

CTF Hunter

1-What is the computer name of the suspect machine?

1- من خلال المسار نحمل ملف System

`%Windir%\System32\Config`

Name	Size	Type	Date Modified
DRIVERS.LOG1	12	Regular File	8/22/2013 3:31:28 PM
DRIVERS.LOG2	8	Regular File	8/22/2013 1:25:30 PM
DRIVERSe1e1793794-0b3d-11e3-9dfe-80de...	64	Regular File	6/21/2016 8:18:56 AM
DRIVERSe1e1793794-0b3d-11e3-9dfe-80de...	512	Regular File	6/21/2016 8:18:56 AM
DRIVERSe1e1793794-0b3d-11e3-9dfe-80de...	512	Regular File	6/21/2016 8:18:56 AM
ELAM	8	Regular File	8/22/2013 2:47:12 PM
ELAM.LOG1	8	Regular File	8/22/2013 1:25:30 PM
ELAM.LOG2	0	Regular File	8/22/2013 1:25:30 PM
FP	1	Regular File	8/22/2013 1:25:29 PM
SAM	256	Regular File	6/21/2016 1:34:50 AM
SAM.LOG1	16	Regular File	8/22/2013 1:25:30 PM
SAM.LOG2	8	File Slack	
SAM.LOG1.FileSlack	16	Regular File	8/22/2013 1:25:30 PM
SAM.LOG2.FileSlack	12	File Slack	
SECURITY	256	Regular File	6/21/2016 1:34:50 AM
SECURITY.LOG	0	Regular File	8/22/2013 1:25:30 PM
SECURITY.LOG1	8	Regular File	8/22/2013 1:25:30 PM
SECURITY.LOG1.FileSlack	12	File Slack	
SECURITY.LOG2	8	Regular File	8/22/2013 1:25:30 PM
SECURITY.LOG2.FileSlack	5,192	File Slack	
SOFTWARE	59,136	Regular File	6/21/2016 1:34:50 AM
SOFTWARE.FileSlack	208	File Slack	
SOFTWARE.LOG	0	Regular File	8/22/2013 1:25:30 PM
SOFTWARE.LOG1	21,900	Regular File	8/22/2013 1:25:30 PM
SOFTWARE.LOG2	3,228	Regular File	8/22/2013 1:25:30 PM
SOFTWARE.LOG2.FileSlack	156	File Slack	
SYSTEM	7,680	Regular File	6/21/2016 1:34:50 AM
SYSTEM.FileSlack	0	File Slack	
SYSTEM.LOG	1,720	Regular File	8/22/2013 1:25:30 PM
SYSTEM.LOG1	824	Regular File	8/22/2013 1:25:30 PM
SYSTEM.LOG2			

بعد كذا نفتح Registry Explorer

ونبحث عن اسم الكمبيوتر من خلال هذا المسار !

`\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`

Value Name	Value Type	Data	Data Rec...	Is Deleted	Value Slack
(default)	RegSz	mmsrvvc	<input type="checkbox"/>	<input type="checkbox"/>	02-00-D4-00
ComputerName	RegSz	4ORENSICS	<input type="checkbox"/>	<input type="checkbox"/>	30-00-37-0...

2-What is the computer IP?

ملف الـ Registry ومن ثم System خلال هذا المسار

`\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\`

Value Name	Type	Data	Data Record Reallocated	Is Deleted	Value Slack
DhcpSubnetMask	RegDword	255.255.255.0			
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0			00-00-76-68-00-00
Lease	RegDword	1466475852			

3-What was the DHCP LeaseObtainedTime?

ملف الـ System ومن ثم Registry Explorer خلال هذا المسار

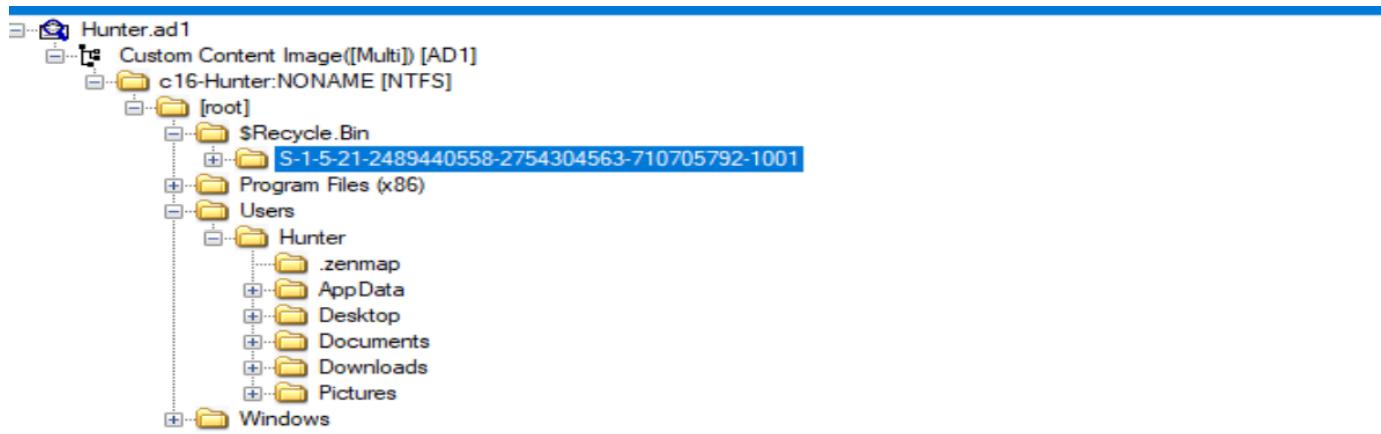
\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\

وما ننسى نحو التاريخ باستخدام Dcoder

Value Name	Type	Data	Data Record Reallocated	Is Deleted	Value Slack
Lease	RegDword	1466475852			

4-What is the computer SID?

من FTK



أو من تحميل ملف Software

Evidence Tree

Name	Type	Date Modified
SECURITY.LOG1.FileStack	File Stack	8/22/2013 1:25:30 PM
SECURITY.LOG2	Regular File	6/21/2016 1:34:50 AM
SOFTWARE	File Slack	59,136
SOFTWARE.FileStack	File Stack	208
SOFTWARE.LOG	Regular File	0
SOFTWARE.LOG1	Regular File	21,900
SOFTWARE.LOG2	Regular File	3,228
SOFTWARE.LOG2.FileStack	File Stack	5,192
SYSTEM	Regular File	6/21/2016 1:34:50 AM
SYSTEM.FileStack	File Stack	7,680
SYSTEM.LOG	Regular File	0
SYSTEM.LOG1	Regular File	1,720
SYSTEM.LOG2	Regular File	624

ومن ثم Registry Explorer خلال هذا المسار

\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser

Registry Explorer v1.5.2.0

Key name	# values	# subkeys	Last write timestamp
BootAnimation	1	0	2013-08-22 15:37:08
ClearAutologon	1	0	2013-08-22 15:37:08
FingerprintLogon	0	1	2013-08-22 15:37:08
PicturePassword	0	0	2013-08-22 15:37:08
PTNLogonEnrollment	0	0	2013-08-22 15:37:08
UserSwitch	2	0	2013-08-22 15:37:08
ValidatedUsername	1	0	2013-08-22 15:37:08
WPSLogon	2	0	2013-08-22 15:37:08
Credential Providers	0	14	2016-06-21 09:34:13
MFDDevices	0	4	2013-08-22 15:37:08
PropertyHandler	0	1	2013-08-22 15:37:08
AppHost	1	3	2013-08-22 15:37:08
AppModel	1	3	2013-08-22 15:37:08
DateTime	0	1	2013-08-22 15:37:08
DeviceAccess	0	5	2013-08-22 15:37:08
EventCollector	0	3	2013-08-22 15:37:08
Uve	0	1	2013-08-22 15:37:08
Syntegr	1	2	2013-08-22 15:37:08
WINEVT	0	3	2013-08-22 15:37:08
GameInstaller	1	0	2013-08-22 15:37:08

Values

Value Name	Type	Data	Data Record Reallocated	Is Deleted	Value Slack
IdleTime	RegDword	90016			
LastLoggedOnProvider	RegSz	{60B7E8B8-EAD8-445C-9C...}			50-61-63-6B-61-67
LastLoggedOnSAMUser	RegSz	.Hunter			BE-01
LastLoggedOnUser	RegSz	Hunter			
LastLoggedOnUserID	RegSz	S-1-5-21-2489440558-2754...			72-00-00-00-61-00-74-00-6F-0...
NetworkStatusType	RegDword	0			
SelectedUserID	RegDword	S-1-5-21-2489440558-2754...			
ShowTabletKeyboard	RegDword	0			

أو من

ProfileList	Count	Created
NetworkList	3	2016-06-21 08:29:53
ProfileList	4	2016-06-21 08:37:45
S-1-5-18	5	2013-08-22 13:25:43
S-1-5-20	3	2013-08-22 14:45:16
S-1-5-19	3	2013-08-22 14:45:17
S-1-5-21-2489440558-27543...	10	2016-06-21 12:29:55
Notifications	51	2016-06-21 08:38:13

Key: Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2489440558-2754304563-710705792-1001
Selected hive: SOFTWARE Last write: 2016-06-21 12:29:55 10 of 10 values shown (100.00%) Load complete

5-What is the Operating System(OS) version?

من ملف Software ومن ثم Registry Explorer خلال هذا المسار

6-What was the computer timezone?

من ملف الـ System ومن ثم Registry Explorer خلال هذا المسار

\System\CurrentControlSet\Control\TimeZoneInformation

The screenshot shows the Registry Explorer interface with the following details:

- Title Bar:** Registry Explorer v1.5.2.0
- Menu Bar:** File, Tools, Options, Bookmarks (26/0), View, Help
- Toolbar:** Enter text to search..., Find
- Left pane (Key list):**
 - Selected key: \Control\TimeZoneInformation
 - Subkeys: WorkplaceJoin, Keyboard Layouts, StorageManagement, NetworkProvider, SecurityProviders, ACPI, CrashControl, EarlyLaunch, MUI, CoDeviceInstallers, StepPort, NetTrace, Notifications, COM Name Arbitrator, MSIPC, Windows, Print, DeviceClasses, usbFlags, DeviceContainers, Hibernation, Video, CMF, TimeZoneInformation, GroupOrderList, GraphicsDrivers, Lsa, ProductOptions, PnP.
 - Values: ActiveTimeBias (RegDword, Value: 420, Raw value: A4-01-00-00)
- Right pane (Value list):**

Value Name	Value Data	Value Data Raw
ActiveTimeBias	420	A4-01-00-00
DaylightBias	-60	
DaylightName	@tzres.dll,-211	@tzres.dll,-211
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:00:00	00-00-08-00-01-00-02-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
Bias	480	480
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:00:00	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	420	420
- Bottom status bar:** Selected hive: SYSTEM | Last write: 2016-06-21 09:14:37 | 10 of 10 values shown (100.00%) | Load complete

The screenshot shows a Google search results page with the following details:

- Search Query:** PST timezone
- Results:**
 - Estimated results: حوالي ١٠٩٠٠,٠٥٧ نتائجة (٠,٥٧ ثانية)
 - Links include: الأدوات, المزيد, فيديو, الأخبار, خرائط Google, صور, الكل.
 - Top result snippet for "Pacific Time Zone" includes:
 - Pacific Time Zone**
 - Pacific Time Zone**
 - UTC offset**
 - UTC-08:00** (PST)
 - UTC-07:00** (PDT)
 - 5 صحف أخرى

7-How many times did this user log on to the computer?

من خلال تحميل ملف SAM

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical view of the 'Hunter.ad1' image, including sub-directories like 'Custom Content Image(Multi) [AD1]', '16-Munter-NONAME [NTFS]', 'Root', 'Program Files (x86)', 'User', 'Hunter', 'Windows', and 'System32'. The File List pane on the right shows a detailed list of files from the 'User\Hunter\SAM' directory, including 'SAM', 'SAM.LOG1', 'SAM.LOG2', 'SAM.LOG2.FileSlack', 'SAM.LOG2.FileSlack', 'SECURITY', 'SECURITY.LOG', 'SECURITY.LOG1', and 'SECURITY.LOG1.FileSlack'. Each entry includes columns for Name, Size, Type, and Date Modified.

Name	Size	Type	Date Modified
ELAM	8	Regular File	8/22/2013 2:47:12 PM
ELAM.LOG1	8	Regular File	8/22/2013 1:25:30 PM
ELAM.LOG2	0	Regular File	8/22/2013 1:25:30 PM
FP	1	Regular File	8/22/2013 1:29:29 PM
SAM	256	Regular File	6/21/2016 1:34:50 AM
SAM.LOG1	16	Regular File	8/22/2013 1:25:30 PM
SAM.LOG1.FileSlack	8	File Slack	
SAM.LOG2	16	Regular File	8/22/2013 1:25:30 PM
SAM.LOG2.FileSlack	12	File Slack	
SECURITY	256	Regular File	6/21/2016 1:34:50 AM
SECURITY.LOG	0	Regular File	8/22/2013 1:25:30 PM
SECURITY.LOG1	8	Regular File	8/22/2013 1:25:30 PM
SECURITY.LOG1.FileSlack	12	File Slack	

ومن ثم Registry Explorer خلال هذا المسار

\SAM\Domains\Account

8-When was the last login time for the discovered account? Format: one-space between date and time?

9-There was a “Network Scanner” running on this computer, what was it? And when was the last time the suspect used it? Format: program.exe.YYYY-MM-DD HH:MM:SS UTC?

```
L="64">></state><service product="Apache httpd" name="httpd" osgen="" accuracy="87"></osclass></osmatch><osmatch id="RAD Data Communications" osgen="" accuracy="87"></osclass><runstats><finished timestr="Tue Jun 21 05:12:09 2016">
```

11-How many ports were scanned?

The screenshot shows the Encase Forensic software interface. The Evidence Tree on the left displays a hierarchical structure of files and folders, including 'Hunter.ad1' and its contents like 'c16-Hunter-NONAME (NTFS)', 'Program Files (x86)', 'Users', and 'Windows'. The 'File List' pane on the right shows a detailed view of files from the 'User' folder, including 'zenmap.conf', 'zenmap.conf.FileSlack', 'zenmap.db', 'zenmap.versi', and 'ZENMAP-1.C'. A context menu is open over 'ZENMAP-1.C', with options like 'Export Files...', 'Export File Hash List...', and 'Add to Custom Content Image (AD1)'. The bottom of the screen shows a memory dump with hex and ASCII data.

```
SQLite format 3 || @  ||  
x || x  
scans_id INTEGER PRIMARY KEY AUTOINCREMENT,  
scan_name TEXT,  
nmap_xml_output TEXT,  
digest TEXT,  
date TINTGFR)  
  
Find  
<?xml-  
<?xml- Find what: 1000| Find Next  
||100,  
||1100,  
||3306, Direction  
||3404, Up  
||36) /Nma  
||36) /Nm  
Match case  
||8002, Down  
||8093, Cancel  
||8099, Wrap around  
||49999  
,1126,  
,3404,  
8093,  
,49999  
Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-21 05  
NSE: Loaded 138 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 05:10  
Completed NSE at 05:10, 0.08s elapsed  
Initiating NSE at 05:10  
Completed NSE at 05:10, 0.01s elapsed  
Initiating Ping Scan at 05:10  
Scanning scanme.nmap.org (45.33.32.156) [4 ports]  
Completed Ping Scan at 05:10, 0.05s elapsed (1 total host)  
Initiating Parallel DNS resolution of 1 host. at 05:10  
Completed Parallel DNS resolution of 1 host. at 05:10, 0  
Initiating SYN Stealth Scan at 05:10  
Scanning scanme.nmap.org (45.33.32.156) [1000]
```

12-What ports were found "open"? (comma-separated, ascending)?

Hunter.ad1

- Custom Content Image(Multi) [AD1]
 - c15-Hunter-NONAME (NTFS)
 - [root]
 - SRecycle.Bin
 - S-1-5-21-248940558-2754304563-710705792-1001
 - Program Files (x86)
 - User
 - Hunter
 - zmap
 - AppData
 - Dropbox
 - Documents
 - Downloads
 - Pictures
 - Windows
 - Prefetch
 - System32
 - config
 - winevt

Properties

Name	nmapscan.xml
File Class	Regular File
File Size	13,137
Physical Size	16,384
Start Cluster	745,340
Date Accessed	6/21/2016 12:13:57 PM
Date Created	6/21/2016 12:13:57 PM
Date Modified	6/21/2016 12:13:57 PM

Name

Name	Type	Date Modified
Tor Browser	1 Directory	6/21/2016 10:53:12 AM
\$10	4 NTFS Index All...	6/21/2016 12:13:57 PM
desktop.ini	1 Regular File	6/21/2016 8:37:53 AM
Dropbox.Ink	2 Regular File	6/21/2016 1:50:12 AM
Google Drive.Ink	2 Regular File	6/21/2016 1:54:21 AM
Google Drive.Ink.FileSlack	3 File Slack	
Nmap - Zenmap GUI.Ink	1 Regular File	6/21/2016 11:06:18 AM
Nmap - Zenmap GUI.Ink.FileSlack	4 File Slack	
nmapscan.xml	13 Regular File	6/21/2016 12:13:57 PM
nmapscan.FileSlack	4 File Slack	
OLLYDBGEXE - Shortcut.Ink	2 Regular File	6/21/2016 11:08:05 AM
pscp.exe - Shortcut.Ink	2 Regular File	6/21/2016 11:08:15 AM
putty.exe - Shortcut.Ink	2 Regular File	6/21/2016 11:08:15 AM

Address

45.33.32.156 - (ipv4)

Hostnames

scannee.nmap.org (user)
scannee.nmap.org (PTR)

Ports

The 994 ports scanned but not shown below are in state: closed

Port	State (tcp filtered {2})	Service	Reason	Product	Version	Extra info
22	tcp open	ssh	syn-ack	OpenSSH	6.6.1p1 Ubuntu 2ubuntu2.7	Ubuntu Linux; protocol 2.0
25	tcp filtered	smtp	no-response			
26	tcp filtered	rsftp	no-response			
80	tcp open	http	syn-ack	Apache httpd	2.4.7	(Ubuntu)
9929	tcp open	nping-echo	syn-ack	Nping echo		
31937	tcp open	ncat-chat	syn-ack	Ncat chat		users: nobody

13-What was the version of the network scanner running on this computer?

Evidence Tree

- Hunter.ad1
 - Custom Content Image([Multi]) [AD1]
 - c16-Hunter:NONAME [NTFS]
 - [root]
 - \$Recycle.Bin
 - S-1-5-21-2489440558-2754304563-710705792-1001
 - Program Files (x86)
 - Users
 - Hunter
 - zenmap
 - AppData
 - Desktop
 - Documents
 - Downloads
 - Pictures
 - Windows
 - Prefetch
 - System32
 - config
 - winevt

File List

Name	Size	Type	Date Modified
\$130	4	NTFS Index All...	6/21/2016 12:14:11 PM
recent_scans.txt	1	Regular File	6/21/2016 12:13:57 PM
scan_profile.usp	2	Regular File	6/21/2016 12:08:14 PM
scan_profile.usp.FileSlack	3	File Slack	
target_list.txt	1	Regular File	6/21/2016 12:10:42 PM
zenmap.conf	2	Regular File	6/21/2016 12:14:11 PM
zenmap.conf.FileSlack	3	File Slack	
zenmap.db	27	Regular File	6/21/2016 12:14:11 PM
zenmap_version	1	Regular File	6/21/2016 12:08:14 PM
ZENMAP~1.CON	\$130	INDX Entry	

7.12

أو من خلال :

Evidence Tree

- Hunter.ad1
 - Custom Content Image([Multi]) [AD1]
 - c16-Hunter:NONAME [NTFS]
 - [root]
 - \$Recycle.Bin
 - S-1-5-21-2489440558-2754304563-710705792-1001
 - Program Files (x86)
 - Users
 - Hunter
 - zenmap
 - AppData
 - Desktop
 - Documents
 - Downloads
 - Pictures
 - Windows
 - Prefetch
 - System32
 - config
 - winevt

File List

Name	Size	Type	Date Modified
Tor Browser	1	Directory	6/21/2016 10:53:12 AM
\$130	4	NTFS Index All...	6/21/2016 12:13:57 PM
desktop.ini	1	Regular File	6/21/2016 8:37:53 AM
Dropbox.lnk	2	Regular File	6/21/2016 1:50:12 AM
Google Drive.lnk	2	Regular File	6/21/2016 1:54:21 AM
Google Drive.lnk.FileSlack	3	File Slack	
Nmap - Zenmap GUI.lnk	1	Regular File	6/21/2016 11:06:18 AM
Nmap - Zenmap GUI.lnk.FileSlack	4	File Slack	
nmapscan.xml	13	Regular File	6/21/2016 12:13:57 PM
nmapscan.xml.FileSlack	4	File Slack	
OLLYDBG.EXE - Shortcut.lnk	2	Regular File	6/21/2016 11:08:05 AM
pscp.exe - Shortcut.lnk	2	Regular File	6/21/2016 11:08:15 AM
putty.exe - Shortcut.lnk	2	Regular File	6/21/2016 11:08:15 AM

Nmap Scan Report - Scanned at Tue Jun 21 05:10:43 2016

Scan Summary | [scanme.nmap.org \(45.33.32.156\)](#)

Scan Summary

Nmap 7.12 was initiated at Tue Jun 21 05:10:43 2016 with these arguments:
nmap -T4 -A -v scanme.nmap.org

Verbosity: 1; Debug level 0

45.33.32.156 / scanme.nmap.org / scanme.nmap.org

Address

45.33.32.156 - (ipv4)

Properties

Name	nmapscan.xml
File Class	Regular File
File Size	13,137
Diskfile Size	16.384

14-The employee engaged in a Skype conversation with someone. What is the skype username of the other party?

S Skyperious - hunttereht\main.db

File Help

Databases C:\Users\asalah\Desktop\Skype\hunttereht\main.db

Database "C:\Users\asalah\Desktop\Skype\hunttereht\main.db": Search in messages: Search for..

All chat entries in database:

Chat	Messages	Created	First message	Last message	Type	People
Linux rul3z	45	2016-06-21	2016-06-21 03:36	2016-06-21 14:48	Single	linux-rul3z
Echo / Sound Test Service	0	2016-06-21			Single	echo123

Chats

Informati...

Data tables

SQL wind...

Online

Find messages with text:

Show messages from time period:

Show messages from:

Apply filter Export filter Restore initial

Chat with Linux rul3z:

03:36 EHPT Msds
EHPT Msds would like to add you on Skype

Hi Linux rul3z, I'd like to add you as a contact. I need your help with Data Exfiltration. Regards, Hunter

03:36 Linux rul3z
Has shared contact details with EHPT Msds.

03:36 EHPT Msds
hello

03:37 Linux rul3z
hello

03:37 EHPT Msds
I have some pics that need to send outside my network

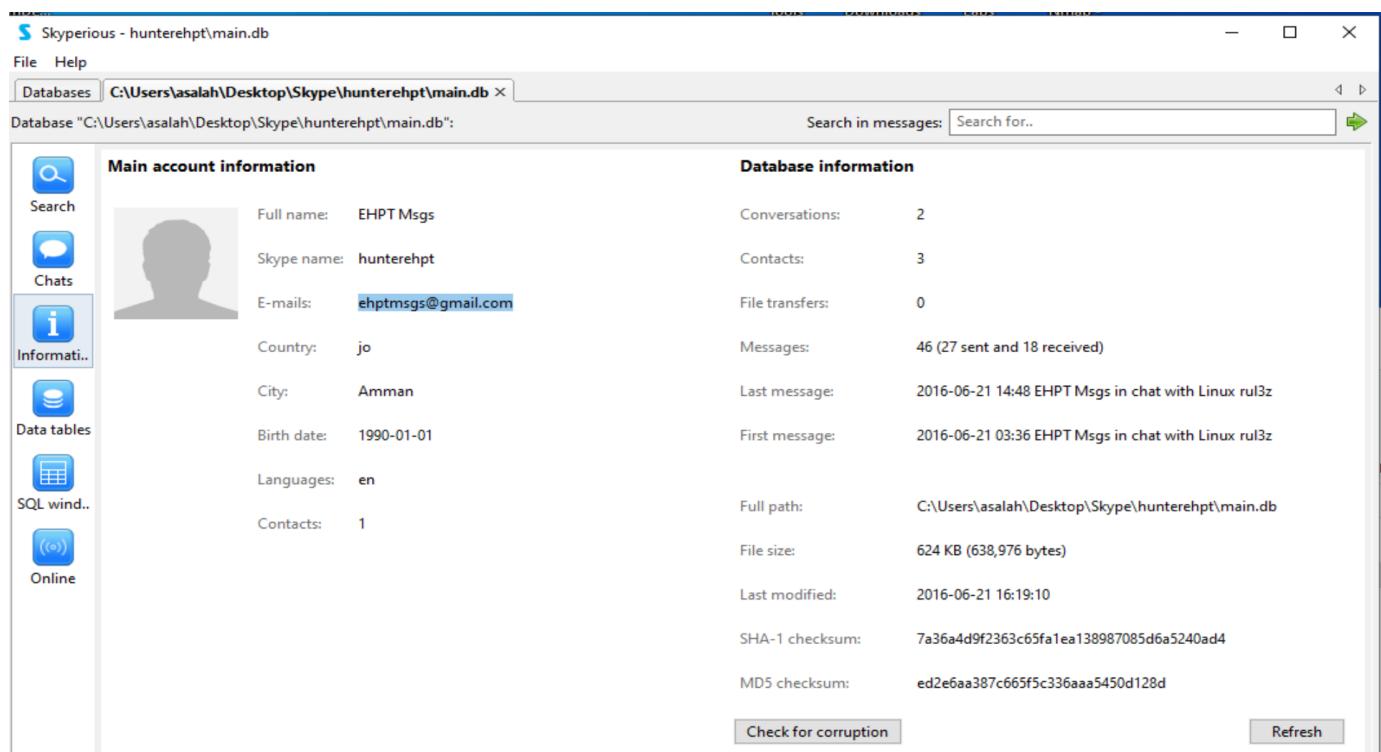
03:37 EHPT Msds

15-What is the name of the application both parties agreed to use to exfiltrate data and provide remote access for the external attacker in their Skype conversation?

03:47 Linux rul3z
can you install team viewer?

03:47 EHPT Msgs
I am not sure

16-What is the Gmail email address of the suspect employee?



The screenshot shows the Skypurious application interface. The main window title is "Skypurious - hunterehpt\main.db". The left sidebar has icons for Search, Chats, Informati.. (selected), Data tables, SQL wind.., and Online. The main area is divided into two sections: "Main account information" and "Database information".

Main account information	Database information
Full name: EHPT Msgs	Conversations: 2
Skype name: hunterehpt	Contacts: 3
E-mails: ehptmsgs@gmail.com	File transfers: 0
Country: jo	Messages: 46 (27 sent and 18 received)
City: Amman	Last message: 2016-06-21 14:48 EHPT Msgs in chat with Linux rul3z
Birth date: 1990-01-01	First message: 2016-06-21 03:36 EHPT Msgs in chat with Linux rul3z
Languages: en	Full path: C:\Users\asalah\Desktop\Skype\hunterehpt\main.db
Contacts: 1	File size: 624 KB (638,976 bytes)
	Last modified: 2016-06-21 16:19:10
	SHA-1 checksum: 7a36a4d9f2363c65fa1ea138987085d6a5240ad4
	MD5 checksum: ed2e6aa387c665f5c336aaa5450d128d

Buttons at the bottom right include "Check for corruption" and "Refresh".

17-It looks like the suspect user deleted an important diagram after his conversation with the external attacker. What is the file name of the deleted diagram?

SysTools Outlook PST Viewer v5.0 - FREEWARE

File Help Add File Load Scan Tag Close File Exit Upgrade to Pro

Switch View

Folder List

- C:\Users\asalah\Desktop\backup.pst
 - IMPRoot
 - Search Root
 - Top of Outlook data file
 - [Gmail]
 - Drafts
 - Important
 - Sent Mail
 - Spam
 - Starred
 - Trash
 - Calendar (This computer only)
 - Contacts (This computer only)
 - Conversation Action Settings
 - Deleted Items
 - Drafts
 - Inbox
 - Journal
 - Journal (This computer only)
 - Notes (This computer only)
 - Outbox
 - Quick Step Settings (This computer only)
 - Sync Issues (This computer only)
 - Local Failures (This computer only)
 - Tasks (This computer only)

Mail Calendar Contacts Tasks Notes Journal Search Folder List

8 items

Trash

From	Subject	To	Sent	Received	Size(KB)
no-reply@accounts.google...	New sign-in from Chrome ...	ehptmsgs@gmail.com;	6/21/2016 2:09:26 AM	6/21/2016 2:09:34 AM	20
no-reply@accounts.google...	Your recovery email address...	ehptmsgs@gmail.com;	6/21/2016 2:01:23 AM	6/21/2016 2:01:29 AM	15
no-reply@accounts.google...	New sign-in from Chrome ...	ehptmsgs@gmail.com;	6/21/2016 2:00:59 AM	6/21/2016 2:01:05 AM	19
ehptmsgs@gmail.com	Attachment		6/21/2016 4:00:27 AM	6/21/2016 4:00:27 AM	1809
ehptmsgs@gmail.com	Attachment		6/21/2016 5:01:15 AM	6/21/2016 5:01:15 AM	333
ehptmsgs@gmail.com	Attachment		6/21/2016 2:50:22 PM	6/21/2016 2:50:22 PM	735
ehptmsgs@gmail.com	Attachment		6/21/2016 3:19:31 PM	6/21/2016 3:19:31 PM	330
aafras@accessdata.com	Don't forget to register for ...	ehptmsgs@gmail.com;	6/3/2016 8:47:20 PM	6/3/2016 8:47:22 PM	11

Normal Mail View Hex Properties Message Header MIME HTML RTF Attachments

Attachment Name Subject Size (KB)

home-network-design.... Attachment 328

18-The user Documents' directory contained a PDF file discussing data exfiltration techniques.
What is the name of the file?

Evidence Tree

Hunter.ad1

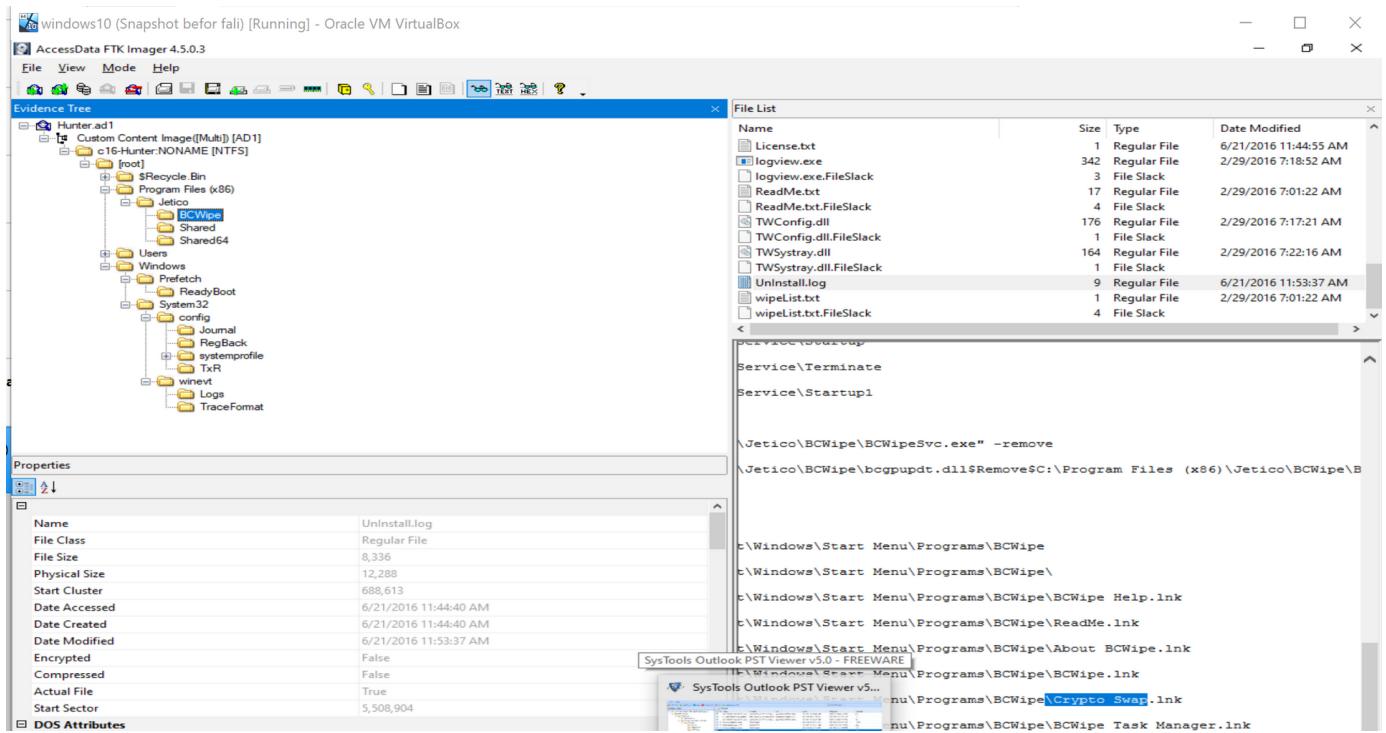
- Custom Content Image[Multi] [AD1]
- c16-Hunter-NONAME [NTFS]
 - Users
 - Hunter
 - AppData
 - Local
 - Documents
 - Custom Office Templates
 - defcon-16-ricks.pdf
 - DEFCON-22-Zoltan-Bypass-firewalls-application-whitelists-in-20-seconds-UPDATED.pdf
 - how_to_threat_actors_stole_your_data.pdf
 - mrvn-detecting-denying both.pdf
 - My Music
 - My Pictures
 - My Videos
 - Outlook Files
 - Ryan_VanAntwerp_thesis.pdf
 - Thumbs.db
 - Downloads
 - Windows
 - Prefetch
 - System32
 - config
 - winevt

File List

Name	Size	Type	Date Modified
Custom Office Templates	1	Directory	6/21/2016 1:59:52 AM
My Music	1	Reparse Point	6/21/2016 8:27:45 AM
My Pictures	1	Reparse Point	6/21/2016 8:37:46 AM
My Videos	1	Reparse Point	6/21/2016 8:37:46 AM
Outlook Files	1	Directory	6/21/2016 1:13:48 PM
\$130	4	NTFS Index All...	6/21/2016 1:13:40 PM
Accounts.txt	1	Regular File	6/21/2016 1:46:16 AM
Conf.jpg	331	Regular File	6/21/2016 1:59:27 AM
Conf.jpg.FileSlack	2	File Slack	
Confidential Document.docx	17	Regular File	6/21/2016 1:59:20 AM
Confidential Document.pdf	331	Regular File	6/21/2016 1:59:27 AM
Confidential Document.pdf.FileSlack	2	File Slack	
defcon-16-ricks.pdf	766	Regular File	6/21/2016 9:40:45 AM
DEFCON-22-Zoltan-Bypass-firewa...	4,073	Regular File	6/20/2016 11:58:09 PM
desktop.ini	1	Regular File	6/21/2016 8:37:53 AM
how_to_threat_actors_stole_your_data.pdf	547	Regular File	6/21/2016 9:39:47 AM
mrvn-detecting-denying both.pdf	1,039	Regular File	6/21/2016 9:40:22 AM
Ryan_VanAntwerp_thesis.pdf	593	Regular File	6/21/2016 9:40:07 AM
Thumbs.db	15	Regular File	6/21/2016 12:19:27 PM
tools.txt	1	Regular File	6/21/2016 9:21:53 AM
Welcome.docx	12	Regular File	6/21/2016 12:27:46 PM
-WRL0005.tmp	\$130	INDX Entry	

Properties

19-What was the name of the Disk Encryption application Installed on the victim system? (two words space separated)



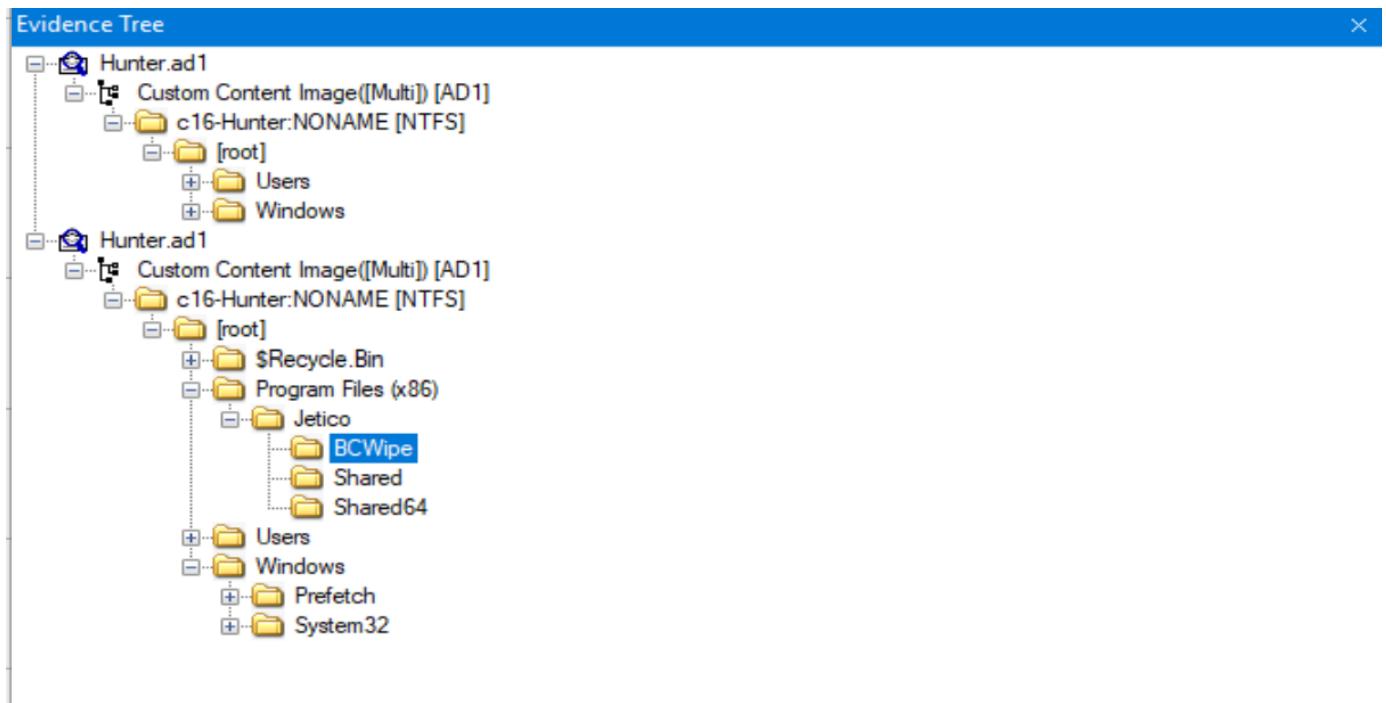
20-What are the serial numbers of the two identified USB storage?

من ملف System Registry Explorer ومن ثم خلال هذا المسار

\SYSTEM\CurrentControlSet\Enum\USB\

	Key name	# values	# subkeys	Last write timestamp
▼	RBC	=	=	=
◀	C:\Users\asalah\Desktop\...			2013-08-22 14:52:2
	Unassociated deleted values	2	0	
	CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}	0	8	2016-06-21 11:40:4
	Select	4	0	2013-08-22 13:25:4
	ControlSet001	0	5	2013-08-22 15:37:0
	Policies	0	0	2013-08-22 15:37:0
	Enum	24	12	2016-06-21 01:53:1
	HTREE	0	1	2013-08-22 14:44:3
	SWD	0	6	2016-06-21 01:53:1
	USB	0	5	2016-06-21 02:01:5
	VID_0718&PID_063D	0	1	2016-06-21 01:53:1
	07B20C03C8083...	11	2	2016-06-21 01:53:1
	VID_05DC&PID_A...	0	1	2016-06-21 02:01:5
	AAI6UXDKZD...	11	2	2016-06-21 02:01:5
	ROOT_HUB20	0	1	2016-06-21 08:14:3
	ROOT_HUB	0	1	2016-06-21 08:14:4
	VID_80EE&PID_0021	0	1	2016-06-21 08:14:4
	USBSTOR	0	2	2016-06-21 02:01:5
	ACPI_HAL	0	1	2016-06-21 08:14:3
	PCI	0	8	2016-06-21 08:14:3
	ACPI	0	9	2016-06-21 08:14:3
	SCSI	0	2	2016-06-21 08:14:3
	ROOT	0	13	2016-06-21 08:14:4
	HID	0	1	2016-06-21 08:14:4
	DISPLAY	0	1	2016-06-21 08:14:5
	STORAGE	0	2	2016-06-21 08:30:5
	Hardware Profiles	0	3	2016-06-21 11:40:4
	Control	11	101	2016-06-21 11:40:4

21-One of the installed applications is a file shredder. What is the name of the application? (two words space separated)?



22-How many prefetch files were discovered on the system?

AccessData FTK Imager 4.5.0.3

Evidence Tree

- Hunter.ad1
 - Custom Content Image([Multi]) [AD1]
 - c16-Hunter:NONAME [NTFS]
 - [root]
 - Users
 - Windows
 - Prefetch
 - System32

Name	Type	Date Modified
ReadyBoot	Directory	6/21/2016 1:42:19 AM
\$130	NTFS Index All..	6/21/2016 1:17:51 PM
7Z1602-X64.EXE-9254A0E7.pf	Regular File	6/21/2016 9:18:15 AM
7Z1602-X64.EXE-9254A0E7.pf.FileSlack	File Slack	
7ZFM.EXE-69B8961D.pf	Regular File	6/21/2016 9:43:06 AM
7ZG.EXE-0F8C4081.pf	Regular File	6/21/2016 11:48:10 AM
7ZG.EXE-0F8C4081.pf.FileSlack	File Slack	
ACRORD32.EXE-ACF2947E.pf	Regular File	6/21/2016 2:00:10 AM
ACRORD32.EXE-ACF2947E.pf.FileSlack	File Slack	
AgAppLaunch.db	Regular File	6/21/2016 8:15:54 AM
AgAppLaunch.db.FileSlack	File Slack	
AgCx_SC4.db	Regular File	6/21/2016 1:43:42 AM

<input checked="" type="checkbox"/> Pcmd	12/26/2021 9:44 AM	File folder
<input checked="" type="checkbox"/> PECmd-master	12/15/2021 8:48 PM	File folder
<input checked="" type="checkbox"/> pestudio	11/14/2021 10:49 AM	File folder

```
C:\Users\asalah\Desktop\Tools\Pcmd>PECmd.exe -d C:\Users\asalah\Desktop\Prefetch
```

```
----- Processed 'C:\Users\asalah\Desktop\Prefetch\ZENMAP.EXE-56B17C4C.pf' in 0.04484180 seconds -----
Processed 174 out of 174 files in 7.2692 seconds
```

23-How many times was the file shredder application executed?

AccessData FTK Imager 4.5.0.3

Evidence Tree

File List

Properties

Browse For Folder

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left displays two entries: 'Hunter.ad1' and 'Hunter.ad1'. The 'Hunter.ad1' entry has two sub-folders: 'c16-Hunter:NONAME [NTFS]' and 'c16-Hunter:NONAME [AD1]'. The 'c16-Hunter:NONAME [AD1]' folder contains several sub-folders like 'root', 'Users', and 'Windows'. The File List pane on the right shows a list of files with columns for Name, Size, Type, and Date Modified. A 'Browse For Folder' dialog is open in the center, prompting to 'Select the destination folder' with options like Desktop, OneDrive, This PC, Libraries, Network, and Ali. The Properties pane shows details for a selected file: Name (BCWIPE.EXE-36F3F2DF.pf), File Class (Regular File), and File Size (72,524).

```
C:\Users\asalah\Desktop\Tools\Pcmd>PECmd.exe -f "C:\Users\asalah\Desktop\BCWIPE.EXE-36F3F2DF.pf"
PECmd version 1.4.0.0
```

```
Executable name: BCWIPE.EXE
Hash: 36F3F2DF
File size (bytes): 72,524
Version: Windows 8.0, Windows 8.1, or Windows Server 2012(R2)

Run count: 5
Last run: 2016-06-21 12:02:35
Other run times: 2016-06-21 12:02:39, 2016-06-21 12:01:35, 2016-06-21 12:01:00, 2016-06-21 12:00:56

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 669B1B2A Created: 2016-06-21 09:09:24 Directories: 14 File references: 84
#1: Name: \DEVICE\HARDDISKVOLUMESHADOWCOPY1 Serial: 669B1B2A Created: 2016-06-21 09:09:24 Directories: 0 File references
: 0
#2: Name: \DEVICE\HARDDISKVOLUMESHADOWCOPY2 Serial: 669B1B2A Created: 2016-06-21 09:09:24 Directories: 0 File references
: 0
```

24-Using prefetch, determine when was the last time ZENMAP.EXE-56B17C4C(pf) was executed?

```
C:\Users\asalah\Desktop\Tools\Pcmd>PECmd.exe -f "C:\Users\asalah\Desktop\ZENMAP.EXE-56B17C4C.pf"
PECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Users\asalah\Desktop\ZENMAP.EXE-56B17C4C.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing 'C:\Users\asalah\Desktop\ZENMAP.EXE-56B17C4C.pf'

Created on: 2016-06-21 12:08:21
Modified on: 2016-06-21 12:08:21
Last accessed on: 2021-12-27 09:02:09

Executable name: ZENMAP.EXE
Hash: 56B17C4C
File size (bytes): 93,524
Version: Windows 8.0, Windows 8.1, or Windows Server 2012(R2)

Run count: 1
Last run: 2016-06-21 12:08:13
```

25-A JAR file for an offensive traffic manipulation tool was executed. What is the absolute path of the file?

The screenshot displays the EnCase Forensic software interface with two main panes: the Evidence Tree and the File List.

Evidence Tree:

- Hunter.ad1
 - Custom Content Image([Multi]) [AD1]
 - c16-Hunter.NONAME [NTFS]
 - [root]
 - Users
 - Hunter
 - Windows
- Hunter.ad1
 - Custom Content Image([Multi]) [AD1]
 - c16-Hunter.NONAME [NTFS]
 - [root]
 - \$Recycle.Bin
 - S-1-5-21-2489440558-2754304563-710705792-1001
 - Program Files(x86)
 - Jetico
 - BCWipe
 - Shared
 - Shared64
 - Users
 - Hunter
 - zenmap
 - AppData

26-The suspect employee tried to exfiltrate data by sending it as an email attachment. What is the name of the suspected attachment?

windows10 (Snapshot befor fail) [Running] - Oracle VM VirtualBox

SysTools Outlook PST Viewer v5.0 - FREEWARE

File Help

Add File Load Scan Tag Close File Exit Upgrade to Pro

Switch View

Folder List

C:\Users\asalah\Desktop\backup.pst

- Backup.pst
- IMPRoot
 - Search Root
 - Top of Outlook data file
 - [Gmail]
 - Drafts
 - Important
 - Sent Mail
 - Spam
 - Starred
 - Trash
 - Calendar (This computer only)
 - Contacts (This computer only)
 - Conversation Action Settings
 - Deleted Items
 - Drafts
 - Inbox
 - Journal
 - Journal (This computer only)
 - Notes (This computer only)
 - Outbox
 - Quick Step Settings (This computer only)
 - RSS Feeds
 - Sync Issues (This computer only)
 - Local Failures (This computer only)
 - Tasks (This computer only)

Sent Mail

From	Subject	To	Sent	Received	Size(KB)
ehptmsgs@gmail.com	TeamViewer	linux-rul3z@hotmail.com;	6/21/2016 3:53:13 AM	6/21/2016 3:53:13 AM	4
ehptmsgs@gmail.com	Re: TeamViewer	Linux rul3z <linux-rul3z@hot...	6/21/2016 3:57:50 AM	6/21/2016 3:57:50 AM	6
ehptmsgs@gmail.com	Pics	Linux rul3z <linux-rul3z@hot...	6/21/2016 4:00:51 AM	6/21/2016 4:00:51 AM	1810
ehptmsgs@gmail.com	Re: File Extensions	Linux rul3z <linux-rul3z@hot...	6/21/2016 4:57:53 AM	6/21/2016 4:57:53 AM	5
ehptmsgs@gmail.com	Re: File Extensions	Linux rul3z <linux-rul3z@hot...	6/21/2016 5:01:17 AM	6/21/2016 5:01:17 AM	338
ehptmsgs@gmail.com	Hangouts?	linux-rul3z@gmail.com;	6/21/2016 2:32:14 PM	6/21/2016 2:32:14 PM	3
ehptmsgs@gmail.com	Nice Pics	Linux rul3z <linux-rul3z@hot...	6/21/2016 2:50:24 PM	6/21/2016 2:50:24 PM	737
ehptmsgs@gmail.com	Re: DNS Exfil Videos	Linux rul3z <linux-rul3z@hot...	6/21/2016 2:51:04 PM	6/21/2016 2:51:04 PM	6
ehptmsgs@gmail.com	Re: DNS Exfil Videos	Linux rul3z <linux-rul3z@hot...	6/21/2016 2:57:47 PM	6/21/2016 2:57:47 PM	9
ehptmsgs@gmail.com	Network Design	Linux rul3z <linux-rul3z@hot...	6/21/2016 3:19:33 PM	6/21/2016 3:19:33 PM	333
ehptmsgs@gmail.com	Microsoft Outlook Test Me...	EHPH <ehptmsgs@gmail.co...	6/21/2016 4:12:22 PM	6/21/2016 4:12:22 PM	4

Normal Mail View Hex Properties Message Header MIME HTML RTF Attachments

Date Time : 6/21/2016 4:00:31 AM

Path : \backup.pst\IMPRoot\Top of Outlook data file\[Gmail]\Sent Mail

From : ehptmsgs@gmail.com

To : Linux rul3z <linux-rul3z@hotmail.com>

Cc :

Bcc :

Subject : Pics

Attachment(s) : Pictures.7z

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,
Hunter

27-Shellbags shows that the employee created a folder to include all the data he will exfiltrate.

What is the full path of that folder?

The screenshot shows the BCWipe interface. The Evidence Tree pane on the left displays a directory structure under a user account named 'Hunter'. The File List pane on the right shows a list of files with columns for Name, Size, Type, and Date Modified. The 'Exfil' folder is highlighted in blue in the file list.

Name	Size	Type	Date Modified
backgrounds	1	Directory	6/20/2016 11:52:2
Exfil	1	Directory	6/21/2016 9:38:1
Private	1	Directory	6/21/2016 12:04:1
\$I30	4	NTFS Index All...	6/21/2016 12:01:1
desktop.ini	1	Regular File	6/21/2016 8:37:5
mofygvdh.mcp	0	Regular File	4/30/1986 11:43:3
Thumbs.db	160	Regular File	6/21/2016 9:37:3

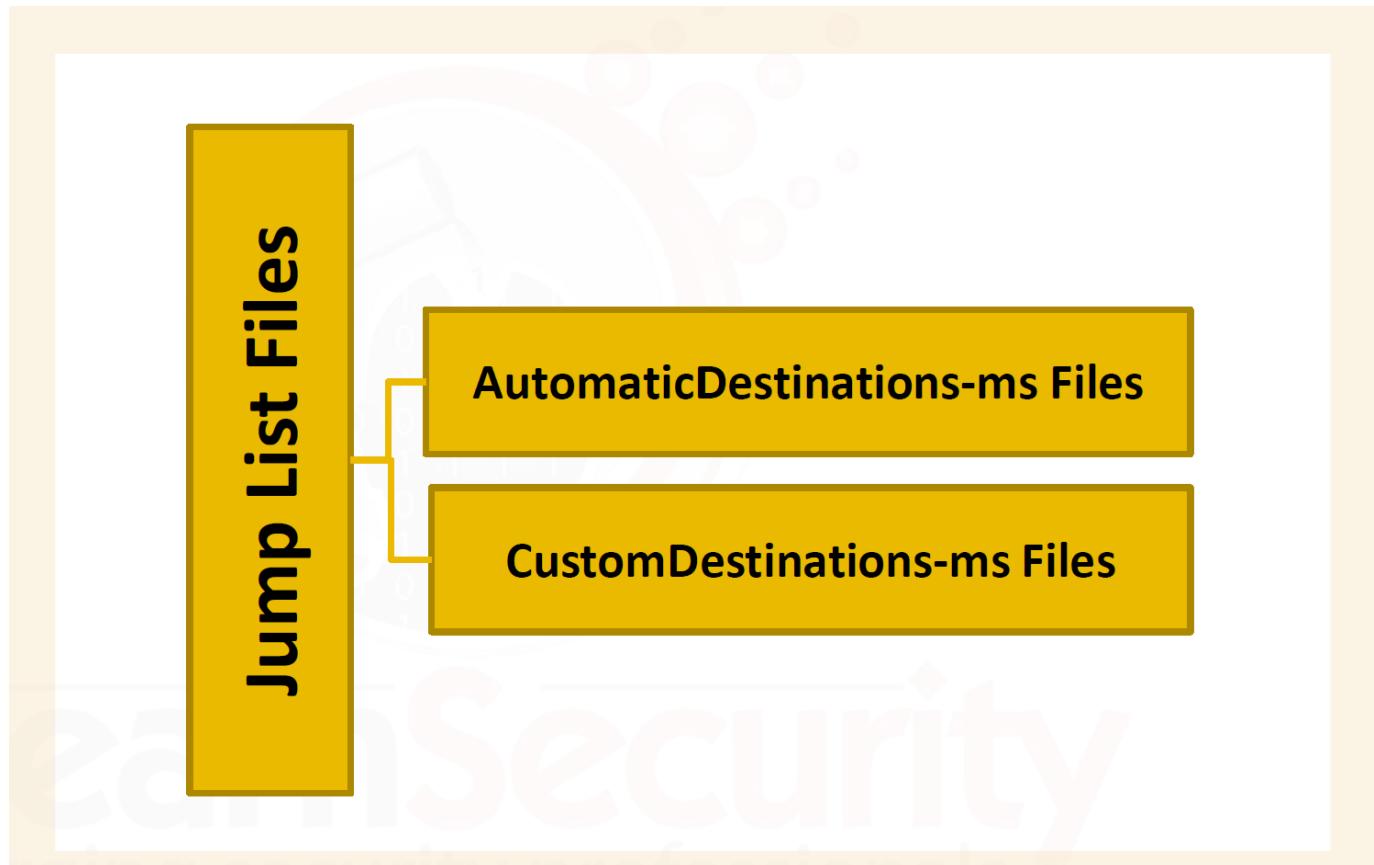
28-The user deleted two JPG files from the system and moved them to \$Recycle-Bin. What is the file name that has the resolution of 1920x1200?

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left shows a file system structure. The File List pane on the right shows a list of files with columns for Name, Size, Type, and Date Modified. A preview window on the right displays a small kitten image.

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	6/21/2016 12:04:15 PM
6966997-sleeping-kitties.jpg	972	Regular File	6/21/2016 9:30:46 AM
Adorable-kitties-kitties-18082642-670-50...	87	Regular File	6/21/2016 9:30:49 AM
big-eyes-cat-cats-cute-Favim.com-2674...	117	Regular File	6/21/2016 9:31:33 AM
Breathtaking-Kitties14.jpg	42	Regular File	6/21/2016 9:30:23 AM
gutter.jpg	140	Regular File	6/21/2016 9:30:06 AM
Kitties-cats-22092221-500-374.jpg	109	Regular File	6/21/2016 9:30:02 AM
slide-cat-laying-down.png	329	Regular File	6/21/2016 9:29:58 AM
Thumbs.db	175	Regular File	6/21/2016 12:03:40 PM
ws_Small_cute_kitty_1920x1200.jpg	381	Regular File	6/21/2016 9:31:12 AM

29-Provide the name of the directory where information about jump lists items (created automatically by the system) is stored?

AutomaticDestinations-ms



30-Using JUMP LIST analysis, provide the full path of the application with the AppID of "aa28770954eaaaaa" used to bypass network security monitoring controls?

\AppData\Roaming\Microsoft\Windows\

AccessData FTK Imager 4.5.0.3

Evidence Tree

File List

Name	Size	Type	Date Modified
AutomaticDestinations	1	Directory	6/21/2016 12:27:37 PM
CustomDestinations	1	Directory	6/21/2016 1:12:35 PM
\$100	16	NTFS Index All...	6/21/2016 1:05:19 PM
00.jpg.lnk	4	Regular File	6/21/2016 11:47:42 AM
00.jpg.lnk.FileSlack	1	File Slack	6/21/2016 11:46:45 AM
150902_WILD_CutePenguins.jpg.CROP.pr...	4	Regular File	6/21/2016 11:46:57 AM
150902_WILD_CutePenguins.jpg.CROP.pr...	1	File Slack	6/21/2016 11:46:57 AM
608d733d64d0cd8080a087adb8278c7.jpg....	4	Regular File	6/21/2016 11:46:16 AM
63bb616a33fc209cd3a48795c981f46d.jpg....	4	Regular File	6/21/2016 11:46:16 AM
AUTOMA-1	\$130	INDEX Entry	
backup.pst.lnk	1	Regular File	6/21/2016 1:15:00 PM
backup.pst.lnk.FileSlack	4	File Slack	6/21/2016 11:46:39 AM
Beautiful-Pictures-Of-Cute-Animals-6.jp...	4	Regular File	6/21/2016 11:17:44 AM
bursuite_free_v1.7.03.jar.lnk	1	Regular File	6/21/2016 11:17:44 AM
catt-cute-animals-cute-catt-hamster-rab...	4	Regular File	6/21/2016 11:46:53 AM
cute-baby-animals-3.jpg.lnk	4	Regular File	6/21/2016 11:47:47 AM
defcon-16-ricks.lnk	3	Regular File	6/20/2016 11:51:29 PM
defcon-16-ricks.lnk.FileSlack	2	File Slack	6/20/2016 11:51:29 PM
DEFCON-22-Zoltan-Balazs-Bypass-firewa...	3	Regular File	6/20/2016 11:58:09 PM
DEFCON-22-Zoltan-Balazs-Bypass-firewa...	\$130	INDEX Entry	
desktop.ini	1	Regular File	6/21/2016 8:37:53 AM
dns-exfiltration-using-sqlmap-18-728.jp...	4	Regular File	6/21/2016 12:17:39 PM
Downloads.lnk	1	Regular File	6/21/2016 11:17:44 AM
Exfil.lnk	2	Regular File	6/21/2016 12:17:42 PM
Exfil.lnk.FileSlack	3	Regular File	6/21/2016 9:38:13 AM
Exfiltration_Diagram.lnk	3	Regular File	6/21/2016 8:37:49 AM
Exfiltration_Diagram.png.lnk.FileSlack	4	Regular File	6/21/2016 12:17:42 PM
Exfiltration_Diagram.png.lnk	1	File Slack	6/21/2016 11:47:42 AM
fakeporn.7z.lnk	3	Regular File	6/21/2016 11:50:29 AM

Properties

Name: CustomDestinations

JumpList Explorer v1.3.3.0

File Tools Help

Drag a column header here to group by that column

Source File Name	Jump List Type	App ID	App ID Description	Link File Count	File Size
C:\Users\asalah\Desktop\CustomDestinations\28...	Custom	28c8b86deab549a1	Internet Explorer 8.0.7600.16385 / 9	3	5,062
C:\Users\asalah\Desktop\CustomDestinations\74...	Custom	74ea779831912e30	Skype 7.24.0.104	2	2,666
C:\Users\asalah\Desktop\CustomDestinations\92...	Custom	92586431a03f316d	Unknown AppId	1	1,837
C:\Users\asalah\Desktop\CustomDestinations\aa...	Custom	aa28770954eaeaaa	Unknown AppId	3	5,212
C:\Users\asalah\Desktop\CustomDestinations\ccc...	Custom	cc0fa1b9f86f7b3	CCleaner 5.15.5513 64-bit	6	8,450

Drag a column header here to group by that column

Name	Value
aa28770954eaeaaa.customDestinations-ms	
Link #: 000 - Tor Browser\Browser\firefox.exe	
Link #: 001 - Tor Browser\Browser\firefox.exe	
Link #: 002 - Tor Browser\Browser\firefox.exe	
Name	
TargetCreationDate	2000-01-01 00:00:00
TargetModificationDate	2000-01-01 00:00:00
TargetLastAccessedDate	2016-06-21 10:51:23
Header.DataFlags	HasTargetIdList, HasLinkInfo, HasName, HasArguments, HasIconLocation, IsUnicode, DisableKnownFolder...
Header.FileAttributes	FileAttributeArchive
Header.FileSize	336,896
Header.IconIndex	3
Header.ShowWindow	SwNormal
Absolute path	Tor Browser\Browser\firefox.exe
Arguments	-new-tab about:blank
CommonPath	Hunter\Desktop\Tor Browser\Browser\firefox.exe
IconLocation	C:\Users\Hunter\Desktop\Tor Browser\Browser\firefox.exe
LocalPath	C:\Users\
Name	Open a new browser tab.
NetworkShareInfo.NetworkShareName	\VORNENSCS\Users
NetworkShareInfo.NetworkProviderType	WmflNetLanman
NetworkShareInfo.ShareFlags	ValidNetType
NetworkShareInfo.Size	38
LocationFlags	VolumeIdAndLocalBasePath, CommonNetworkRelativeLinkAndPathSuffix

Properties

AsalahMohammed..