

Friday, 17 June, 2022 10:13 PM

AccessData Registry Viewer (Demo Mode) - [SYSTEM]

File Edit Report View Window Help

svrpr  
Synth3dVnc  
SysMain  
SystemEventsBroker  
TabletInputService  
TapSrv  
Tcpip  
Linkage  
Parameters  
Adapters  
(8718928D-CBEB-43EA-A621-800A9249001D)  
(BCB9BF6-AE23-4E1C-AA0A-E23CBAFE736)  
DNFRegisteredAdapters  
Interfaces  
(8718928D-CBEB-43EA-A621-800A9249001D)  
(BCB9BF6-AE23-4E1C-AA0A-E23CBAFE736)  
(bbed3a08-0b41-11e4-8249-806e0f6e963)  
NioObjectSecurity  
PersistentRoutes  
Winsock  
Performance  
Security  
ServiceProvider  
TCP/IP6  
TCP/IP6TUNNEL

Name	Type	Data
UseZeroB...	REG_DWORD	0x00000000 (0)
EnableDead...	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
Registration...	REG_DWORD	0x00000001 (1)
RegisterAda...	REG_DWORD	0x00000000 (0)
DhcpPAddr...	REG_SZ	10.0.2.15
DhcpSubnet...	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	10.0.2.2
Lease	REG_DWORD	0x00011180 (86400)
LeaseObtain...	REG_DWORD	0x5768A54C (1466475852)
T1	REG_DWORD	0x5768A54C (1466475852)
T2	REG_DWORD	0x5768C9C (1466551452)
LeaseTermin...	REG_DWORD	0x5768F6CC (1466562352)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNap...	REG_DWORD	0x00000000 (0)
DhcpConnF...	REG_DWORD	0x00000000 (0)
DhcpNameS...	REG_SZ	10.0.2.3
DhcpDefault...	REG_MULTI_SZ	10.0.2.2
DhcpSubnet...	REG_MULTI_SZ	255.255.255.0
DhcpInterfa...	REG_BINARY	FC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0C 4E ...

Key Properties  
Last Written Time: 21/6/2016 2:34:12 UTC

#4 What is the computer SID? S-1-5-21-2489440558-2754304563-710705792  
A computer's SID is stored in the Registry's SECURITY hive under HKLM\SECURITY\SAM\Domains  
\Account.  
S-1-5-21-2489440558-2754304563-710705792

Registry Explorer V1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry Hives (7) Available bookmarks (113/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\SANSDFIR\Desktop\c16-Hunter\SYSTEM_clean	...	...	2013-08-22 14:52:22
C:\Users\SANSDFIR\Desktop\c16-Hunter\SYSTEM	...	...	2013-08-22 14:52:22
C:\Users\SANSDFIR\Desktop\SECURITY_clean	...	...	2013-08-22 14:50:33
C:\Users\SANSDFIR\Desktop\c16-Hunter\SECURITY	...	...	2013-08-22 14:50:33
C:\Users\SANSDFIR\Desktop\c16-Hunter\SOFTWARE_clean	...	...	2013-08-22 15:14:44
C:\Users\SANSDFIR\Desktop\c16-Hunter\SOFTWARE	...	...	2013-08-22 15:14:44
C:\Users\SANSDFIR\Desktop\c16-Hunter\SAM	...	...	2013-08-22 13:25:44
CatTool-CreativeLive-[00000000-0000-0000-0000-000000000000]	0	1	2013-08-22 14:45:10
SAM	2	3	2014-03-18 09:52:38
Domains	1	2	2013-08-22 14:45:11
Account	2	3	2016-06-21 08:40:06
Aliases	1	4	2016-06-21 08:40:05
000003E8	1	0	2013-08-22 14:46:01
000003EA	1	0	2016-06-21 08:40:06
Members	1	2	2016-06-21 08:40:06
S-1-5-21-2489440558-2754304563-710705792	1	2	2016-06-21 08:40:06
000003E9	1	0	2016-06-21 08:40:06
000003EB	1	0	2016-06-21 08:40:06
S-1-5-80-2375682873-76804050-3534595160-10055450	1	1	2016-06-21 08:40:05
Names	1	2	2016-06-21 08:40:05
Groups	1	2	2013-08-22 14:45:11
Users	1	5	2016-06-21 08:40:06
Builtin	2	3	2016-06-21 08:37:43
LastSkuUpgrade	1	0	2014-03-18 09:52:38
RXACT	1	0	2013-08-22 14:45:10

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Stack	Is Deleted
(default)	RegExpandSz			

Type viewer Binary viewer

Value name: (default)

Value type: RegExpandSz

Value:

Raw value:

Key: CatTool-CreativeLive-[00000000-0000-0000-0000-000000000000]\SAM\Domains\Account\Aliases\Members\S-1-5-21-2489440558-2754304563-710705792

What is the Operating System(OS) version?  
8.1

Registry Explorer V1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry Hives (6) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
WindowsUpdate	2	5	2016-06-21 08:30:05
WINEVT	0	3	2013-08-22 15:37:08
Wordpad	0	1	2013-08-22 15:37:08
WSMAN	1	6	2013-08-22 15:37:08
WUSA	0	0	2016-06-21 11:09:39
XblGame	0	3	2013-08-22 15:37:08
Help	6	0	2016-06-20 23:59:34
HTML Help	3	0	2016-06-20 23:56:03
ITSStorage	0	1	2013-08-22 15:37:08
ScheduledDiagnostics	1	0	2013-08-22 15:37:08
ScriptedDiagnosticsProvider	6	1	2013-08-22 15:37:08
Shell	0	1	2013-08-22 15:37:08
Tablet PC	2	0	2013-08-22 14:44:50
TabletPC	0	2	2014-03-18 09:43:20
Windows Error Reporting	5	7	2016-06-21 08:37:43
Windows Search	0	1	2013-08-22 15:37:08
Windows Defender	8	13	2016-06-21 12:46:24
Windows Desktop Search	1	0	2014-03-18 10:18:07
Windows Embedded	0	1	2014-03-18 09:43:20
Windows Mail	5	4	2013-08-22 15:37:08
Windows Media Device Manager	1	3	2013-08-22 15:37:08
Windows Media Foundation	0	7	2013-08-22 15:37:08
Windows Media Player NSS	0	1	2013-08-22 15:37:08
Windows Messaging Subsystem	6	1	2016-06-20 23:57:05
Windows NT	0	1	2013-08-22 13:25:43
CurrentVersion	19	73	2016-06-21 09:47:33
Windows Photo Viewer	0	1	2013-08-22 15:37:08
Windows Portable Devices	0	2	2013-08-22 15:37:09
Windows Script Host	0	1	2013-08-22 15:37:09
Windows Search	9	19	2016-06-21 08:33:37
WindowsRuntime	2	4	2014-03-18 10:18:07
Wlap	0	3	2013-08-22 15:37:09
WlanSvc	0	1	2013-08-22 15:37:09
WSDAPI	0	1	2013-08-22 15:37:09
WwanSvc	0	8	2013-08-22 15:37:09

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Stack	Is Deleted
SystemRoot	RegSz	C:\Windows	00-05-12-00-00-00	
SoftwareType	RegSz	System	00-00-78-F8-00-00	
RegisteredOwner	RegSz	Hunter	20-00-55-00-73-00-...	
InstallDate	RegDword	1466488265		
CurrentVersion	RegSz	6.3	F8-00-01-00	
CurrentBuild	RegSz	9600	00-00	
RegisteredOrganization	RegSz			
CurrentType	RegSz	MultiProcessor Free	65-00-44-00-00-00...	
InstallationType	RegSz	Client	00-00-F4-E2-87-53	
EditionID	RegSz	Enterprise	00-00-00-00-00-00	
ProductName	RegSz	Windows 8.1 Enterprise	00-00-00-00-00-00	
ProductId	RegSz	00261-30000-00000-AA625	5C-00-46-00	
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-32-38-31-2...		
DigitalProductID4	RegBinary	F8-04-00-00-04-00-00-00-30-00-30-00-30-0...	00-00-00-00	
CurrentBuildNumber	RegSz	9600	88-02	
BuildLab	RegSz	9600.winblue_gdr.140221-1952	00-00	
BuildLabEx	RegSz	9600.17031.amd64fre.winblue_gdr.140221-...	00-00-00-00	
BuildGUID	RegSz	ffffff-fff-fff-fff-ffffff	00-00	

Type viewer Slack viewer Binary viewer

Value name: ProductName

Value type: RegSz

Value: Windows 8.1 Enterprise

Raw value: 07-00-69-00-6E-00-64-00-6F-00-77-00-73-00-30-38-00-3E-00-31-00-20-00-45-00-6E-00-74-00-6

Slack: 00-00-00-00-00-00

Key: CatTool-CreativeLive-[00000000-0000-0000-0000-000000000000]\Microsoft\Windows NT\CurrentVersion

What was the computer timezone?  
UTC-07:00

Registry hives (6) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
StlImage	0	0	3 2013-08-22 13:37:10
Storage	0	0	3 2013-08-22 14:45:19
StorageManagement	0	0	3 2013-08-22 13:37:10
Startup	0	0	0 2014-03-18 09:53:33
SystemResources	0	0	3 2013-08-22 13:25:43
TabletPC	0	0	1 2013-08-22 15:37:10
Terminal Server	16	12	2016-06-21 11:41:03
TimeZoneInformation	10	0	2016-06-21 09:14:37
Udm	8	0	2013-08-22 15:37:09
usb	0	0	1 2013-08-22 15:37:09
usbafage	0	2	2016-06-21 02:01:59
usbtor	0	0	5 2013-08-22 15:33:18
VAN	0	0	5 2013-08-22 15:37:09
Vids	0	0	4 2016-06-21 08:15:21
WcmSvc	0	2	2013-08-22 15:37:10
Wdf	0	0	4 2013-08-22 15:37:10
Wdi	0	0	3 2013-08-22 15:37:10
Windows	10	0	2016-06-21 01:34:49
Winlogon	0	1	2013-08-22 13:25:43
WMI	0	2	2013-08-22 13:25:43
WorkplaceJoin	1	0	2013-08-22 15:37:10
WPN	0	1	2013-08-22 15:37:09
Enum	24	12	2016-06-21 01:53:14
Hardware Profiles	0	2	2016-06-21 11:40:41
Policies	0	0	2013-08-22 15:37:09
Services	0	496	2016-06-21 13:18:45
DriverDatabase	3	4	2016-06-21 06:47:28
HardwareConfig	2	1	2016-06-21 11:40:41
MountedDevices	8	0	2016-06-21 02:01:59
RNG	2	0	2016-06-21 11:40:41
Select	4	0	2013-08-22 13:25:43
Setup	12	0	2016-06-21 01:53:15
AllowStart	0	13	2013-08-22 15:37:10
DXGDI	0	0	2013-08-22 15:37:10
Rid	1	0	2013-08-22 15:37:10

Key: C:\Tool-CreativeLive-(00000000-0000-0000-0000-000000000000)\ControlSet001\Control\TimeZoneInformation

Value: DaylightBias

Values TimeZoneInformation

Drag a column header here to group by that column

Value Name	Value Data	Value Data Raw
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-00-00-01-00-02-00-00-00-00-00-00-00-00
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 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00
TimeKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	420	420

Total rows: 9

Type viewer Binary viewer

Value name DaylightBias

Value type RegDword

Value 4294967236

Raw value C4FF FF FF

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

3

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry hives (7) Available bookmarks (113/0)

Enter text to search... Find

Values User accounts

Drag a column header here to group by that column

User Id	Invalid	Total Logon Count	Created On	Last Login Time	Last Password Change	Last T...	Expires	User Name	Full ...	Pass...	Groups	Comments	Use...	Home...	Inter...	Acc...	Home...	Pass...
501	0	0	2016-06-21 08:...					Guest			Guest	Built-in account for guest access to the computer (domain)						
1001	1	3	2016-06-21 08:...	2016-06-21 ...	2016-06-21 08:37:43	2016...		Hunter			Administrators							
1003	0	0	2016-06-21 08:...		2016-06-21 08:40:06			HomeGroupUser\$	HomeGroupUser\$		Built-in account for homegroup access to the computer							

Total rows: 4

Type viewer Binary viewer

Value name (default)

Value type RegDword

Value 0

Raw value

Key: C:\Tool-CreativeLive-(00000000-0000-0000-0000-000000000000)\SAM\Domains\Account\Users

When was the last login time for the discovered account? Format: one-space between date and time  
2016-06-21 01:42:40

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry hives (7) Available bookmarks (113/0)

Enter text to search... Find

Values User accounts

Drag a column header here to group by that column

User Id	Invalid	Total Logon Count	Created	Last Login Time	Last Pa...	Last In...	Expires	User N...	Full Na...	Passw...	Groups	Comments	User C...	Home ...
500	0	3	2016-06...	2014-03-18 10:20:36	2014-0...			Administrator			Administrators	Built-in account for administering the computer (domain)		
501	0	0	2016-06...					Guest			Guests	Built-in account for guest access to the computer (domain)		
1001	1	3	2016-06...	2016-06-21 01:42:40	2016-0...	2016-9...		Hunter			Administrators			
1003	0	0	2016-06...					HomeGroupUser\$	HomeGroupUser\$		Built-in account for homegroup access to the computer			

Total rows: 4

Type viewer Binary viewer

#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

[illegible]







Timeline Explorer v1.1.2.0

File Tools Tabs Help

202208151609\_PeCond\_Output.csv

Drag a column header here to group by that column

Line	Tag	Note	Source Filename	Source Created	Source Modified	Source Accessed	Executable Name	Run Count	Hash	Size	Version	Last Run	Previous Run#	Previous Run1
141			Prefetch\TEAMVIEWER_EXE-F6CE775B.pf	2016-06-21 12:00:53	2016-06-21 12:00:53	2022-08-28 15:16:10	TEAMVIEWER_EXE	1	F6CE775B	157498	windows 8.0.	2016-06-21 12:00:43		
142			Prefetch\TEAMVIEWER_EXE-C5613E0.pf	2016-06-21 00:57:32	2016-06-21 00:57:32	2022-08-28 15:16:10	TEAMVIEWER_EXE	2	C5613E0	222164	windows 8.0.	2016-06-21 00:57:29	2016-06-21 00:57:29	
143			Prefetch\TEAMVIEWER_DESKTOP_EXE-2068AA88.pf	2016-06-21 12:05:41	2016-06-21 12:05:41	2022-08-28 15:16:10	TEAMVIEWER_DESKTOP_EXE	1	2068AA88	65858	windows 8.0.	2016-06-21 12:05:31		

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

SQLite Administrator - main.db

Database Table Index View Trigger Query Data Help

SQL Query Result Edit Data

read_receipt_optout	hidden_expression_tabs	owner_under_legal_age	type	skypename	psnnumber	fullname	birthday	gender	languages	country	province	city	phone_home	phone_office	phone_mobile	emails	homepage	about
				hunterehpt		EHPT Mgs	19900101		0 en	jo		Amman				ehptmgs@gmail.com		

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?

SQLite Administrator - main.db

Database Table Index View Trigger Query Data Help

SQL Query Result Edit Data

guid	dialog_partner	timestamp	type	sending_status	option_bits	consumption_status	edited_by	edited_timestamp	param_key	param_value	body_xml	id
1466496603	linux-ru3z	1466496603	61	2		0					some of the docs are for products	1
1466496616	linux-ru3z	1466496616	61	2		0					others are for other misc stuff	2
1466496630	linux-ru3z	1466496630	61	2		0					no worries	3
1466496655	linux-ru3z	1466496655	61	2		0					let us work on them separately	4
1466496663	linux-ru3z	1466496663	61	2		0					what do you mean?	5
1466496675	linux-ru3z	1466496675	61	2		0					I mean, let us first find away to access your device	6
1466496691	linux-ru3z	1466496691	61	2		0					and then, see what can we do in order to exfil the docs/pics outside ur network	7
1466496693	linux-ru3z	1466496693	61	2		0					ok	8
1466496697	linux-ru3z	1466496697	61	2		0					that sounds great	9
1466496703	linux-ru3z	1466496703	61	2		0					but is this truly doable?	10
1466496707	linux-ru3z	1466496707	61	2		0					there is no limits	11
1466496711	linux-ru3z	1466496711	61	2		0					sure it is <ss type="wink">-></ss>	12
1466496719	linux-ru3z	1466496719	61	2		0					when shall we start	13
1466496720	linux-ru3z	1466496720	61	2		0					?	14
1466496732	linux-ru3z	1466496732	61	2		0					Can I access your machine?	15
1466496746	linux-ru3z	1466496746	61	2		0					hmm, not sure since our network is monitored as I told u	16
1466496753	linux-ru3z	1466496753	61	2		0					okay wait	17
1466470037	linux-ru3z	1466470037	61	2		0					can you install team viewer?	18
1466470056	linux-ru3z	1466470056	61	2		0					I am not sure	19
1466470059	linux-ru3z	1466470059	61	2		0					but let me see	20
1466470067	linux-ru3z	1466470067	61	2		0					I will inform you once I am finished	21
1466470071	linux-ru3z	1466470071	61	2		0					how can I reach u?	22
1466470092	linux-ru3z	1466470092	61	2		0					send an email to my Hotmail account	23
1466470097	linux-ru3z	1466470097	61	2		0					which one?	24
1466470105	linux-ru3z	1466470105	61	2		0					same as Skype <ss type="wink">-></ss>	25
1466470112	linux-ru3z	1466470112	61	2		0					ok <ss type="laugh">-></ss>	26
1466470114	linux-ru3z	1466470114	61	2		0					understood	27
1466470126	linux-ru3z	1466470126	61	2		0					see you soon	28
1466470132	linux-ru3z	1466470132	61	2		0					yeah	29
1466470134	linux-ru3z	1466470134	61	2		0					bye bye	30
1466470136	linux-ru3z	1466470136	61	2		0					bye	31
1466509717	linux-ru3z	1466509717	254	2		0					<URIObject type="File.1" uri="https://api.lsm.skype.com/v1/objects/0-weu-d2-a958c1f0bec3-1466509717" data-bbox="1466509717 1466509717 1466509717 1466509717" data-kind="parent" data-rs="2"></URIObject>	32
1466509726	linux-ru3z	1466509726	61	2		0					Back pics<ss type="wink">-></ss>	33

AccessData FTK Imager 4.1.1.1

File View Mode Help

Evidence Tree

- Jeico
  - BCWipe
  - Shared
  - Shared54
- Users
  - Hunter
    - Desktop
    - Documents
      - Custom Office Templates
      - defcon16oska.pdf
      - DEFCON-22-Zohar-Balazs-Bypass-firewalls-appliance.pdf
      - how\_to\_threat\_actors\_steal\_your\_data.pdf
      - msf-detecting-dataring-both.pdf
      - My Music
      - My Pictures
      - My Videos
      - Outlook Files
      - Ryan\_VanAntwerp\_threats.pdf
      - Thumbnail.db
    - Downloads

File List

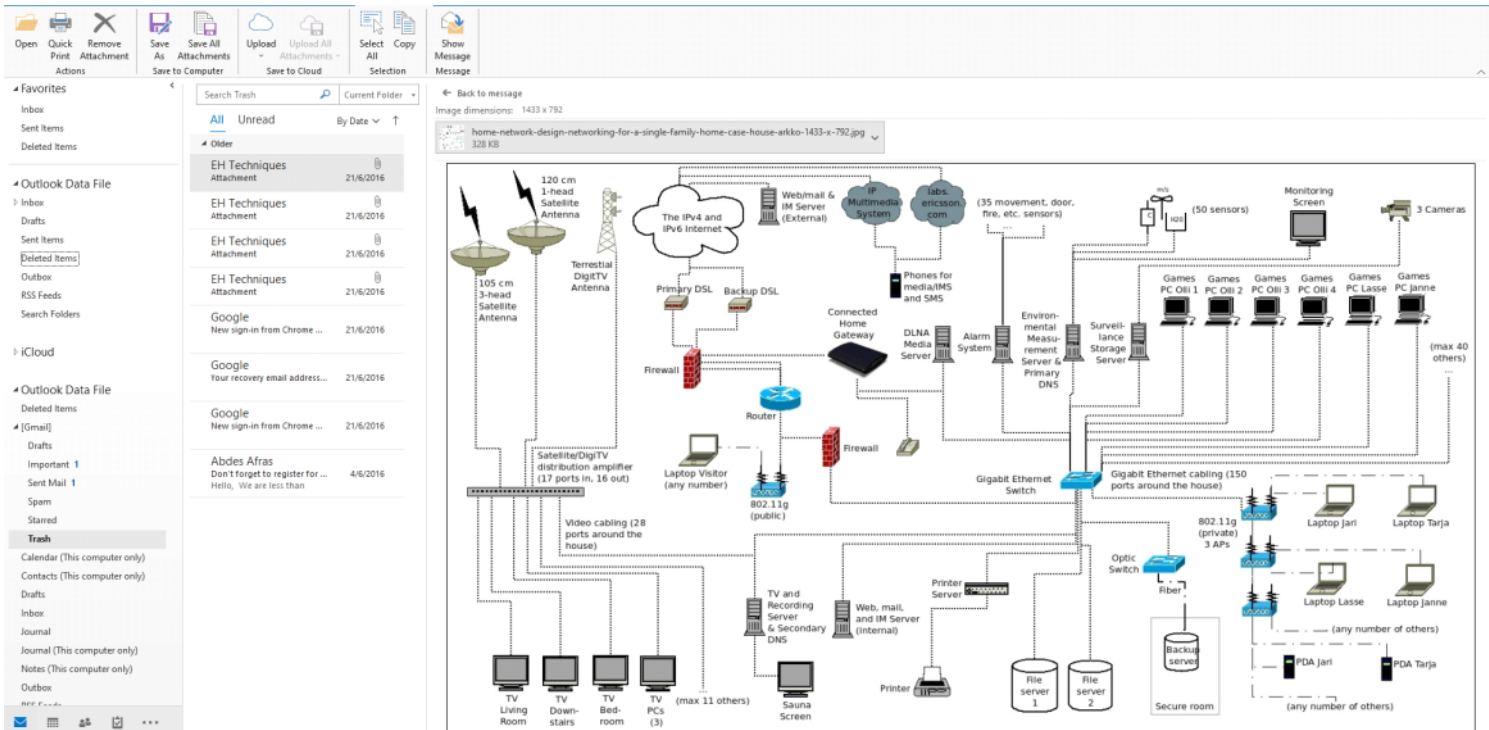
Name	Size	Type	Date Modified
backup.pst.File Slack	248	File Slack	
backup.pst	10,185	Regular File	2016-06-21 1:13:48 PM

Custom Content Sources

Evidence File System Path/File Options

Properties Hex Value Interpreter Custom Content Sources

Cursor pos = 0



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

AccessData FTK Imager 4.1.1.1

File View Mode Help

Evidence Tree

- Program Files (x86)
  - Jetico
    - Users
      - Hunter
        - zennap
          - AppData
            - Documents
              - Custom Office Templates
                - DECON-16-ricks.pdf
                  - DECON-22-Zoltan-Balazs-Bypass-firewalls-application-...
                  - how\_to\_threat\_actors\_steal\_your\_data.pdf
                  - mini-detecting-detecting-both.pdf
                  - My Music
                    - My Videos
                      - Outlook Files
                        - Ryan\_VanAntwerp\_thesis.pdf
                        - Thumbs.db

Custom Content Sources

Evidence:File System(Path)\File Options

| Name  | Size  | Type              | Date Modified          |
|---|-------|-------------------|------------------------|
| Custom Office Templates                                       | 1     | Directory         | 2016-06-21 1:58:52 AM  |
| My Music  | 1     | Reparse Point     | 2016-06-21 8:37:46 AM  |
| My Videos   | 1     | Reparse Point     | 2016-06-21 8:37:46 AM  |
| My Pictures   | 1     | Reparse Point     | 2016-06-21 8:37:46 AM  |
| Outlook Files   | 1     | Directory         | 2016-06-21 1:13:48 PM  |
| zennap  | 500   | NTFS Index Entry  | 2016-06-21 1:46:16 AM  |
| Accounts.txt  | 1     | Regular File      | 2016-06-21 9:21:53 AM  |
| tools.txt   | 1     | Regular File      | 2016-06-21 8:37:53 AM  |
| desktop.ini   | 1     | Regular File      | 2016-06-21 1:13:48 PM  |
| Confidential Document.pdf                                     | 2     | File Stack        | 2016-06-21 1:13:48 PM  |
| Conf.jpg  | 2     | File Stack        | 2016-06-21 1:13:48 PM  |
| NTFS Index All...   | 4     | NTFS Index All... | 2016-06-21 12:37:46 PM |
| 12  | 12    | Regular File      | 2016-06-21 12:37:46 PM |
| Thumbs.db   | 15    | Regular File      | 2016-06-21 12:19:27 PM |
| Confidential Document.docx                                    | 17    | Regular File      | 2016-06-21 1:59:20 AM  |
| Confidential Document.pdf                                     | 331   | Regular File      | 2016-06-21 1:59:27 AM  |
| Conf.jpg  | 331   | Regular File      | 2016-06-21 1:59:27 AM  |
| how_to_threat_actors_steal_your_data.pdf                      | 547   | Regular File      | 2016-06-21 9:39:47 AM  |
| Ryan_VanAntwerp_thesis.pdf                                    | 593   | Regular File      | 2016-06-21 9:40:07 AM  |
| defcon-16-ricks.pdf   | 766   | Regular File      | 2016-06-21 9:40:46 AM  |
| mini-detecting-detecting-both.pdf                             | 1,039 | Regular File      | 2016-06-21 9:40:22 AM  |
| DECON-22-Zoltan-Balazs-Bypass-firewalls-application-whitel... | 4,073 | Regular File      | 2016-06-20 11:58:09 PM |

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

AccessData FTK Imager 4.1.1.1

File View Mode Help

Evidence Tree

- Hunter.ad1
  - Custom Content Image (Multi) (AD1)
    - c:\16-Hunter\NONAME (NTFS)
      - root
        - Program Files (x86)
          - Jetico
            - BCWipe
              - Shared
                - Shared54

Custom Content Sources

Evidence:File System(Path)\File Options

| Name                    | Size | Type              | Date Modified          |
|-------------------------|------|-------------------|------------------------|
| BCWipeSample.bat        | 3    | File Stack        | 2016-06-21 1:44:55 AM  |
| bcwipeSetup.ver         | 3    | File Stack        | 2016-06-21 1:44:55 AM  |
| wipeList.txt            | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| ReadMe.txt              | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| BCWipeTH.exe.manifest   | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| BCResident.exe.manifest | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| BCWipeSvc.exe.manifest  | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| BCView.exe.manifest     | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| BCWipe.exe.manifest     | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| BCWipeSvc.exe           | 4    | File Stack        | 2016-06-21 1:44:55 AM  |
| S30                     | 8    | NTFS Index All... | 2016-06-21 11:44:55 AM |
| Uninstall.log           | 9    | Regular File      | 2016-06-21 11:53:37 AM |
| ReadMe.txt              | 17   | Regular File      | 2016-02-29 7:01:22 AM  |
| langfile.dll            | 86   | Regular File      | 2016-02-29 7:17:00 AM  |
| BCWipeSvc.exe           | 89   | Regular File      | 2016-02-29 7:19:29 AM  |
| bcwipevsh.dll           | 124  | Regular File      | 2016-02-29 7:18:57 AM  |

C 0 6/21/2016 4:14 AM  
B 0 "C:\Program Files (x86)\Jetico\BCWipe\BCWipeSvc.exe" -remove  
C 0 6/21/2016 4:14 AM  
19 0 C:\Program Files (x86)\Jetico\BCWipe\bcgupdtd.dllRemoveC:\Program Files (x86)\Jetico\BCWipe\BCWipeTH.exe  
C 0 6/21/2016 4:14 AM  
8000000A 0 fsh  
C 0 6/21/2016 4:14 AM  
8000000A 0 HrcWipeFilter  
C 0 6/21/2016 4:14 AM  
7 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe  
C 0 6/21/2016 4:14 AM  
4 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\  
C 0 6/21/2016 4:14 AM  
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\BCWipe Help.lnk  
C 0 6/21/2016 4:14 AM  
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\ReadMe.lnk  
C 0 6/21/2016 4:14 AM  
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\About BCWipe.lnk  
C 0 6/21/2016 4:14 AM  
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\BCWipe.lnk  
C 0 6/21/2016 4:14 AM  
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\BCWipe Task Manager.lnk  
C 0 6/21/2016 4:14 AM  
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\Automatic Update.lnk  
C 0 6/21/2016 4:14 AM  
C 1 DisableReboot

Listed 47 Selected: 1 Hunter.ad1\Custom Content Image (Multi) (AD1)\c:\16-Hunter\NONAME (NTFS)\root\Program Files (x86)\Jetico\BCWipe\Uninstall.log

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



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

Google BCWipe X

All Images Videos Shopping News More Tools

About 34,200 results (0.46 seconds)

<https://www.jetico.com> + data-wiping + wipe-files-bcwipe

## Wipe Files with BCWipe - Jetico

**BCWipe** is a file shredder tool designed to selectively remove all traces of unwanted files beyond recovery. **BCWipe** can wipe files, folders, Data Remanence, Wipe ...

<https://www.jetico.com>

Jetico: Encryption Software & Wiping Software

Jetico provides wiping and encryption software for all sensitive information throughout the lifecycle: Wipe with **BCWipe** & Encrypt with **BestCrypt**.

People also ask

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

Timeline Explorer v1.1.2.0

File Tools Tabs Help

20220828151609\_PECmd\_Output.csv

Drag a column header here to group by that column

| Line | Tag | Note              | Source Filename                        | Source Created      | Source Modified     | Source Accessed     | Executable Name   | Run Count | Hash      | Size   | Version      | Last Run            | Previo |
|------|-----|-------------------|--|---------------------|---------------------|---------------------|-------------------|-----------|-----------|--------|--------------|---------------------|--------|
| 1    |     |                   | Prefetch\721602-X64-9254A8E7.pf        | 2016-06-21 09:18:15 | 2016-06-21 09:18:15 | 2022-08-28 15:16:16 | 721602-X64.EXE    | 1         | 9254A8E7  | 66352  | Windows 8.0. | 2016-06-21 09:18:10 |        |
| 2    |     |                   | Prefetch\72FH.EXE-698B961D.pf          | 2016-06-21 09:43:06 | 2016-06-21 09:43:06 | 2022-08-28 15:16:16 | 72FH.EXE          | 1         | 698B961D  | 32412  | Windows 8.0. | 2016-06-21 09:43:04 |        |
| 3    |     |                   | Prefetch\72G.EXE-0F8C4081.pf           | 2016-06-21 09:42:02 | 2016-06-21 11:44:02 | 2022-08-28 15:16:16 | 72G.EXE           | 7         | F8C4081   | 293782 | Windows 8.0. | 2016-06-21 11:48:04 | 2016   |
| 4    |     |                   | Prefetch\ACRORD32.EXE-ACF2947E.pf      | 2016-06-20 23:49:49 | 2016-06-21 02:00:06 | 2022-08-28 15:16:16 | ACRORD32.EXE      | 8         | ACF2947E  | 106750 | Windows 8.0. | 2016-06-21 02:00:01 | 2016   |
| 5    |     |                   | Prefetch\BCRESIDENT.EXE-7C7E7A8BC.pf   | 2016-06-21 11:45:03 | 2016-06-21 11:45:03 | 2022-08-28 15:16:16 | BCRESIDENT.EXE    | 1         | 7C7E7A8BC | 26286  | Windows 8.0. | 2016-06-21 11:44:55 |        |
| 6    |     | File contains > 2 | Prefetch\BQIPE.EXE-36F3F2DF.pf         | 2016-06-21 12:01:05 | 2016-06-21 12:02:02 | 2022-08-28 15:16:16 | BQIPE.EXE         | 5         | 36F3F2DF  | 72524  | Windows 8.0. | 2016-06-21 12:02:35 | 2016   |
| 7    |     |                   | Prefetch\BQIPESETUP.EXE-A82C77E1.pf    | 2016-06-21 11:44:42 | 2016-06-21 11:44:42 | 2022-08-28 15:16:16 | BQIPESETUP.EXE    | 1         | A82C77E1  | 67728  | Windows 8.0. | 2016-06-21 11:44:32 |        |
| 8    |     |                   | Prefetch\BQIPESETUPVSC.EXE-64B3C913.pf | 2016-06-21 11:44:53 | 2016-06-21 11:44:53 | 2022-08-28 15:16:16 | BQIPESETUPVSC.EXE | 2         | 64B3C913  | 34714  | Windows 8.0. | 2016-06-21 11:44:53 | 2016   |
| 9    |     |                   | Prefetch\BQIPESETUPVSC.EXE-7A3038F4.pf | 2016-06-21 11:45:01 | 2016-06-21 11:45:01 | 2022-08-28 15:16:16 | BQIPESETUPVSC.EXE | 2         | 7A3038F4  | 32844  | Windows 8.0. | 2016-06-21 11:44:53 | 2016   |
| 10   |     |                   | Prefetch\BSPATCH.EXE-D09E5E46.pf       | 2016-06-21 11:22:39 | 2016-06-21 11:22:39 | 2022-08-28 15:16:16 | BSPATCH.EXE       | 1         | D09E5E46  | 23126  | Windows 8.0. | 2016-06-21 11:22:35 |        |
| 11   |     |                   | Prefetch\CALC.EXE-77FD17F.pf           | 2016-06-20 23:54:12 | 2016-06-20 23:54:12 | 2022-08-28 15:16:16 | CALC.EXE          | 1         | 77FD17F   | 23540  | Windows 8.0. | 2016-06-20 23:54:10 |        |
| 12   |     |                   | Prefetch\CLEANER.EXE-D4D76A60.pf       | 2016-06-21 12:01:44 | 2016-06-21 12:02:02 | 2022-08-28 15:16:16 | CLEANER.EXE       | 3         | D4D76A60  | 16592  | Windows 8.0. | 2016-06-21 12:02:08 | 2016   |
| 13   |     |                   | Prefetch\CLEANER64.EXE-779D0542.pf     | 2016-06-21 11:43:08 | 2016-06-21 12:02:02 | 2022-08-28 15:16:16 | CLEANER64.EXE     | 7         | 779D0542  | 120478 | Windows 8.0. | 2016-06-21 12:02:08 | 2016   |
| 14   |     |                   | Prefetch\CCSETUP519PRO.EXE-80E5525D.pf | 2016-06-21 11:06:37 | 2016-06-21 11:44:42 | 2022-08-28 15:16:16 | CCSETUP519PRO.EXE | 2         | 80E5525D  | 310754 | Windows 8.0. | 2016-06-21 11:44:16 | 2016   |
| 15   |     |                   | Prefetch\CHROME.EXE-D99981BA.pf        | 2016-06-21 08:43:06 | 2016-06-21 12:52:24 | 2022-08-28 15:16:16 | CHROME.EXE        | 6         | D99981BA  | 229924 | Windows 8.0. | 2016-06-21 12:52:23 | 2016   |
| 16   |     |                   | Prefetch\CHROME.EXE-D99981B8.pf        | 2016-06-21 08:43:06 | 2016-06-21 13:12:04 | 2022-08-28 15:16:16 | CHROME.EXE        | 40        | D99981B8  | 77118  | Windows 8.0. | 2016-06-21 13:12:04 | 2016   |
| 17   |     |                   | Prefetch\CHROME.EXE-D99981BC.pf        | 2016-06-21 12:52:36 | 2016-06-21 12:52:36 | 2022-08-28 15:16:16 | CHROME.EXE        | 1         | D99981BC  | 41828  | Windows 8.0. | 2016-06-21 12:52:24 |        |
| 18   |     |                   | Prefetch\CHROME.EXE-D99981BD.pf        | 2016-06-21 09:17:08 | 2016-06-21 09:46:06 | 2022-08-28 15:16:16 | CHROME.EXE        | 7         | D99981BD  | 44640  | Windows 8.0. | 2016-06-21 09:46:00 | 2016   |
| 19   |     |                   | Prefetch\CHROME.EXE-D99981C1.pf        | 2016-06-21 09:22:05 | 2016-06-21 12:52:24 | 2022-08-28 15:16:16 | CHROME.EXE        | 5         | D99981C1  | 19350  | Windows 8.0. | 2016-06-21 12:52:23 | 2016   |
| 20   |     |                   | Prefetch\CHROME.EXE-D99981C2.pf        | 2016-06-21 08:43:06 | 2016-06-21 12:52:24 | 2022-08-28 15:16:16 | CHROME.EXE        | 45        | D99981C2  | 92418  | Windows 8.0. | 2016-06-21 12:52:24 | 2016   |
| 21   |     |                   | Prefetch\CMD.EXE-4A81B364.pf           | 2016-06-20 23:53:46 | 2016-06-21 12:02:02 | 2022-08-28 15:16:16 | CMD.EXE           | 3         | 4A81B364  | 8850   | Windows 8.0. | 2016-06-21 12:02:43 | 2016   |
| 22   |     |                   | Prefetch\CMD.EXE-AC133AAB.pf           | 2016-06-20 23:57:01 | 2016-06-21 11:22:39 | 2022-08-28 15:16:16 | CMD.EXE           | 5         | AC133AAB  | 9678   | Windows 8.0. | 2016-06-21 11:22:53 | 2016   |
| 23   |     |                   | Prefetch\CONHOST.EXE-1F3E907E.pf       | 2016-06-21 08:31:04 | 2016-06-21 12:58:02 | 2022-08-28 15:16:16 | CONHOST.EXE       | 34        | 1F3E907E  | 18886  | Windows 8.0. | 2016-06-21 12:58:02 | 2016   |
| 24   |     |                   | Prefetch\CONSENT.EXE-531B09EA.pf       | 2016-06-21 08:38:35 | 2016-06-21 13:18:02 | 2022-08-28 15:16:16 | CONSENT.EXE       | 24        | 531B09EA  | 108232 | Windows 8.0. | 2016-06-21 13:18:12 | 2016   |
| 25   |     |                   | Prefetch\DLLHOST.EXE-46FA2603.pf       | 2016-06-21 11:51:28 | 2016-06-21 11:51:28 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 2         | 46FA2603  | 20956  | Windows 8.0. | 2016-06-21 11:51:33 | 2016   |
| 26   |     |                   | Prefetch\DLLHOST.EXE-4F28A26F.pf       | 2016-06-21 09:43:36 | 2016-06-21 12:17:30 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 2         | 4F28A26F  | 190030 | Windows 8.0. | 2016-06-21 12:17:30 | 2016   |
| 27   |     |                   | Prefetch\DLLHOST.EXE-5E46F48D.pf       | 2016-06-21 08:38:08 | 2016-06-21 13:17:30 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 43        | 5E46F48D  | 24554  | Windows 8.0. | 2016-06-21 13:17:32 | 2016   |
| 28   |     |                   | Prefetch\DLLHOST.EXE-766398D2.pf       | 2016-06-21 08:37:51 | 2016-06-21 13:17:30 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 31        | 766398D2  | 14304  | Windows 8.0. | 2016-06-21 13:17:43 | 2016   |
| 29   |     |                   | Prefetch\DLLHOST.EXE-766398D5.pf       | 2016-06-21 11:48:32 | 2016-06-21 13:17:30 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 3         | 766398D5  | 22406  | Windows 8.0. | 2016-06-21 13:17:49 | 2016   |
| 30   |     |                   | Prefetch\DLLHOST.EXE-82E81806.pf       | 2016-06-21 09:22:52 | 2016-06-21 11:19:30 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 4         | 82E81806  | 25214  | Windows 8.0. | 2016-06-21 11:19:28 | 2016   |
| 31   |     |                   | Prefetch\DLLHOST.EXE-ECB71776.pf       | 2016-06-21 08:38:07 | 2016-06-21 09:25:02 | 2022-08-28 15:16:16 | DLLHOST.EXE       | 8         | ECB71776  | 25744  | Windows 8.0. | 2016-06-21 09:25:23 | 2016   |
| 32   |     |                   | Prefetch\DROPBOX.EXE-8C41F124.pf       | 2016-06-21 01:47:19 | 2016-06-21 12:54:12 | 2022-08-28 15:16:16 | DROPBOX.EXE       | 4         | 8C41F124  | 249728 | Windows 8.0. | 2016-06-21 12:54:11 | 2016   |
| 33   |     |                   | Prefetch\DROPBOX\BQIPE.EXE-8E53AC71.pf | 2016-06-21 11:45:13 | 2016-06-21 11:45:13 | 2022-08-28 15:16:16 | BQIPESETUPVSC.EXE | 14        | 8E53AC71  | 40418  | Windows 8.0. | 2016-06-21 11:45:08 | 2016   |

C:\Users\SANSDFIR\Desktop\c16-Hunter\20220828151609\_PECmd\_Output.csv

Total lines 174 Visible lines 174 Search options

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

Timeline Explorer v1.1.2.0

File Tools Tabs Help

20220828151609\_PECmd\_Output.csv

Drag a column header here to group by that column

| Line | Tag | Note              | Source Filename                        | Source Created      | Source Modified     | Source Accessed     | Executable Name   | Run Count | Hash     | Size  | Version      | Last Run            |
|------|-----|-------------------|--|---------------------|---------------------|---------------------|-------------------|-----------|----------|-------|--------------|---------------------|
| 6    |     | File contains > 2 | Prefetch\BQIPE.EXE-36F3F2DF.pf         | 2016-06-21 12:01:05 | 2016-06-21 12:02:02 | 2022-08-28 15:16:16 | BQIPE.EXE         | 5         | 36F3F2DF | 72524 | Windows 8.0. | 2016-06-21 12:02:35 |
| 7    |     |                   | Prefetch\BQIPESETUP.EXE-A82C77E1.pf    | 2016-06-21 11:44:42 | 2016-06-21 11:44:42 | 2022-08-28 15:16:16 | BQIPESETUPVSC.EXE | 1         | A82C77E1 | 67728 | Windows 8.0. | 2016-06-21 11:44:32 |
| 8    |     |                   | Prefetch\BQIPESETUPVSC.EXE-64B3C913.pf | 2016-06-21 11:44:53 | 2016-06-21 11:44:53 | 2022-08-28 15:16:16 | BQIPESETUPVSC.EXE | 2         | 64B3C913 | 34714 | Windows 8.0. | 2016-06-21 11:44:53 |
| 9    |     |                   | Prefetch\BQIPESETUPVSC.EXE-7A3038F4.pf | 2016-06-21 11:45:01 | 2016-06-21 11:45:01 | 2022-08-28 15:16:16 | BQIPESETUPVSC.EXE | 2         | 7A3038F4 | 32844 | Windows 8.0. | 2016-06-21 11:44:53 |

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

Timeline Explorer v1.1.2.0

File Tools Tabs Help

20220828151609\_PECmd\_Output.csv

Drag a column header here to group by that column

| Line | Tag | Note | Source Filename                 | Source Created      | Source Modified     | Source Accessed     | Executable Name | Run Count | Hash     | Size  | Version      | Last Run            |
|------|-----|------|---------------------------------|---------------------|---------------------|---------------------|-----------------|-----------|----------|-------|--------------|---------------------|
| 174  |     |      | Prefetch\ZENMAP.EXE-56B17C4C.pf | 2016-06-21 12:08:21 | 2016-06-21 12:08:02 | 2022-08-28 15:16:16 | ZENMAP.EXE      | 1         | 56B17C4C | 93524 | Windows 8.0. | 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?

AccessData FTK Imager 4.1.1.1

File View Mode Help

20220828151609\_PECmd\_Output.csv

Drag a column header here to group by that column

| Name   | Size | Type            | Date Modified          |
|--|------|-----------------|------------------------|
| https-www.kali.org-.lnk  |      | S30 INDEX Entry |                        |
| xXOGCUI.lnk  |      | S30 INDEX Entry |                        |
| xXOGCUI.lnk  |      | S30 INDEX Entry |                        |
| DEFCON-2.LNK   |      | S30 INDEX Entry |                        |
| https-www.kali.org-.lnk  | 1    | Regular File    | 2016-06-21 9:26:50 AM  |
| http-www.metasploit.com-.lnk                                   | 1    | Regular File    | 2016-06-21 9:27:00 AM  |
| desktop.ini  | 1    | Regular File    | 2016-06-21 8:37:53 AM  |
| Downloads.lnk  | 1    | Regular File    | 2016-06-21 11:17:44 AM |
| 150902_WILD_CutePenguins.jpg.CROP.promo-slange2.jpg.lnk.Fil... | 1    | File Slack      |                        |
| rmagican.mi.lnk  | 1    | Regular File    | 2016-06-21 1:05:19 PM  |
| Outlook.lnk  | 1    | Regular File    | 2016-06-21 1:15:00 PM  |
| Hackers Got real Brain.lnk.FileSlack                           | 1    | File Slack      |                        |
| Hash_Suite_Free_3_4.zip.lnk                                    | 1    | Regular File    | 2016-06-21 11:06:24 AM |
| Exfiltration_Diagram.png.lnk.FileSlack                         | 1    | File Slack      |                        |
| info.lnk   | 1    | Regular File    | 2016-06-21 11:52:07 AM |
| burpsuite_free_v1.7.03.jar.lnk                                 | 1    | Regular File    | 2016-06-21 11:17:44 AM |
| backlog.gpt.lnk  | 1    | Regular File    | 2016-06-21 1:15:00 PM  |
| TechnicalInfo.txt.lnk  | 1    | Regular File    | 2016-06-21 11:52:06 AM |
| 00.jpg.lnk.FileSlack   | 1    | File Slack      |                        |
| home-network-design-networking-for-a-single-family-home.c...   | 2    | File Slack      |                        |
| how_do_threat_actors_steal_your_data.lnk.FileSlack             | 2    | File Slack      |                        |
| Rym_VanAntwerp_thesis.lnk.FileSlack                            | 2    | File Slack      |                        |
| defcon-16-nicks.lnk.FileSlack                                  | 2    | File Slack      |                        |
| fakemem.7z.lnk.FileSlack                                       | 2    | File Slack      |                        |

Custom Content Sources

Evidence File System Path File Options

000|4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 |.....A....  
010 00 00 00 46 9B 00 20 00 00 00 00 7A 3D C8 30 |...F... ..pE0  
020 AC CB D1 01 7A 3D C8 30 AC CB D1 01 8F 14 69 5E |...pE0-EB-1-1\*

```

C:\Users\SANSDFIR\Desktop\c16-Hunter>clean
'clean' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\SANSDFIR\Desktop\c16-Hunter>LECmd -f burpsuite_free_v1.7.03.jar.lnk
LECmd version 1.4.0.0

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

Command line: -f burpsuite_free_v1.7.03.jar.lnk

Processing 'burpsuite_free_v1.7.03.jar.lnk'

Source file: C:\Users\SANSDFIR\Desktop\c16-Hunter\burpsuite_free_v1.7.03.jar.lnk
Source created: 2016-06-21 11:17:44
Source modified: 2016-06-21 11:17:44
Source accessed: 2022-08-30 15:59:53

--- Header ---
Target created: 2016-06-21 11:00:58
Target modified: 2016-06-21 11:02:14
Target accessed: 2016-06-21 11:00:58

File size: 12,397,221
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode, DisableKnownFolderTracking
File attributes: FileAttributeArchive
Icon index: 0
Show window: SuNormal (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)

Relative Path: ..\..\..\..\Downloads\burpsuite_free_v1.7.03.jar
Working Directory: C:\Users\Hunter\Downloads

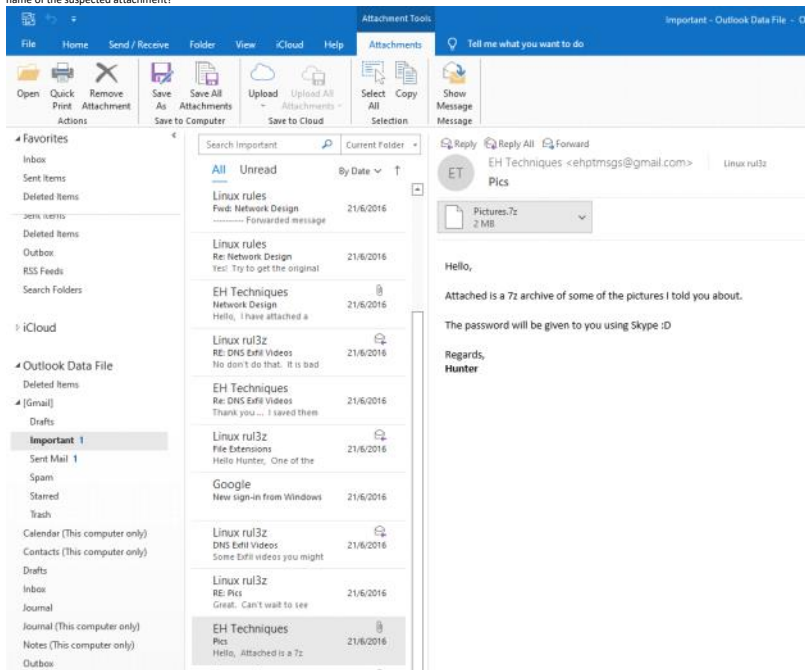
--- Link information ---
Flags: VolumeIdAndLocalBasePath, CommonNetworkRelativeLinkAndPathSuffix

>>Volume information
Drive type: Fixed storage media (Hard drive)
Serial number: 669B1B2A
Label: (No label)

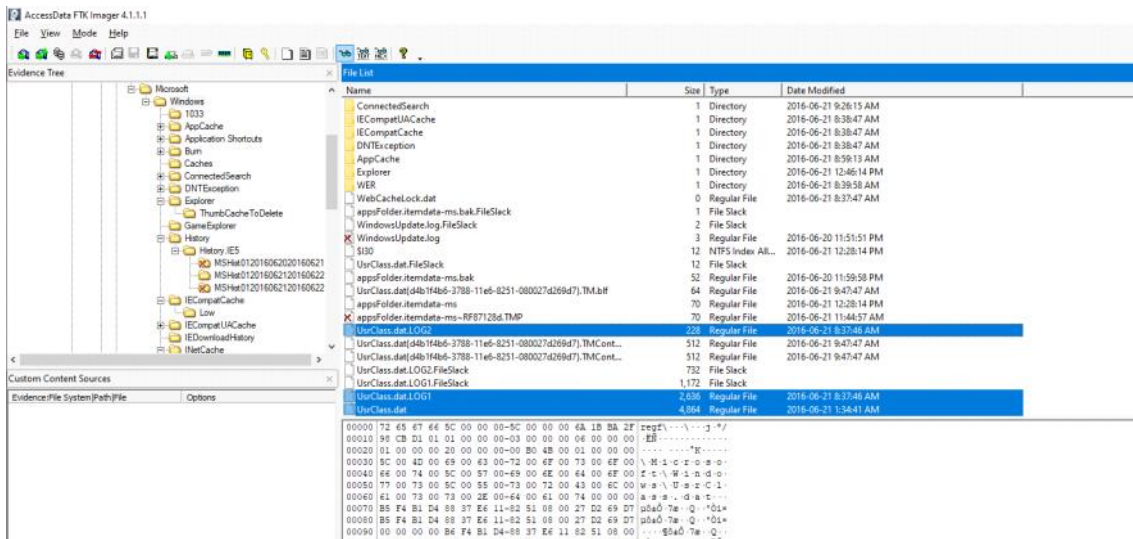
Network share information
Share name: \\MORENSICS\Users
Provider type: WnnNetlannan
Share flags: ValidNetType
File name: burpsuite_free_v1.7.03.jar

```

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



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?



ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

My Computer

Downloads

Documents

C:

Users

Hunter

Documents

Downloads

Pictures

Exfil

Links

Desktop

Contacts

Dropbox

Tracing

Info

Google Drive

New folder

Program Files (x86)

PerfLogs

Pictures

E:

Music

Shared Documents Folder (Users Files)

Computers and Devices

Recent Places

Control Panel

Drag a column header here to group by that column

| Value | Icon    | Shell Type | MRU Position | Created On | Modified On | Accessed On | First Interacted | Last Interacted | Has Explored | Miscellaneous |
|-------|---------|------------|--------------|------------|-------------|-------------|------------------|-----------------|--------------|---------------|
|       | No m... |            | --           | --         | --          | --          | --               | --              |              |               |

Summary Details Hex

**Name:** Exfil  
**Absolute path:** Desktop\My Computer\C:\Users\Hunter\Pictures\Exfil  
**Key-Value name path:** BagMRU\1\0\1\0\8-0  
**Registry last write time:** 2016-06-21 12:17:36.631

**Target timestamps**  
**Created on:** 2016-06-21 09:37:38.000  
**Modified on:** 2016-06-21 09:38:14.000  
**Last accessed on:** 2016-06-21 09:38:14.000

**Miscellaneous**  
**Shell type:** Directory  
**Node slot:** 52  
**MRU position:** 0  
**# of child bags:** 0

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?

AccessData FTK Imager 4.1.1.1

File View Mode Help

Evidence Tree

Custom Content Image(NTFS) [AD1]

c:\16-Hunter\NONAME [NTFS]

boot

\$Recycle.Bin

Program Files (x86)

Users

Hunter

zerrmap

AppData

Desktop

Documents

Downloads

Pictures

backgrounds

Exfil

dns-exfiltration-using-sqlmap-18-728.jpg

Exfiltration\_Diagram.png

Thumbs.db

Private

Thumbs.db

Windows

File List

| Name                                     | Size | Type         | Date Modified          |
|--|------|--------------|------------------------|
| Thumbs.db                                | 24   | Regular File | 2016-06-21 12:03:26 PM |
| dns-exfiltration-using-sqlmap-18-728.jpg | 71   | Regular File | 2016-06-21 9:38:13 AM  |
| Exfiltration_Diagram.png                 | 98   | Regular File | 2016-06-21 9:37:50 AM  |

Custom Content Sources

Evidence File System(Path/File) Options

AccessData FTK Imager 4.1.1.1

File View Mode Help

Evidence Tree

Custom Content Image(NTFS) [AD1]

c:\16-Hunter\NONAME [NTFS]

boot

\$Recycle.Bin

Program Files (x86)

Users

Hunter

zerrmap

AppData

Desktop

Documents

Downloads

Pictures

backgrounds

Exfil

dns-exfiltration-using-sqlmap-18-728.jpg

Exfiltration\_Diagram.png

Thumbs.db

Private

Thumbs.db

Windows

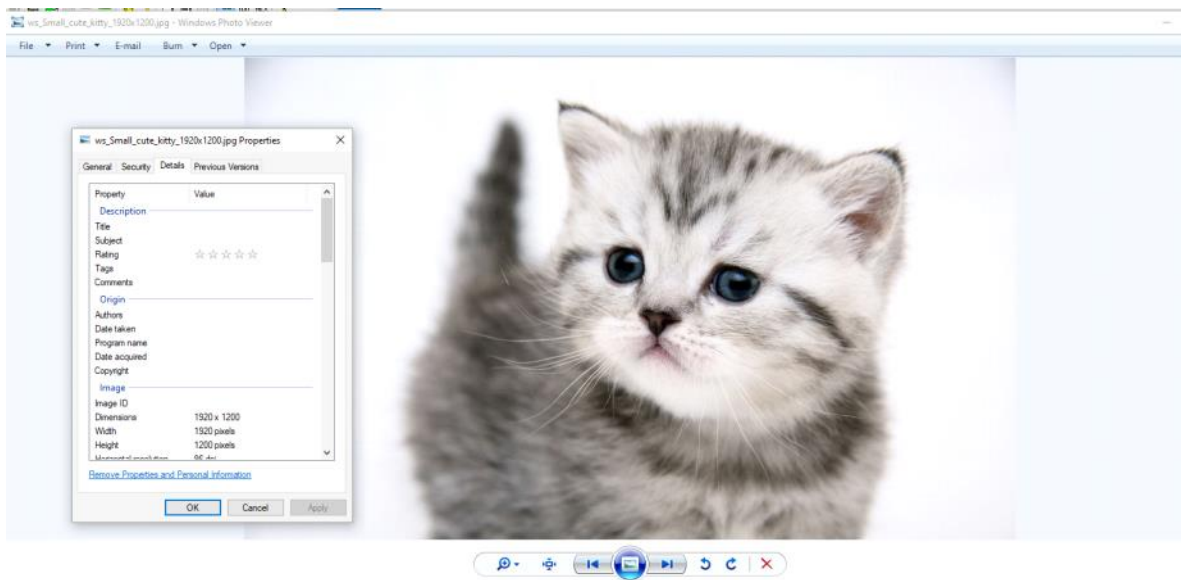
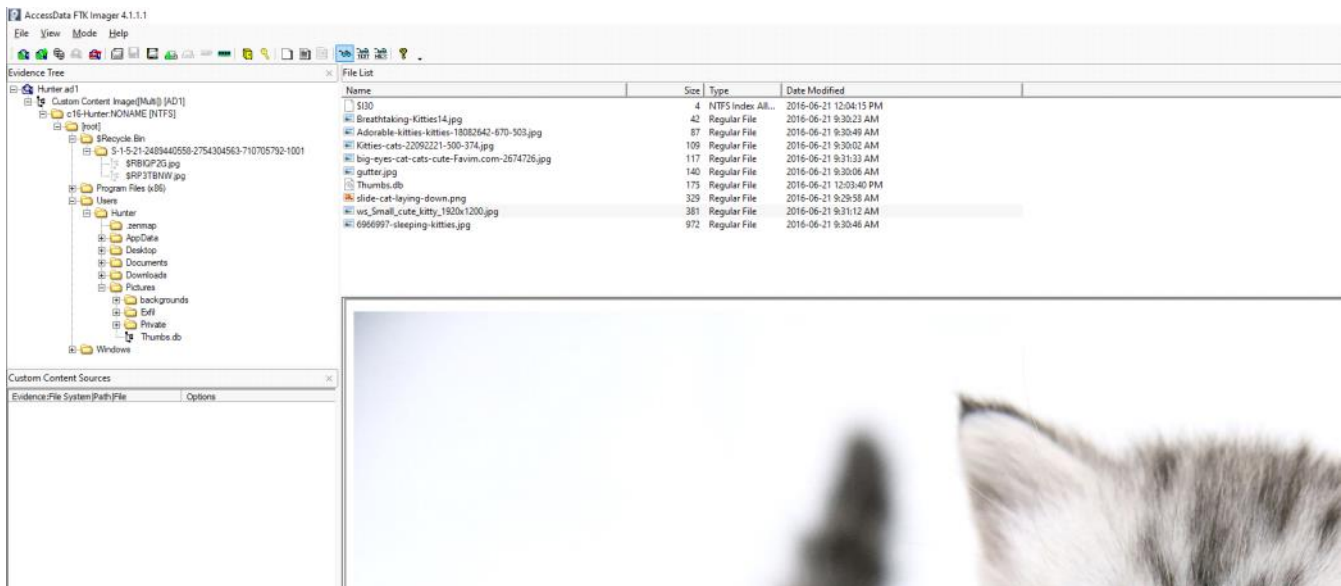
File List

| Name         | Size | Type         | Date Modified         |
|--------------|------|--------------|-----------------------|
| desktop.ini  | 1    | Regular File | 2016-06-21 8:38:00 AM |
| SRBICP2G.jpg | 17   | Regular File | 2016-06-21 9:31:40 AM |
| SRP3TBNW.jpg | 381  | Regular File | 2016-06-21 9:31:20 AM |

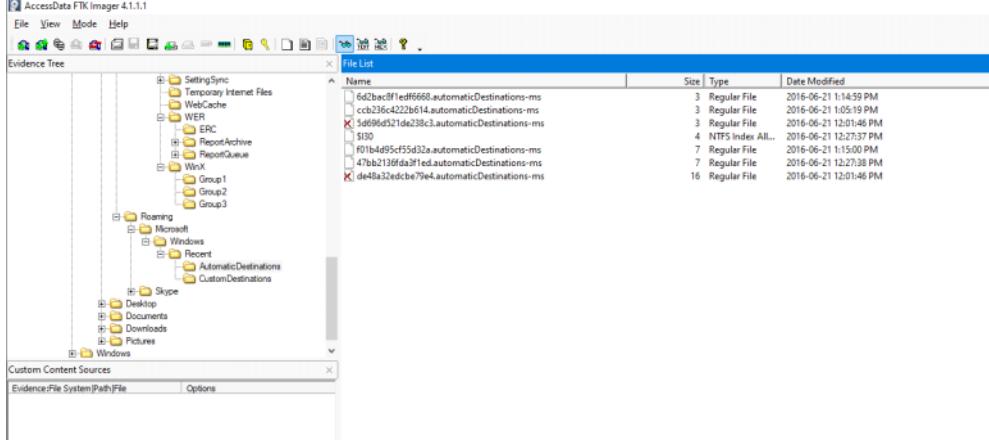
Custom Content Sources

Evidence File System(Path/File) Options





29. Provide the name of the directory where information about jump lists items (created automatically by the system) is stored?  
 C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations



30. Using JUMP LIST analysis, provide the full path of the application with the AppID of "aa28770954eaeaaa" used to bypass network security monitoring controls.

