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 Абдельраззак	Ahmed Shaaban Abdelrazzak	Nouralla	nginx-st14
15	Нафиков Искандер Маратович	Iskander	Nafikov	nginx-st15
16	Окоре Джоэль Чидике	Joel Chidike	Okore	nginx-st16

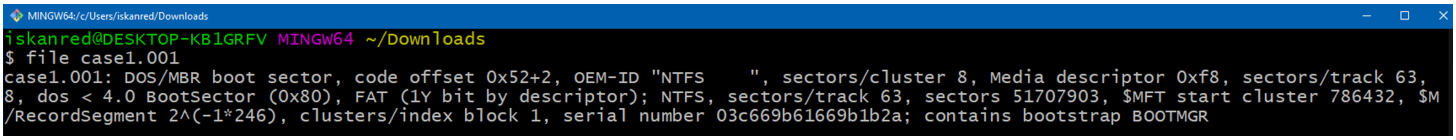
Task 2 - Black box Forensics analysis

> **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

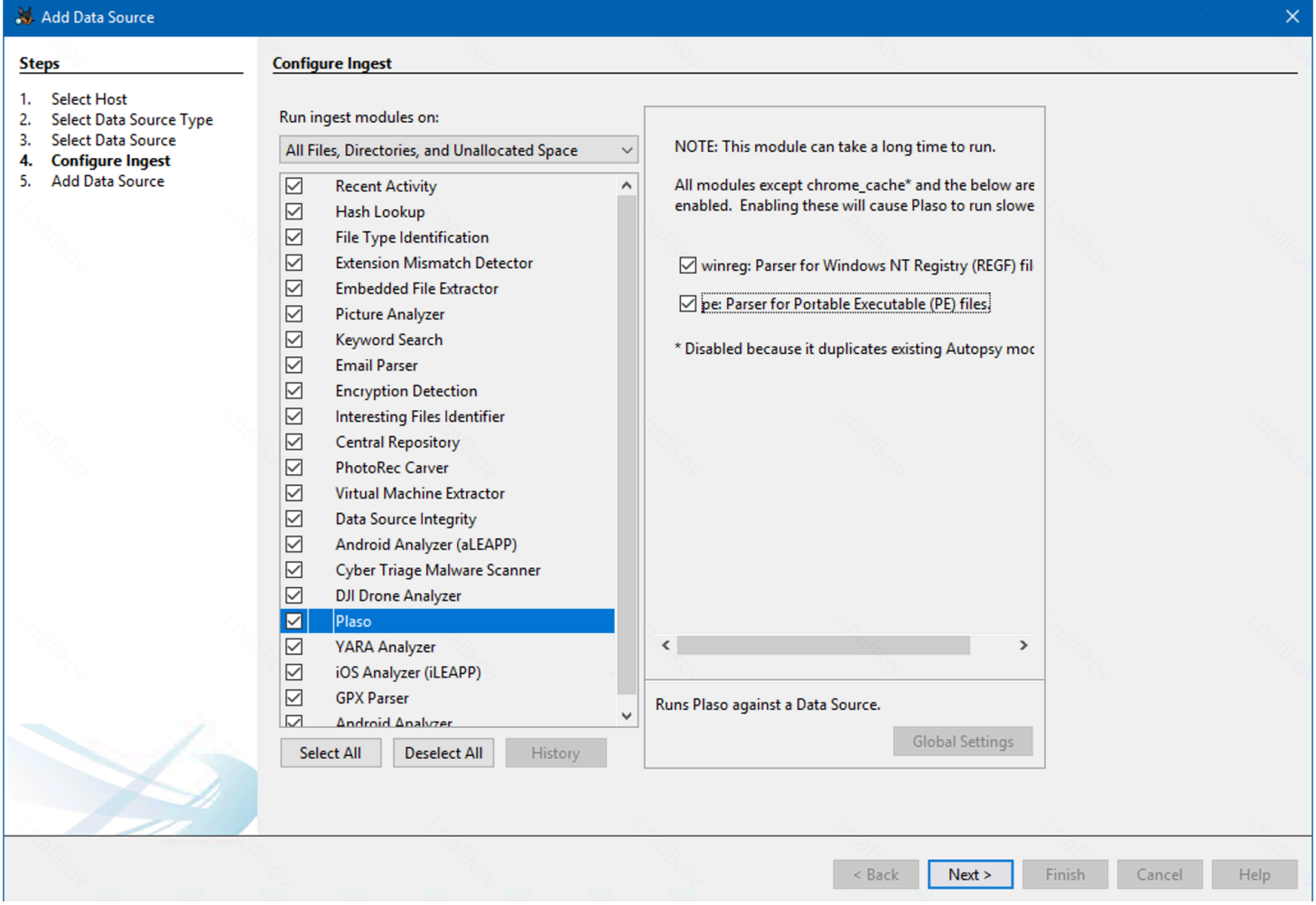
- First, I ran `file` command on my Windows machine using MinGW to investigate what type of file I received



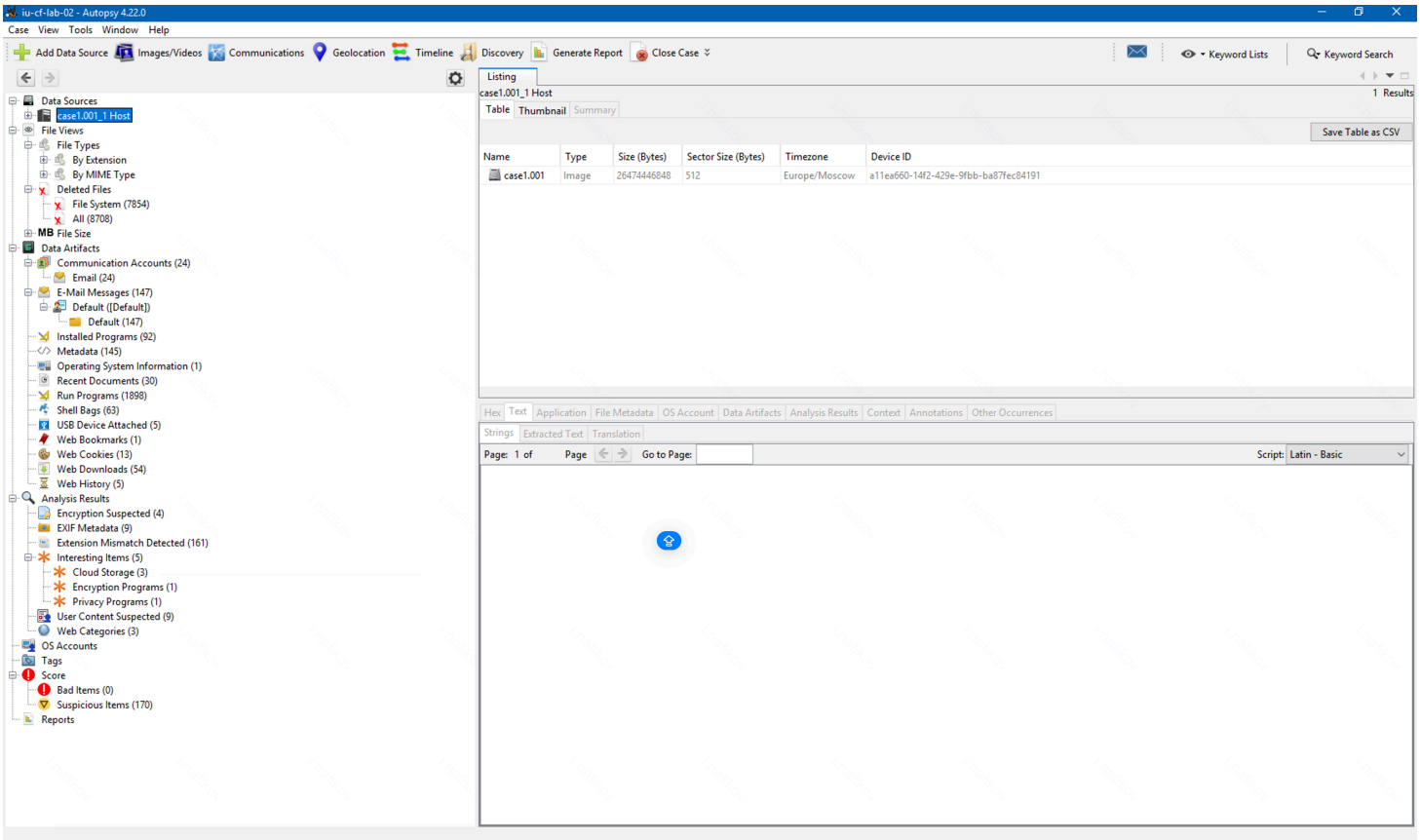
- Here we can see that this is actually some Windows OS image because it contains:
  - NTFS filesystem
  - DOS/MBR boot sector with 1.5Gb of size
  - BOOTMGR which used starting from Windows Vista or Windows Server 2008

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`)



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

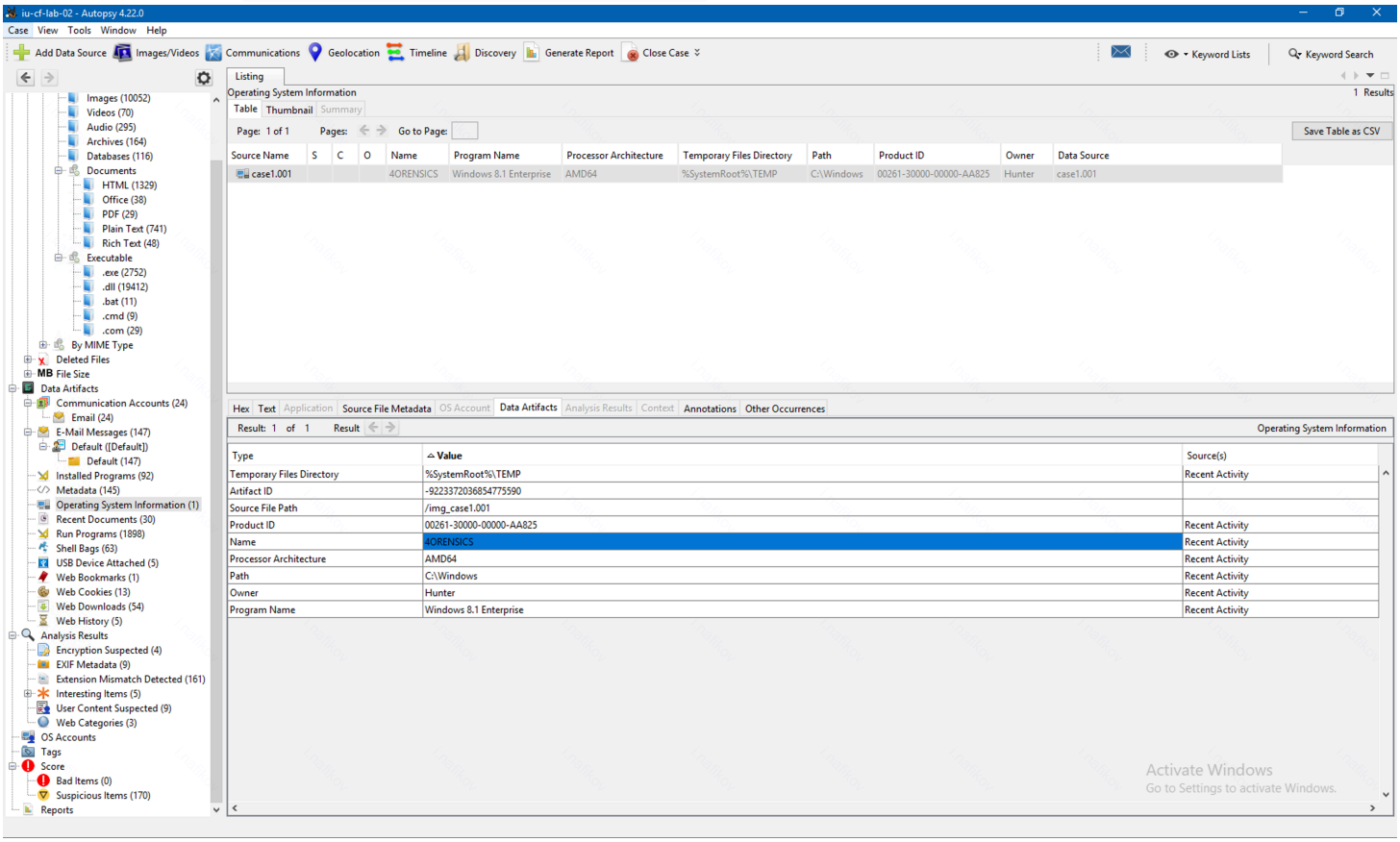


Investigation

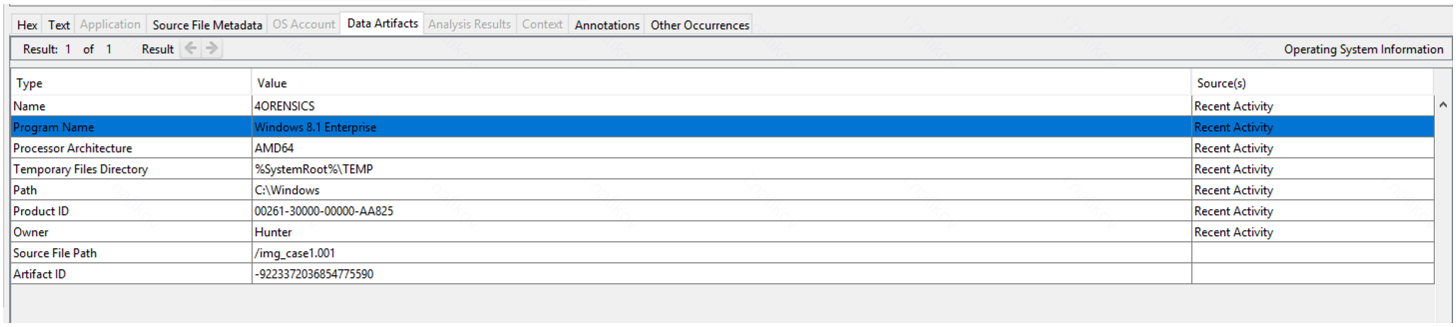
Basic system information & Timeline

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

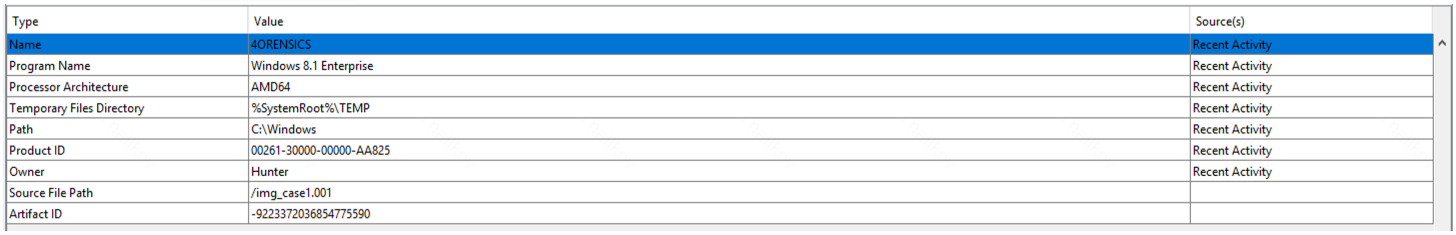
- From the section `Operating System Information` we can extract a lot of useful information



- **OS version** = `Windows 8.1 Enterprise`



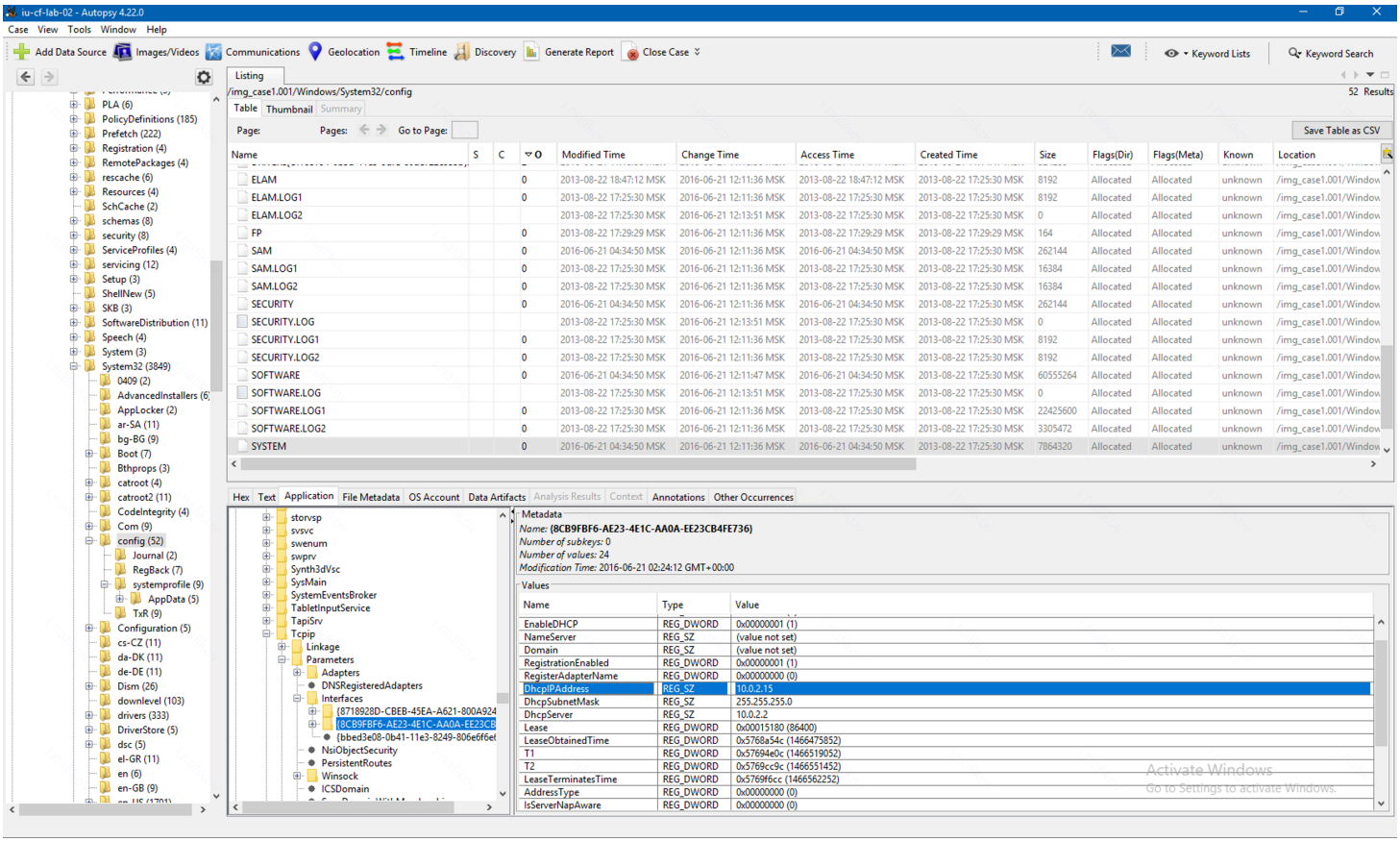
- **Hostname** = `4ORENSICS`



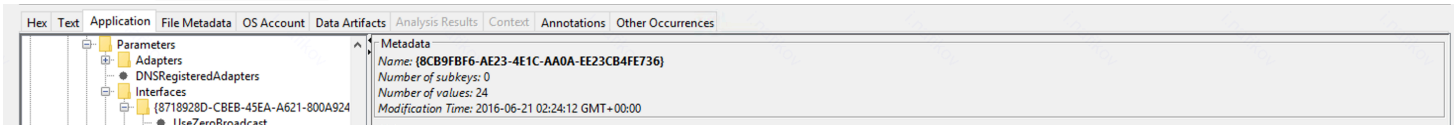
- **Owner's username =** `hunter`

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.

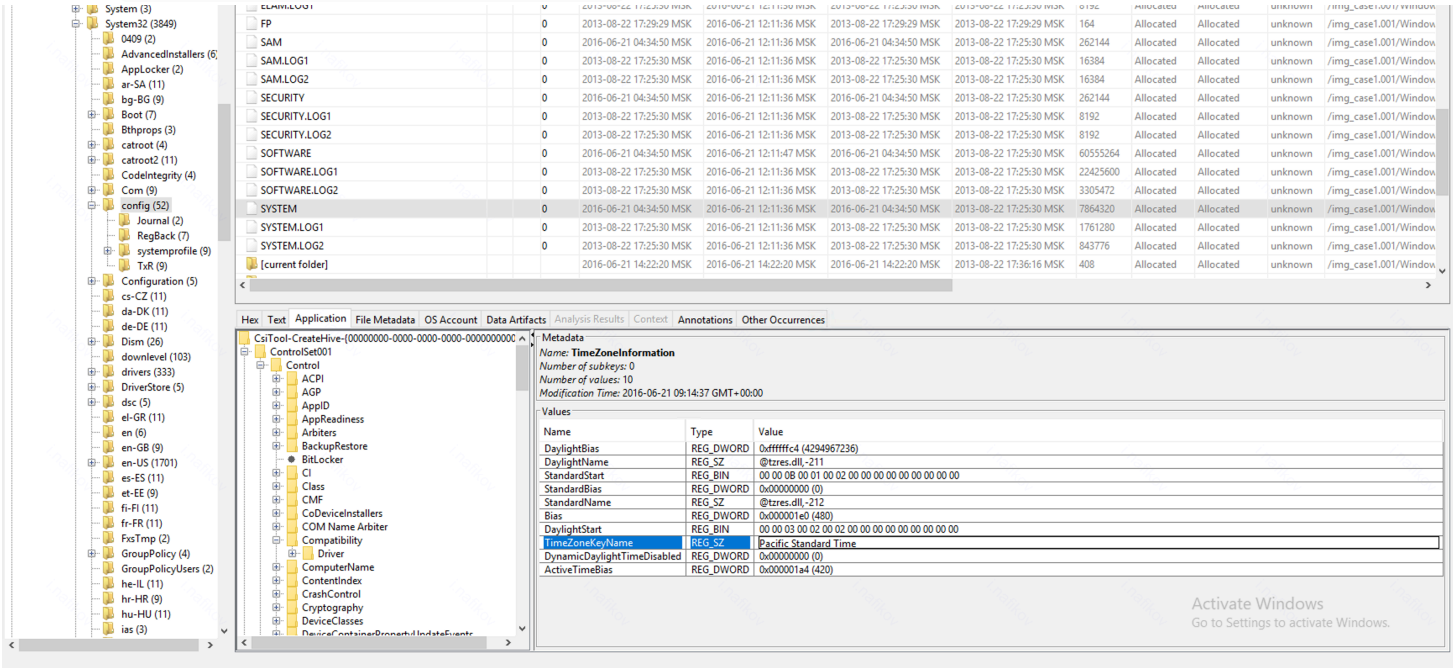


- In addition, using this metadata section we see this registry part modification time from which we can infer that the last time the the IP address was assigned to this interface using DHCP was `2016-06-21 02:23:12 GMT+00:00` or `2016-06-20 04:23:12 GMT+03:00` which is quite late, so let's try to determine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

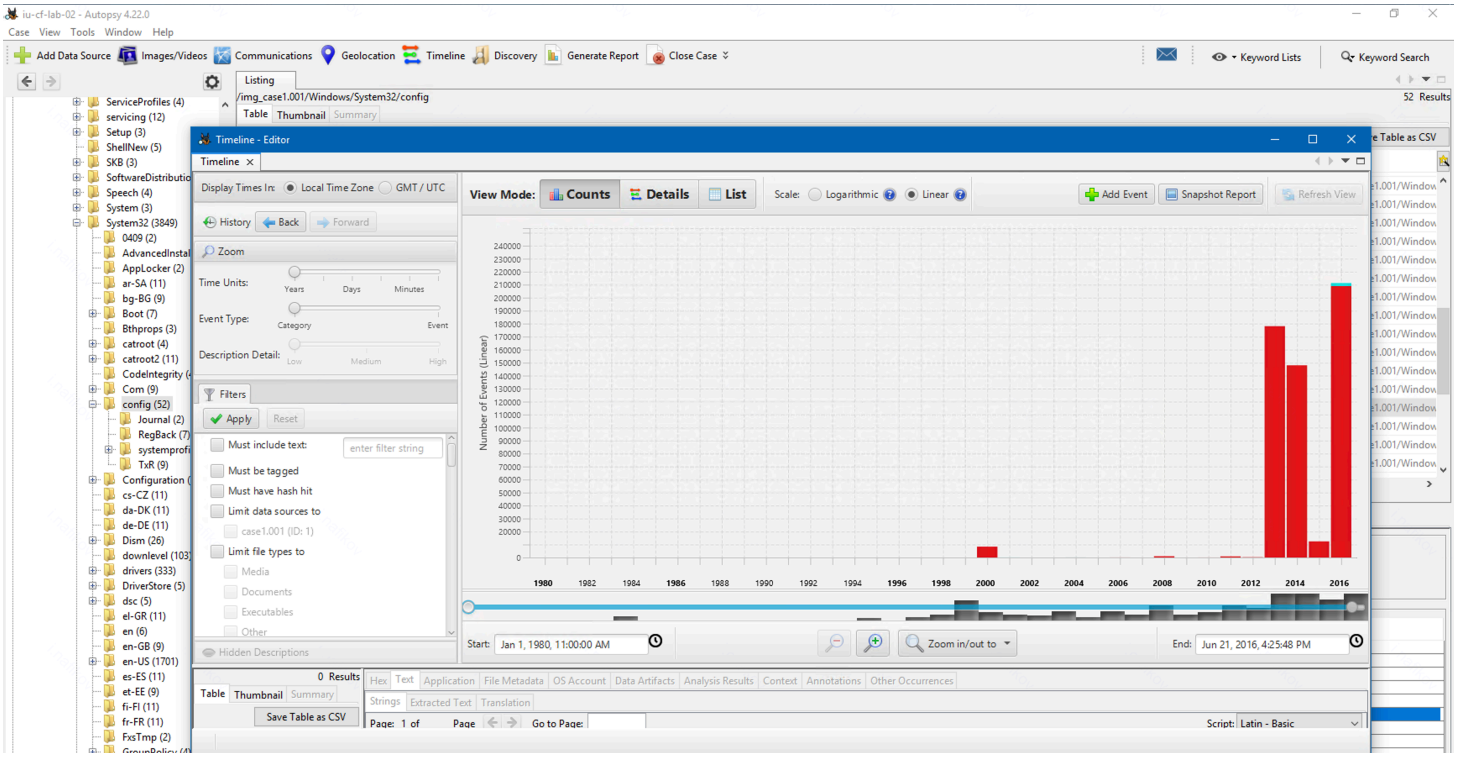


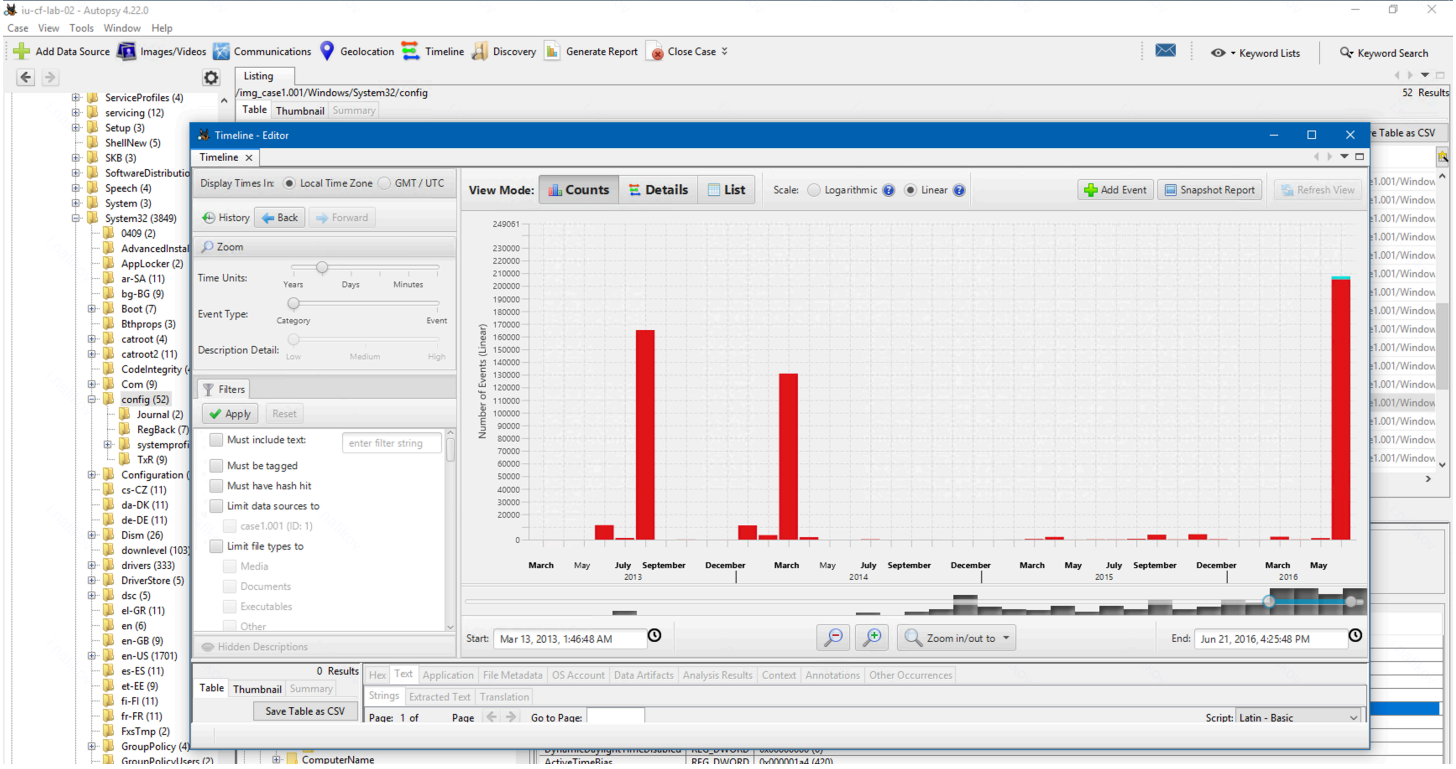
- **Timezone & location =** `UTC-8:00` which is the same as Pacific Standard Time. I also found it inside the registry hive `HKEY_LOCAL_MACHINE\SYSTEM`. This means that the last DHCP lease obtain time was

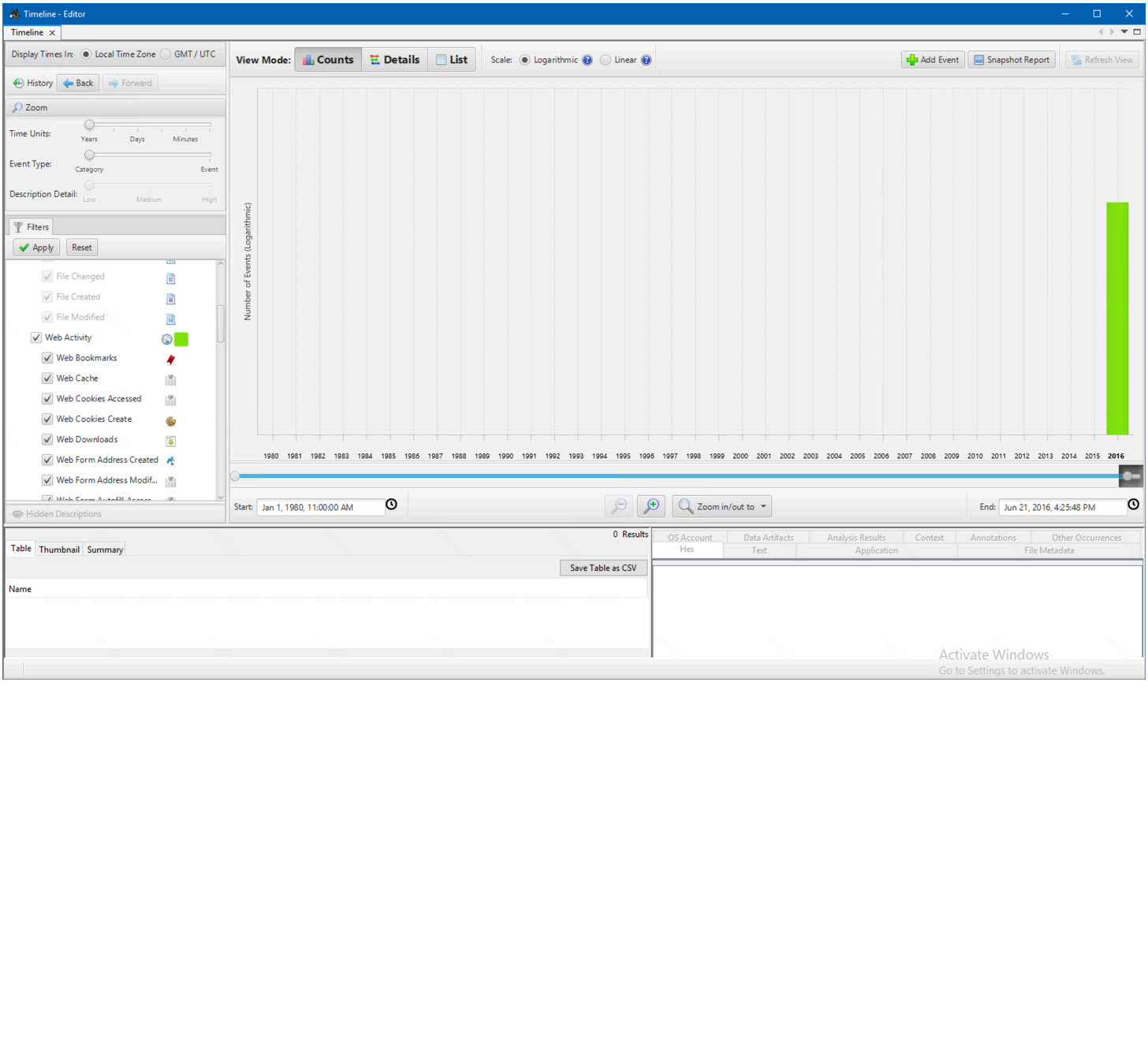
actually `2016-06-20 18:23:12 GMT-08:00`.

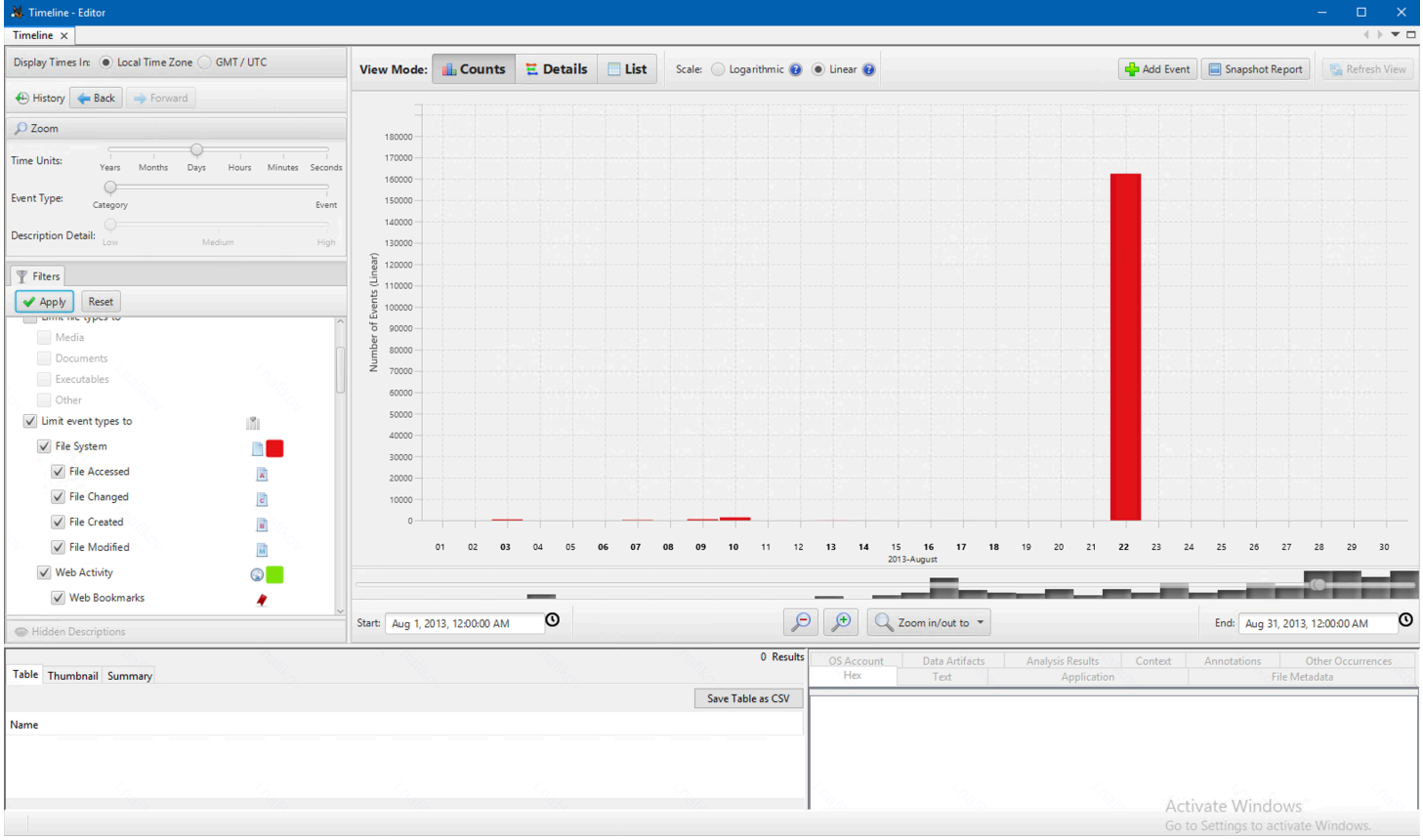


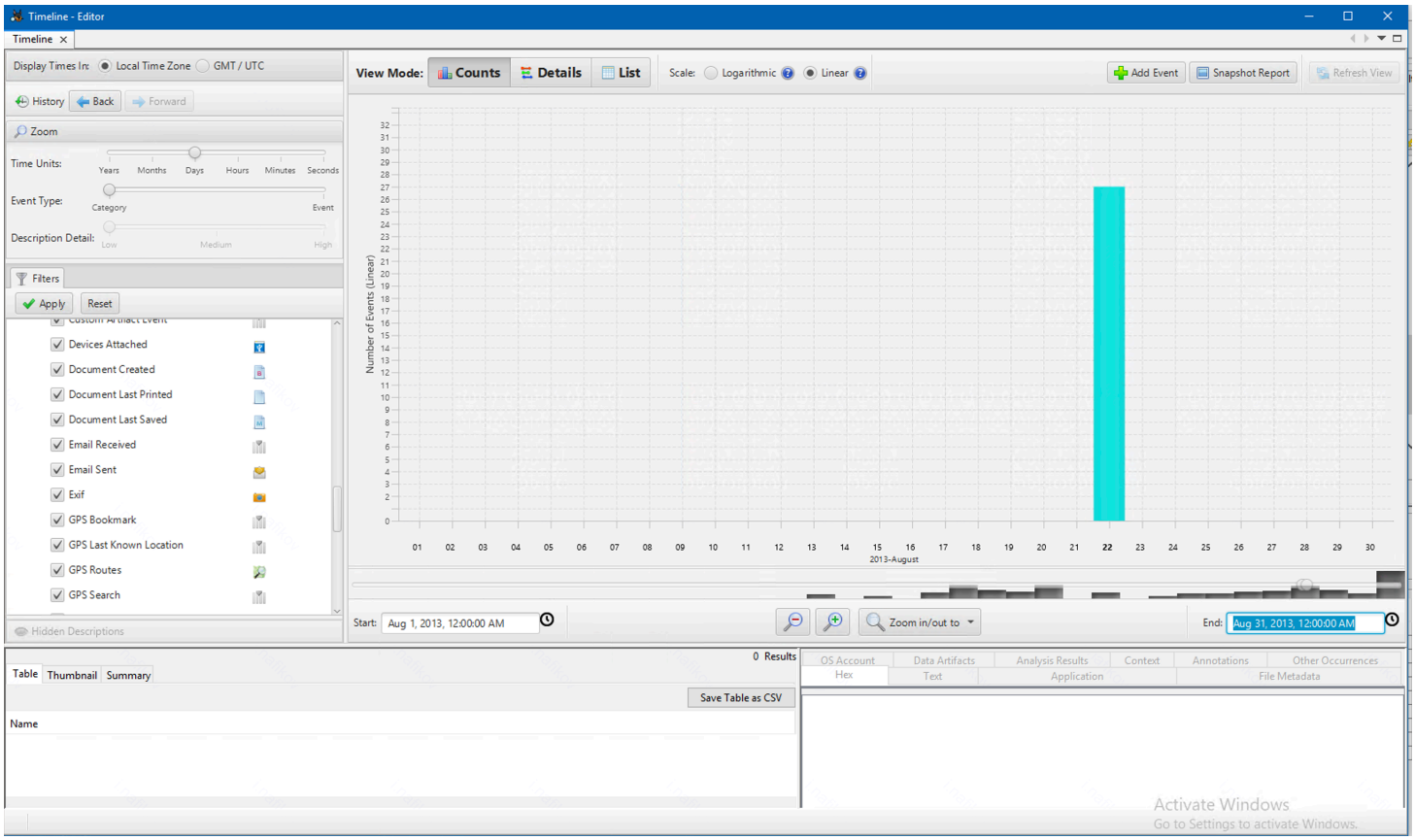
- **OS usage**, by my first assumption, is ≈ 3 years (Jun 2013 - Jun 2016) since the absolute majority of events happened in this time period which I obtained using AutoPsy timeline. An interesting part is that the device was most actively used periodically (22nd of August 2013, 18th of March 2014, 21st 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.

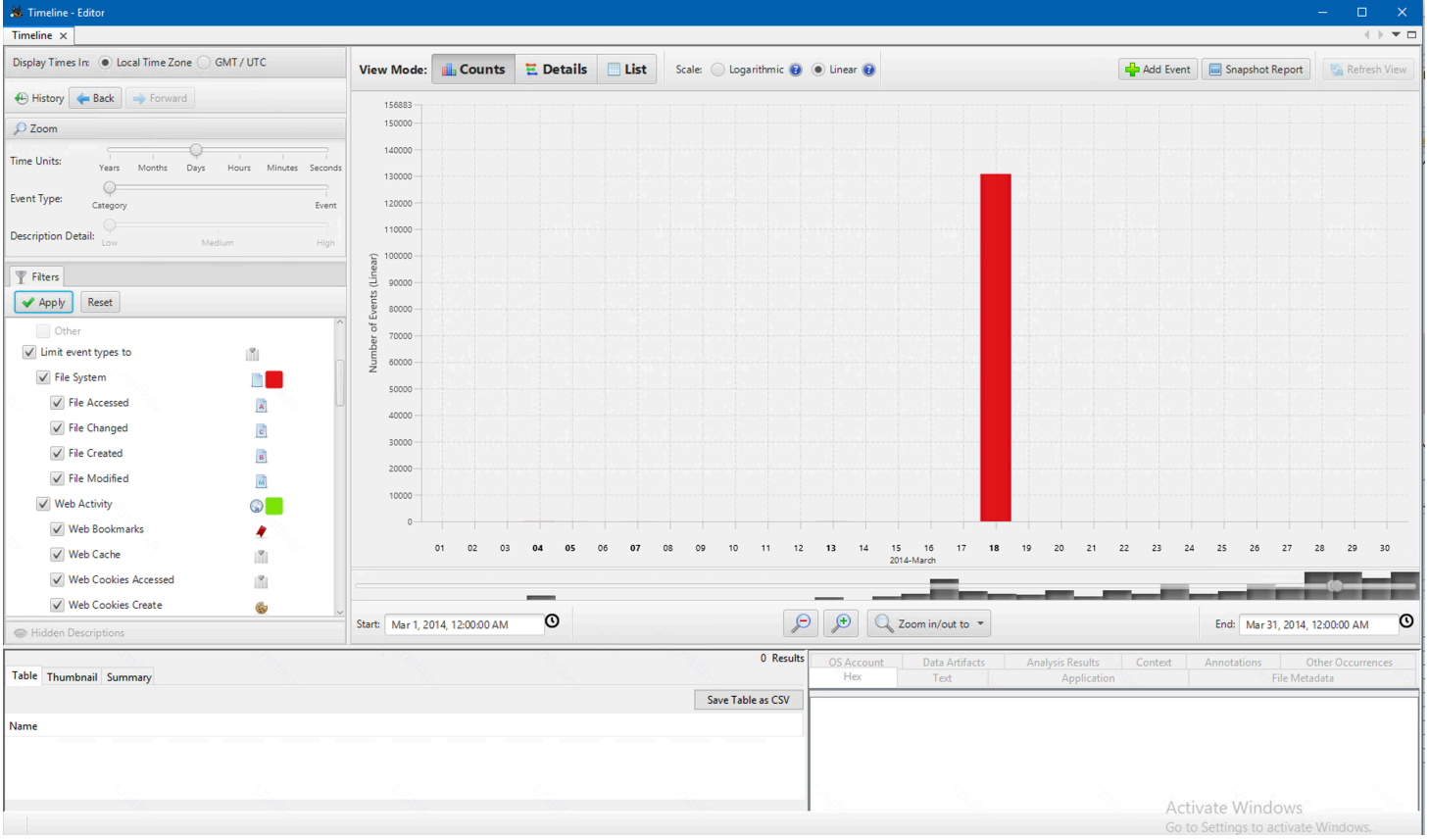


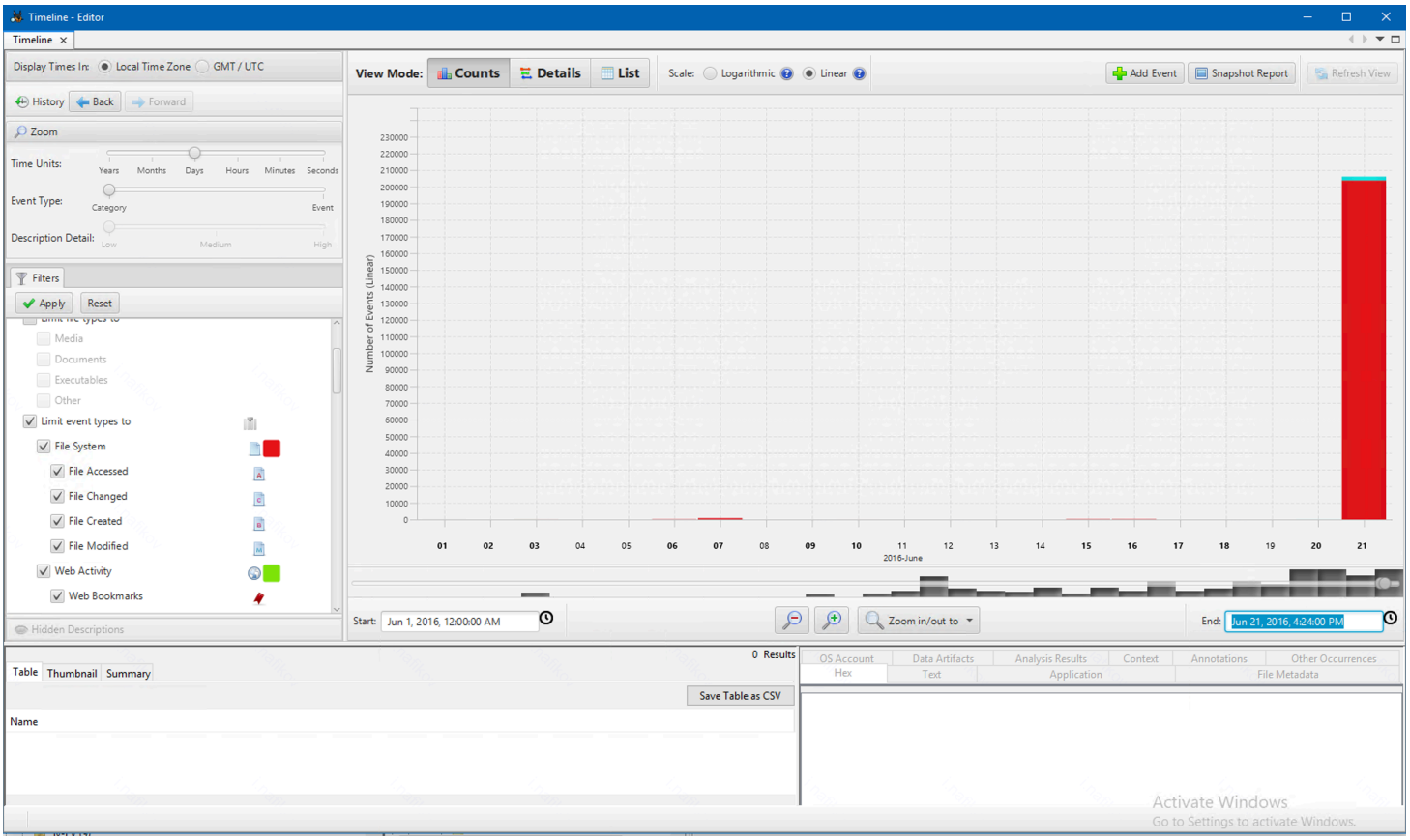

lu-cf-lab-02 - Autopsy 4.22.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
/img_case1.001/Windows/System32/config
52 Results
Table Thumbnail Summary
Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
Must include text: enter filter string
Must be tagged
Must have hash hit
Limit data sources to
case1.001 (ID: 1)
Limit file types to
Media
Documents
Executables
Other
Hidden Descriptions
View Mode: Counts Details List
Scale: Logarithmic Linear
Add Event Snapshot Report Refresh View
Number of Events (Linear)
March May July September December March May July September December March May July September December March May
2013 2014 2015 2016
Start: Mar 13, 2013, 1:46:48 AM
Zoom in/out to
End: Jun 21, 2016, 4:25:48 PM
0 Results
Table Thumbnail Summary
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


Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
File Changed
File Created
File Modified
Web Activity
Web Bookmarks
Web Cache
Web Cookies Accessed
Web Cookies Create
Web Downloads
Web Form Address Created
Web Form Address Modif...
Hidden Descriptions
View Mode: Counts Details List
Scale: Logarithmic Linear
Add Event Snapshot Report Refresh View
Number of Events (Logarithmic)
1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016
Start: Jan 1, 1980, 11:00:00 AM
Zoom in/out to
End: Jun 21, 2016, 4:25:48 PM
0 Results
Table Thumbnail Summary
Save Table as CSV
Name
OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Hex Text Application File Metadata
Activate Windows
Go to Settings to activate Windows.


Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Months Days Hours Minutes Seconds
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
Media
Documents
Executables
Other
Limit event types to
File System
File Accessed
File Changed
File Created
File Modified
Web Activity
Web Bookmarks
Hidden Descriptions
View Mode: Counts Details List
Scale: Logarithmic Linear
Add Event
Snapshot Report
Refresh View
Number of Events (Linear)
2013-August
Start: Aug 1, 2013, 12:00:00 AM
Zoom in/out to
End: Aug 31, 2013, 12:00:00 AM
0 Results
Table Thumbnail Summary
Save Table as CSV
Name
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Hex
Text
Application
File Metadata
Activate Windows
Go to Settings to activate Windows.

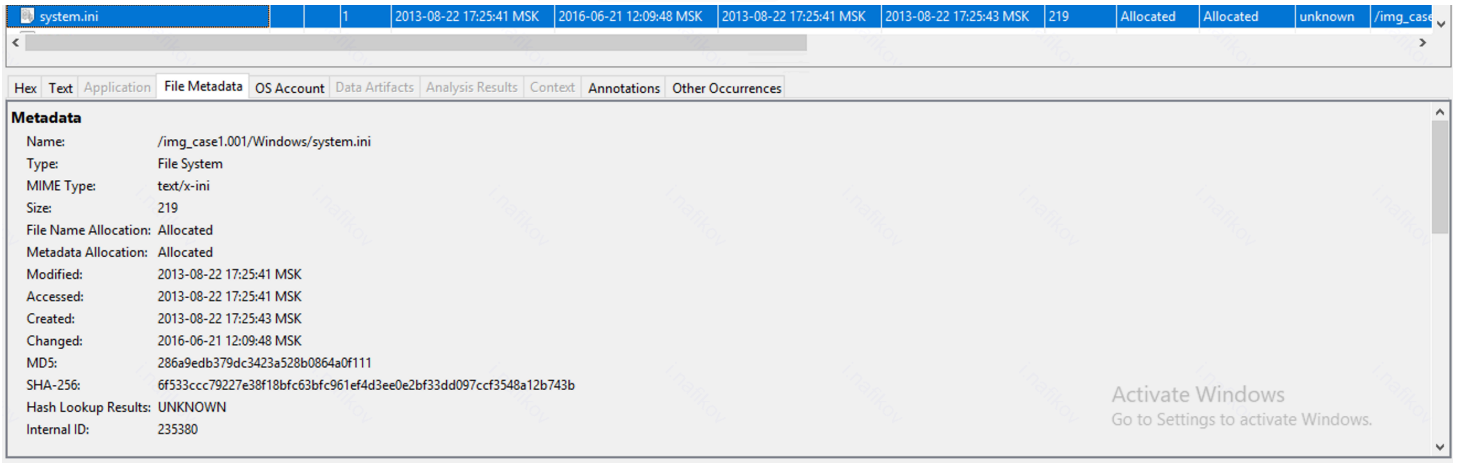

Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Months Days Hours Minutes Seconds
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
Devices Attached
Document Created
Document Last Printed
Document Last Saved
Email Received
Email Sent
Exif
GPS Bookmark
GPS Last Known Location
GPS Routes
GPS Search
Hidden Descriptions
View Mode: Counts Details List
Scale: Logarithmic Linear
Add Event
Snapshot Report
Refresh View
Number of Events (Linear)
2013-August
Start: Aug 1, 2013, 12:00:00 AM
Zoom in/out to
End: Aug 31, 2013, 12:00:00 AM
0 Results
Table Thumbnail Summary
Save Table as CSV
Name
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Hex
Text
Application
File Metadata
Activate Windows
Go to Settings to activate Windows.



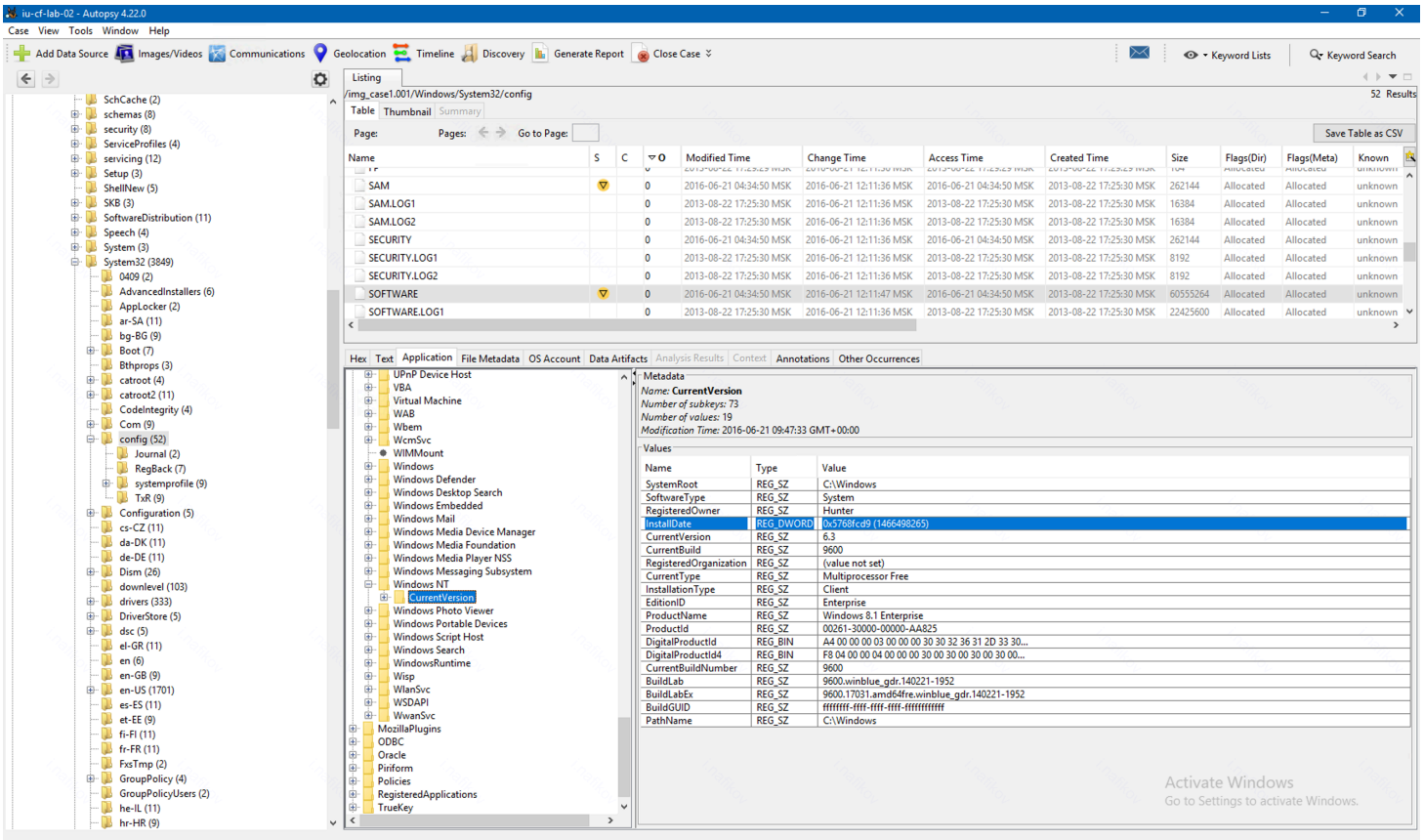


- But before moving to the login information I decided to check the **system installation timestamp** which is `2013-08-22 17:25:41 GMT+03:00`. I took it from the creation date of `system.ini` file. Also,

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



- 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.



Convert epoch to human-readable date and vice versa

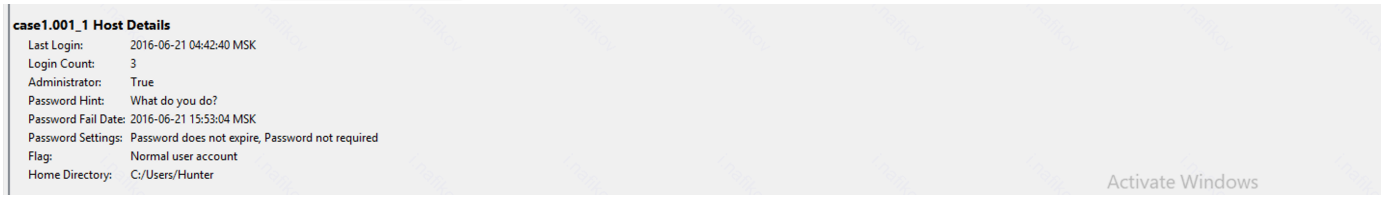
1466498265 Timestamp to Human date [batch convert]

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

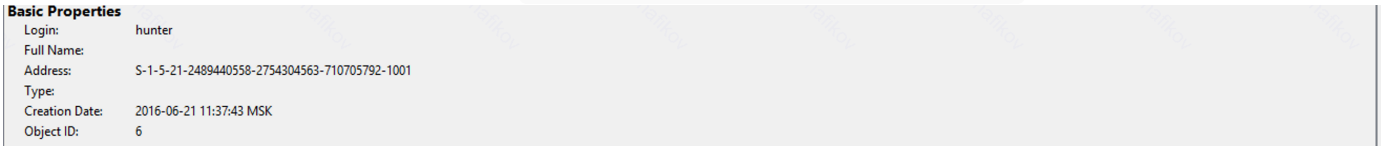
Assuming that this timestamp is in **seconds**:
GMT : Tuesday, June 21, 2016 8:37:45 AM
Your time zone : Tuesday, June 21, 2016 11:37:45 AM GMT+03:00
Relative : 9 years ago

- **Login information**

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



- From the same screenshot we see that the **last login** is `2016-06-21 04:42:40 GMT+03:00`
- The **account creation** timestamp is `2016-06-21 11:37:43 GMT+03:00`



- **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:
    1. 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.
    2. Someone changed the proper date information trying to hide the actual timeline.
    3. 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.

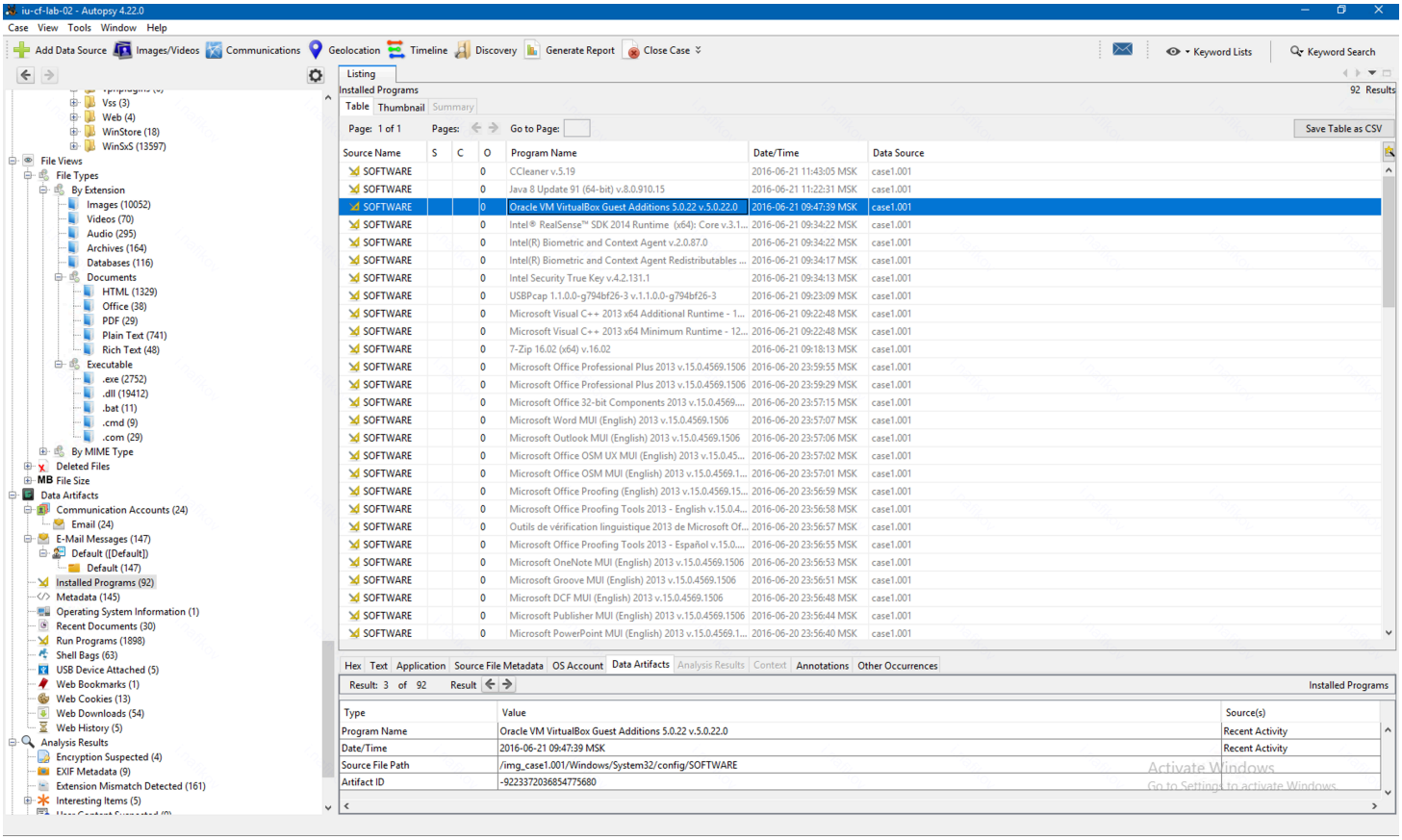
Applications

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

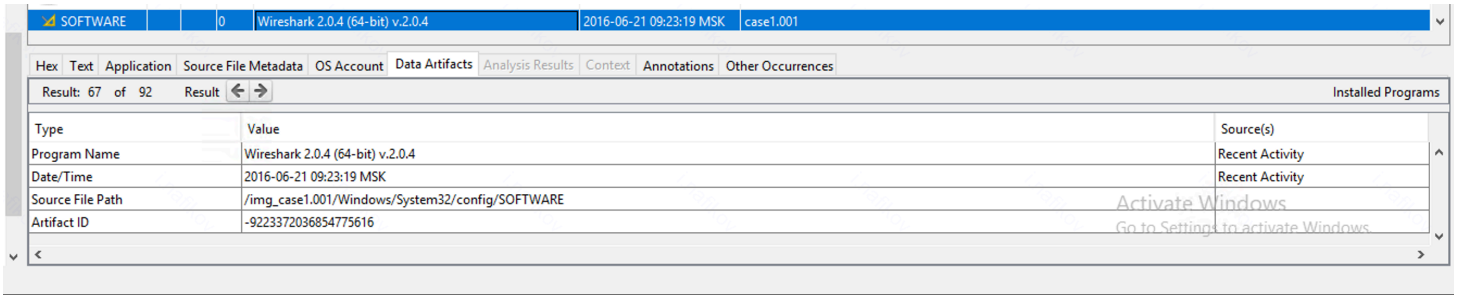
- First, I found USBPcap which is a USB sniffer and 7-zip

SOFTWARE			0	USBPcap 1.1.0.0-g794bf26-3 v.1.1.0.0-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

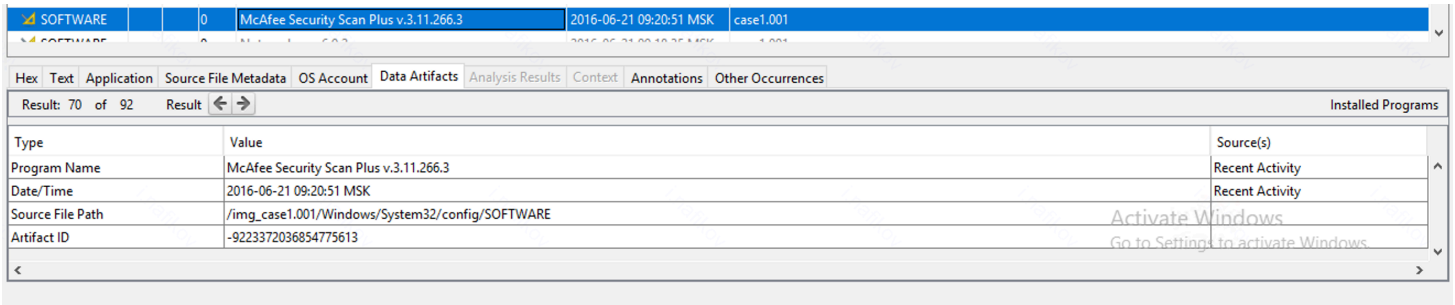
- I found that he had a **VirtualBox** installed which means he's not a usual user of PC but some IT guy



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



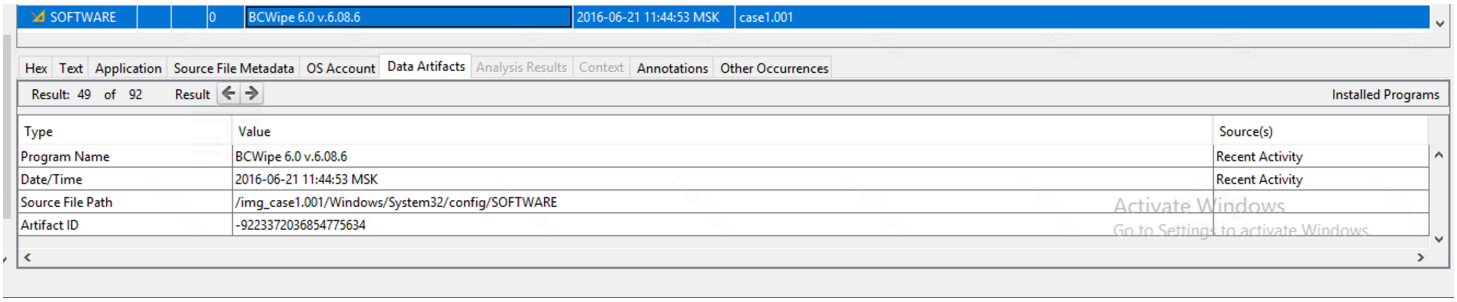
- Btw, he has an antivirus **McAfee** installed



- Also, the user has **Notepad++**, **Skype**, **Dropbox**, **Google Drive**, and **TeamViewer** installed which is 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 use 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



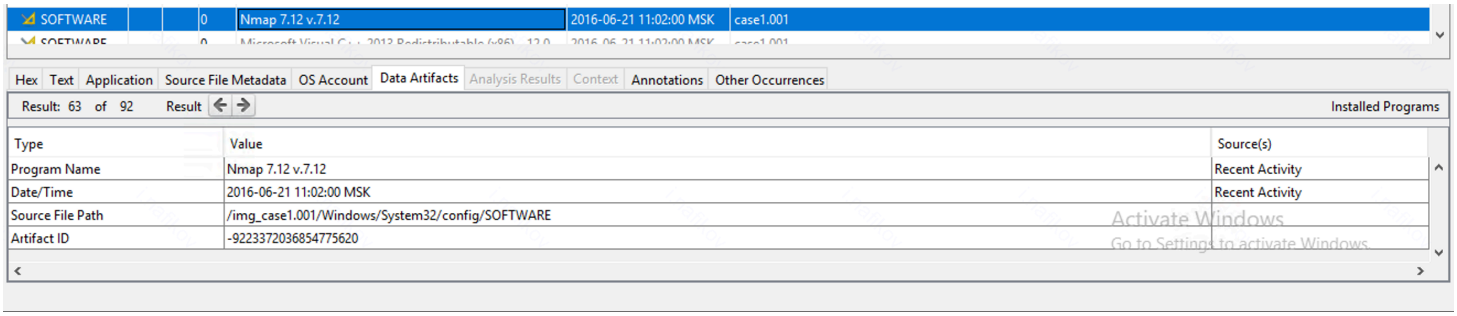
SOFTWARE | 0 | BCWipe 6.0 v.6.08.6 | 2016-06-21 11:44:53 MSK | case1.001

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

Result: 49 of 92 | Result | Installed Programs

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	
Artifact ID	-9223372036854775634	

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



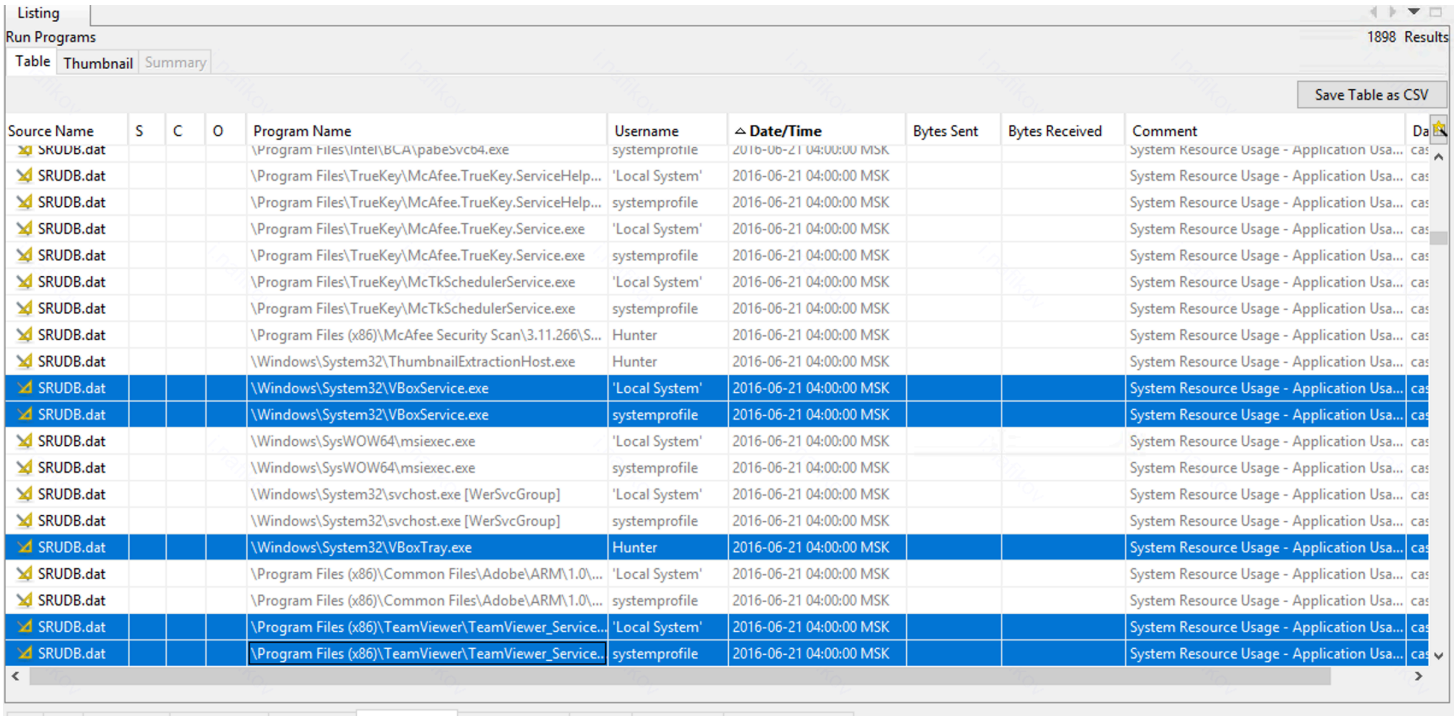
SOFTWARE | 0 | Nmap 7.12 v.7.12 | 2016-06-21 11:02:00 MSK | case1.001

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

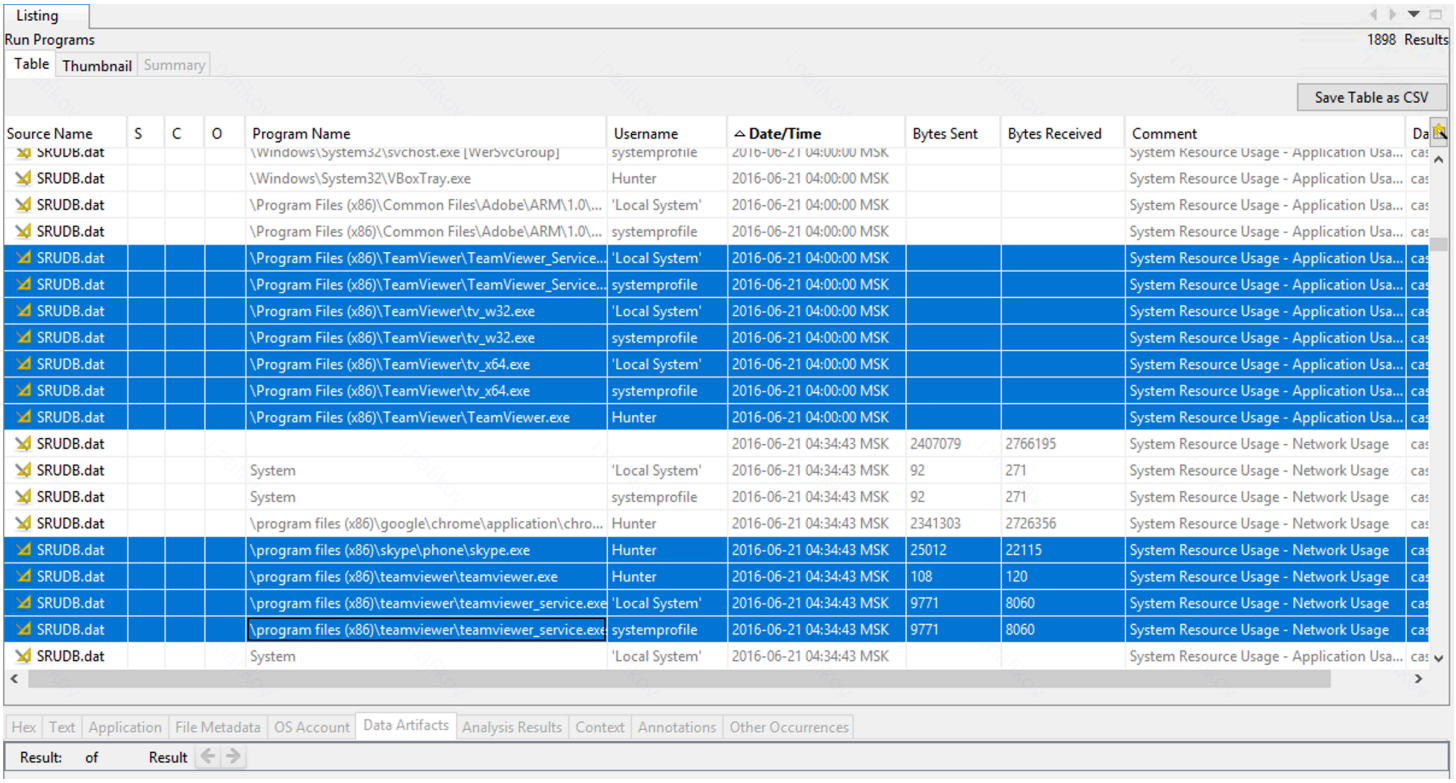
Result: 63 of 92 | Result | Installed Programs

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	
Artifact ID	-9223372036854775620	

- The **VirtualBox** was used on Jun 21

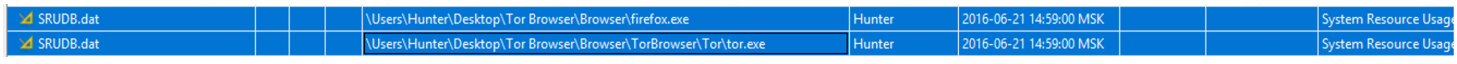


- Also, **TeamViewer** was used at the same time with the Skype

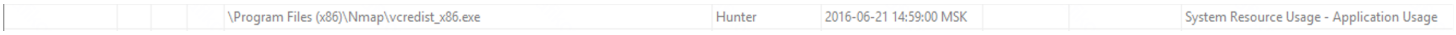


- **Wireshark** was also used

- **Tor Browser** was used



- Yeah, **Nmap** too



- **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\Python35-32\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

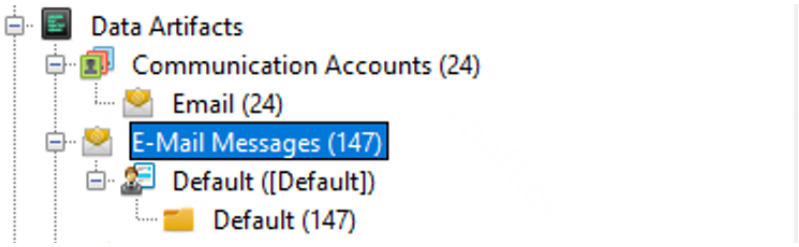
- What is more, I found Zenmap which is a powerful GUI tool for port scanning based on Nmap

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

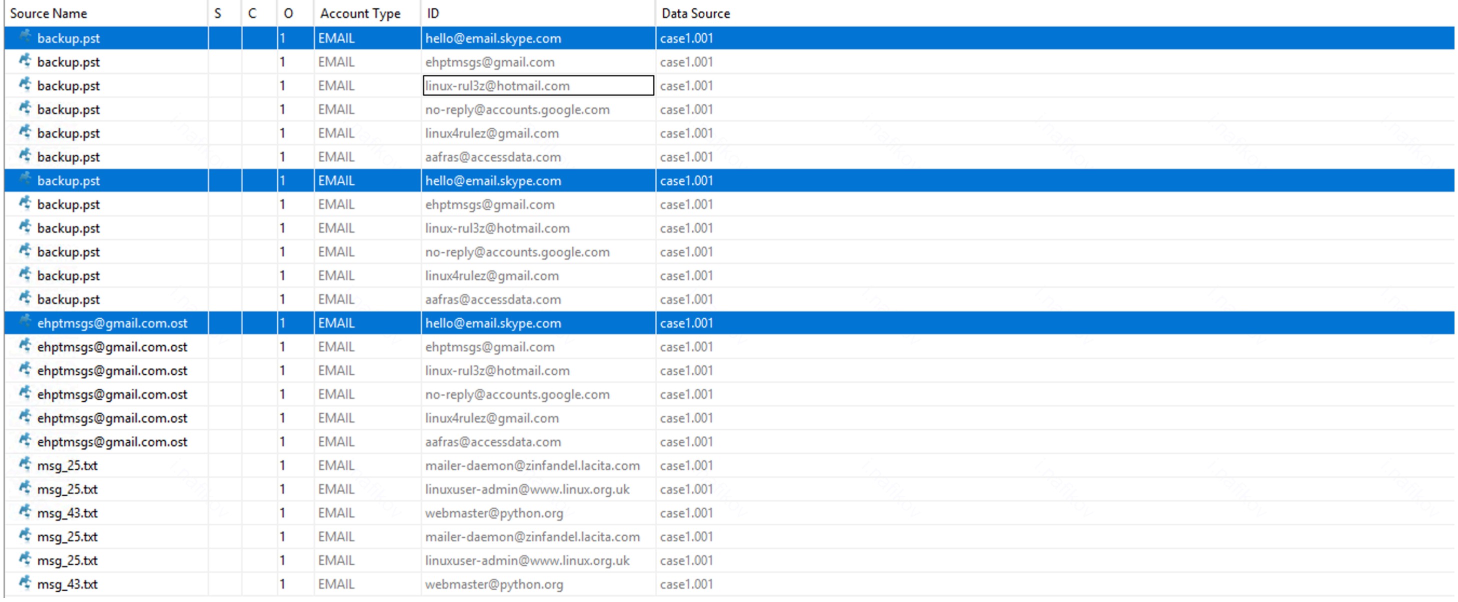
- **Conclusion**:
  - From all above, I can conclude that the owner used: Tor Browser for something probably not legal, port scanning using Zenmap, BCWipe and CCleaner for wiping data, TeamViewer for remote access (maybe someone worked instead of him), Skype for communications, DropBox, Google Drive, 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 😏

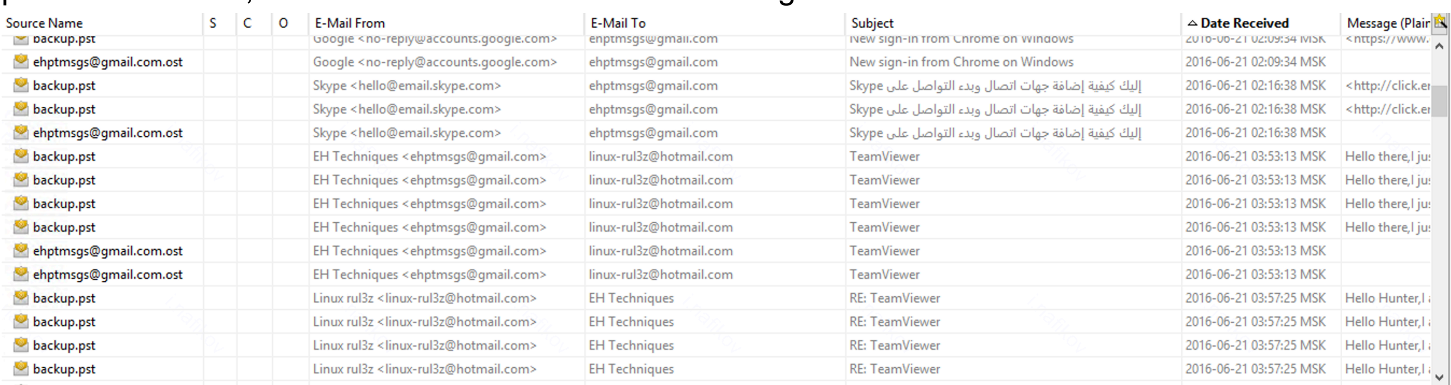


- First, I discovered all the E-Mail accounts participated in communications on this device including skype



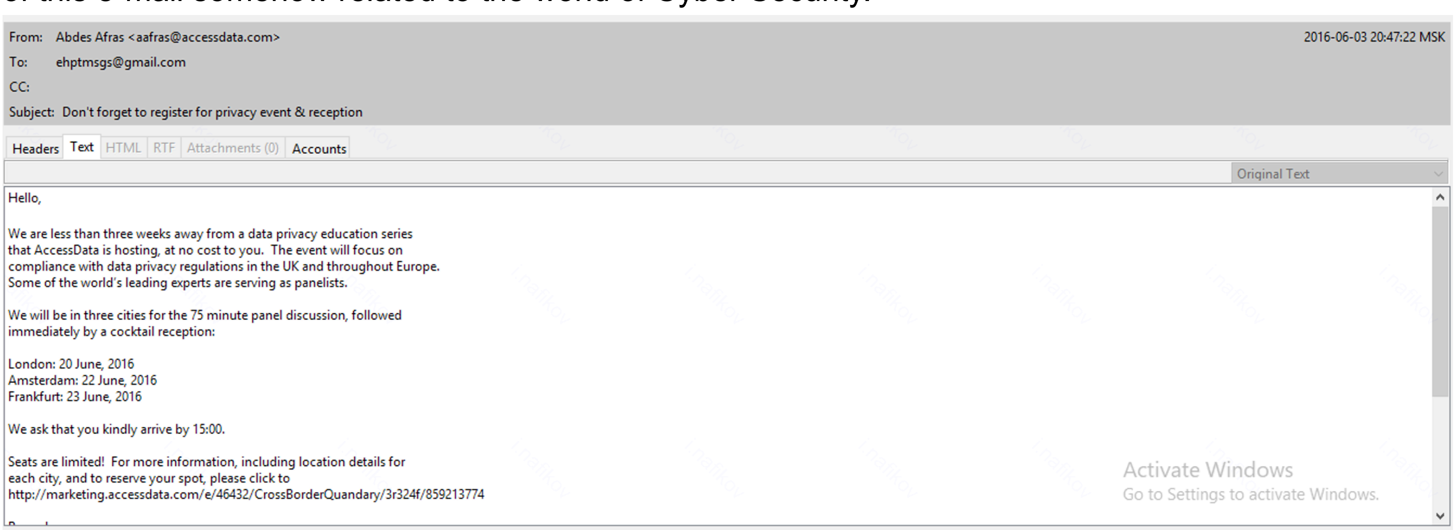
Source Name	S	C	O	Account Type	ID	Data Source
backup.pst			1	EMAIL	hello@email.skype.com	case1.001
backup.pst			1	EMAIL	ehptmsgs@gmail.com	case1.001
backup.pst			1	EMAIL	linux-rul3z@hotmail.com	case1.001
backup.pst			1	EMAIL	no-reply@accounts.google.com	case1.001
backup.pst			1	EMAIL	linux4rulez@gmail.com	case1.001
backup.pst			1	EMAIL	aafras@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	aafras@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	aafras@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 (Plair
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.
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	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
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,I
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,I
backup.pst				Linux rul3z <linux-rul3z@hotmail.com>	EH Techniques	RE: TeamViewer	2016-06-21 03:57:25 MSK	Hello Hunter,I

- 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 <aafras@accessdata.com> 2016-06-03 20:47:22 MSK
To: ehptmsgs@gmail.com
CC:
Subject: Don't forget to register for privacy event & reception

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

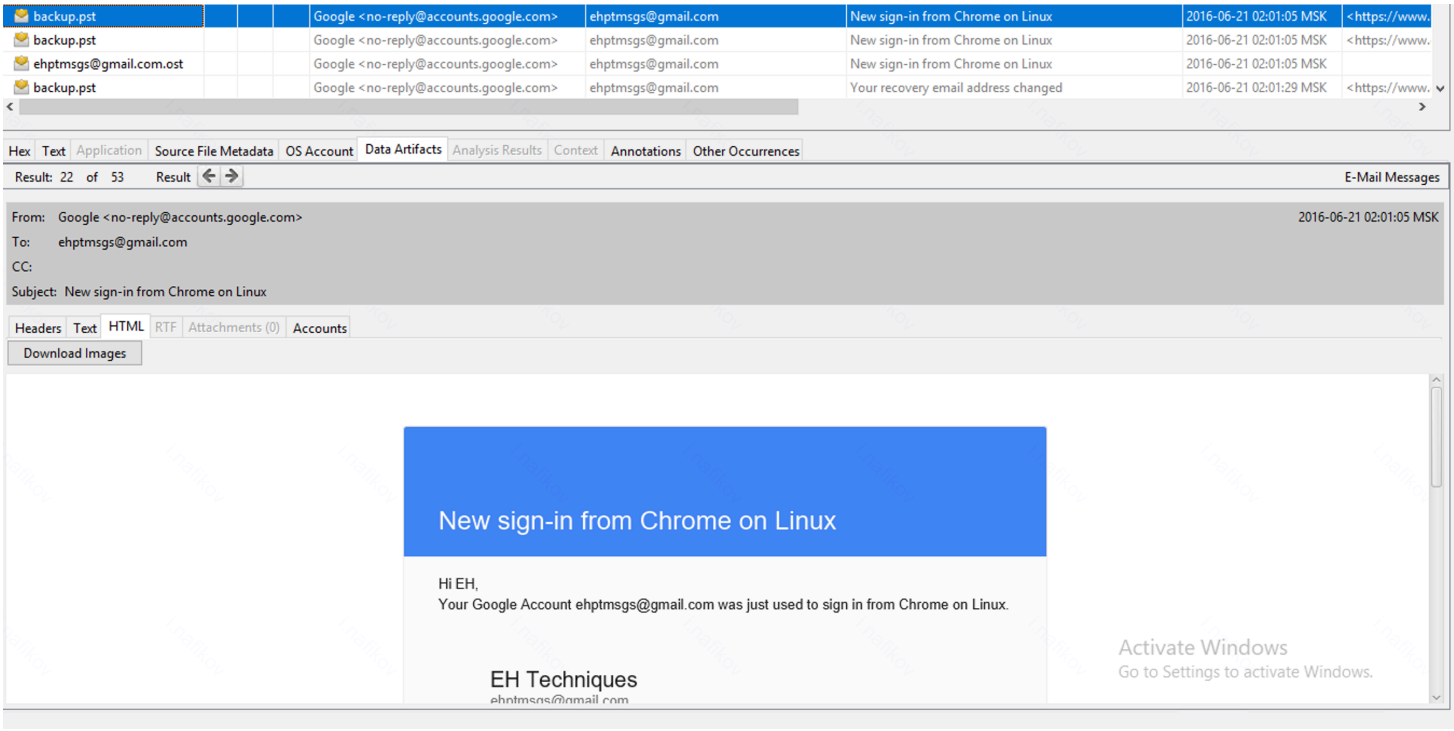
We ask that you kindly arrive by 15:00.

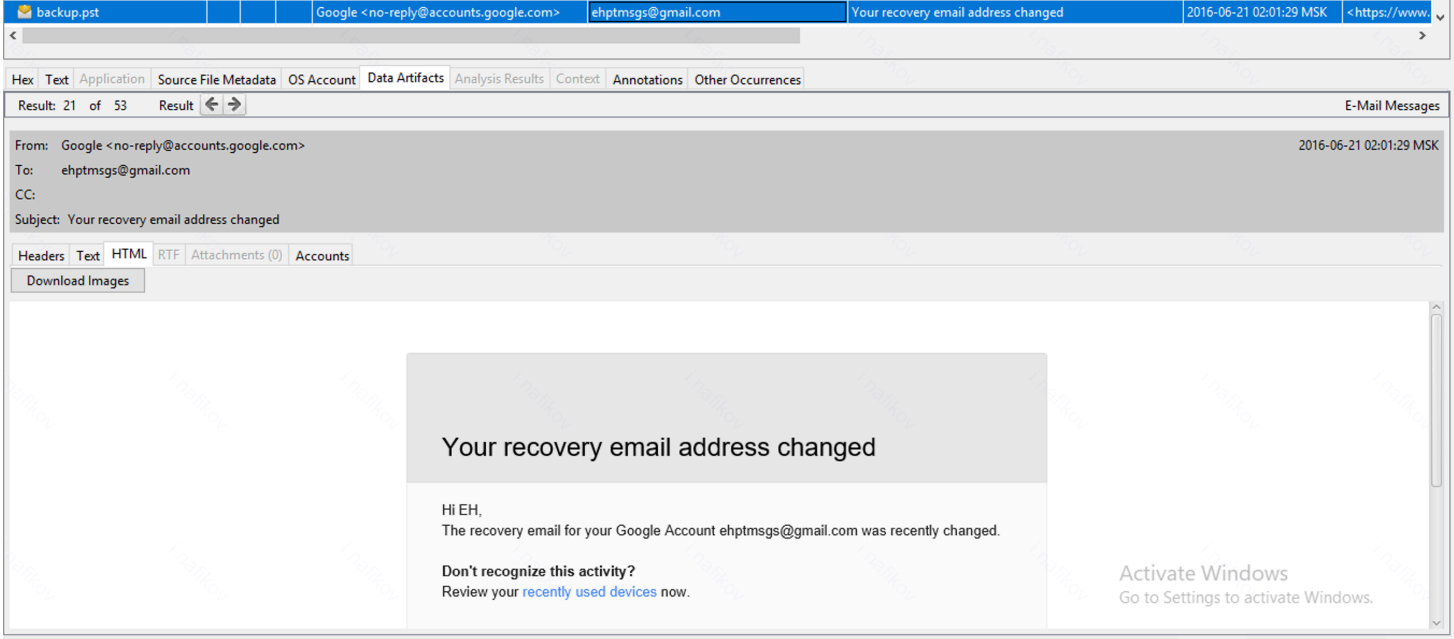
Seats are limited! For more information, including location details for
each city, and to reserve your spot, please click to
http://marketing.accessdata.com/e/46432/CrossBorderQuandary/3r324f/859213774

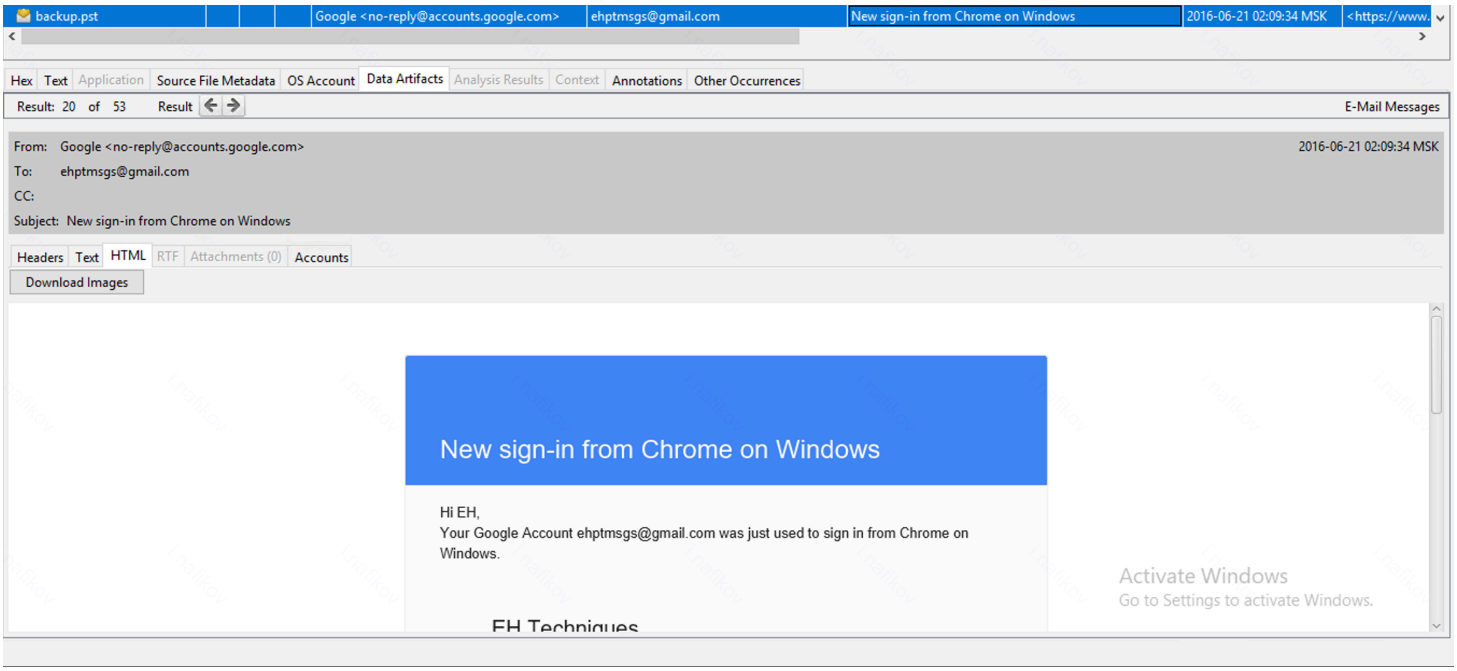
Activate Windows
Go to Settings to activate Windows.

- 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`

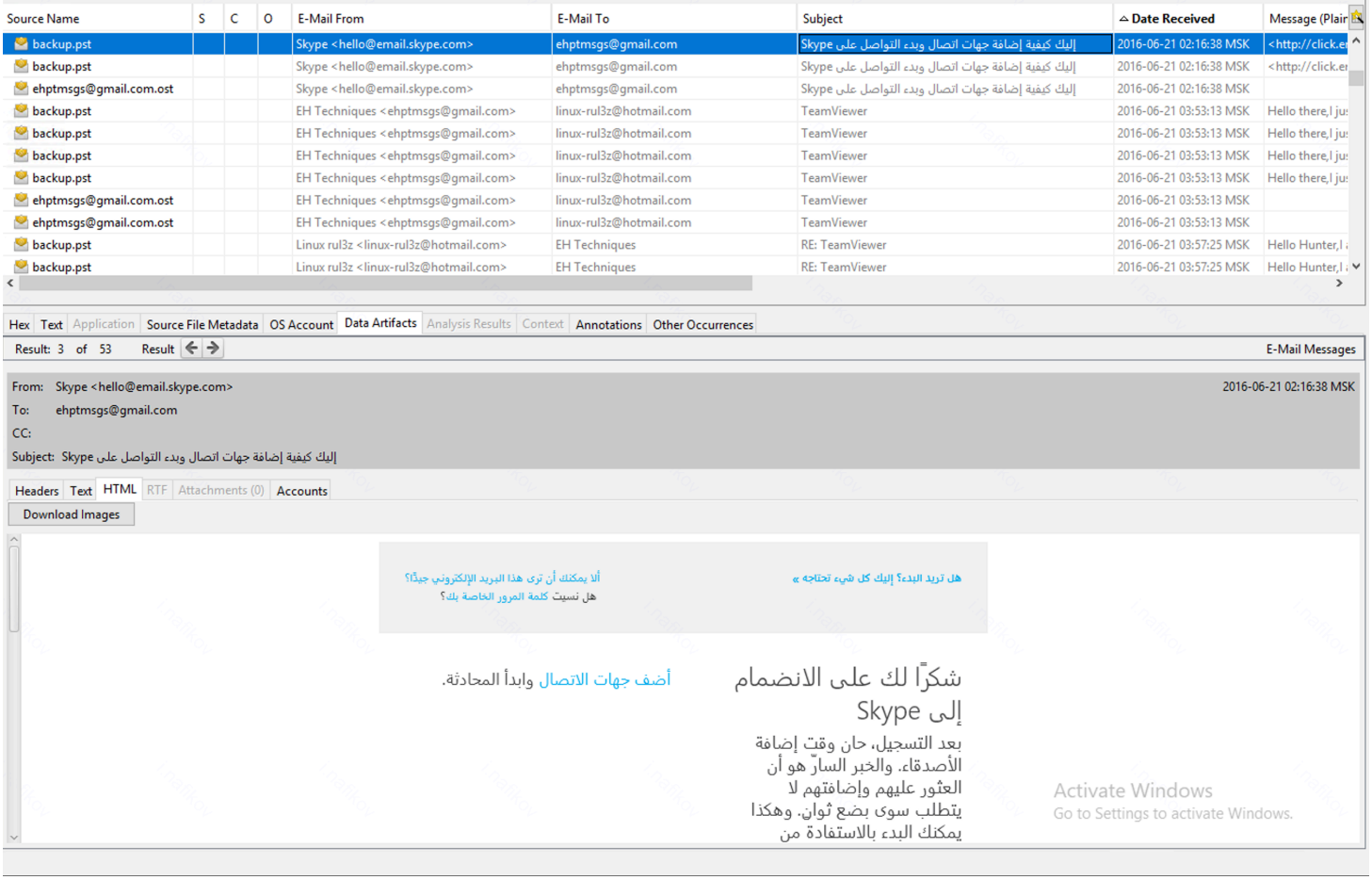
`02:01:29+03:00`. What is more, I found the next e-mail with the similar content `Your recovery email address changed` and `New sign-in from Chrome on Windows`. And everything happened around the same time.



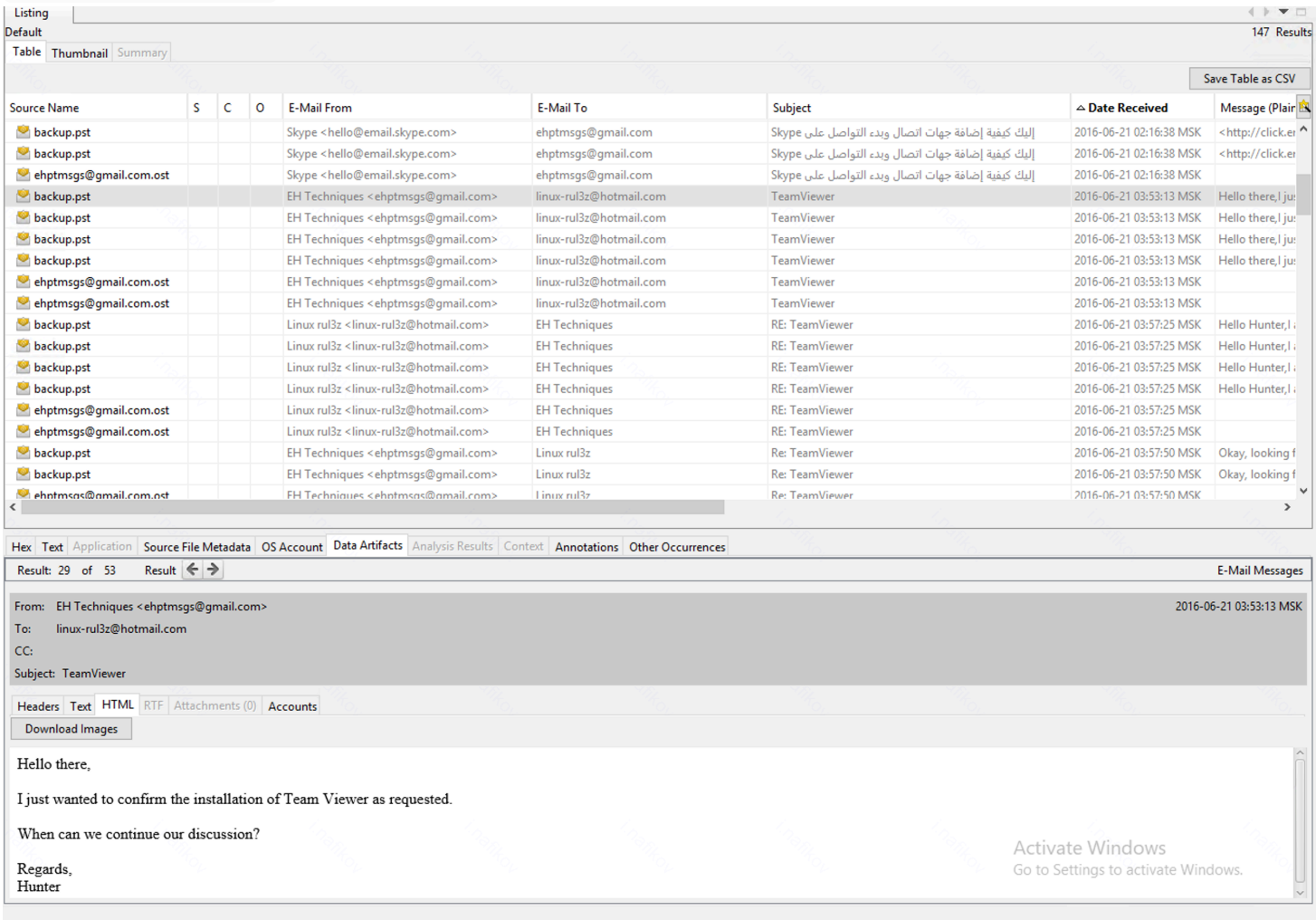




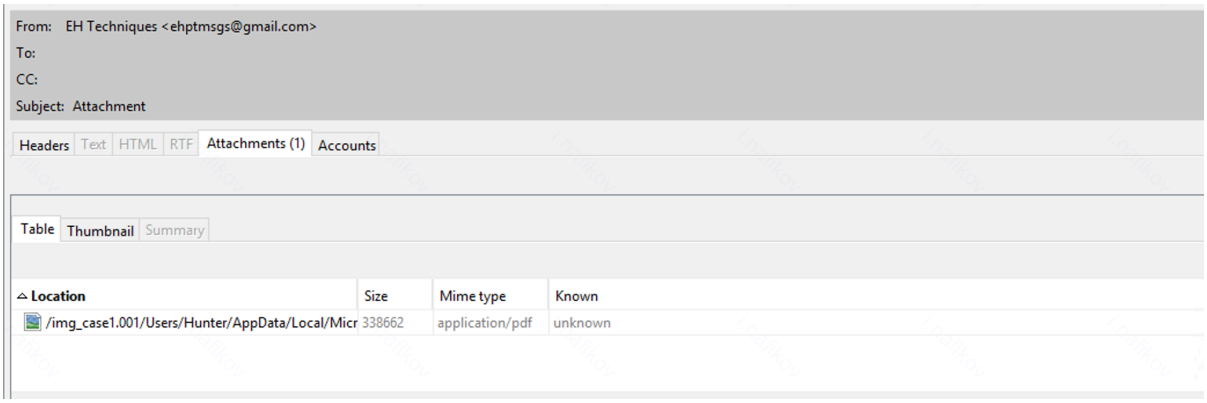
- Also, I found a strange e-mail from Skype in Arabic language which is basically just an invitation to install Skype and find your friends there

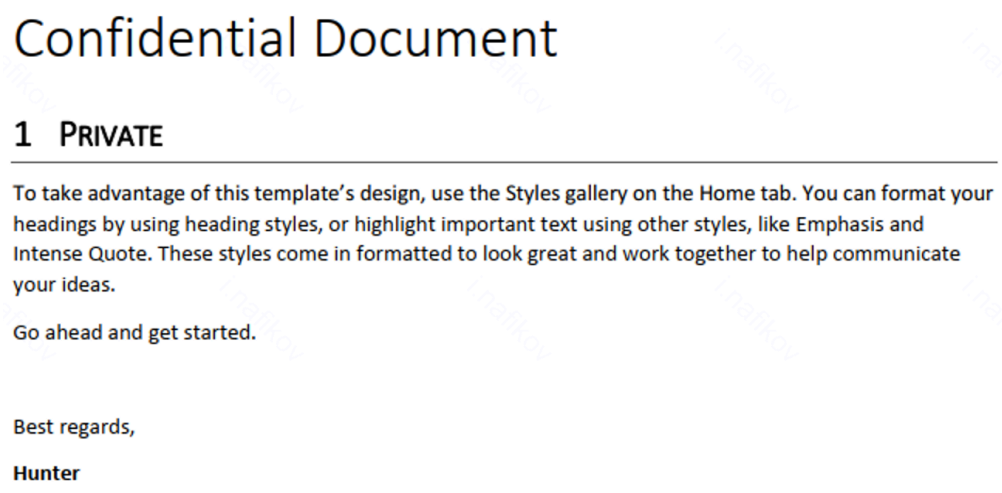


- And further there is a long conversation between the `ehptmsgs@gmail.com` and `linux-rul3z@hotmail.com` which I described shortly below:

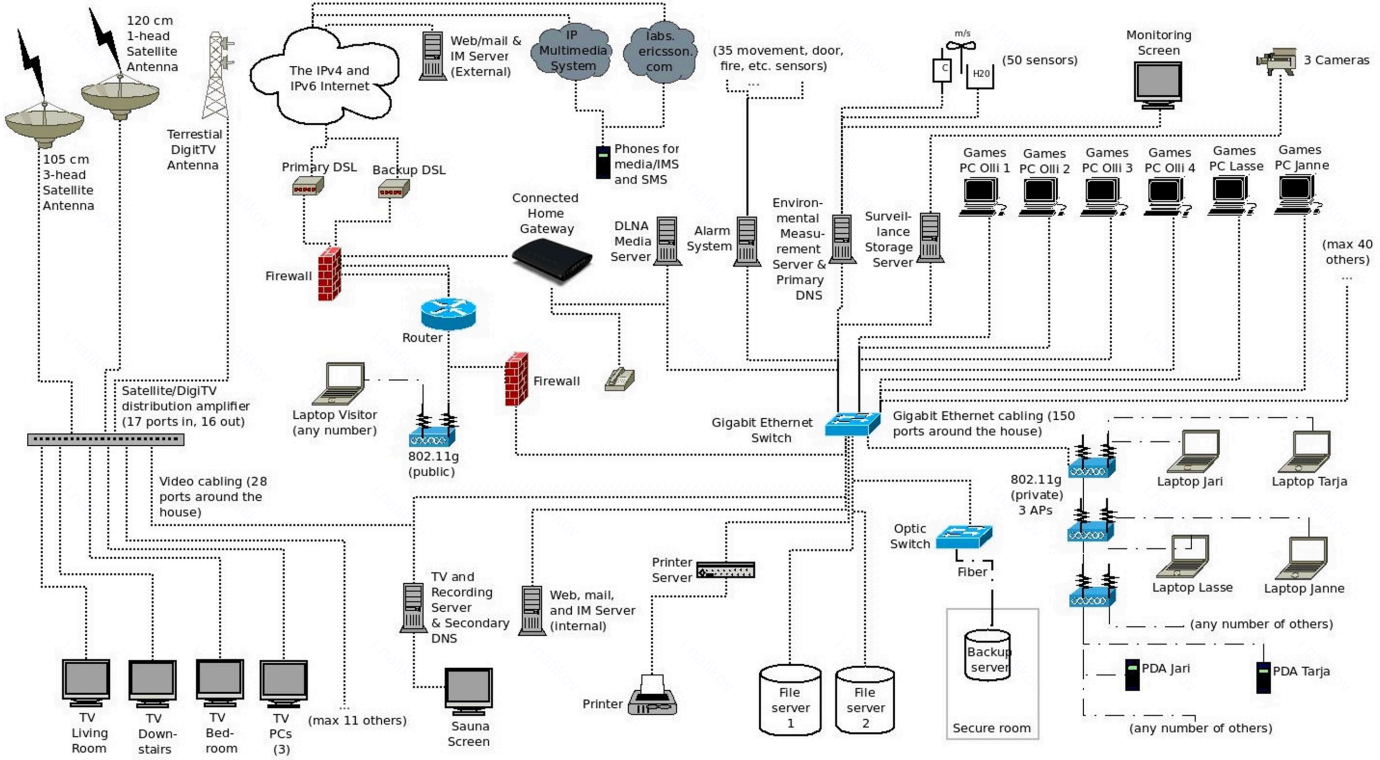


- So, the content of this E-mail conversation is the following
  - Hunter connected with some guy who seems to understand something in attacks / penetration testing to teach him and help him to attack or pentest some network (probably of their organization but I am not sure yet).
  - Their dialogue established with a Hunter's message about TeamViewer which I suppose lets the other guy to access his device remotely.
  - They conversate 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





  - Furthemore, 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.

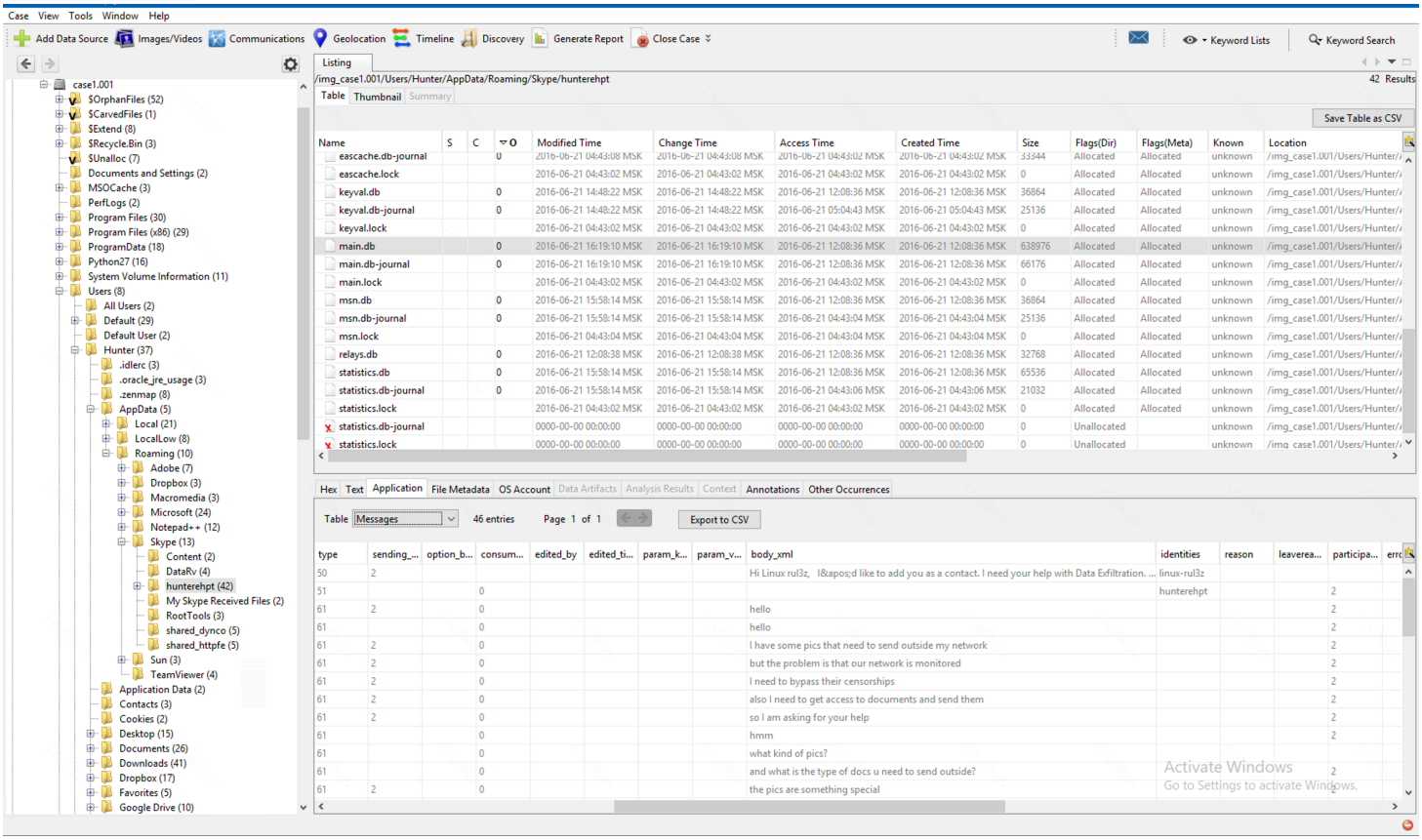


- Finally, Hunter asked the other guy to finish the project ASAP and told him that his out Outlook setup is working correctly.

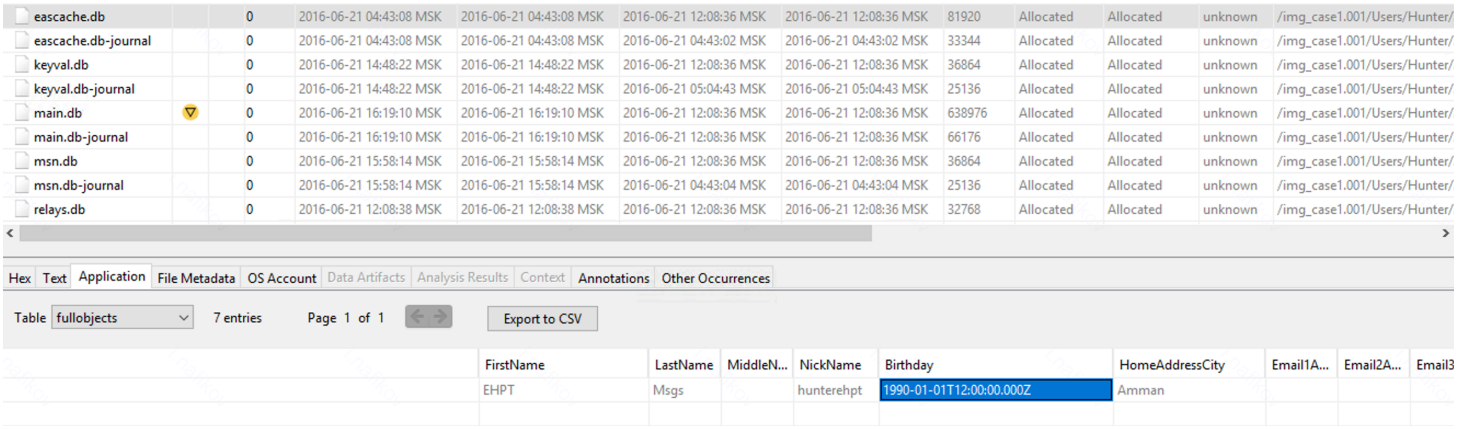
Communications: Skype

- 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 `hunterepht` which is a Hunter's username in Skype with the

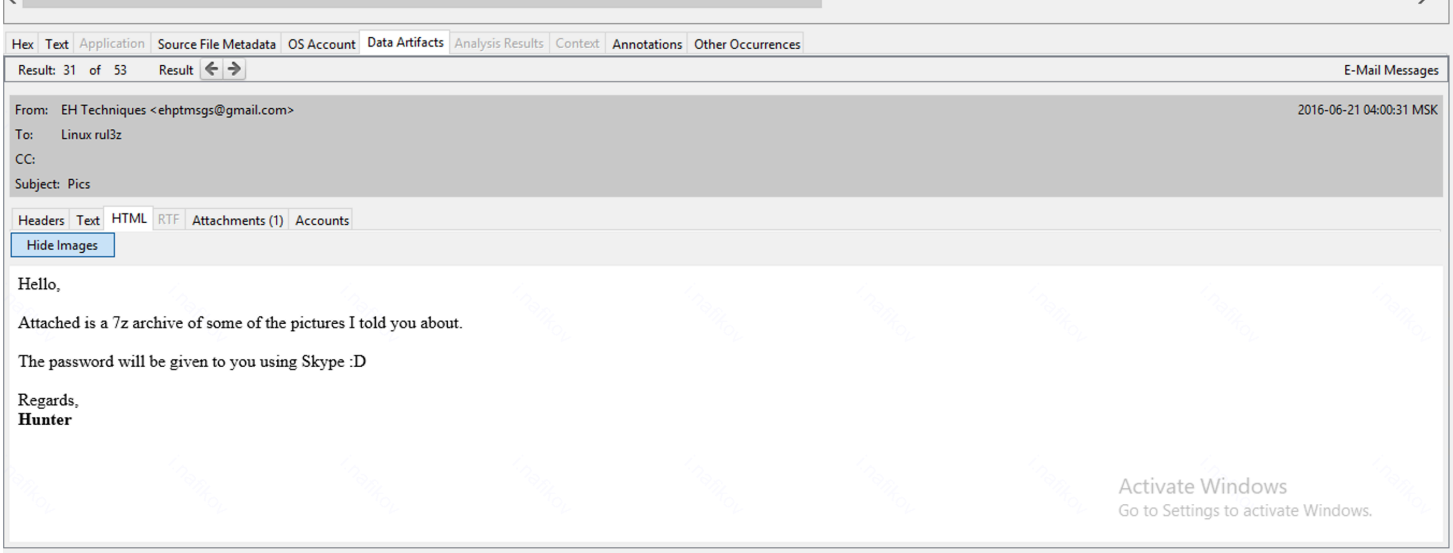
`linux-rul3z` which is an other guy's username.

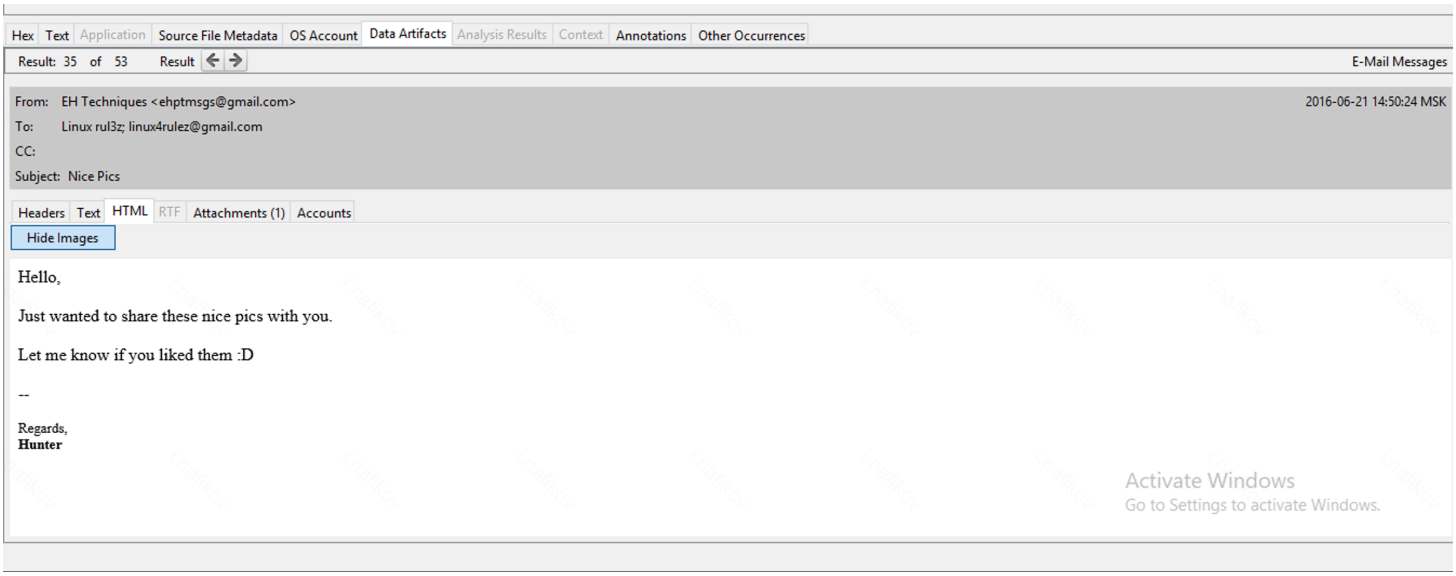


- From their conversation I got that Hunter asking `linux-rul3z` to help him to transfer some pictures and documents outside an organization's network since it is monitored. This guys agreed to help him and asks if he is able to access Hunter's device remotely via TemViewer. Hunter downloaded TeamViewer 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`



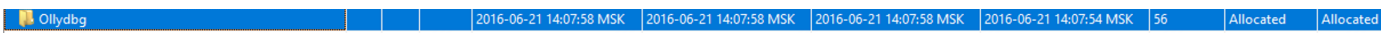
- Unfortunately, I couldn't find any password Hunter told about in mails to unarchive `Pics.7z` or `fakeporn.7z` neither in Skype databases, nor in Skype journals. It seems that Hunter quickly removed this message.



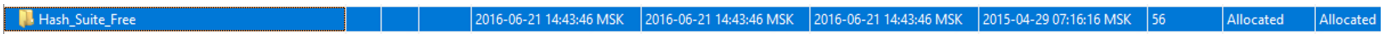


Files

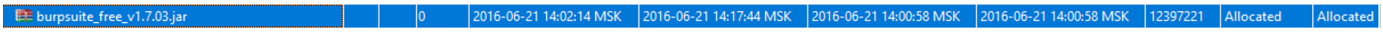
- After figuring out what's probably happened I finally need to investigate Hunter's files and check for a suspicious things
- In `Downloads` I found a lot of interesting installers. Besides the programs I've mentioned in `Applicaitons` section I also found out the following:
  - **Ollydbg** which is a 32-bit assembler level analysing debugger for Windows.

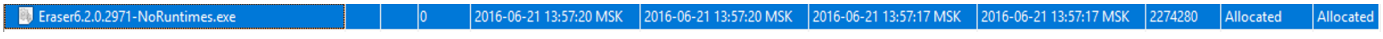
  - **Hash Suite Free** which is a Windows program to test security of password hashes.

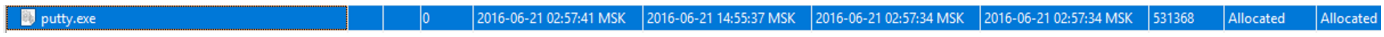
  - **BurpSuite** which is a proprietary software tool for security assessment and penetration testing of web applications.

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

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

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

pscp.exe			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

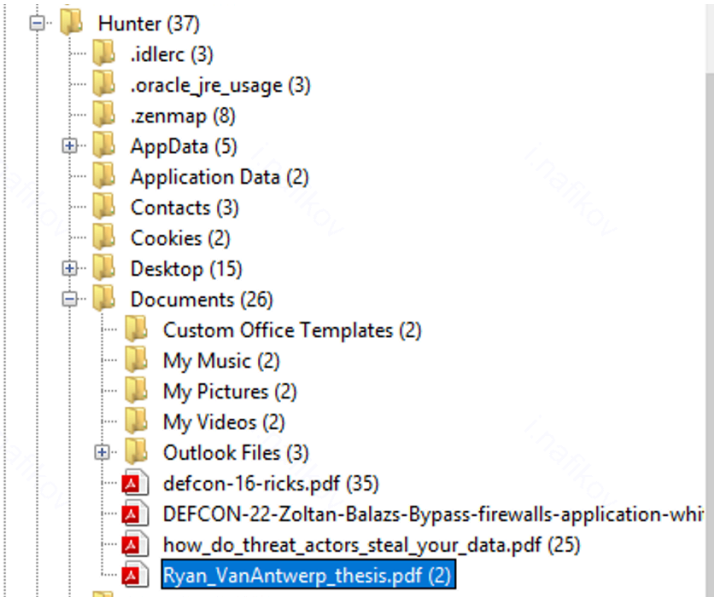
- **SetupSSH** which is a OpenSSH client.

setupssh381-20040709.zip			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

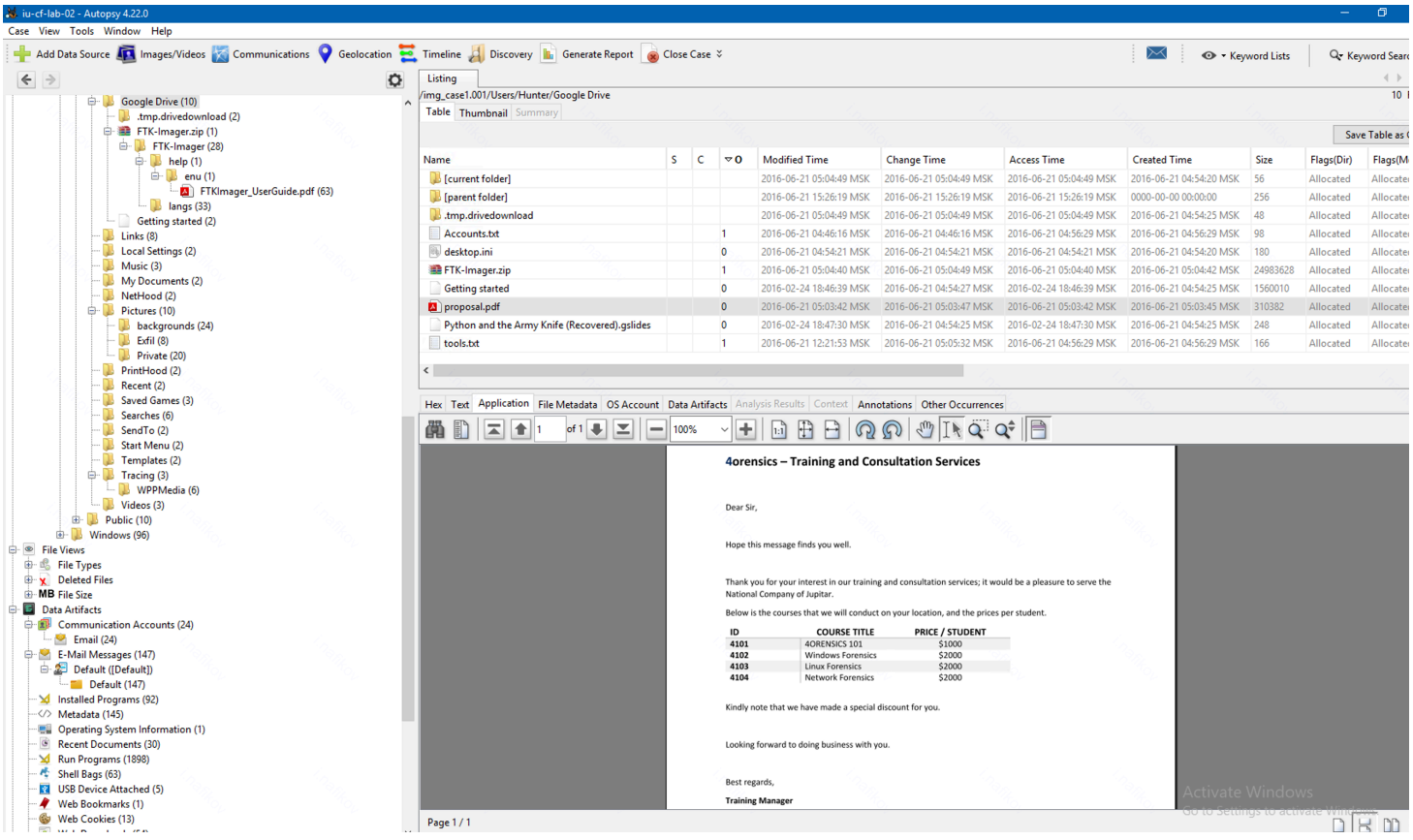
- **SysinternalSuite** which are technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Windows environment.

SysinternalsSuite.zip			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

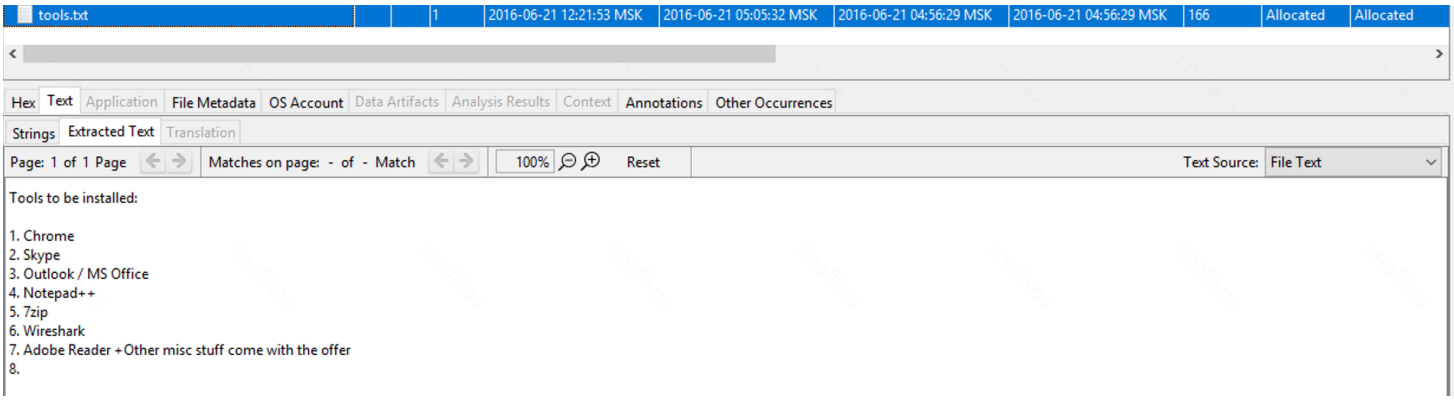
- In `Documents` folder I found 4 documents related to performing Data Exfiltration using different techniques (DNS, FTP, SQL Injection, etc.) and Bypassing Firewall.



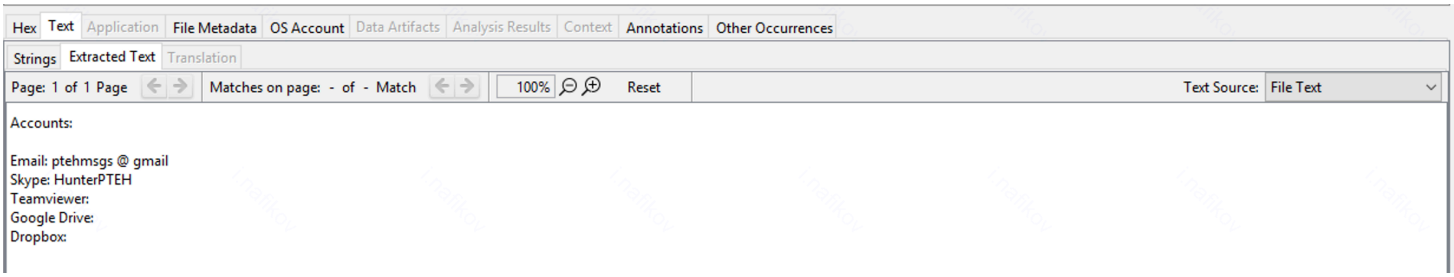
- Inside the `Google Drive` folder I found a proposal for Hunter to buy Forensics courses which are quite expensibe and some other interesting documents



- Some tools list



- And accounts list, unfortunately without passwords 😅



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

Listing

/img_case1.001/Users/Hunter/Pictures — 10 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)	Known	Locatic
[current 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	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	0000-00-00 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

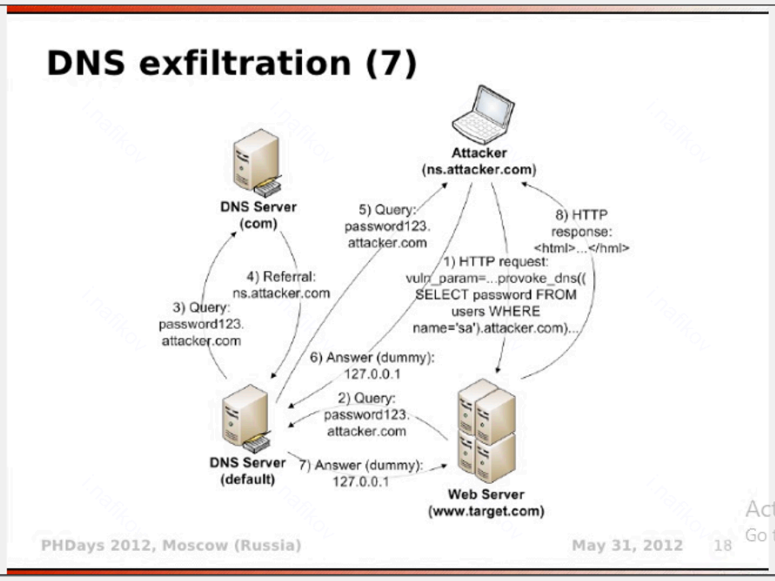
Save Table as CSV

Name	S	C	O	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	0000-00-00 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.Ide			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
Exfiltration_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
Exfiltration_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

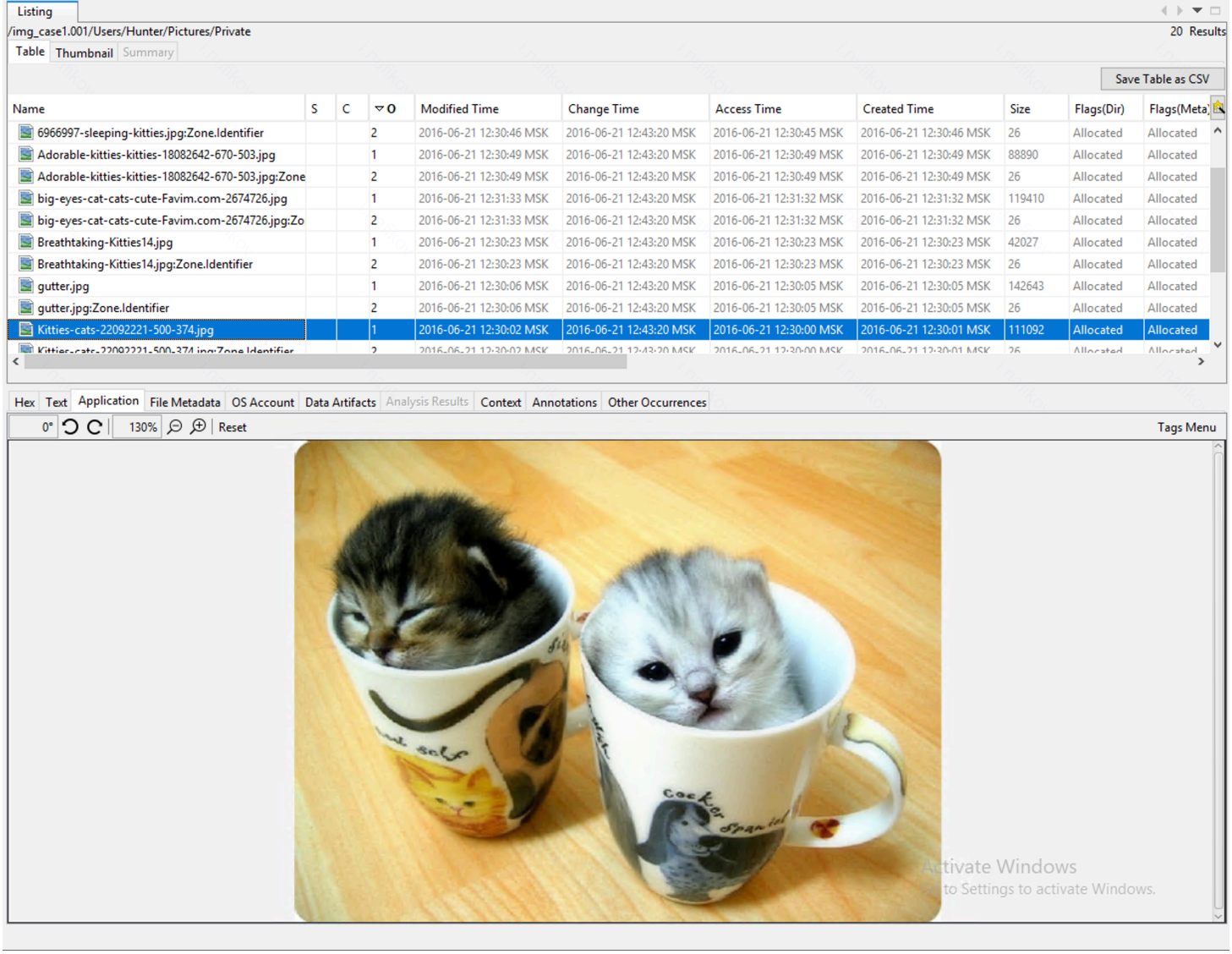
[current folder]

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

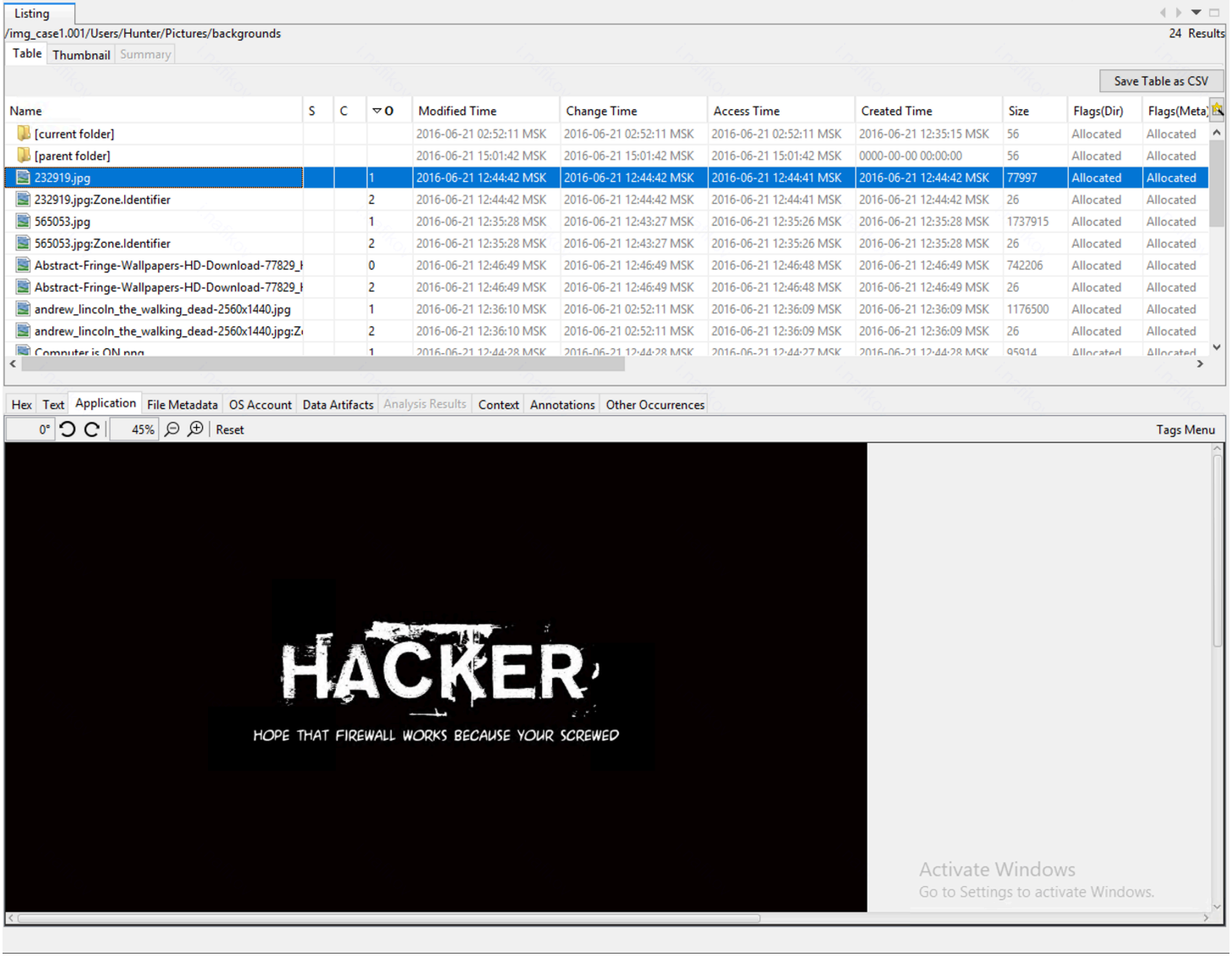
0° | 89% | Reset — Tags Menu



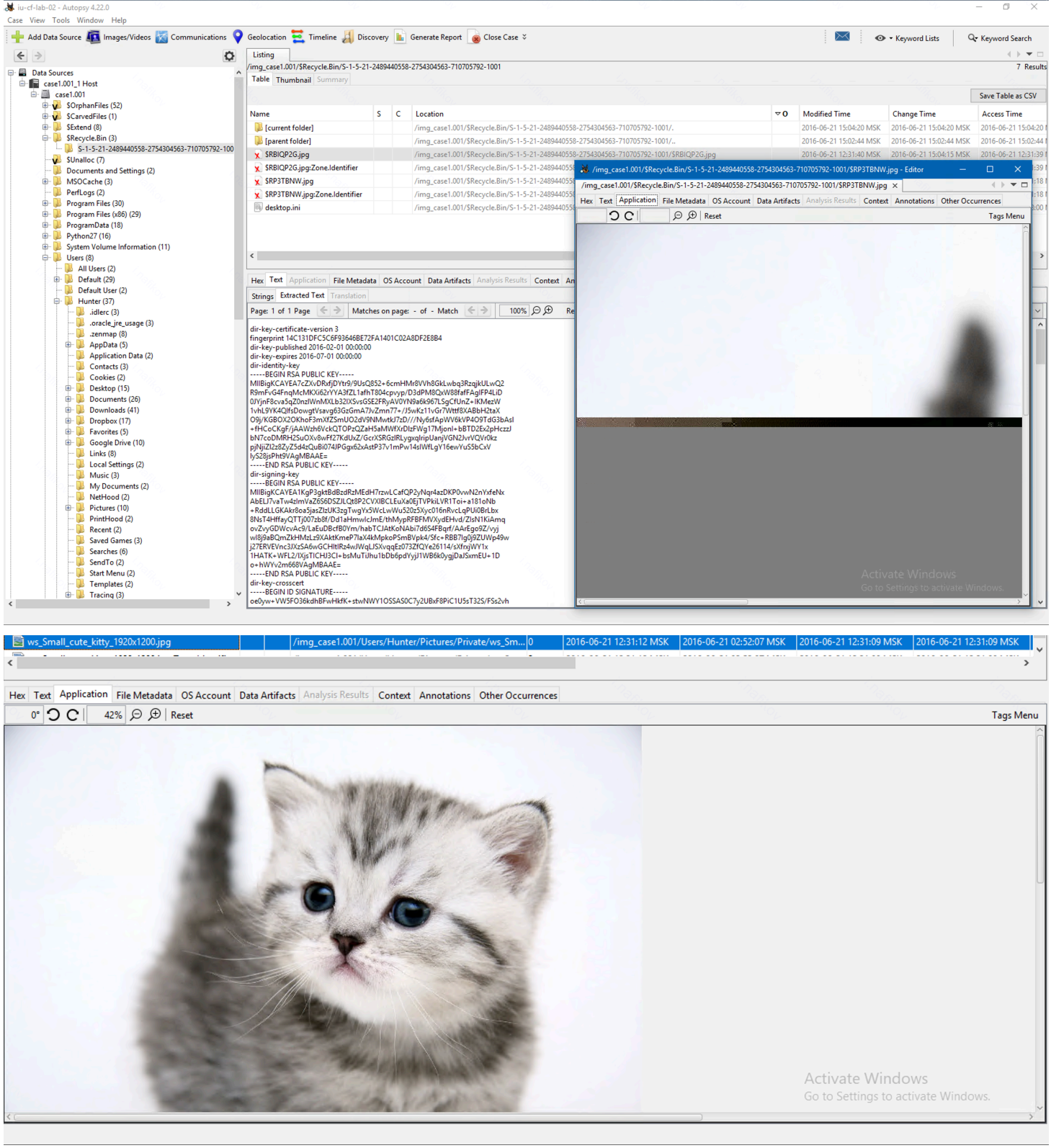
- Inside the `Pictures/Private` there are a log of kittys' photos. Maybe he sent some of them to `linux-r3lz`



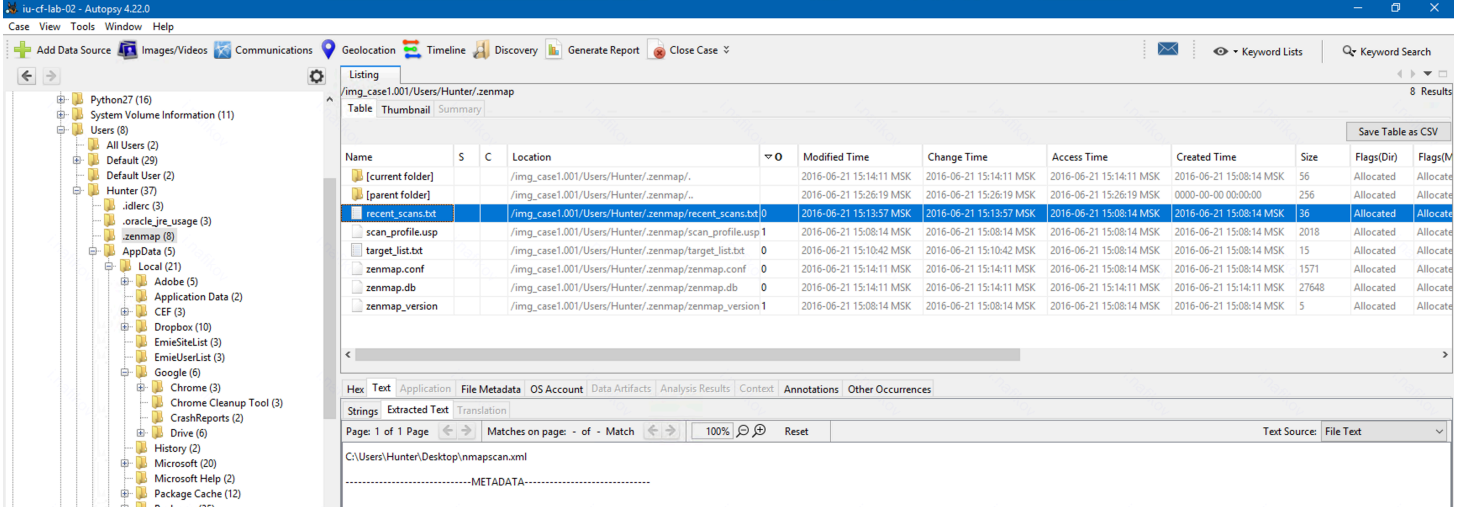
- Inside the `Pictures/background` there a lot of wallpapers on hackers, securityf, Kali Linux and all this stuff

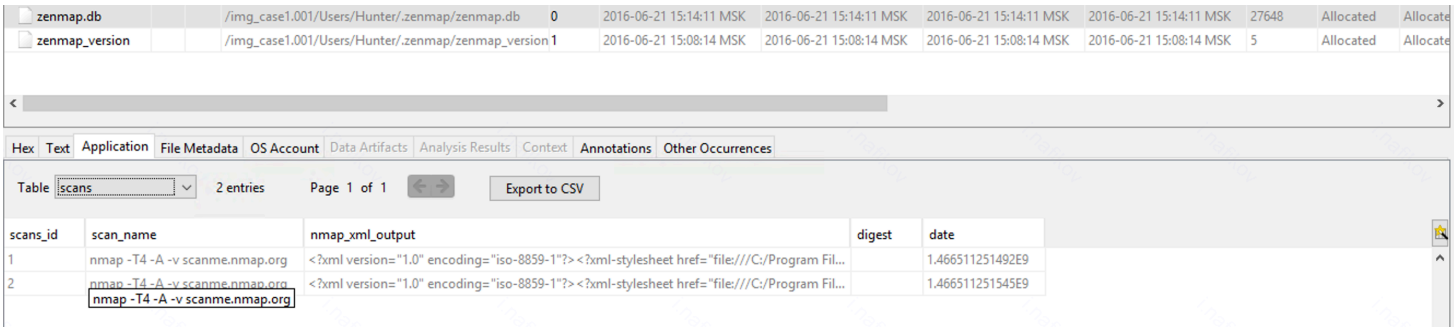


- Inside the Recycle Bin I found two JPG files. One of them was actual corrupted JPG image which copy is still stored inside the `Pictures/Private`, while another file only has `.jpg` extension, but it some file with certificates and public RSA keys for Tor Browser as far as I got (from this `dir-key-certificate-version`).

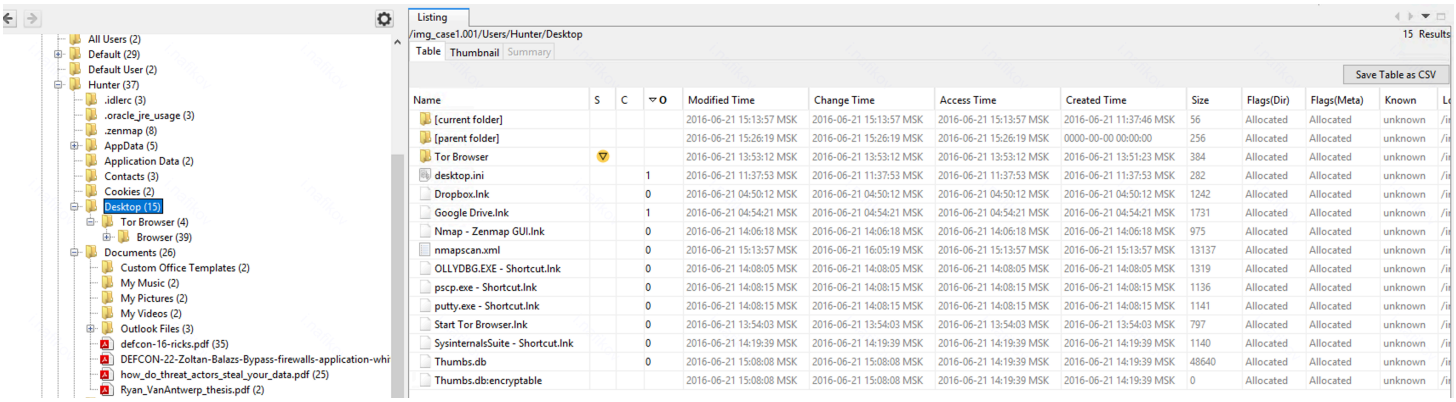


- Also inside the user's folder I found `.zenmap` folder with Zenmap configuration from which I figured out that the version of Zenmap is `7.12`. He scanned only `scanme.nmap.org` for training purposes maybe. I found no traces that he tried to scan his organization's network. The recent scans are saved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

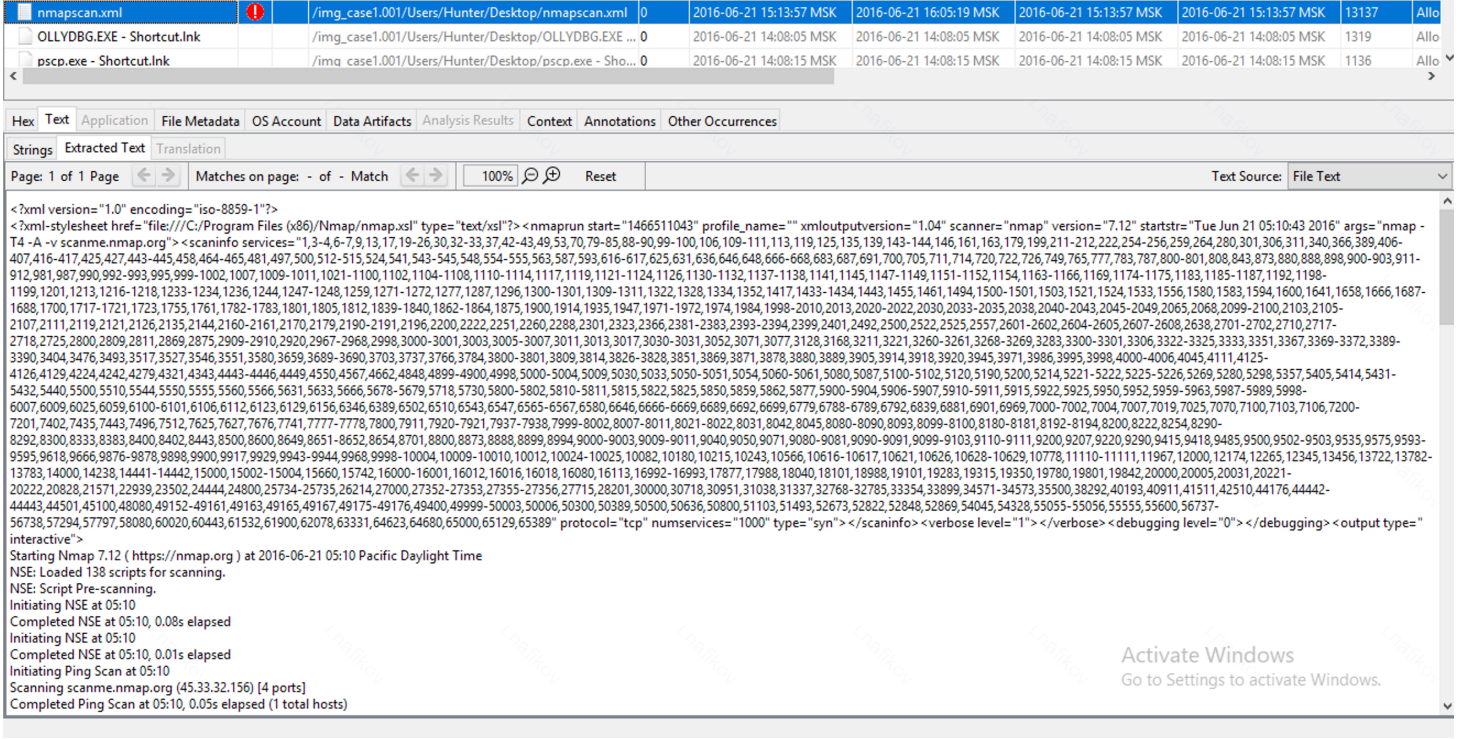




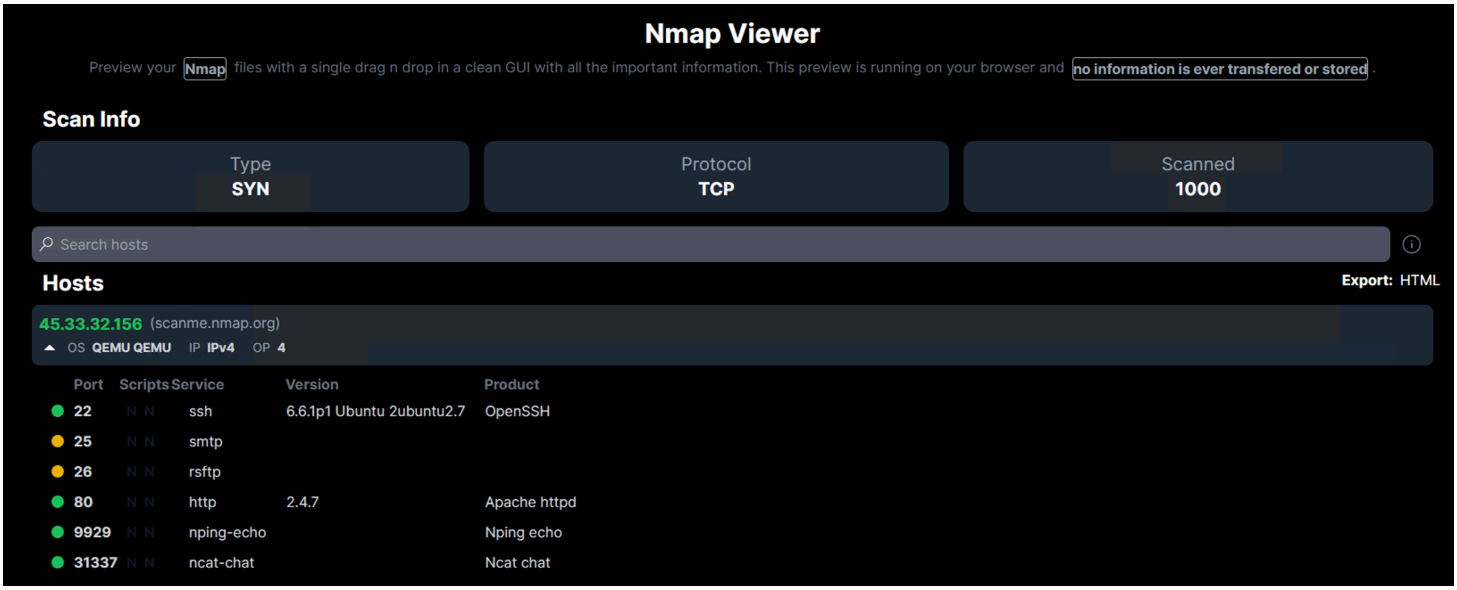
- On the Desktop he had already had all the necessary links 😄

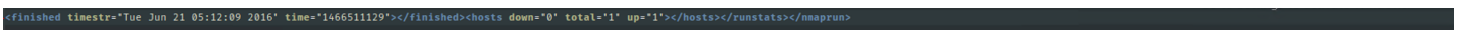


- And bingo! The file `nmapscan.xml` was there. I immediately marked it as highly notable as you can see 😄



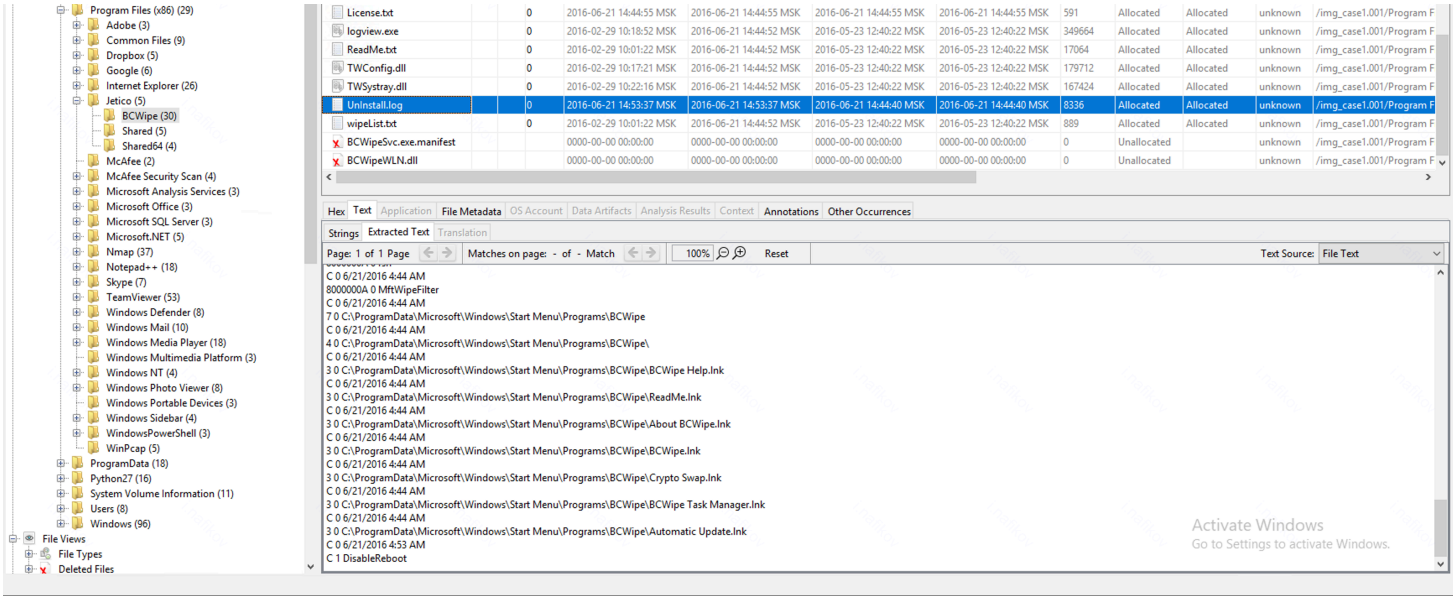
- To see it beautiful I used Onine Nmap Viewer. We can see there which ports, protocols, and clients were available: OpenSSH, SMPT, RSFTP, Apache HTTP, Nping Echo, Ncat. Four of them were open (22, 80, 9929, 31337). There were 1000 ports scanned in total. However, GUI was not so detailed as XML, e.g.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





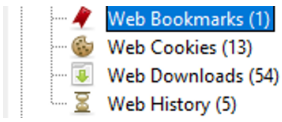
- Since I explored that BCWipe was actually used I thought that the user could use it for deleting files and applications also. So, I decided to check if BCWipe has logs about its actions. Unfortunately but not surprisingly there were no such information. However, BCWipe's directory contained exactly 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

could



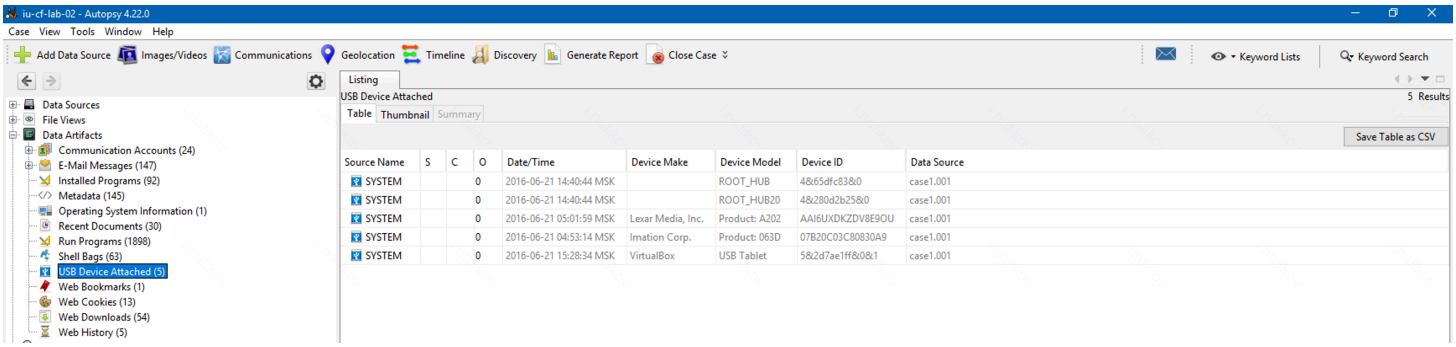
Web history

- 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.



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

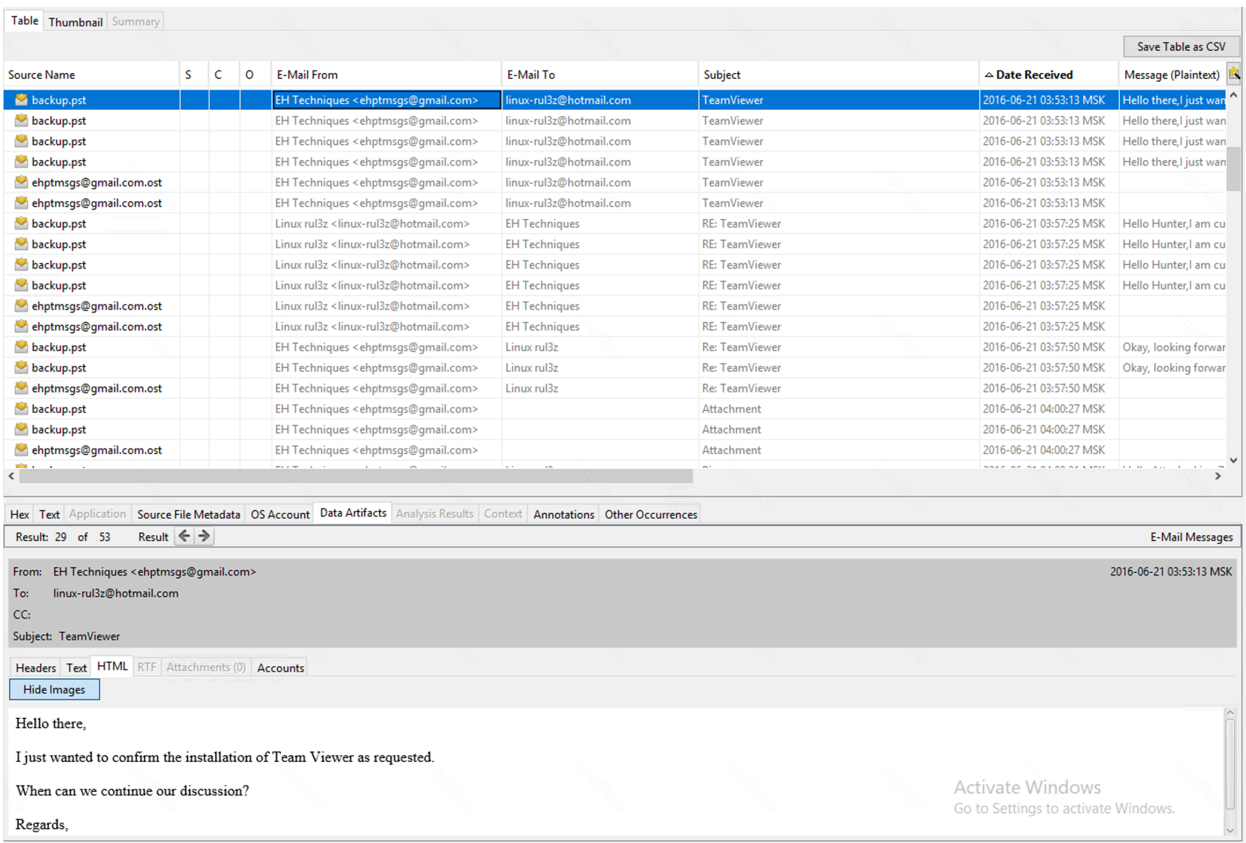
The forensic tools employed in the performance of this investigation were as follows:

- **Forensics analysis and collecting data** - AutoPsy 4.22.0
- Displaying the port scanning results - Nmap Viewer

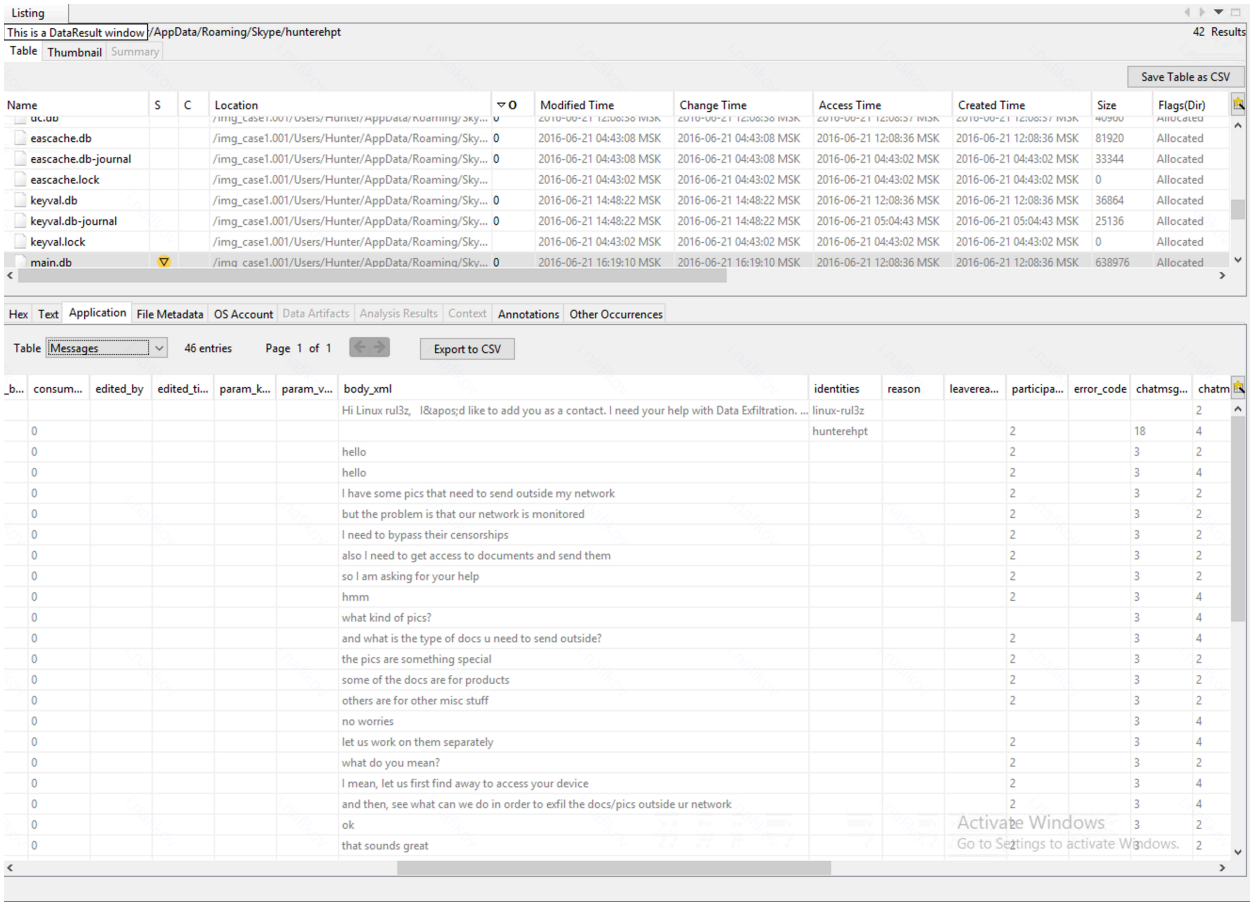
Analysis

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

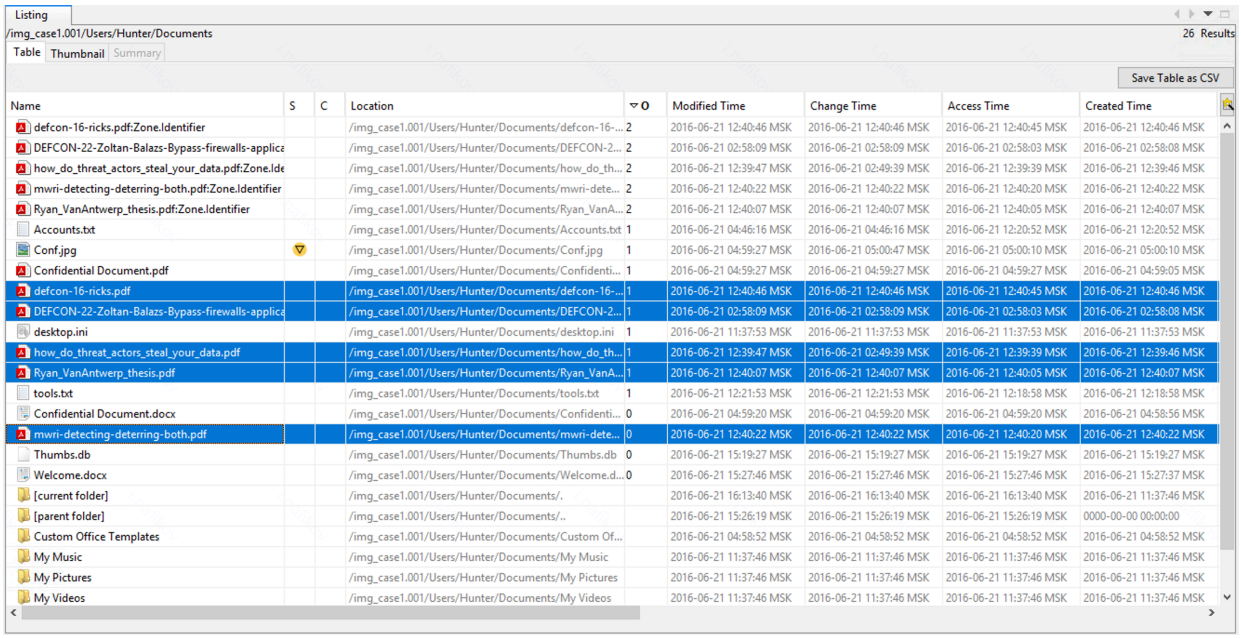
Key	Value
Artifact Name	E-mail conversation with linux-rul3z@hotmail.com
File name	ehptmsgs@gmail.com.ost
File path	/img_case1.001/Users/Hunter/AppData/Local/Microsoft/Outlook/ehptmsgs@gmail.com.ost
Created timestamp	2016-06-21 16:07:07 MSK

Key	Value
Discovering	AutoPsy: Emails
Owner's mail	ehptmsgs@gmail.com
Useful Content	The conversation provides the following information: - 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 conversate 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	

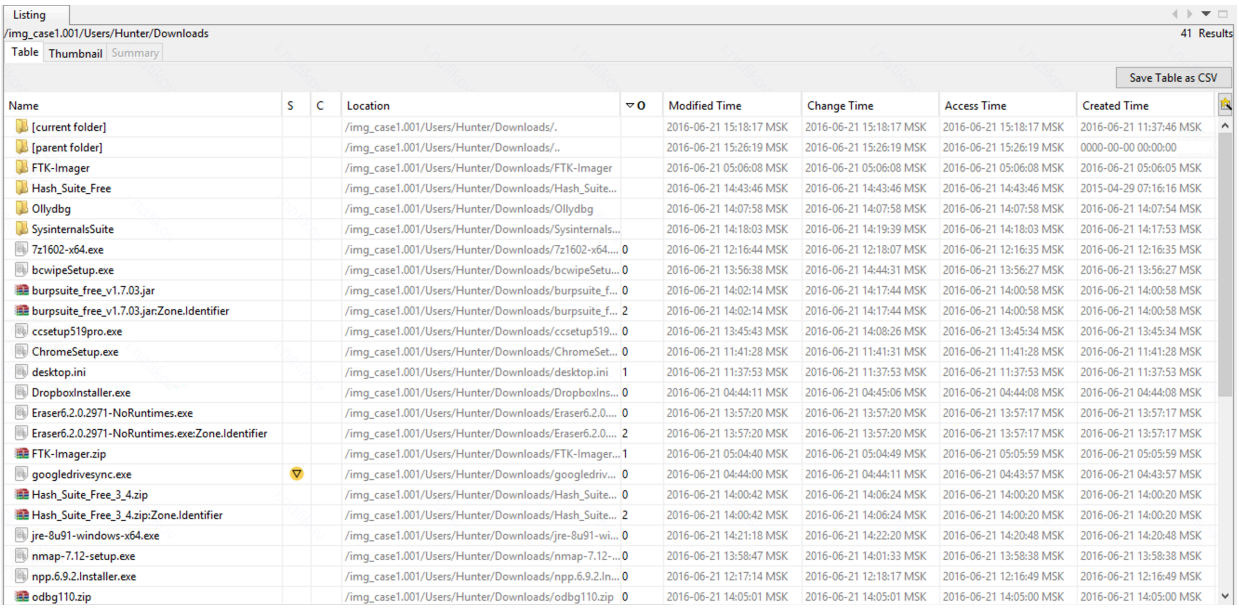
Key	Value
Artifact Name	Skype conversation with linux-rul3z@hotmail.com
File name	main.db
File path	/img_case1.001/Users/Hunter/AppData/Roaming/Skype/hunterehpt/main.db
Created timestamp	2016-06-21 12:08:36 MSK
Discovering	AutoPsy: Data source exploration

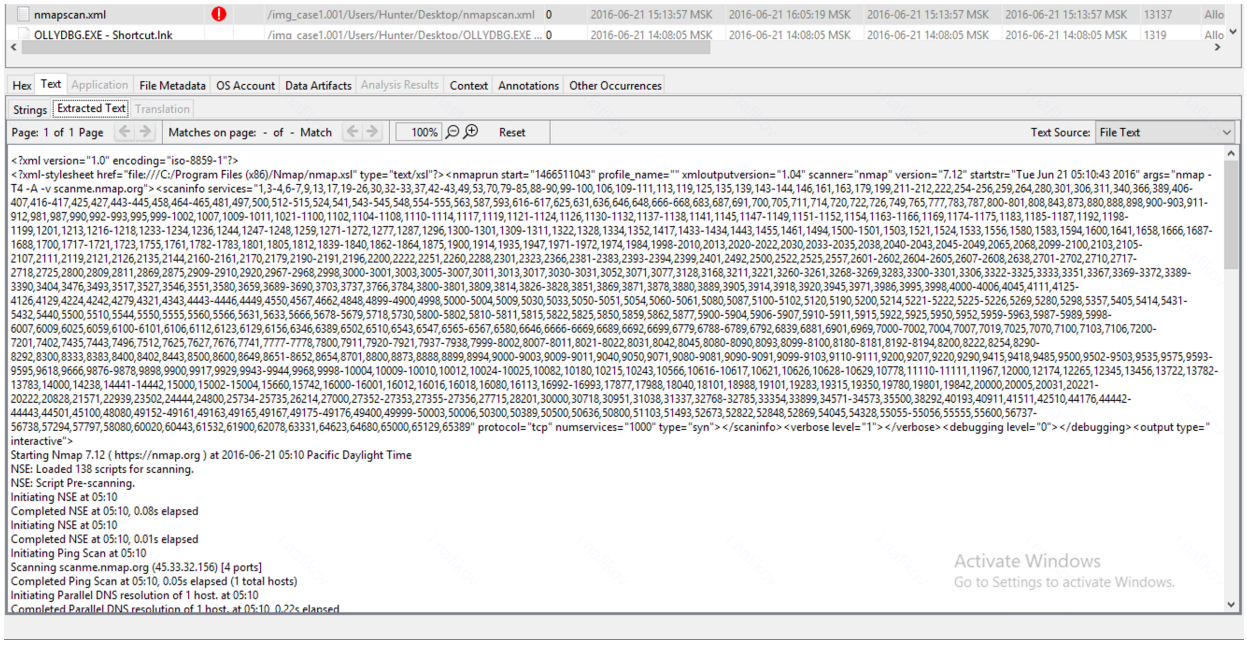
Key	Value
Owner's Skype login	hunterehpt
Useful Content	Hunter asks `linux-rul3z` to help him to transfer some pictures and documents outside an organization's network since it is monitored. This guys agreed to help him and asks if he is able to access Hunter's device remotely via TemViewer. Hunter downloaded TeamViewer and then their conversation goes to e-mail which we already saw.
Screenshot	

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	

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	Installers or executables of the following tools: - 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, firewallbypassing 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.