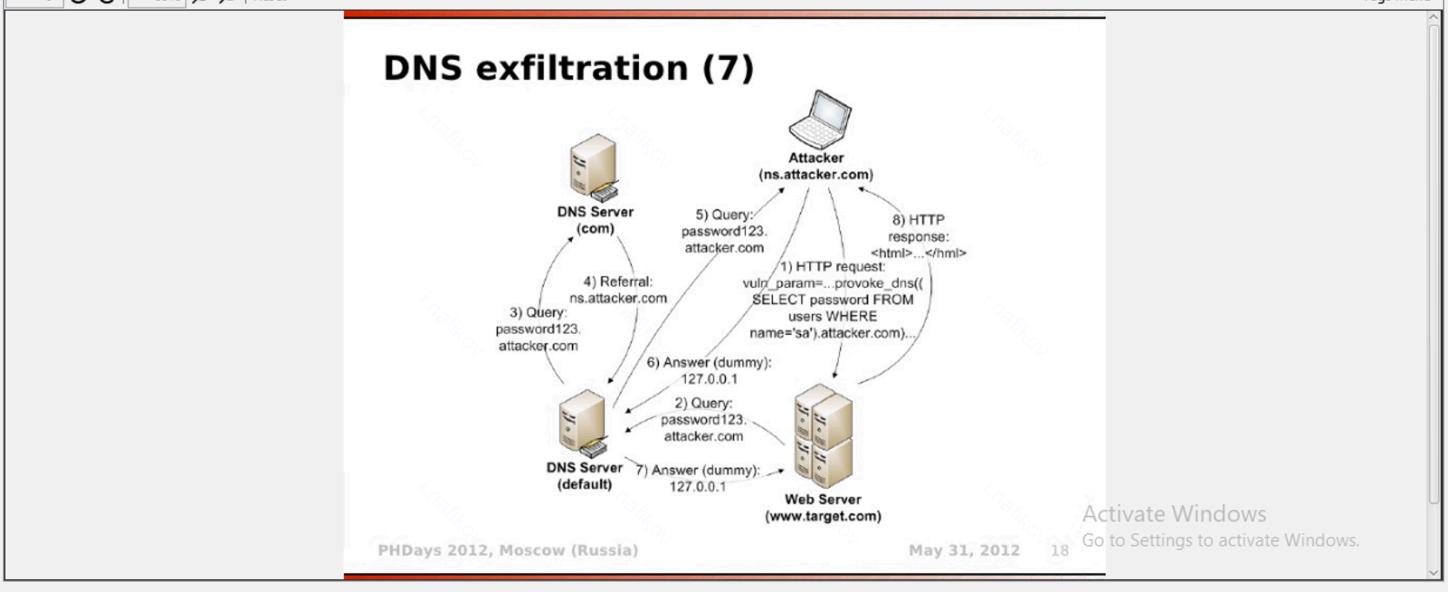
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]			2016-06-21 12:38:13 MSK	2016-06-21 12:38:13 MSK	2016-06-21 12:38:13 MSK	2016-06-21 12:37:36 MSK	680	Allocated	Allocated
[parent folder]			2016-06-21 15:01:42 MSK	2016-06-21 15:01:42 MSK	2016-06-21 15:01:42 MSK	2000-00-00 00:00:00	56	Allocated	Allocated
dns-exfiltration-using-sqlmap-18-728.jpg	1		2016-06-21 12:38:13 MSK	2016-06-21 15:17:39 MSK	2016-06-21 12:38:12 MSK	2016-06-21 12:38:13 MSK	71910	Allocated	Allocated
dns-exfiltration-using-sqlmap-18-728.jpg:Zone.Identifier	2		2016-06-21 12:38:13 MSK	2016-06-21 15:17:39 MSK	2016-06-21 12:38:12 MSK	2016-06-21 12:38:13 MSK	26	Allocated	Allocated
Efiltration_Diagram.png	1		2016-06-21 12:37:50 MSK	2016-06-21 15:17:41 MSK	2016-06-21 12:37:32 MSK	2016-06-21 12:37:49 MSK	100256	Allocated	Allocated
Efiltration_Diagram.png:Zone.Identifier	2		2016-06-21 12:37:50 MSK	2016-06-21 15:17:41 MSK	2016-06-21 12:37:32 MSK	2016-06-21 12:37:49 MSK	26	Allocated	Allocated
Thumbs.db	0		2016-06-21 15:03:26 MSK	2016-06-21 15:03:26 MSK	2016-06-21 12:38:13 MSK	2016-06-21 12:38:13 MSK	24064	Allocated	Allocated
Thumbs.db:encryptable			2016-06-21 15:03:26 MSK	2016-06-21 15:03:26 MSK	2016-06-21 12:38:13 MSK	2016-06-21 12:38:13 MSK	0	Allocated	Allocated

< >

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

0° C 89% ⌂ ⌃ ⌁ Reset

Tags Menu



- Inside the Pictures/Private there are a log of kittys' photos. Maybe he sent some of them to linux-r3lz

Listing /img_case1.001/Users/Hunter/Pictures/Private 20 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	▼ O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
6966997-sleeping-kitties.jpg:Zone.Identifier			2	2016-06-21 12:30:46 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:45 MSK	2016-06-21 12:30:46 MSK	26	Allocated	Allocated
Adorable-kitties-kitties-18082642-670-503.jpg			1	2016-06-21 12:30:49 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:49 MSK	2016-06-21 12:30:49 MSK	88890	Allocated	Allocated
Adorable-kitties-kitties-18082642-670-503.jpg:Zone			2	2016-06-21 12:30:49 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:49 MSK	2016-06-21 12:30:49 MSK	26	Allocated	Allocated
big-eyes-cat-cats-cute-Favim.com-2674726.jpg			1	2016-06-21 12:31:33 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:31:32 MSK	2016-06-21 12:31:32 MSK	119410	Allocated	Allocated
big-eyes-cat-cats-cute-Favim.com-2674726.jpg:Zo			2	2016-06-21 12:31:33 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:31:32 MSK	2016-06-21 12:31:32 MSK	26	Allocated	Allocated
Breathtaking-Kitties14.jpg			1	2016-06-21 12:30:23 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:23 MSK	2016-06-21 12:30:23 MSK	42027	Allocated	Allocated
Breathtaking-Kitties14.jpg:Zone.Identifier			2	2016-06-21 12:30:23 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:23 MSK	2016-06-21 12:30:23 MSK	26	Allocated	Allocated
gutter.jpg			1	2016-06-21 12:30:06 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:05 MSK	2016-06-21 12:30:05 MSK	142643	Allocated	Allocated
gutter.jpg:Zone.Identifier			2	2016-06-21 12:30:06 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:05 MSK	2016-06-21 12:30:05 MSK	26	Allocated	Allocated
Kitties-cats-2209221-500-374.jpg			1	2016-06-21 12:30:02 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:00 MSK	2016-06-21 12:30:01 MSK	111092	Allocated	Allocated
Kitties-cats-2209221-500-374.jpg:Zone.Identifier			2	2016-06-21 12:30:02 MSK	2016-06-21 12:43:20 MSK	2016-06-21 12:30:00 MSK	2016-06-21 12:30:01 MSK	26	Allocated	Allocated

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

0° C C | 130% ⌂ ⌂ | Reset Tags Menu

Activate Windows
Go to Settings to activate Windows.

- Inside the Pictures/background there a lot of wallpapers on hackers, securityf, Kali Linux and all this stuff

Listing /img_case1.001/Users/Hunter/Pictures/backgrounds 24 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	▼ O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2016-06-21 02:52:11 MSK	2016-06-21 02:52:11 MSK	2016-06-21 02:52:11 MSK	2016-06-21 12:35:15 MSK	56	Allocated	Allocated
[parent folder]				2016-06-21 15:01:42 MSK	2016-06-21 15:01:42 MSK	2016-06-21 15:01:42 MSK	0000-00-00 00:00:00	56	Allocated	Allocated
232919.jpg			1	2016-06-21 12:44:42 MSK	2016-06-21 12:44:42 MSK	2016-06-21 12:44:41 MSK	2016-06-21 12:44:42 MSK	77997	Allocated	Allocated
232919.jpg:Zone.Identifier			2	2016-06-21 12:44:42 MSK	2016-06-21 12:44:42 MSK	2016-06-21 12:44:41 MSK	2016-06-21 12:44:42 MSK	26	Allocated	Allocated
565053.jpg			1	2016-06-21 12:35:28 MSK	2016-06-21 12:35:27 MSK	2016-06-21 12:35:26 MSK	2016-06-21 12:35:28 MSK	1737915	Allocated	Allocated
565053.jpg:Zone.Identifier			2	2016-06-21 12:35:28 MSK	2016-06-21 12:35:27 MSK	2016-06-21 12:35:26 MSK	2016-06-21 12:35:28 MSK	26	Allocated	Allocated
Abstract-Fringe-Wallpapers-HD-Download-77829_l			0	2016-06-21 12:46:49 MSK	2016-06-21 12:46:49 MSK	2016-06-21 12:46:48 MSK	2016-06-21 12:46:49 MSK	742206	Allocated	Allocated
Abstract-Fringe-Wallpapers-HD-Download-77829_l			2	2016-06-21 12:46:49 MSK	2016-06-21 12:46:49 MSK	2016-06-21 12:46:48 MSK	2016-06-21 12:46:49 MSK	26	Allocated	Allocated
andrew_lincoln_the_walking_dead-2560x1440.jpg			1	2016-06-21 12:36:10 MSK	2016-06-21 02:52:11 MSK	2016-06-21 12:36:09 MSK	2016-06-21 12:36:09 MSK	1176500	Allocated	Allocated
andrew_lincoln_the_walking_dead-2560x1440.jpg:Z			2	2016-06-21 12:36:10 MSK	2016-06-21 02:52:11 MSK	2016-06-21 12:36:09 MSK	2016-06-21 12:36:09 MSK	26	Allocated	Allocated
Computer is ON now			1	2016-06-21 12:44:28 MSK	2016-06-21 12:44:28 MSK	2016-06-21 12:44:27 MSK	2016-06-21 12:44:28 MSK	95014	Allocated	Allocated

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

0° C C | 45% | Reset | Tags Menu

Activate Windows
Go to Settings to activate Windows.

- Inside the Recycle Bin I found two JPG files. One of them was actual corrupted JPG image which copy is still stored inside the Pictures/Private , while another file only has .jpg extension, but it some file with certificates and public RSA keys for Tor Browser as far as I got (from this [dir-key-certificate-version](#)).

lu-cf-lab-02 - Autopsy 4.22.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001

Data Sources case1.001_1 Host case1.001

- SOrphanFiles (52)
- SCarved Files (1)
- SEnter (8)
- \$Recycle.Bin (3)
 - S-1-5-21-2489440558-2754304563-710705792-1001
 - SRB1Q2G.jpg
- SUnalloc (7)
- Documents and Settings (2)
- MSCCache (3)
- PerfLogs (2)
- Program Files (30)
- Program Files (v86) (29)
- Python27 (16)
- System Volume Information (11)
- Users (8)
 - All Users (2)
 - Default (29)
 - Default User (2)
 - Hunter (37)
 - idlerc (3)
 - oracle_ir_usage (3)
 - zenmap (8)
 - AppData (5)
 - Application Data (2)
 - Contacts (3)
 - Cookies (2)
 - Desktop (15)
 - Documents (26)
 - Downloads (41)
 - Dropbox (17)
 - Favorites (5)
 - Google Drive (10)
 - Links (8)
 - Local Settings (2)
 - Music (3)
 - My Documents (2)
 - NetHood (2)
 - PrintHood (2)
 - Recent (2)
 - Saved Games (3)
 - Searches (6)
 - SendTo (2)
 - Start Menu (2)
 - Templates (2)
 - Tracing (3)

Table | Thumbnail | Summary | Save Table as CSV

Name	S	C	Location	O	Modified Time	Change Time	Access Time
[current folder]			/img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001/.		2016-06-21 15:04:20 MSK	2016-06-21 15:04:20 MSK	2016-06-21 15:04:20 MSK
[parent folder]			/img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001/..		2016-06-21 15:02:44 MSK	2016-06-21 15:02:44 MSK	2016-06-21 15:02:44 MSK
SRB1Q2G.jpg			/img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001/SRB1Q2G.jpg		2016-06-21 12:31:40 MSK	2016-06-21 15:04:15 MSK	2016-06-21 12:31:39
SRP3TBNW.jpg			/img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001/SRP3TBNW.jpg		2016-06-21 12:31:40 MSK	2016-06-21 15:04:15 MSK	2016-06-21 12:31:39
SRP3TBNW.jpg.Identifier			/img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001/SRP3TBNW.jpg.Identifier		2016-06-21 12:31:40 MSK	2016-06-21 15:04:15 MSK	2016-06-21 12:31:39
desktop.ini			/img_case1.001/\$Recycle.Bin/S-1-5-21-2489440558-2754304563-710705792-1001/desktop.ini		2016-06-21 12:31:40 MSK	2016-06-21 15:04:15 MSK	2016-06-21 12:31:39

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

String Extracted Text Translation

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

```

dir-key-certificate-version 3
fingerprint 14C131DFC5CF93646BE72FA1401C02A8DF2E8B4
dir-key-expire 2016-02-01 00:00:00
dir-key-expire 2016-07-01 00:00:00
dir-identity -key
-----BEGIN RSA PRIVATE KEY-----
MIIBIgCAYEAt7ZxwDRbfjYt9/9UsQ52+6cmHMr8VWh8GkLwbq3RzqjkULwQ2
R9mFv4F4RnqMcMKi62YrYA3fZL1afhT304cpyp/D3dpM8Qw/88fafFa!fP4Ld
0YjnF8cv45q20ndWnXb32IXsvsGSE2FrAyVOVNsak967LsgCtUnZ+KMfeW
1vh3Y9K40iflDwgvf3svwg63GmAT7vZmn77+/J5wKs1v1Gr7Wttf8ABH2taX
09/KGOX20Kh0f3mXfZ5mUO2d9NMrwk7d//Nyy6fApVV6kVPA097dg3bAsl
+CocCkgFjAAVwZdLckQTOpzQ2AH5mMWYxd0fVg17hJnn+ bTD2ExZphfczz
bN7zC9yfZ54dQub747PQg962uAstP37v1mPw14sIWLgY16ewYuS5bCxv
pNjIZLz-22_Z54dQub747PQg962uAstP37v1mPw14sIWLgY16ewYuS5bCxv
-----END RSA PRIVATE KEY-----
dir-signing-key
-----BEGIN RSA PUBLIC KEY-----
MIIBIgCAYEAtkP9gBd82zRzMEDh77wLCafQjPjNq4azKPK0v0vN2nryefNx
AbEJ7uVa7100rlmVa26505ZLjQtP2CVXBCEuAo0TVPk1VR1to+ a110Nb
+RdLLGKAkr8o3ja5jZ1EU3gTwg9y3WClwVu0205yv016nRvcLqPU0B1bx
8000000000000000000000000000000000000000000000000000000000000000
o7yGDUvC14cJLcUDB-f89f.../habtCIAhKvNab7d454BfrfAAc...-82/vy
o78paCmZHM1tL9x4LeKmep7u4t4MpcfSmBypl4/St<- RBB7tg9jZUWp49w
j2TERVEn3t3CsA6u/GCHIRr4wJWqlJSxqqEd732fQvz6114/sXfnyWY1u
1HATK-WFL2/Ig7tICH3J1+btMuJuh1bDb6pdyjIW86kOygDaSxmEu+1D
o-hWVv2m668AgMBAEAE
-----END RSA PUBLIC KEY-----
dir-key-crosscert
-----BEGIN ID SIGNATURE-----
ce09yw+VW5FO36khBwHkK+stwNWY10SSA05C7y2UBxf8Pic1U5t32S/Fs2vh

```

Activate Windows Go to Settings to activate Windows.

ws_Small_cute_kitty_1920x1200.jpg | /img_case1.001/Users/Hunter/Pictures/Private/ws_Sm... | 0 | 2016-06-21 12:31:12 MSK | 2016-06-21 02:52:07 MSK | 2016-06-21 12:31:09 MSK | 2016-06-21 12:31:09 MSK

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

0% C | 42% | Reset

Activate Windows Go to Settings to activate Windows.

- Also inside the user's folder I found .zenmap folder with Zenmap configuration from which I figured out that the version of Zenmap is 7.12 . He scanned only scanme.nmap.org for training purposes maybe. I found no traces that he tried to scan his organization's network. The recent scans are saved to C:\Users\Hunter\Desktop\nmapscan.xml . This triggered me to check Desktop folder.

iu-cf-lab-02 - Autopsy 4.2.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

8 Results

Listing /img_case1.001/Users/Hunter/zenmap

Table Thumbnail Summary Save Table as CSV

Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]			/img_case1.001/Users/Hunter/zenmap/.	2016-06-21 15:14:11 MSK	2016-06-21 15:14:11 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	56	Allocated	Allocated
[parent folder]			/img_case1.001/Users/Hunter/zenmap/..	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	0000-00-00 00:00:00	0000-00-00 00:00:00	256	Allocated	Allocated
recent_scans.txt		0	/img_case1.001/Users/Hunter/zenmap/recent_scans.txt	2016-06-21 15:13:57 MSK	2016-06-21 15:13:57 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	36	Allocated	Allocated
scan_profile.usp		0	/img_case1.001/Users/Hunter/zenmap/scan_profile.usp	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2018	Allocated	Allocated
target_list.txt		0	/img_case1.001/Users/Hunter/zenmap/target_list.txt	2016-06-21 15:10:42 MSK	2016-06-21 15:10:42 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	15	Allocated	Allocated
zenmap.conf		0	/img_case1.001/Users/Hunter/zenmap/zenmap.conf	2016-06-21 15:14:11 MSK	2016-06-21 15:14:11 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	1571	Allocated	Allocated
zenmap.db		0	/img_case1.001/Users/Hunter/zenmap/zenmap.db	2016-06-21 15:14:11 MSK	2016-06-21 15:14:11 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	27648	Allocated	Allocated
zenmap_version		1	/img_case1.001/Users/Hunter/zenmap/zenmap_version	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	5	Allocated	Allocated

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

Page: 1 of 1 Page Matches on page: - of - Match 100% ⌂ Reset Text Source: File Text

C:\Users\Hunter\Desktop\nmapscan.xml

-----METADATA-----

File	Path	Size	Flags(Dir)	Flags(Meta)					
zenmap.db	/img_case1.001/Users/Hunter/zenmap/zenmap.db	0	2016-06-21 15:14:11 MSK	2016-06-21 15:14:11 MSK	2016-06-21 15:14:11 MSK	27648	Allocated	Allocated	
zenmap_version	/img_case1.001/Users/Hunter/zenmap/zenmap_version	1	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	2016-06-21 15:08:14 MSK	5	Allocated	Allocated

- On the Desktop he had already had all the necessary links 😊

Listing /img_case1.001/Users/Hunter/Desktop

Table Thumbnail Summary Save Table as CSV

Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Last Seen
[current folder]			/img_case1.001/Users/Hunter/Desktop/	2016-06-21 15:13:57 MSK	2016-06-21 15:13:57 MSK	2016-06-21 11:37:46 MSK	2016-06-21 11:37:46 MSK	56	Allocated	Allocated	unknown	/d
[parent folder]			/img_case1.001/Users/Hunter/	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	0000-00-00 00:00:00	0000-00-00 00:00:00	256	Allocated	Allocated	unknown	/d
Tor Browser		1	/img_case1.001/Users/Hunter/Desktop/Tor Browser	2016-06-21 13:53:12 MSK	2016-06-21 13:53:12 MSK	2016-06-21 13:52:12 MSK	2016-06-21 13:52:12 MSK	384	Allocated	Allocated	unknown	/d
desktop.ini	1	0	/img_case1.001/Users/Hunter/Desktop/desktop.ini	2016-06-21 11:37:53 MSK	2016-06-21 11:37:53 MSK	2016-06-21 11:37:53 MSK	2016-06-21 11:37:53 MSK	282	Allocated	Allocated	unknown	/d
Dropbox.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/Dropbox.Ink	2016-06-21 04:50:12 MSK	2016-06-21 04:50:12 MSK	2016-06-21 04:50:12 MSK	2016-06-21 04:50:12 MSK	1242	Allocated	Allocated	unknown	/d
Google Drive.Ink	1	0	/img_case1.001/Users/Hunter/Desktop/Google Drive.Ink	2016-06-21 04:54:21 MSK	2016-06-21 04:54:21 MSK	2016-06-21 04:54:21 MSK	2016-06-21 04:54:21 MSK	1731	Allocated	Allocated	unknown	/d
Nmap - Zenmap GUI.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/Nmap - Zenmap GUI.Ink	2016-06-21 14:06:18 MSK	2016-06-21 14:06:18 MSK	2016-06-21 14:06:18 MSK	2016-06-21 14:06:18 MSK	975	Allocated	Allocated	unknown	/d
nmapscan.xml	0	0	/img_case1.001/Users/Hunter/Desktop/nmapscan.xml	2016-06-21 15:13:57 MSK	2016-06-21 16:05:19 MSK	2016-06-21 15:13:57 MSK	2016-06-21 15:13:57 MSK	13137	Allocated	Allocated	unknown	/d
OLLYDBG.EXE - Shortcut.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/OLLYDBG.EXE - Shortcut.Ink	2016-06-21 14:08:05 MSK	2016-06-21 14:08:05 MSK	2016-06-21 14:08:05 MSK	2016-06-21 14:08:05 MSK	1319	Allocated	Allocated	unknown	/d
pscp.exe - Shortcut.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/pscp.exe - Shortcut.Ink	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	1136	Allocated	Allocated	unknown	/d
putty.exe - Shortcut.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/putty.exe - Shortcut.Ink	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	1141	Allocated	Allocated	unknown	/d
Start Tor Browser.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/Start Tor Browser.Ink	2016-06-21 13:54:03 MSK	2016-06-21 13:54:03 MSK	2016-06-21 13:54:03 MSK	2016-06-21 13:54:03 MSK	797	Allocated	Allocated	unknown	/d
SystemInternalsSuite - Shortcut.Ink	0	0	/img_case1.001/Users/Hunter/Desktop/SystemInternalsSuite - Shortcut.Ink	2016-06-21 14:19:39 MSK	2016-06-21 14:19:39 MSK	2016-06-21 14:19:39 MSK	2016-06-21 14:19:39 MSK	1140	Allocated	Allocated	unknown	/d
Thumbs.db	0	0	/img_case1.001/Users/Hunter/Desktop/Thumbs.db	2016-06-21 15:08:08 MSK	2016-06-21 15:08:08 MSK	2016-06-21 14:19:39 MSK	2016-06-21 14:19:39 MSK	48640	Allocated	Allocated	unknown	/d
Thumbs.db:encryptable	0	0	/img_case1.001/Users/Hunter/Desktop/Thumbs.db:encryptable	2016-06-21 15:08:08 MSK	2016-06-21 15:08:08 MSK	2016-06-21 14:19:39 MSK	2016-06-21 14:19:39 MSK	0	Allocated	Allocated	unknown	/d

- And bingo! The file nmapscan.xml was there. I immediately marked it as highly notable as you can see 😊

nmapscan.xml		/img_case.1.001/Users/Hunter/Desktop/nmapscan.xml	0	2016-06-21 15:13:57 MSK	2016-06-21 16:05:19 MSK	2016-06-21 15:13:57 MSK	2016-06-21 15:13:57 MSK	13137	Allo
OLLYDBG.EXE - Shortcut.lnk		/img_case.1.001/Users/Hunter/Desktop/OLLYDBG.EXE ...	0	2016-06-21 14:08:05 MSK	2016-06-21 14:08:05 MSK	2016-06-21 14:08:05 MSK	2016-06-21 14:08:05 MSK	1319	Allo
psc.exe - Shortcut.lnk		/img_case.1.001/Users/Hunter/Desktop/psc.exe - Sho ...	0	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	2016-06-21 14:08:15 MSK	1136	Allo

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

Strings Extracted Text Translation

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

```
<?xml version="1.0" encoding="iso-8859-1"?>
<?xml-stylesheet href="file:///C:/Program Files (x86)/Nmap/nmap.xsl" type="text/xsl"?> <nmaprun start="1466511043" profile_name="" xmloutputversion="1.04" scanners="nmap" version="7.12" startstr="Tue Jun 21 21:05:10 2016" args="--nmap -T4 -A -v scanme.nmap.org"> <scaninfo services="1-3,4-6,7,9,13,17,19-26,30-32-33,37-42,43,49,53,70-79,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425-427,445,458,464-465,481,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141-1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198,1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971,1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2360,2388,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3353,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3765,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4002,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4446,4449,4549,4567,4662,4846,4849,4899,4900,5000-5004,5009,5030,5033,5035-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5511,5544,5550,5555,5560,5561,5633,5666,5678-5679,5718,5730,5800-5802,5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5998-5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6689,6699,6699,6779,6788,6792,6829,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7432,7449,7512,7625,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8089,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8338,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8904,9000-9003,9009-9011,9040,9050,9071,9080-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15020-15044,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20031,20221-20222,20282,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,4501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55505,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63311,64623,64690,65000,65129,65389> protocol="tcp" numservices="1000" type="syn">> <scaninfo><verbose level="1"></verbose><debugging level="0"></debugging><output type="interactive">
```

Starting Nmap 7.12 (<https://nmap.org>) at 2016-06-21 05:10 Pacific Daylight Time
NSE: Script pre-scanning.
Initiating NSE at 0:10
Completed NSE at 0:10, 0.08s elapsed
Initiating NSE at 0:10
Completed NSE at 0:10, 0.01s elapsed
Initiating Ping Scan at 0:10
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 0:10, 0.05s elapsed (1 total hosts)

Activate Windows
Go to Settings to activate Windows.

- To see it beautiful I used [Onine Nmap Viewer](#). We can see there which ports, protocols, and clients were available: OpenSSH, SMPT, RSFTP, Apache HTTP, Nping Echo, Ncat. Four of them were open (22, 80, 9929, 31337). There were 1000 ports scanned in total. However, GUI was not so detailed as XML, e.g. form XML file I also extracted the timestamp of performing this scan, again 2016-06-21 .

Nmap Viewer

Preview your [Nmap](#) files with a single drag n drop in a clean GUI with all the important information. This preview is running on your browser and [no information is ever transferred or stored](#).

Scan Info

Type	Protocol	Scanned
SYN	TCP	1000

Search hosts Export: HTML

Hosts

45.33.32.156 (scanme.nmap.org)

OS: QEMU QEMU IP: IPv4 OP: 4

Port	Scripts	Service	Version	Product
22	N	ssh	6.6.1p1 Ubuntu 2ubuntu2.7	OpenSSH
25	N	smtp		
26	N	rsftp		
80	N	http	2.4.7	Apache httpd
9929	N	nping-echo		Nping echo
31337	N	ncat-chat		Ncat chat

- <finished timestr="Tue Jun 21 05:12:09 2016" time="1466511129"></finished><hosts down="0" total="1" up="1"><c/hosts></runstats></nmaprun>
- Since I explored that BCWipe was actually used I thought that the user could use it for deleting files and applications also. So, I decided to check if BCWipe has logs about its actions. Unfortunately but not surprisingly there were no such information. However, BCWipe's directory contained exactly one [.log](#) file which purpose I haven't got: [UnInstall.log](#) file. Nevertheless, inside this file I also haven't found any interesting but the [Crypto Swap](#) which is a function of BCWipe that allows to encrypt Windows Swap file. I haven't found if Hunter actually used it, but we should take into account that he

The screenshot shows a forensic analysis interface with two main panes. The left pane displays a tree view of files and folders, including common system files like 'Program Files (x86)', 'Common Files', 'Dropbox', 'Google', 'Internet Explorer', 'Jetico', 'BCWipe', 'Shared', 'Shared64', 'McAfee', 'McAfee Security Scan', 'Microsoft Analysis Services', 'Microsoft Office', 'Microsoft SQL Server', 'Microsoft.NET', 'Nmap', 'Notepad+', 'Skype', 'TeamViewer', 'Windows Defender', 'Windows Mail', 'Windows Media Player', 'Windows Multimedia Platform', 'Windows NT', 'Windows Photo Viewer', 'Windows Portable Devices', 'Windows Sidebar', 'Windows PowerShell', 'WinPcap', 'Python27', 'System Volume Information', 'Users', and 'Windows'. The right pane shows a table of memory dump artifacts with columns for file name, timestamp, size, and status (Allocated or Unallocated). Below the table is a search bar and a text viewer showing log entries related to BCWipe.

Web history

- Analyzing files related to web browsers (Edge, Tor, Chrome), but haven't found anything really interesting, so he just visited all the sites of the tools we have already explored (Tor, FTK, BCWipe, etc.) to download them



Block Devices

- I haven't found anything interesting also in USB Devices that were attached to this device. Two of them were identified.

The screenshot shows the Autopsy 4.22.0 interface with a table titled 'USB Device Attached' listing two entries:

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM	0			2016-06-21 14:40:44 MSK	ROOT_HUB	4&65dfc83&0		case1.001
SYSTEM	0			2016-06-21 14:40:44 MSK	ROOT_HUB20	4&280d2b25&0		case1.001

Task 3 - Create a Forensics Report

Task description

Prepare a forensic report on the results of the investigation on behalf of the investigator. This should include a timestamp, evidence/artifact, proof (specify your action, tool, screenshot - if possible). Try to follow to the the generally accepted standards for the preparation of a report on forensics.

Example. However, it is not strict and mandatory to observe exactly such formatting.

- Since I did the report in a free format above I will not focus on much detail I have already mentioned because there a lot of findings as you can see. So, I will try to include the most important artifacts only:
 - Presence of attacking software
 - Conversation with `linux-rul3z` and important attachments
 - Port scanning results with Nmap

Innopolis University: Digital Forensics Report

- **Prepared by:** Iskander Nafikov
 - **Specialist field:** Digital Forensics
-

Tools

The forensic tools employed in the performance of this investigation were as follows:

- **Forensics analysis and collecting data** - AutoPsy 4.22.0
- Displaying the port scanning results - [Nmap Viewer](#)

Analysis

Key	Value	Found in
System	Windows 8.1 Enterprise	AutoPsy: OS Information
Owner's username	Hunter	AutoPsy: OS Accounts
PC Name	4ORENSICS	AutoPsy: OS Information
Timezone	Pacific Standard Time	/img_case1.001/Windows/System32/config/SYSTEM
IP address	10.0.2.15/25	/img_case1.001/Windows/System32/config/SYSTEM
Login count	3	AutoPsy: OS Accounts
Last login	2016-06-21 04:42:40 MSK	AutoPsy: OS Accounts

Key	Value
Artifact Name	E-mail conversation with linux-rul3z@hotmail.com
File name	ehptmsgs@gmail.com.ost
File path	/img_case1.001/Users/Hunter/AppData/Local/Microsoft/Outlook/ ehptmsgs@gmail.com.ost
Created timestamp	2016-06-21 16:07:07 MSK

Key	Value
Discovering	AutoPsy: Emails
Owner's mail	ehptmsgs@gmail.com
Useful Content	<p>The conversation provides the following information:</p> <ul style="list-style-type: none"> - Hunter connected with some guy who seems to understand something in attacks / penetration testing to teach him and help him to attack or pentest some network (probably of their organization but I am not sure yet). - Their dialogue established with a Hunter's message about TeamViewer which I suppose lets the other guy to access his device remotely. - They converse via E-mail and Skype. - In Skype there is some password that can help to unarchive some 7-zip attachments from Hunter with pictures. - The other guy sent to Hunter links on YouTube videos about Data Exfiltration and advices Hunter to disguise file using changing their extensions. So, Hunter uses this method and send him a PDF document with the JPG extension
Screenshot	<p>The screenshot shows the AutoPsy application interface. At the top, there are tabs for 'Table', 'Thumbnail', and 'Summary'. Below this is a table with columns: Source Name, S, C, O, E-Mail From, E-Mail To, Subject, Date Received, and Message (Plaintext). The table lists several emails between 'EH Techniques <ehptmsgs@gmail.com>' and 'linux-rul3z@hotmail.com'. The messages are mostly about TeamViewer installation and include attachments like 'backup.pst' and 'ehptmsgs@gmail.com.ost'. The 'Message (Plaintext)' column shows parts of the conversations, such as 'Hello there, I just wan' and 'Hello there, I just wan'. Below the table, there are tabs for Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. A message preview window is open, showing the full text of an email from 'EH Techniques <ehptmsgs@gmail.com>'. The message content includes a greeting, a request for continued discussion, and a signature. There is also a watermark for 'Activate Windows Go to Settings to activate Windows.'</p>

Key	Value
Artifact Name	Skype conversation with linux-rul3z@hotmail.com
File name	main.db
File path	/img_case1.001/Users/Hunter/AppData/Roaming/Skype/hunterehpt/main.db
Created timestamp	2016-06-21 12:08:36 MSK
Discovering	AutoPsy: Data source exploration

Key	Value																																																																																																																																																																																																																																																																																																																																																																																																																												
Owner's Skype login	hunterehtp																																																																																																																																																																																																																																																																																																																																																																																																																												
Useful Content	Hunter asks linux-rul3z to help him to transfer some pictures and documents outside an organization's network since it is monitored. This guys agreed to help him and asks if he is able to access Hunter's device remotely via TemViewer. Hunter downloaded TeamViewer and then their conversation goes to e-mail which we already saw.																																																																																																																																																																																																																																																																																																																																																																																																																												
Screenshot	<p>The screenshot shows two windows from a forensic analysis tool. The top window is a 'Listing' view of files in the directory 'AppData\Roaming\Skype\hunterehtp'. It includes columns for Name, S, C, Location, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The bottom window is a 'Messages' view showing a conversation between 'linux-rul3z' and 'hunterehtp'. The messages discuss sending pictures, bypassing censorship, and using TeamViewer.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>S</th> <th>C</th> <th>Location</th> <th>Modified Time</th> <th>Change Time</th> <th>Access Time</th> <th>Created Time</th> <th>Size</th> <th>Flags(Dir)</th> </tr> </thead> <tbody> <tr><td>uc.uu</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 12:08:30 MSK</td><td>2016-06-21 12:08:30 MSK</td><td>2016-06-21 12:08:36 MSK</td><td>2016-06-21 12:08:37 MSK</td><td>40900</td><td>Allocated</td></tr> <tr><td>eascache.db</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 04:43:08 MSK</td><td>2016-06-21 04:43:08 MSK</td><td>2016-06-21 04:43:08 MSK</td><td>2016-06-21 04:43:08 MSK</td><td>81920</td><td>Allocated</td></tr> <tr><td>eascache.db-journal</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 04:43:08 MSK</td><td>2016-06-21 04:43:08 MSK</td><td>2016-06-21 04:43:08 MSK</td><td>2016-06-21 04:43:08 MSK</td><td>33344</td><td>Allocated</td></tr> <tr><td>eascache.lock</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 04:43:02 MSK</td><td>2016-06-21 04:43:02 MSK</td><td>2016-06-21 04:43:02 MSK</td><td>2016-06-21 04:43:02 MSK</td><td>0</td><td>Allocated</td></tr> <tr><td>keyval.db</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 14:48:22 MSK</td><td>2016-06-21 14:48:22 MSK</td><td>2016-06-21 12:08:36 MSK</td><td>2016-06-21 12:08:36 MSK</td><td>36864</td><td>Allocated</td></tr> <tr><td>keyval.db-journal</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 14:48:22 MSK</td><td>2016-06-21 14:48:22 MSK</td><td>2016-06-21 05:04:43 MSK</td><td>2016-06-21 05:04:43 MSK</td><td>25136</td><td>Allocated</td></tr> <tr><td>keyval.lock</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 04:43:02 MSK</td><td>2016-06-21 04:43:02 MSK</td><td>2016-06-21 04:43:02 MSK</td><td>2016-06-21 04:43:02 MSK</td><td>0</td><td>Allocated</td></tr> <tr><td>main.db</td><td></td><td></td><td>/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0</td><td>2016-06-21 16:19:10 MSK</td><td>2016-06-21 16:19:10 MSK</td><td>2016-06-21 12:08:36 MSK</td><td>2016-06-21 12:08:36 MSK</td><td>638976</td><td>Allocated</td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>b...</th> <th>consum...</th> <th>edited_by</th> <th>edited_t...</th> <th>param_k...</th> <th>param_v...</th> <th>body_xml</th> <th>identities</th> <th>reason</th> <th>leavere...</th> <th>participa...</th> <th>error_code</th> <th>chatmsg</th> <th>chatm</th> </tr> </thead> <tbody> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>Hi Linux rul3z, I'd like to add you as a contact. I need your help with Data Exfiltration. ... linux-rul3z</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>hunterehtp</td><td></td><td></td><td></td><td></td><td></td><td>18</td><td>4</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>hello</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>hello</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>2</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>I have some pics that need to send outside my network</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>but the problem is that our network is monitored</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>2</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>I need to bypass their censorship</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>also I need to get access to documents and send them</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>2</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>so I am asking for your help</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>hmm</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>4</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>what kind of pics?</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>and what is the type of docs u need to send outside?</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>4</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>the pics are something special</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>some of the docs are for products</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>2</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>others are for other misc stuff</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>no worries</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>4</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>let us work on them separately</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>what do you mean?</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td>2</td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>I mean, let us first find away to access your device</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>and then, see what can we do in order to exfil the docs/pics outside ur network</td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>ok</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td></tr> <tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td>that sounds great</td><td></td><td></td><td></td><td></td><td></td><td>4</td><td></td></tr> </tbody> </table>	Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	uc.uu			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 12:08:30 MSK	2016-06-21 12:08:30 MSK	2016-06-21 12:08:36 MSK	2016-06-21 12:08:37 MSK	40900	Allocated	eascache.db			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	81920	Allocated	eascache.db-journal			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	33344	Allocated	eascache.lock			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	0	Allocated	keyval.db			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 14:48:22 MSK	2016-06-21 14:48:22 MSK	2016-06-21 12:08:36 MSK	2016-06-21 12:08:36 MSK	36864	Allocated	keyval.db-journal			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 14:48:22 MSK	2016-06-21 14:48:22 MSK	2016-06-21 05:04:43 MSK	2016-06-21 05:04:43 MSK	25136	Allocated	keyval.lock			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	0	Allocated	main.db			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 16:19:10 MSK	2016-06-21 16:19:10 MSK	2016-06-21 12:08:36 MSK	2016-06-21 12:08:36 MSK	638976	Allocated	b...	consum...	edited_by	edited_t...	param_k...	param_v...	body_xml	identities	reason	leavere...	participa...	error_code	chatmsg	chatm	0						Hi Linux rul3z, I'd like to add you as a contact. I need your help with Data Exfiltration. ... linux-rul3z						2		0						hunterehtp						18	4	0						hello						2		0						hello						3	2	0						I have some pics that need to send outside my network						2		0						but the problem is that our network is monitored						3	2	0						I need to bypass their censorship						2		0						also I need to get access to documents and send them						3	2	0						so I am asking for your help						2		0						hmm						3	4	0						what kind of pics?						2		0						and what is the type of docs u need to send outside?						3	4	0						the pics are something special						2		0						some of the docs are for products						3	2	0						others are for other misc stuff						2		0						no worries						3	4	0						let us work on them separately						2		0						what do you mean?						3	2	0						I mean, let us first find away to access your device						2		0						and then, see what can we do in order to exfil the docs/pics outside ur network						3		0						ok						2		0						that sounds great						4	
Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)																																																																																																																																																																																																																																																																																																																																																																																																																				
uc.uu			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 12:08:30 MSK	2016-06-21 12:08:30 MSK	2016-06-21 12:08:36 MSK	2016-06-21 12:08:37 MSK	40900	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
eascache.db			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	81920	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
eascache.db-journal			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	2016-06-21 04:43:08 MSK	33344	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
eascache.lock			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	0	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
keyval.db			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 14:48:22 MSK	2016-06-21 14:48:22 MSK	2016-06-21 12:08:36 MSK	2016-06-21 12:08:36 MSK	36864	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
keyval.db-journal			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 14:48:22 MSK	2016-06-21 14:48:22 MSK	2016-06-21 05:04:43 MSK	2016-06-21 05:04:43 MSK	25136	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
keyval.lock			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	2016-06-21 04:43:02 MSK	0	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
main.db			/img_case1.001/Users/Hunter/AppData/Roaming/Sky... 0	2016-06-21 16:19:10 MSK	2016-06-21 16:19:10 MSK	2016-06-21 12:08:36 MSK	2016-06-21 12:08:36 MSK	638976	Allocated																																																																																																																																																																																																																																																																																																																																																																																																																				
b...	consum...	edited_by	edited_t...	param_k...	param_v...	body_xml	identities	reason	leavere...	participa...	error_code	chatmsg	chatm																																																																																																																																																																																																																																																																																																																																																																																																																
0						Hi Linux rul3z, I'd like to add you as a contact. I need your help with Data Exfiltration. ... linux-rul3z						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						hunterehtp						18	4																																																																																																																																																																																																																																																																																																																																																																																																																
0						hello						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						hello						3	2																																																																																																																																																																																																																																																																																																																																																																																																																
0						I have some pics that need to send outside my network						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						but the problem is that our network is monitored						3	2																																																																																																																																																																																																																																																																																																																																																																																																																
0						I need to bypass their censorship						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						also I need to get access to documents and send them						3	2																																																																																																																																																																																																																																																																																																																																																																																																																
0						so I am asking for your help						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						hmm						3	4																																																																																																																																																																																																																																																																																																																																																																																																																
0						what kind of pics?						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						and what is the type of docs u need to send outside?						3	4																																																																																																																																																																																																																																																																																																																																																																																																																
0						the pics are something special						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						some of the docs are for products						3	2																																																																																																																																																																																																																																																																																																																																																																																																																
0						others are for other misc stuff						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						no worries						3	4																																																																																																																																																																																																																																																																																																																																																																																																																
0						let us work on them separately						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						what do you mean?						3	2																																																																																																																																																																																																																																																																																																																																																																																																																
0						I mean, let us first find away to access your device						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						and then, see what can we do in order to exfil the docs/pics outside ur network						3																																																																																																																																																																																																																																																																																																																																																																																																																	
0						ok						2																																																																																																																																																																																																																																																																																																																																																																																																																	
0						that sounds great						4																																																																																																																																																																																																																																																																																																																																																																																																																	

Key	Value
Artifact Name	Data exfiltration instructions
Folder name	Documents
Folder path	/img_case1.001/Users/Hunter/Documents
Created timestamp	2016-06-21 11:37:46 MSK
Discovering	AutoPsy: Data source exploration
Useful Content	5 PDF documents that provide instructions on performing data exfiltration or firewall bypassing

Key	Value																																																																																																																																																																																																																																				
Screenshot	<p>Listing /img_case1.001/Users/Hunter/Documents Table Thumbnail Summary Save Table as CSV</p> <table border="1"> <thead> <tr> <th>Name</th> <th>S</th> <th>C</th> <th>Location</th> <th>Modified Time</th> <th>Change Time</th> <th>Access Time</th> <th>Created Time</th> </tr> </thead> <tbody> <tr><td>defcon-16-ricks.pdf</td><td>Zone.Identifier</td><td></td><td>/img_case1.001/Users/Hunter/Documents/defcon-16..._2</td><td>2016-06-21 12:40:46 MSK</td><td>2016-06-21 12:40:46 MSK</td><td>2016-06-21 12:40:46 MSK</td><td>2016-06-21 12:40:46 MSK</td></tr> <tr><td>DEFCON-22-Zoltan-Balazs-Bypass-firewalls-appla...</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/DEFCON-2..._2</td><td>2016-06-21 02:58:09 MSK</td><td>2016-06-21 02:58:09 MSK</td><td>2016-06-21 02:58:08 MSK</td><td>2016-06-21 02:58:08 MSK</td></tr> <tr><td>how_to_threat_actors_stole_your_data.pdf</td><td>Zone.Identifier</td><td></td><td>/img_case1.001/Users/Hunter/Documents/how_to_th..._2</td><td>2016-06-21 12:39:47 MSK</td><td>2016-06-21 02:49:39 MSK</td><td>2016-06-21 12:39:39 MSK</td><td>2016-06-21 12:39:46 MSK</td></tr> <tr><td>mwni-detecting-deterring-both.pdf</td><td>Zone.Identifier</td><td></td><td>/img_case1.001/Users/Hunter/Documents/mwni-dete..._2</td><td>2016-06-21 12:40:22 MSK</td><td>2016-06-21 12:40:22 MSK</td><td>2016-06-21 12:40:20 MSK</td><td>2016-06-21 12:40:22 MSK</td></tr> <tr><td>Ryan_VanAntwerp_thesis.pdf</td><td>Zone.Identifier</td><td></td><td>/img_case1.001/Users/Hunter/Documents/Ryan_VanA..._2</td><td>2016-06-21 12:40:07 MSK</td><td>2016-06-21 12:40:07 MSK</td><td>2016-06-21 12:40:05 MSK</td><td>2016-06-21 12:40:07 MSK</td></tr> <tr><td>Accounts.txt</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Accounts.txt</td><td>1</td><td>2016-06-21 04:46:16 MSK</td><td>2016-06-21 04:46:16 MSK</td><td>2016-06-21 12:20:52 MSK</td><td>2016-06-21 12:20:52 MSK</td></tr> <tr><td>Conf.jpg</td><td></td><td>V</td><td>/img_case1.001/Users/Hunter/Documents/Conf.jpg</td><td>1</td><td>2016-06-21 04:59:27 MSK</td><td>2016-06-21 05:00:47 MSK</td><td>2016-06-21 05:00:10 MSK</td><td>2016-06-21 05:00:10 MSK</td></tr> <tr><td>Confidential Document.pdf</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Confidenti..._1</td><td>2016-06-21 04:59:27 MSK</td><td>2016-06-21 04:59:27 MSK</td><td>2016-06-21 04:59:27 MSK</td><td>2016-06-21 04:59:05 MSK</td><td>2016-06-21 04:59:05 MSK</td></tr> <tr><td>defcon-16-ricks.pdf</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/defcon-16..._1</td><td>2016-06-21 12:40:46 MSK</td><td>2016-06-21 12:40:45 MSK</td><td>2016-06-21 12:40:46 MSK</td><td>2016-06-21 12:40:46 MSK</td><td>2016-06-21 12:40:46 MSK</td></tr> <tr><td>DEFCON-22-Zoltan-Balazs-Bypass-firewalls-appla...</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/DEFCON-2..._1</td><td>2016-06-21 02:58:09 MSK</td><td>2016-06-21 02:58:08 MSK</td><td>2016-06-21 02:58:08 MSK</td><td>2016-06-21 02:58:08 MSK</td><td>2016-06-21 02:58:08 MSK</td></tr> <tr><td>desktop.ini</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/desktop.ini</td><td>1</td><td>2016-06-21 11:37:53 MSK</td><td>2016-06-21 11:37:53 MSK</td><td>2016-06-21 11:37:53 MSK</td><td>2016-06-21 11:37:53 MSK</td><td>2016-06-21 11:37:53 MSK</td></tr> <tr><td>how_to_threat_actors_stole_your_data.pdf</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/how_to_th..._1</td><td>2016-06-21 12:39:47 MSK</td><td>2016-06-21 02:49:39 MSK</td><td>2016-06-21 12:39:39 MSK</td><td>2016-06-21 12:39:46 MSK</td><td>2016-06-21 12:39:46 MSK</td></tr> <tr><td>Ryan_VanAntwerp_thesis.pdf</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Ryan_VanA..._1</td><td>2016-06-21 12:40:07 MSK</td><td>2016-06-21 12:40:07 MSK</td><td>2016-06-21 12:40:05 MSK</td><td>2016-06-21 12:40:07 MSK</td><td>2016-06-21 12:40:07 MSK</td></tr> <tr><td>tools.txt</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/tools.txt</td><td>1</td><td>2016-06-21 12:21:53 MSK</td><td>2016-06-21 12:21:53 MSK</td><td>2016-06-21 12:18:58 MSK</td><td>2016-06-21 12:18:58 MSK</td></tr> <tr><td>Confidential Document.docx</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Confidenti..._0</td><td>2016-06-21 04:59:20 MSK</td><td>2016-06-21 04:59:20 MSK</td><td>2016-06-21 04:59:20 MSK</td><td>2016-06-21 04:58:56 MSK</td><td>2016-06-21 04:58:56 MSK</td></tr> <tr><td>mwni-detecting-deterring-both.pdf</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/mwni-dete..._0</td><td>2016-06-21 12:40:22 MSK</td><td>2016-06-21 12:40:22 MSK</td><td>2016-06-21 12:40:20 MSK</td><td>2016-06-21 12:40:22 MSK</td><td>2016-06-21 12:40:22 MSK</td></tr> <tr><td>Thumbs.db</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Thumbs.db</td><td>0</td><td>2016-06-21 15:19:27 MSK</td><td>2016-06-21 15:19:27 MSK</td><td>2016-06-21 15:19:27 MSK</td><td>2016-06-21 15:19:27 MSK</td><td>2016-06-21 15:19:27 MSK</td></tr> <tr><td>Welcome.docx</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Welcome.._0</td><td>2016-06-21 15:27:46 MSK</td><td>2016-06-21 15:27:46 MSK</td><td>2016-06-21 15:27:46 MSK</td><td>2016-06-21 15:27:37 MSK</td><td>2016-06-21 15:27:37 MSK</td><td>2016-06-21 15:27:37 MSK</td></tr> <tr><td>[current folder]</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/...</td><td>2016-06-21 16:13:40 MSK</td><td>2016-06-21 16:13:40 MSK</td><td>2016-06-21 16:13:40 MSK</td><td>2016-06-21 16:13:40 MSK</td><td>2016-06-21 16:13:40 MSK</td><td>2016-06-21 16:13:40 MSK</td></tr> <tr><td>[parent folder]</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/..</td><td>2016-06-21 15:26:19 MSK</td><td>2016-06-21 15:26:19 MSK</td><td>2016-06-21 15:26:19 MSK</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td></tr> <tr><td>Custom Office Templates</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/Custom Of...</td><td>2016-06-21 04:58:52 MSK</td><td>2016-06-21 04:58:52 MSK</td><td>2016-06-21 04:58:52 MSK</td><td>2016-06-21 04:58:52 MSK</td><td>2016-06-21 04:58:52 MSK</td><td>2016-06-21 04:58:52 MSK</td></tr> <tr><td>My Music</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/My Music</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td></tr> <tr><td>My Pictures</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/My Pictures</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td></tr> <tr><td>My Videos</td><td></td><td></td><td>/img_case1.001/Users/Hunter/Documents/My Videos</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td><td>2016-06-21 11:37:46 MSK</td></tr> </tbody> </table>	Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time	defcon-16-ricks.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/defcon-16..._2	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	DEFCON-22-Zoltan-Balazs-Bypass-firewalls-appla...			/img_case1.001/Users/Hunter/Documents/DEFCON-2..._2	2016-06-21 02:58:09 MSK	2016-06-21 02:58:09 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK	how_to_threat_actors_stole_your_data.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/how_to_th..._2	2016-06-21 12:39:47 MSK	2016-06-21 02:49:39 MSK	2016-06-21 12:39:39 MSK	2016-06-21 12:39:46 MSK	mwni-detecting-deterring-both.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/mwni-dete..._2	2016-06-21 12:40:22 MSK	2016-06-21 12:40:22 MSK	2016-06-21 12:40:20 MSK	2016-06-21 12:40:22 MSK	Ryan_VanAntwerp_thesis.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/Ryan_VanA..._2	2016-06-21 12:40:07 MSK	2016-06-21 12:40:07 MSK	2016-06-21 12:40:05 MSK	2016-06-21 12:40:07 MSK	Accounts.txt			/img_case1.001/Users/Hunter/Documents/Accounts.txt	1	2016-06-21 04:46:16 MSK	2016-06-21 04:46:16 MSK	2016-06-21 12:20:52 MSK	2016-06-21 12:20:52 MSK	Conf.jpg		V	/img_case1.001/Users/Hunter/Documents/Conf.jpg	1	2016-06-21 04:59:27 MSK	2016-06-21 05:00:47 MSK	2016-06-21 05:00:10 MSK	2016-06-21 05:00:10 MSK	Confidential Document.pdf			/img_case1.001/Users/Hunter/Documents/Confidenti..._1	2016-06-21 04:59:27 MSK	2016-06-21 04:59:27 MSK	2016-06-21 04:59:27 MSK	2016-06-21 04:59:05 MSK	2016-06-21 04:59:05 MSK	defcon-16-ricks.pdf			/img_case1.001/Users/Hunter/Documents/defcon-16..._1	2016-06-21 12:40:46 MSK	2016-06-21 12:40:45 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	DEFCON-22-Zoltan-Balazs-Bypass-firewalls-appla...			/img_case1.001/Users/Hunter/Documents/DEFCON-2..._1	2016-06-21 02:58:09 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK	desktop.ini			/img_case1.001/Users/Hunter/Documents/desktop.ini	1	2016-06-21 11:37:53 MSK	how_to_threat_actors_stole_your_data.pdf			/img_case1.001/Users/Hunter/Documents/how_to_th..._1	2016-06-21 12:39:47 MSK	2016-06-21 02:49:39 MSK	2016-06-21 12:39:39 MSK	2016-06-21 12:39:46 MSK	2016-06-21 12:39:46 MSK	Ryan_VanAntwerp_thesis.pdf			/img_case1.001/Users/Hunter/Documents/Ryan_VanA..._1	2016-06-21 12:40:07 MSK	2016-06-21 12:40:07 MSK	2016-06-21 12:40:05 MSK	2016-06-21 12:40:07 MSK	2016-06-21 12:40:07 MSK	tools.txt			/img_case1.001/Users/Hunter/Documents/tools.txt	1	2016-06-21 12:21:53 MSK	2016-06-21 12:21:53 MSK	2016-06-21 12:18:58 MSK	2016-06-21 12:18:58 MSK	Confidential Document.docx			/img_case1.001/Users/Hunter/Documents/Confidenti..._0	2016-06-21 04:59:20 MSK	2016-06-21 04:59:20 MSK	2016-06-21 04:59:20 MSK	2016-06-21 04:58:56 MSK	2016-06-21 04:58:56 MSK	mwni-detecting-deterring-both.pdf			/img_case1.001/Users/Hunter/Documents/mwni-dete..._0	2016-06-21 12:40:22 MSK	2016-06-21 12:40:22 MSK	2016-06-21 12:40:20 MSK	2016-06-21 12:40:22 MSK	2016-06-21 12:40:22 MSK	Thumbs.db			/img_case1.001/Users/Hunter/Documents/Thumbs.db	0	2016-06-21 15:19:27 MSK	Welcome.docx			/img_case1.001/Users/Hunter/Documents/Welcome.._0	2016-06-21 15:27:46 MSK	2016-06-21 15:27:46 MSK	2016-06-21 15:27:46 MSK	2016-06-21 15:27:37 MSK	2016-06-21 15:27:37 MSK	2016-06-21 15:27:37 MSK	[current folder]			/img_case1.001/Users/Hunter/Documents/...	2016-06-21 16:13:40 MSK	[parent folder]			/img_case1.001/Users/Hunter/Documents/..	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	Custom Office Templates			/img_case1.001/Users/Hunter/Documents/Custom Of...	2016-06-21 04:58:52 MSK	My Music			/img_case1.001/Users/Hunter/Documents/My Music	2016-06-21 11:37:46 MSK	My Pictures			/img_case1.001/Users/Hunter/Documents/My Pictures	2016-06-21 11:37:46 MSK	My Videos			/img_case1.001/Users/Hunter/Documents/My Videos	2016-06-21 11:37:46 MSK																																	
Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time																																																																																																																																																																																																																														
defcon-16-ricks.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/defcon-16..._2	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK																																																																																																																																																																																																																														
DEFCON-22-Zoltan-Balazs-Bypass-firewalls-appla...			/img_case1.001/Users/Hunter/Documents/DEFCON-2..._2	2016-06-21 02:58:09 MSK	2016-06-21 02:58:09 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK																																																																																																																																																																																																																														
how_to_threat_actors_stole_your_data.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/how_to_th..._2	2016-06-21 12:39:47 MSK	2016-06-21 02:49:39 MSK	2016-06-21 12:39:39 MSK	2016-06-21 12:39:46 MSK																																																																																																																																																																																																																														
mwni-detecting-deterring-both.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/mwni-dete..._2	2016-06-21 12:40:22 MSK	2016-06-21 12:40:22 MSK	2016-06-21 12:40:20 MSK	2016-06-21 12:40:22 MSK																																																																																																																																																																																																																														
Ryan_VanAntwerp_thesis.pdf	Zone.Identifier		/img_case1.001/Users/Hunter/Documents/Ryan_VanA..._2	2016-06-21 12:40:07 MSK	2016-06-21 12:40:07 MSK	2016-06-21 12:40:05 MSK	2016-06-21 12:40:07 MSK																																																																																																																																																																																																																														
Accounts.txt			/img_case1.001/Users/Hunter/Documents/Accounts.txt	1	2016-06-21 04:46:16 MSK	2016-06-21 04:46:16 MSK	2016-06-21 12:20:52 MSK	2016-06-21 12:20:52 MSK																																																																																																																																																																																																																													
Conf.jpg		V	/img_case1.001/Users/Hunter/Documents/Conf.jpg	1	2016-06-21 04:59:27 MSK	2016-06-21 05:00:47 MSK	2016-06-21 05:00:10 MSK	2016-06-21 05:00:10 MSK																																																																																																																																																																																																																													
Confidential Document.pdf			/img_case1.001/Users/Hunter/Documents/Confidenti..._1	2016-06-21 04:59:27 MSK	2016-06-21 04:59:27 MSK	2016-06-21 04:59:27 MSK	2016-06-21 04:59:05 MSK	2016-06-21 04:59:05 MSK																																																																																																																																																																																																																													
defcon-16-ricks.pdf			/img_case1.001/Users/Hunter/Documents/defcon-16..._1	2016-06-21 12:40:46 MSK	2016-06-21 12:40:45 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK	2016-06-21 12:40:46 MSK																																																																																																																																																																																																																													
DEFCON-22-Zoltan-Balazs-Bypass-firewalls-appla...			/img_case1.001/Users/Hunter/Documents/DEFCON-2..._1	2016-06-21 02:58:09 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK	2016-06-21 02:58:08 MSK																																																																																																																																																																																																																													
desktop.ini			/img_case1.001/Users/Hunter/Documents/desktop.ini	1	2016-06-21 11:37:53 MSK																																																																																																																																																																																																																																
how_to_threat_actors_stole_your_data.pdf			/img_case1.001/Users/Hunter/Documents/how_to_th..._1	2016-06-21 12:39:47 MSK	2016-06-21 02:49:39 MSK	2016-06-21 12:39:39 MSK	2016-06-21 12:39:46 MSK	2016-06-21 12:39:46 MSK																																																																																																																																																																																																																													
Ryan_VanAntwerp_thesis.pdf			/img_case1.001/Users/Hunter/Documents/Ryan_VanA..._1	2016-06-21 12:40:07 MSK	2016-06-21 12:40:07 MSK	2016-06-21 12:40:05 MSK	2016-06-21 12:40:07 MSK	2016-06-21 12:40:07 MSK																																																																																																																																																																																																																													
tools.txt			/img_case1.001/Users/Hunter/Documents/tools.txt	1	2016-06-21 12:21:53 MSK	2016-06-21 12:21:53 MSK	2016-06-21 12:18:58 MSK	2016-06-21 12:18:58 MSK																																																																																																																																																																																																																													
Confidential Document.docx			/img_case1.001/Users/Hunter/Documents/Confidenti..._0	2016-06-21 04:59:20 MSK	2016-06-21 04:59:20 MSK	2016-06-21 04:59:20 MSK	2016-06-21 04:58:56 MSK	2016-06-21 04:58:56 MSK																																																																																																																																																																																																																													
mwni-detecting-deterring-both.pdf			/img_case1.001/Users/Hunter/Documents/mwni-dete..._0	2016-06-21 12:40:22 MSK	2016-06-21 12:40:22 MSK	2016-06-21 12:40:20 MSK	2016-06-21 12:40:22 MSK	2016-06-21 12:40:22 MSK																																																																																																																																																																																																																													
Thumbs.db			/img_case1.001/Users/Hunter/Documents/Thumbs.db	0	2016-06-21 15:19:27 MSK																																																																																																																																																																																																																																
Welcome.docx			/img_case1.001/Users/Hunter/Documents/Welcome.._0	2016-06-21 15:27:46 MSK	2016-06-21 15:27:46 MSK	2016-06-21 15:27:46 MSK	2016-06-21 15:27:37 MSK	2016-06-21 15:27:37 MSK	2016-06-21 15:27:37 MSK																																																																																																																																																																																																																												
[current folder]			/img_case1.001/Users/Hunter/Documents/...	2016-06-21 16:13:40 MSK																																																																																																																																																																																																																																	
[parent folder]			/img_case1.001/Users/Hunter/Documents/..	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	2016-06-21 15:26:19 MSK	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00																																																																																																																																																																																																																												
Custom Office Templates			/img_case1.001/Users/Hunter/Documents/Custom Of...	2016-06-21 04:58:52 MSK																																																																																																																																																																																																																																	
My Music			/img_case1.001/Users/Hunter/Documents/My Music	2016-06-21 11:37:46 MSK																																																																																																																																																																																																																																	
My Pictures			/img_case1.001/Users/Hunter/Documents/My Pictures	2016-06-21 11:37:46 MSK																																																																																																																																																																																																																																	
My Videos			/img_case1.001/Users/Hunter/Documents/My Videos	2016-06-21 11:37:46 MSK																																																																																																																																																																																																																																	

Key	Value
Artifact Name	Attacking or suspicious software
Folder name	Downloads
Folder path	/img_case1.001/Users/Hunter/Downloads
Created timestamp	2016-06-21 11:37:46 MSK
Discovering	AutoPsy: Data source exploration
Useful Content	<p>Installers or executables of the following tools:</p> <ul style="list-style-type: none"> - Hash Suite Free - BurpSuite - Eraser - Putty - PSCP - SetupSSH - SysinternalSuite - Zenmap - Tor Browser - Wireshark - Skype - TeamViewer - BCWipe - Notepad++

Key	Value
Screenshot	

Key	Value
Artifact Name	Port scanning results
File name	nmapscan.xml
File path	/img_case1.001/Users/Hunter/Desktop/nmapscan.xml
Created timestamp	2016-06-21 15:13:57 MSK
Scan target	scanme.nmap.org (45.33.32.156)
Discovering	AutoPsy: Data source exploration
Useful Content	Hunter used Zenmap actually to make port scanning, but for training purposes only on the website: scanme.nmap.org
Screenshot	

Opinion based on findings

Summing up all the artifacts found, I can summarize that Hunter tried to upload pictures and documents containing the organization's documentation, despite the fact that this is prohibited. He spent some time studying data exfiltration, hacking, firewall bypassing techniques and consulted with an outsider via E-mail and Skype. There is reason to believe that he is not an expert in this field, so he resorted to numerous training materials and consultations. Unfortunately, it is not known for sure whether Hunter achieved the desired result, but since this image ended up in my hands, it was probably quickly detected when trying to perform data exfiltration using constant network monitoring. Nevertheless, he definitely had the intention to steal the organization's data.