CS5332: Individual/Group Assignment 2

Questions 1 - 12

1. What are the hash values (MD5 & SHA-1) of all images?

PC ‘DD’ image MD5:

```
root@kali:~/Desktop/Assignment2_Images# md5sum cfreds_2015_data_leakage_pc.dd
a49d1254c873808c58e6f1bcd60b5bde  cfreds_2015_data_leakage_pc.dd
```

PC ‘DD’ image SHA-1:

```
root@kali:~/Desktop/Assignment2_Images# sha1sum cfreds_2015_data_leakage_pc.dd
afe5c9ab487bd47a8a9856b1371c2384d44fd785  cfreds_2015_data_leakage_pc.dd
```

Removable media #1 ‘EnCase’ image MD5:

```
root@kali:~/Desktop/Assignment2_Images# md5sum cfreds_2015_data_leakage_rm#1.E01
7cd7bc148d3a1e5f329cb3580d4d4f8f  cfreds_2015_data_leakage_rm#1.E01
```

Removable media #1 ‘EnCase’ image SHA-1:

```
root@kali:~/Desktop/Assignment2_Images# sha1sum cfreds_2015_data_leakage_rm#1.E01
ffd0f3cba3dfe3291f786b845a06a8aa56c1cd8c  cfreds_2015_data_leakage_rm#1.E01
```

Removable media #2 ‘DD’ image MD5:

```
root@kali:~/Desktop/Assignment2_Images# md5sum cfreds_2015_data_leakage_rm#2.dd
b4644902acab4583a1d0f9f1a08faa77  cfreds_2015_data_leakage_rm#2.dd
```

Removable media #2 ‘DD’ image SHA-1:

```
root@kali:~/Desktop/Assignment2_Images# sha1sum cfreds_2015_data_leakage_rm#2.dd
048961a85ca3eced8cc73f1517442d31d4dca0a3  cfreds_2015_data_leakage_rm#2.dd
```

Removable media #3 (type 2) ‘DD’ image MD5:

```
root@kali:~/Desktop/Assignment2_Images# md5sum cfreds_2015_data_leakage_rm#3_type2.dd
858c7250183a44dd83eb706f3f178990  cfreds_2015_data_leakage_rm#3_type2.dd
```

Removable media #3 (type 2) ‘DD’ image SHA-1:

```
root@kali:~/Desktop/Assignment2_Images# sha1sum cfreds_2015_data_leakage_rm#3_type2.dd
471d3eedca9add872fc0708297284e1960ff44f8  cfreds_2015_data_leakage_rm#3_type2.dd
```

2. Identify the partition information of PC image.

```
root@kali:~/Desktop/Assignment2_Images# mmls cfreds_2015_data_leakage_pc.dd -B
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Size    Description
000:  Meta      0000000000   0000000000   0000000001   0512B   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   1024K   Unallocated
002:  000:000   0000002048   0000206847   0000204800   0100M   NTFS / exFAT (0x07)
003:  000:001   0000206848   0041940991   0041734144   0019G   NTFS / exFAT (0x07)
004:  -------   0041940992   0041943039   0000002048   1024K   Unallocated
```

3. Explain installed OS information in detail.
(OS name, install date, registered owner…)

Hex | Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences

Result: 1 of 118 Result — Operating System Information

Type	Value
Program Name	Windows 7 Ultimate Service Pack 1
Date/Time	2015-03-22 19:34:26
Path	C:\Windows
Product ID	00426-292-0000007-85262
Owner	informant
Organization	
Source File Path	/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Windows/System32/config/RegBack/SOFTWARE
Artifact ID	-9223372036854773948

Hex | Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences

Name	/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Windows/System32/config/RegBack/SOFTWARE
Type	File System
MIME Type	application/octet-stream
Size	48070656
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-25 13:24:09 GMT
Accessed	2015-03-25 13:23:50 GMT
Created	2015-03-25 10:15:19 GMT
Changed	2015-03-25 13:24:09 GMT

Hex | Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences

Result: 1 of 126 Result

Operating System Information

Type	Value
Program Name	Windows 7 Ultimate Service Pack 1
Date/Time	2015-03-22 19:34:26
Path	C:\Windows
Product ID	00426-292-0000007-85262
Owner	informant
Organization	
Source File Path	/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854773886

Hex | Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences

Name	/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Windows/System32/config/SOFTWARE
Type	File System
MIME Type	application/octet-stream
Size	48496640
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-25 15:31:05 GMT
Accessed	2015-03-25 15:31:05 GMT
Created	2009-07-14 02:34:08 GMT
Changed	2015-03-25 15:31:05 GMT

4. What is the timezone setting?

```
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 584  (S-1-5-18)
Last User Journal Update Sequence Number: 69763472
Created:        2009-07-13 21:34:08.088364600 (Central Daylight Time)
File Modified:  2015-03-25 10:31:05.341208900 (Central Daylight Time)
MFT Modified:   2015-03-25 10:31:05.294408800 (Central Daylight Time)
Accessed:       2015-03-25 10:31:05.341208900 (Central Daylight Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: SYSTEM
Parent MFT Entry: 2360  Sequence: 1
Allocated Size: 0       Actual Size: 0
Created:        2015-03-25 06:13:39.503881500 (Central Daylight Time)
File Modified:  2015-03-25 06:13:39.503881500 (Central Daylight Time)
MFT Modified:   2015-03-25 06:13:39.503881500 (Central Daylight Time)
Accessed:       2015-03-25 06:13:39.503881500 (Central Daylight Time)
```

5. What is the computer name?

Source File	Name
SYSTEM	INFORMANT-PC
SYSTEM	INFORMANT-PC

6. List all accounts in OS except the system accounts: Administrator, Guest, systemprofile, LocalService, NetworkService.
(Account name, login count, last logon date…)

Source File	Username	User ID	Path	Data Source	Tags
SOFTWARE	systemprofile	S-1-5-18	%systemroot%\system32\config\systemprofile	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	LocalService	S-1-5-19	C:\Windows\ServiceProfiles\LocalService	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	NetworkService	S-1-5-20	C:\Windows\ServiceProfiles\NetworkService	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	informant	S-1-5-21-2425377081-3129163575-2985601102-1000	C:\Users\informant	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	admin11	S-1-5-21-2425377081-3129163575-2985601102-1001	C:\Users\admin11	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	temporary	S-1-5-21-2425377081-3129163575-2985601102-1003	C:\Users\temporary	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	systemprofile	S-1-5-18	%systemroot%\system32\config\systemprofile	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	LocalService	S-1-5-19	C:\Windows\ServiceProfiles\LocalService	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	NetworkService	S-1-5-20	C:\Windows\ServiceProfiles\NetworkService	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	informant	S-1-5-21-2425377081-3129163575-2985601102-1000	C:\Users\informant	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	admin11	S-1-5-21-2425377081-3129163575-2985601102-1001	C:\Users\admin11	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	temporary	S-1-5-21-2425377081-3129163575-2985601102-1003	C:\Users\temporary	cfreds_2015_data_leakage_pc.E01	

- informant
- admin11
- temporary

7. Who was the last user to login to PC?

Name	Modified Time	Change Time	Access Time	Created Time
[parent folder]	2015-03-25 15:19:05 GMT	2015-03-25 15:19:05 GMT	2015-03-25 15:19:05 GMT	2009-07-14 02:38:56 GMT
informant	2015-03-23 20:05:32 GMT	2015-03-23 20:05:32 GMT	2015-03-23 20:05:32 GMT	2015-03-22 14:34:31 GMT
temporary	2015-03-22 15:56:02 GMT	2015-03-22 15:56:02 GMT	2015-03-22 15:56:02 GMT	2015-03-22 15:55:57 GMT
[current folder]	2015-03-22 15:55:57 GMT	2015-03-22 15:55:57 GMT	2015-03-22 15:55:57 GMT	2009-07-14 03:20:08 GMT
admin11	2015-03-22 15:53:56 GMT	2015-03-22 15:53:56 GMT	2015-03-22 15:53:56 GMT	2015-03-22 15:53:44 GMT
Public	2010-11-21 07:16:46 GMT	2015-03-25 11:13:57 GMT	2010-11-21 07:16:46 GMT	2009-07-14 03:20:08 GMT
Default	2009-07-14 07:07:31 GMT	2015-03-25 11:13:57 GMT	2009-07-14 07:07:31 GMT	2009-07-14 03:20:08 GMT
All Users	2009-07-14 05:08:56 GMT	2015-03-25 11:14:20 GMT	2009-07-14 05:08:56 GMT	2009-07-14 05:08:56 GMT
Default User	2009-07-14 05:08:56 GMT	2015-03-25 11:14:20 GMT	2009-07-14 05:08:56 GMT	2009-07-14 05:08:56 GMT
desktop.ini	2009-07-14 04:54:24 GMT	2015-03-25 11:09:29 GMT	2009-07-14 04:54:24 GMT	2009-07-14 04:54:24 GMT

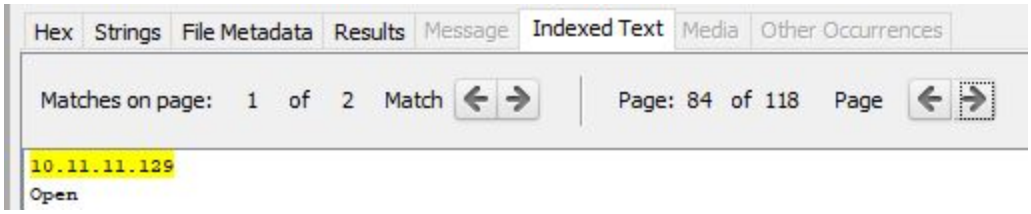
8. When was the last recorded shutdown date/time?

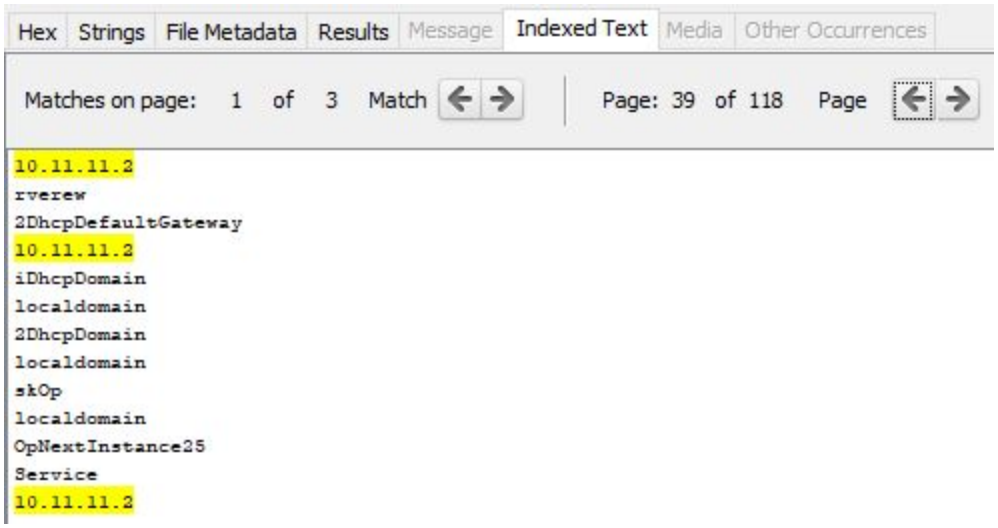
Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time
Microsoft-Windows-Windows Firewall With Advanced Security%4Fi	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-25 10:15:55 GMT	2015-03-25 10:15:55 GMT
Microsoft-Windows-WindowsBackup%4ActionCenter.evtx	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-22 14:36:43 GMT	2015-03-22 14:36:43 GMT
Microsoft-Windows-WindowsSystemAssessmentTool%4Operationa	2015-03-24 21:07:27 GMT	2015-03-24 21:07:27 GMT	2015-03-25 10:33:14 GMT	2015-03-25 10:33:14 GMT
Microsoft-Windows-WindowsUpdateClient%4Operational.evtx	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-25 10:18:28 GMT	2015-03-25 10:18:28 GMT
Microsoft-Windows-Winlogon%4Operational.evtx	2015-03-22 14:38:16 GMT	2015-03-22 14:38:16 GMT	2015-03-22 14:34:33 GMT	2015-03-22 14:34:33 GMT
OAlerts.evtx	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-22 15:03:49 GMT	2015-03-22 15:03:49 GMT
Security.evtx	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-25 10:15:47 GMT	2015-03-25 10:15:47 GMT
Setup.evtx	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-25 10:18:25 GMT	2015-03-25 10:18:25 GMT
System.evtx	2015-03-25 15:31:01 GMT	2015-03-25 15:31:01 GMT	2015-03-25 10:15:47 GMT	2015-03-25 10:15:47 GMT
Windows PowerShell.evtx	2015-03-25 10:18:29 GMT	2015-03-25 10:18:29 GMT	2015-03-25 10:15:47 GMT	2015-03-25 10:15:47 GMT
[current folder]	2015-03-24 15:21:26 GMT	2015-03-24 15:21:26 GMT	2015-03-24 15:21:26 GMT	2009-07-14 03:20:14 GMT
[parent folder]	2009-07-14 03:20:14 GMT	2015-03-25 11:14:02 GMT	2009-07-14 03:20:14 GMT	2009-07-14 03:20:14 GMT

2015-03-25, 10:15:47 GMT

9. Explain the information of network interface(s) with an IP address assigned by DHCP.





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

Source File	Program Name	Date/Time	Data Source	Tags
SOFTWARE	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 19:57:31 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 19:54:33 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 19:54:06 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft .NET Framework 4 Client Profile v.4.0.30319	2015-03-25 19:52:06 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft .NET Framework 4 Client Profile v.4.0.30319	2015-03-25 19:51:39 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	DXM_Runtime	2015-03-25 15:15:21 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	MPlayer2	2015-03-25 15:15:21 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	DXM_Runtime	2015-03-25 15:15:21 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	MPlayer2	2015-03-25 15:15:21 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Google Drive v.1.20.8672.3137	2015-03-24 01:02:46 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Google Drive v.1.20.8672.3137	2015-03-24 01:02:46 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	iCloud v.4.0.6.28	2015-03-24 01:01:54 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Apple Software Update v.2.1.3.127	2015-03-24 01:01:01 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Apple Software Update v.2.1.3.127	2015-03-24 01:01:01 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Bonjour v.3.0.0.10	2015-03-24 01:00:58 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Bonjour v.3.0.0.10	2015-03-24 01:00:58 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Apple Application Support v.3.0.6	2015-03-24 01:00:45 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Apple Application Support v.3.0.6	2015-03-24 01:00:45 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Google Update Helper v.1.3.26.9	2015-03-22 20:16:03 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Google Update Helper v.1.3.26.9	2015-03-22 20:16:03 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Google Chrome v.41.0.2272.101	2015-03-22 20:11:51 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Google Chrome v.41.0.2272.101	2015-03-22 20:11:51 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 20:04:14 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 20:04:14 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 20:03:33 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 20:03:33 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office 32-bit Components 2013 v.15.0.4420.1017	2015-03-22 20:01:46 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office 32-bit Components 2013 v.15.0.4420.1017	2015-03-22 20:01:46 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Word MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:38 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Word MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:38 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Outlook MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:37 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Outlook MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:37 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office OSM MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:34 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office OSM UX MUI (English) 2013 v.15.0.4420.1...	2015-03-22 20:01:34 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office OSM MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:34 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office OSM UX MUI (English) 2013 v.15.0.4420.1...	2015-03-22 20:01:34 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:32 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:32 GMT	cfreds_2015_data_leakage_pc.E01	

Source File	Program Name	Date/Time	Data Source	Tags
SOFTWARE	Microsoft Office Proofing (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:32 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:32 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing Tools 2013 - English v.15.0.4420....	2015-03-22 20:01:31 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing Tools 2013 - English v.15.0.4420....	2015-03-22 20:01:31 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Outils de vérification linguistique 2013 de Microsoft Office -...	2015-03-22 20:01:30 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Outils de vérification linguistique 2013 de Microsoft Office -...	2015-03-22 20:01:30 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing Tools 2013 - Español v.15.0.4420...	2015-03-22 20:01:14 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Proofing Tools 2013 - Español v.15.0.4420...	2015-03-22 20:01:14 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft OneNote MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:13 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft OneNote MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:13 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Groove MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:12 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Groove MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:12 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft DCF MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:11 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft DCF MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:11 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Publisher MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:10 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Publisher MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:10 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft PowerPoint MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:09 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft PowerPoint MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:09 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Excel MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:07 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Excel MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:07 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Lync MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:05 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Lync MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:05 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Shared 32-bit MUI (English) 2013 v.15.0.4...	2015-03-22 20:01:04 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Shared 32-bit MUI (English) 2013 v.15.0.4...	2015-03-22 20:01:04 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft InfoPath MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:03 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft InfoPath MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:03 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Access MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:02 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Access Setup Metadata MUI (English) 2013 v.15....	2015-03-22 20:01:02 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Access MUI (English) 2013 v.15.0.4420.1017	2015-03-22 20:01:02 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Access Setup Metadata MUI (English) 2013 v.15....	2015-03-22 20:01:02 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Shared Setup Metadata MUI (English) 201...	2015-03-22 20:01:01 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Shared Setup Metadata MUI (English) 201...	2015-03-22 20:01:01 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Shared MUI (English) 2013 v.15.0.4420.1...	2015-03-22 20:00:59 GMT	cfreds_2015_data_leakage_pc.E01	
SOFTWARE	Microsoft Office Shared MUI (English) 2013 v.15.0.4420.1...	2015-03-22 20:00:59 GMT	cfreds_2015_data_leakage_pc.E01	

11. List application execution logs.
(Executable path, execution time, execution count...)

/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Users/informant/Desktop/Download

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time
Eraser 6.2.0.2962.exe	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT
Eraser 6.2.0.2962.exe:Zone.Identifier	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT
IE11-Windows6.1-x64-en-us.exe	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT
IE11-Windows6.1-x64-en-us.exe:Zone.Identifier	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT
[current folder]	2015-03-25 15:15:45 GMT	2015-03-25 15:15:45 GMT	2015-03-25 15:15:45 GMT	2015-03-22 15:08:23 GMT
[parent folder]	2015-03-25 15:29:08 GMT	2015-03-25 15:29:08 GMT	2015-03-25 15:29:08 GMT	2015-03-22 14:34:41 GMT
ccsetup504.exe	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT
ccsetup504.exe:Zone.Identifier	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT

/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Program Files/Microsoft Office/Office15

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time
EMABLT32.DLL	2012-10-02 00:36:36 GMT	2015-03-22 15:03:06 GMT	2015-03-22 15:03:06 GMT	2012-10-02 00:36:36 GMT
EMSMDB32.DLL	2012-10-02 00:36:36 GMT	2015-03-22 15:03:06 GMT	2015-03-22 15:03:06 GMT	2012-10-02 00:36:36 GMT
ENGDIC.DAT	2012-09-29 18:11:26 GMT	2015-03-22 15:03:06 GMT	2015-03-22 15:03:06 GMT	2012-09-29 18:11:26 GMT
ENGIDX.DAT	2012-09-29 18:11:26 GMT	2015-03-22 15:03:06 GMT	2015-03-22 15:03:06 GMT	2012-09-29 18:11:26 GMT
ENGLISH.LNG	2012-09-29 18:11:44 GMT	2015-03-22 15:02:46 GMT	2015-03-22 15:01:31 GMT	2012-09-29 18:11:44 GMT
ENVELOPE.DLL	2012-10-02 00:36:36 GMT	2015-03-22 15:03:06 GMT	2015-03-22 15:03:06 GMT	2012-10-02 00:36:36 GMT
EXCEL.EXE	2012-10-02 00:36:36 GMT	2015-03-22 15:03:07 GMT	2015-03-22 15:03:07 GMT	2012-10-02 00:36:36 GMT

Name	Location	Modified Time	Change Time	Access Time	Created Time
ccsetup504.exe	/img_cfreds_2015_...	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT
ccsetup504.exe-slack	/img_cfreds_2015_...	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT	2015-03-25 14:48:28 GMT
standard[1].htm	/img_cfreds_2015_...	2015-03-25 14:48:21 GMT	2015-03-25 14:48:21 GMT	2015-03-25 14:48:21 GMT	2015-03-25 14:48:21 GMT
MTP_ySUJH_bn48VBG8sNSnhCUOGz7vYGh680lGh-uXM[	/img_cfreds_2015_...	2015-03-25 14:47:55 GMT	2015-03-25 14:47:55 GMT	2015-03-25 14:47:55 GMT	2015-03-25 14:47:55 GMT
{D10B9AEF-D2FD-11E4-B734-000C29FF2429}.dat	/img_cfreds_2015_...	2015-03-25 14:47:46 GMT	2015-03-25 14:47:46 GMT	2015-03-25 14:47:11 GMT	2015-03-25 14:47:11 GMT
Eraser 6.2.0.2962.exe	/img_cfreds_2015_...	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT	2015-03-25 14:47:40 GMT

Apple Software Update.lnk	/img_cfreds_2015_data...	2015-03-23 20:01:00 GMT	2015-03-24 15:16:26 GMT	2015-03-23 20:01:00 GMT	2015-03-23 20:01:00 GMT
msvcr80.dll	/img_cfreds_2015_data...	2015-03-23 20:00:48 GMT	2015-03-23 20:00:48 GMT	2015-03-23 20:00:48 GMT	2015-03-23 20:00:48 GMT
icloudsetup.exe	/img_cfreds_2015_data...	2015-03-23 19:56:53 GMT	2015-03-23 19:56:53 GMT	2015-03-23 19:55:47 GMT	2015-03-23 19:55:47 GMT
googledrivesync.exe	/img_cfreds_2015_data...	2015-03-23 19:56:33 GMT	2015-03-23 19:56:33 GMT	2015-03-23 19:56:30 GMT	2015-03-23 19:56:30 GMT
f_00011b	/img_cfreds_2015_data...	2015-03-23 19:55:29 GMT	2015-03-23 19:55:29 GMT	2015-03-23 19:55:29 GMT	2015-03-23 19:55:29 GMT

program_files_internet_explorer_a421d1bfaf856e2b.cd	2015-03-22 15:17:19 GMT	2015-03-22 15:18:58 GMT	2015-03-22 15:17:19 GMT	2009-07-14 02:59:35 GMT
MsSpellCheckingFacility.exe	2015-03-22 15:17:05 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:05 GMT	2015-03-22 15:17:05 GMT
MsSpellCheckingFacility.exe	2015-03-22 15:17:05 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:05 GMT	2015-03-22 15:17:05 GMT

wininet.dll	2015-03-22 15:17:01 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
RegisterIEPKEYs.exe	2015-03-22 15:17:01 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
iedvtool.dll.mui	2015-03-22 15:17:01 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT

iedvtool.dll.mui	2015-03-22 15:17:01 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
iecleanup.exe	2015-03-22 15:17:01 GMT	2015-03-22 15:17:05 GMT	2015-03-22 15:17:00 GMT	2015-03-22 15:17:00 GMT
iexpress.exe.mui	2015-03-22 15:17:01 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT

ConfigureIEOptionalComponents.exe	2015-03-22 15:17:01 GMT	2015-03-22 15:17:05 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
wininet.dll	2015-03-22 15:17:01 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
iedvtool.dll.mui	2015-03-22 15:17:01 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
RegisterIEPKEYs.exe	2015-03-22 15:17:01 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:01 GMT	2015-03-22 15:17:01 GMT
IEShims.dll	2015-03-22 15:17:00 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:00 GMT	2015-03-22 15:17:00 GMT
ieinstal.exe	2015-03-22 15:17:00 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:00 GMT	2015-03-22 15:17:00 GMT
WininetPlugin.dll	2015-03-22 15:17:00 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:00 GMT	2015-03-22 15:17:00 GMT
urlmon.dll	2015-03-22 15:17:00 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:17:00 GMT	2015-03-22 15:17:00 GMT
ieinstal.exe	2015-03-22 15:17:00 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:17:00 GMT	2015-03-22 15:17:00 GMT

wextract.exe	2015-03-22 15:16:59 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:59 GMT	2015-03-22 15:16:59 GMT
inseng.dll	2015-03-22 15:16:59 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:59 GMT	2015-03-22 15:16:59 GMT
msfeeds.dll	2015-03-22 15:16:59 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:59 GMT	2015-03-22 15:16:59 GMT
mshtml.dll	2015-03-22 15:16:59 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:58 GMT	2015-03-22 15:16:58 GMT
wextract.exe	2015-03-22 15:16:59 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:59 GMT	2015-03-22 15:16:59 GMT

ExtExport.exe	2015-03-22 15:16:58 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:16:58 GMT	2015-03-22 15:16:58 GMT
jscript9.dll	2015-03-22 15:16:58 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:58 GMT	2015-03-22 15:16:58 GMT
SetIEInstalledDate.exe	2015-03-22 15:16:58 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:58 GMT	2015-03-22 15:16:58 GMT
ExtExport.exe	2015-03-22 15:16:58 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:16:58 GMT	2015-03-22 15:16:58 GMT
SetIEInstalledDate.exe	2015-03-22 15:16:58 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:58 GMT	2015-03-22 15:16:58 GMT

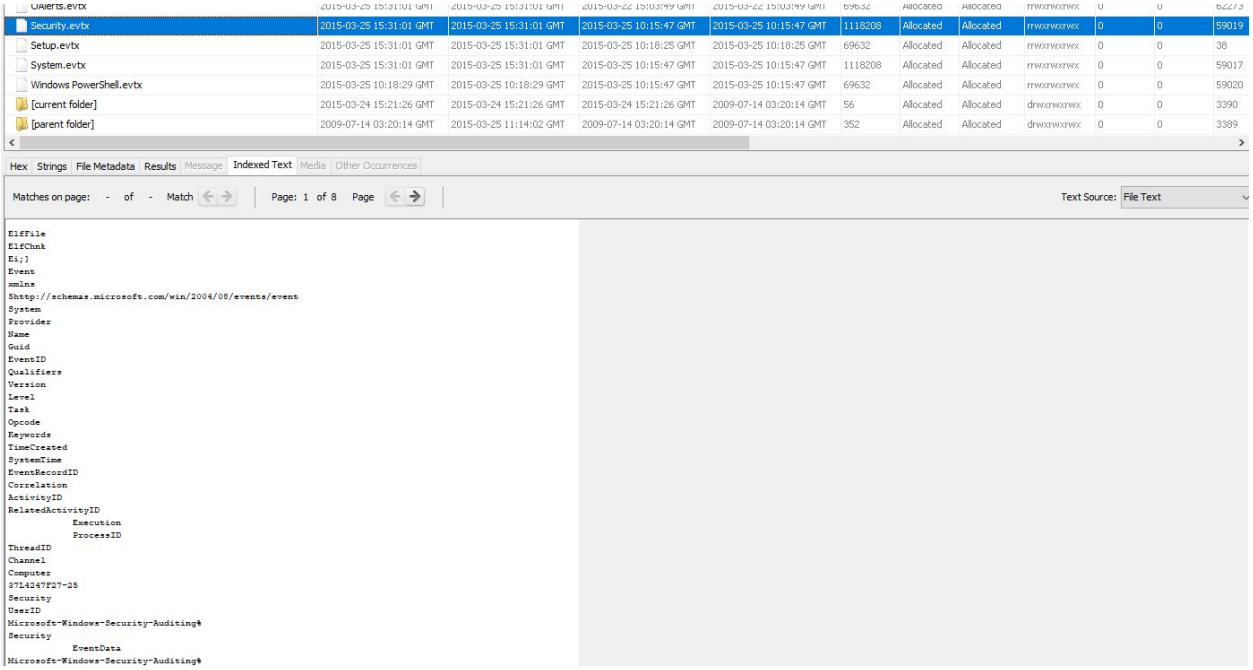
ConfigureIEOptionalComponents.exe	2015-03-22 15:16:56 GMT	2015-03-22 15:17:04 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT
urlmon.dll	2015-03-22 15:16:56 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT
wininet.dll	2015-03-22 15:16:56 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT
WininetPlugin.dll	2015-03-22 15:16:56 GMT	2015-03-22 15:19:00 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT
wininet.dll	2015-03-22 15:16:56 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT
iertutil.dll	2015-03-22 15:16:56 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:16:55 GMT	2015-03-22 15:16:55 GMT
RegisterIEPKEYs.exe	2015-03-22 15:16:56 GMT	2015-03-22 15:18:59 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT
iecleanup.exe	2015-03-22 15:16:56 GMT	2015-03-22 15:17:04 GMT	2015-03-22 15:16:56 GMT	2015-03-22 15:16:56 GMT

GoogleUpdateSetup.exe	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT
GoogleUpdateSetup.exe	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT
GoogleUpdateSetup.exe	2015-03-22 15:11:21 GMT	2015-03-22 15:11:21 GMT	2015-03-22 15:11:26 GMT	2015-03-22 15:11:26 GMT
chrome-installer.min[1].js	2015-03-22 15:11:13 GMT	2076-11-30 00:03:41 GMT	2015-03-22 15:11:12 GMT	2015-03-22 15:11:12 GMT
IE11-Windows6.1-x64-en-us.exe	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT	2015-03-22 15:11:04 GMT

41.0.2272.101_chrome_installer.exe	2015-03-19 21:36:00 GMT	2015-03-22 15:11:42 GMT	2015-03-22 15:11:42 GMT	2015-03-22 15:11:42 GMT
41.0.2272.101_chrome_installer.exe	2015-03-19 21:36:00 GMT	2015-03-22 15:11:42 GMT	2015-03-22 15:11:42 GMT	2015-03-22 15:11:42 GMT

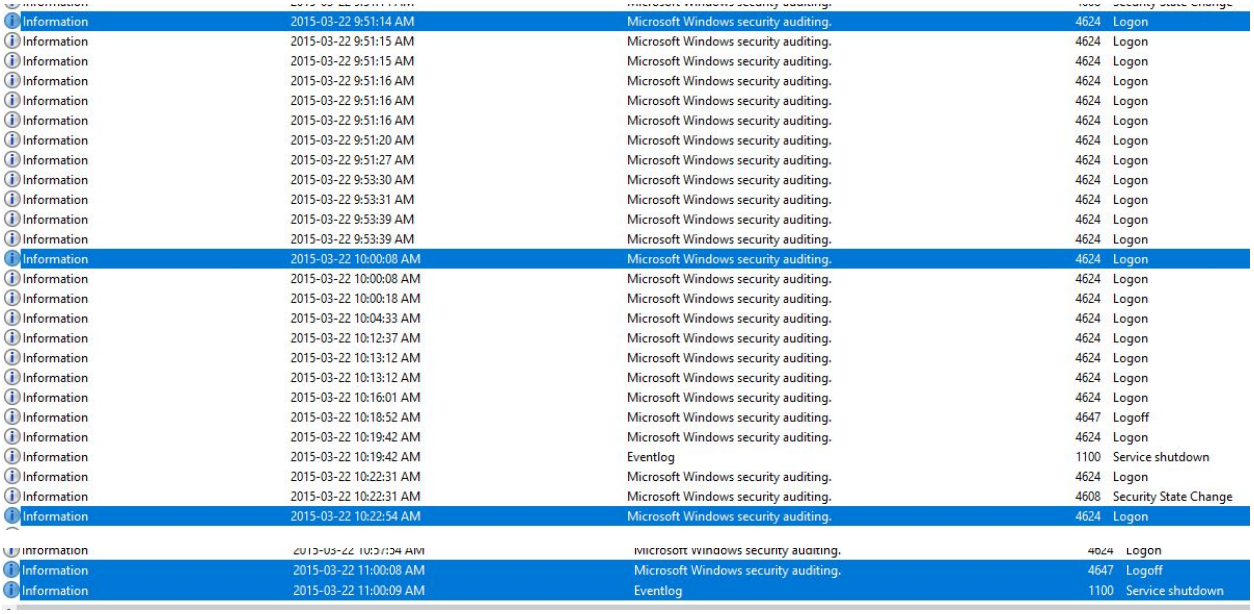
CCleaner.exe	2015-03-13 11:10:26 GMT	2015-03-25 15:18:36 GMT	2015-03-25 14:58:35 GMT	2015-03-13 11:10:26 GMT
CCleaner64.exe	2015-03-13 11:10:26 GMT	2015-03-25 15:18:36 GMT	2015-03-25 14:58:35 GMT	2015-03-13 11:10:26 GMT
CCleaner64.exe-slack	2015-03-13 11:10:26 GMT	2015-03-25 15:18:36 GMT	2015-03-25 14:58:35 GMT	2015-03-13 11:10:26 GMT

12. List all traces about the system on/off and the user logon/logoff.
(It should be considered only during a time range between 09:00 and 18:00 in the timezone from Question 4.)
The system logon/logoff and system on/off information are located in the windows security event logs. The log for security events is shown below:



I currently do not know how to port this over to an event viewer so that I can view the needed information to answer this question. Will keep trying...

Update: Found the required information. I exported the security event log and was able to use my local event viewer to view the log file.



Information	2015-03-23 12:24:23 PM	Microsoft Windows security auditing.	4608	Security State Change
Information	2015-03-23 12:24:23 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:24 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:24 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:24 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:24 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:25 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:26 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:28 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:41 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:41 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:24:53 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 12:26:34 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 1:36:07 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 3:00:22 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 3:00:45 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 3:01:01 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 3:01:02 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-23 4:02:53 PM	Microsoft Windows security auditing.	4647	Logoff
Information	2015-03-23 4:02:59 PM	Eventlog	1100	Service shutdown

Level	Date and Time	Source	Event ID	Task Category
Information	2015-03-24 10:14:30 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 10:21:38 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 10:21:38 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 10:22:39 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 10:46:14 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 1:28:38 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 1:28:38 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 3:58:52 PM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-24 4:07:25 PM	Microsoft Windows security auditing.	4647	Logoff
Information	2015-03-24 4:07:26 PM	Eventlog	1100	Service shutdown

Level	Date and Time	Source	Event ID	Task Category
Information	2015-03-25 9:31:53 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:45:59 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:45:59 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:50:28 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:50:30 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:50:30 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:50:50 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:56:55 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:57:18 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 9:57:18 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 10:18:54 AM	Microsoft Windows security auditing.	4624	Logon
Information	2015-03-25 10:30:57 AM	Microsoft Windows security auditing.	4647	Logoff
Information	2015-03-25 10:31:00 AM	Eventlog	1100	Service shutdown

Questions 13- 24

13. What web browsers were used?

Web Search 37 Results

Table | Thumbnail

Source File	Domain	Text	Program Name	Date Accessed	Data S
History	www.google.com	internet explorer 11	Chrome	2015-03-22 10:10:52 CDT	cfreds_
History	www.google.com	data leakage methods	Chrome	2015-03-23 13:02:09 CDT	cfreds_
History	www.google.com	leaking confidential information	Chrome	2015-03-23 13:02:44 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:03:40 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:05:18 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:05:19 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:05:22 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:05:48 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:06:27 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:14:50 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:15:44 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:16:55 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:17:14 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:18:10 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:18:15 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:18:30 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:18:43 CDT	cfreds_
History	www.google.com	information leakage cases	Chrome	2015-03-23 13:18:46 CDT	cfreds_

Web Search 37 Results

Table Thumbnail

Source File	Domain	Text	Program Name	Date Accessed	Data S
History	www.google.com	information leakage cases	Chrome	2015-03-23 14:47:43 CDT	cfreds_
History	www.google.com	google	Chrome	2015-03-23 14:48:19 CDT	cfreds_
History	www.google.com	apple icloud	Chrome	2015-03-23 14:55:09 CDT	cfreds_
History	www.google.com	google drive	Chrome	2015-03-23 14:56:04 CDT	cfreds_
index.dat	clients1.google.com	int	Internet Explorer	2015-03-22 15:09:43 CDT	cfreds_
index.dat	www.google.com	internet explorer 11	Internet Explorer	2015-03-22 15:09:48 CDT	cfreds_
index.dat	clients1.google.com	intern	Internet Explorer	2015-03-22 15:09:44 CDT	cfreds_
index.dat	clients1.google.com	internet explorer 11	Internet Explorer	2015-03-22 15:09:46 CDT	cfreds_
index.dat	clients1.google.com	internet e	Internet Explorer	2015-03-22 15:09:44 CDT	cfreds_
index.dat	clients1.google.com	i	Internet Explorer	2015-03-22 15:09:43 CDT	cfreds_
index.dat	clients1.google.com	interne	Internet Explorer	2015-03-22 15:09:44 CDT	cfreds_
index.dat	clients1.google.com	internet ex	Internet Explorer	2015-03-22 15:09:44 CDT	cfreds_
index.dat	clients1.google.com	internet explorer	Internet Explorer	2015-03-22 15:09:45 CDT	cfreds_
index.dat	clients1.google.com	internet explorer 1	Internet Explorer	2015-03-22 15:09:46 CDT	cfreds_
index.dat	clients1.google.com	inter	Internet Explorer	2015-03-22 15:09:43 CDT	cfreds_
index.dat	clients1.google.com	inte	Internet Explorer	2015-03-22 15:09:43 CDT	cfreds_
index.dat	clients1.google.com	in	Internet Explorer	2015-03-22 15:09:43 CDT	cfreds_
index.dat	clients1.google.com	internet	Internet Explorer	2015-03-22 15:09:44 CDT	cfreds_

Internet Explorer and **Google chrome** are the browsers that were used.

14. Identify directory/file paths related to the web browser history.

```
\USERS\INFORMANT\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\DEFAULT\MEDIA CACHE\F_000004
\PROGRAM FILES\MICROSOFT OFFICE\OFFICE15\FORMS\1033\TASKREQL.ICO

\USERS\INFORMANT\APPDATA\LOCALLOW\MICROSOFT\CRYPTNETURLCACHE\METADATA\3B6E683A7A45CC59BF035C9BA8C7AB9D

\USERS\INFORMANT\APPDATA\LOCALLOW\MICROSOFT\CRYPTNETURLCACHE\CONTENT\23B523C9E7746F716D33C6527C18EB9D

----\USERS\INFORMANT\APPDATA\ROAMING\MICROSOFT\INTERNET EXPLORER\QUICK LAUNCH\USER PINNED\TASKBAR\INTEF
\WINDOWS\ASSEMBLY\TMP\5ZY4HSUI\MICROSOFT.VISUALSTUDIO.TOOLS.APPLICATIONS.CONTRACT.V10.0.DLL
\WINDOWS\FONTS\SMALLFR.FON
\WINDOWS\FONTS\NIAGENG.TTF
\WINDOWS\INF\LLTDIO.PNF
----\USERS\INFORMANT\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\DEFAULT\EXTENSION STATE\000006.LDB
\WINDOWS\PREFETCH\SVCHOST.EXE-7CFEDEA3.PF
----\USERS\INFORMANT\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\DEFAULT\EXTENSIONS\AOHGHMIGHLIEIAINNEGKCIJNF
\USERS\INFORMANT\APPDATA\LOCAL\TEMP\3DC748A5-EFB9-4B58-B7BC-5CFAB6BE620A\WIN8IP-MICROSOFT-WINDOWS-DOWNL
\USERS\INFORMANT\APPDATA\LOCALLOW\MICROSOFT\CRYPTNETURLCACHE\METADATA\7D266D9E1E69FA1EEFB9699B009B34C8_
\WINDOWS\INSTALLER\8C20C.IPI
\WINDOWS\SYSTEM32\CATROOT\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\MICROSOFT-WINDOWS-MOBILEPC-CLIENT-SENS
\WINDOWS\MEDIA\WINDOWS USER ACCOUNT CONTROL.WAV
\PROGRAM FILES (X86)\GOOGLE\DRIVE\LANGUAGES\EN-US\CONTEXTMENUMODULE.DLL.MUI
-----\USERS\INFORMANT\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\LOW\CONTENT.IE5\4C689SI3
\USERS\INFORMANT\APPDATA\LOCAL\TEMP\3DC748A5-EFB9-4B58-B7BC-5CFAB6BE620A\WIN8IP-MICROSOFT-WINDOWS-DOWNL
```

15. What websites were the suspect accessing?

Web History 1339 Results

Table | Thumbnail

URL	Date Accessed	Referrer URL
http://tools.google.com/chrome/intl/en/welcome.html	2015-03-22 10:55:28 CDT	http://tools.google.com/chrome/intl/en/welcome.ht
https://www.google.com/intl/en/chrome/browser/welcome...	2015-03-22 10:55:28 CDT	https://www.google.com/intl/en/chrome/browser/v
https://www.google.com/webhp?sourceid=chrome-instant...	2015-03-22 10:55:40 CDT	https://www.google.com/webhp?sourceid=chrome
https://www.google.com/webhp?sourceid=chrome-instant...	2015-03-22 10:55:44 CDT	https://www.google.com/webhp?sourceid=chrome
http://windows.microsoft.com/en-us/internet-explorer/ie-1...	2015-03-22 10:10:24 CDT	http://windows.microsoft.com/en-us/internet-explo
https://www.google.com/chrome/browser/thankyou.html?...	2015-03-22 10:11:16 CDT	https://www.google.com/chrome/browser/thankyo
https://www.google.com/search?hl=en&source=hp&q=int...	2015-03-22 10:10:52 CDT	https://www.google.com/search?hl=en&source=hp
http://www.msn.com/?ocid=iehp	2015-03-22 10:09:24 CDT	http://www.msn.com/?ocid=iehp
http://windows.microsoft.com/en-us/internet-explorer/do...	2015-03-22 10:10:50 CDT	http://windows.microsoft.com/en-us/internet-explo
http://www.google.com/url?url=http://windows.microsoft....	2015-03-22 10:09:56 CDT	http://www.google.com/url?url=http://windows.mi
http://windows.microsoft.com/en-US/internet-explorer/pro...	2015-03-22 10:09:20 CDT	http://windows.microsoft.com/en-US/internet-expl
http://go.microsoft.com/fwlink/?LinkID=121792	2015-03-22 10:09:20 CDT	http://go.microsoft.com/fwlink/?LinkID=121792
http://windows.microsoft.com/en-us/internet-explorer/ie-8...	2015-03-22 10:09:22 CDT	http://windows.microsoft.com/en-us/internet-explo

URL	Date Accessed	Referrer URL
https://www.google.com/?gws_rd=ssl	2015-03-22 10:09:40 CDT	https://www.google.com/?gws_rd=ssl
http://www.google.com/url?url=http://windows.microsoft....	2015-03-22 10:09:52 CDT	http://www.google.com/url?url=http://windows.m
https://www.google.com/webhp?hl=en	2015-03-24 16:07:19 CDT	https://www.google.com/webhp?hl=en
https://dl.google.com/update2/1.3.26.9/GoogleInstaller_e...	2015-03-22 10:11:08 CDT	https://dl.google.com/update2/1.3.26.9/GoogleIr
https://www.google.com/chrome/index.html?hl=en&brand...	2015-03-22 10:11:14 CDT	https://www.google.com/chrome/index.html?hl=e
http://go.microsoft.com/fwlink/?LinkId=69157	2015-03-22 10:09:02 CDT	http://go.microsoft.com/fwlink/?LinkId=69157
http://tools.google.com/chrome/intl/en/welcome.html	2015-03-22 10:11:58 CDT	http://tools.google.com/chrome/intl/en/welcome.h
https://www.google.com/intl/en/chrome/browser/welcome...	2015-03-22 10:11:58 CDT	https://www.google.com/intl/en/chrome/browser/
https://www.google.com/	2015-03-24 16:05:40 CDT	https://www.google.com/
http://www.bing.com/	2015-03-24 16:05:40 CDT	http://www.bing.com/
http://www.bing.com/	2015-03-24 16:05:40 CDT	http://www.bing.com/
https://www.google.com/	2015-03-24 16:05:40 CDT	https://www.google.com/
https://www.google.com/#q=outlook+2013+settings	2015-03-22 10:28:16 CDT	https://www.google.com/#q=outlook+2013+sett

https://support.office.com/en-nz/article/Set-up-email-in-O...	2015-03-22 10:28:13 CDT	https://support.office.com/en-nz/article/Set-up-er
https://www.google.com/#q=outlook+2013+settings	2015-03-22 10:28:16 CDT	https://www.google.com/#q=outlook+2013+setti
https://www.google.com/webhp?hl=en	2015-03-24 16:07:19 CDT	https://www.google.com/webhp?hl=en
http://www.bing.com/	2015-03-24 16:05:40 CDT	http://www.bing.com/
https://www.google.com/webhp?hl=en	2015-03-24 16:07:19 CDT	https://www.google.com/webhp?hl=en
https://www.google.com/webhp?hl=en#q=Emmy+Noethe...	2015-03-23 12:27:56 CDT	https://www.google.com/webhp?hl=en#q=Emmy-
https://www.google.com/webhp?hl=en	2015-03-24 16:07:19 CDT	https://www.google.com/webhp?hl=en
https://www.google.com/webhp?hl=en#q=Emmy+Noethe...	2015-03-23 12:27:56 CDT	https://www.google.com/webhp?hl=en#q=Emmy-
https://www.google.com/webhp?hl=en	2015-03-24 16:07:19 CDT	https://www.google.com/webhp?hl=en
https://www.google.com/webhp?hl=en#hl=en&q=data+le...	2015-03-23 13:02:09 CDT	https://www.google.com/webhp?hl=en#hl=en&q=
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:02:17 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://www.sans.org/reading-room/whitepapers/awarenes...	2015-03-23 13:02:18 CDT	http://www.sans.org/reading-room/whitepapers/a
http://www.sans.org/reading-room/whitepapers/awarenes...	2015-03-23 13:02:18 CDT	http://www.sans.org/reading-room/whitepapers/a

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:06:01 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://en.wikipedia.org/wiki/Intellectual_property	2015-03-23 13:06:01 CDT	http://en.wikipedia.org/wiki/Intellectual_property
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:06:27 CDT	https://www.google.com/search?q=information+le
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:06:53 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://research.microsoft.com/en-us/um/people/yael/publi...	2015-03-23 13:06:53 CDT	http://research.microsoft.com/en-us/um/people/ya
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:14:50 CDT	https://www.google.com/search?q=information+le
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:15:09 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://en.wikipedia.org/wiki/Cloud_storage	2015-03-23 13:15:09 CDT	http://en.wikipedia.org/wiki/Cloud_storage
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:15:31 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://www.pcadvisor.co.uk/test-centre/internet/3506734...	2015-03-23 13:15:32 CDT	http://www.pcadvisor.co.uk/test-centre/internet/3
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:15:44 CDT	https://www.google.com/search?q=information+le
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:15:49 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://en.wikipedia.org/wiki/Digital_forensics	2015-03-23 13:15:49 CDT	http://en.wikipedia.org/wiki/Digital_forensics

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:16:05 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://nij.gov/topics/forensics/evidence/digital/pages/welc...	2015-03-23 13:16:37 CDT	http://nij.gov/topics/forensics/evidence/digital/pag
http://nij.gov/Pages/PageNotFoundError.aspx?requestUrl...	2015-03-23 13:16:34 CDT	http://nij.gov/Pages/PageNotFoundError.aspx?req
http://nij.gov/topics/forensics/evidence/digital/pages/welc...	2015-03-23 13:16:37 CDT	http://nij.gov/topics/forensics/evidence/digital/pag
http://nij.gov/topics/forensics/evidence/digital/analysis/pa...	2015-03-23 13:16:42 CDT	http://nij.gov/topics/forensics/evidence/digital/ana
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:16:55 CDT	https://www.google.com/search?q=information+le
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:17:14 CDT	https://www.google.com/search?q=information+le
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:17:19 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
http://forensicswiki.org/wiki/Anti-forensic_techniques	2015-03-23 13:17:19 CDT	http://forensicswiki.org/wiki/Anti-forensic_techniqu
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 13:17:57 CDT	https://www.google.com/url?sa=t&rct=j&q=&esrc
https://defcon.org/images/defcon-20/dc-20-presentations...	2015-03-23 13:18:00 CDT	https://defcon.org/images/defcon-20/dc-20-preser
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:18:10 CDT	https://www.google.com/search?q=information+le
https://www.google.com/search?q=information+leakage+...	2015-03-23 13:18:15 CDT	https://www.google.com/search?q=information+le

16. List all search keywords using web browsers.

ome/intl/en/welcome.html	Getting Started	Chrome	tools.google.com
:l/en/chrome/browser/welcome...	Getting Started	Chrome	www.google.com
ebhp?sourceid=chrome-instant...		Chrome	www.google.com
ebhp?sourceid=chrome-instant...		Chrome	www.google.com
om/en-us/internet-explorer/ie-1...	Download Internet Explorer 11 (Offline installer) - Internet ...	Chrome	windows.microsoft.com
rome/browser/thankyou.html?...	Chrome Browser	Chrome	www.google.com
arch?hl=en&source=hp&q=int...	internet explorer 11 - Google Search	Chrome	www.google.com
=iehp	msn	Chrome	www.msn.com
om/en-us/internet-explorer/do...	Download Web Browser - Internet Explorer	Chrome	windows.microsoft.com
url=http://windows.microsoft....		Chrome	www.google.com
om/en-US/internet-explorer/pro...		Chrome	windows.microsoft.com
ink/?LinkID=121792		Chrome	go.microsoft.com
om/en-us/internet-explorer/ie-8...	Your browser has been upgraded - Microsoft Windows	Chrome	windows.microsoft.com
:om/download/7/1/7/7179A150...		Chrome	download.microsoft.com
ws_rd=ssl	Google	Chrome	www.google.com
url=http://windows.microsoft....		Chrome	www.google.com
ebhp?hl=en	Google	Chrome	www.google.com

	Title	Program Name	Domain
	Google	Chrome	www.google.com
	Bing	Chrome	www.bing.com
	Bing	Chrome	www.bing.com
	Google	Chrome	www.google.com
=outlook+2013+settings	Google	Chrome	www.google.com
n-nz/article/Set-up-email-in-O...	Set up email in Outlook 2010 or Outlook 2013 for Office 36...	Chrome	support.office.com
=outlook+2013+settings	Google	Chrome	www.google.com
ebhp?hl=en	Google	Chrome	www.google.com
	Bing	Chrome	www.bing.com
ebhp?hl=en	Google	Chrome	www.google.com
ebhp?hl=en#q=Emmy+Noethe...	Emmy Noether - Google Search	Chrome	www.google.com
ebhp?hl=en	Google	Chrome	www.google.com
ebhp?hl=en#q=Emmy+Noethe...	Emmy Noether - Google Search	Chrome	www.google.com
ebhp?hl=en	Google	Chrome	www.google.com
ebhp?hl=en#hl=en&q=data+le...	data leakage methods - Google Search	Chrome	www.google.com
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com
g-room/whitepapers/awarenes...		Chrome	www.sans.org

ebhp?hl=en#hl=en&q=leaking...	leaking confidential information - Google Search	Chrome	www.google.com	c
ebhp?hl=en#q=leaking+confid...		Chrome	www.google.com	c
ebhp?hl=en#q=leaking+confid...		Chrome	www.google.com	c
ebhp?hl=en#hl=en&q=informa...	information leakage cases - Google Search	Chrome	www.google.com	c
ebhp?hl=en#q=information+le...		Chrome	www.google.com	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
m/business/technology/top-5-s...	Top 5 sources leaking personal data - Emirates 24|7	Chrome	www.emirates247.com	c
ebhp?hl=en#q=information+le...		Chrome	www.google.com	c
arch?q=information+leakage+...	information leakage cases - Google Search	Chrome	www.google.com	c
arch?q=information+leakage+...	information leakage cases - Google Search	Chrome	www.google.com	c
arch?q=information+leakage+...	intellectual property theft - Google Search	Chrome	www.google.com	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
'publications/article/205047/go...	Google To Settle 'Data Leakage' Case For $8.5 Million 07/2...	Chrome	www.mediapost.com	c
arch?q=information+leakage+...	how to leak a secret - Google Search	Chrome	www.google.com	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
ıs/investigate/white_collar/ipr/ipr	FBI — Intellectual Property Theft	Chrome	www.fbi.gov	c

	Title	Program Name	Domain	I
'Intellectual_property	Intellectual property - Wikipedia, the free encyclopedia	Chrome	en.wikipedia.org	c
arch?q=information+leakage+...	cloud storage - Google Search	Chrome	www.google.com	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
)m/en-us/um/people/yael/publi...		Chrome	research.microsoft.com	c
arch?q=information+leakage+...		Chrome	www.google.com	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
'Cloud_storage	Cloud storage - Wikipedia, the free encyclopedia	Chrome	en.wikipedia.org	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
:/test-centre/internet/3506734...	7 best cloud storage services 2015: Dropbox vs Google Dri...	Chrome	www.pcadvisor.co.uk	c
arch?q=information+leakage+...	digital forensics - Google Search	Chrome	www.google.com	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
'Digital_forensics	Digital forensics - Wikipedia, the free encyclopedia	Chrome	en.wikipedia.org	c
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
cs/evidence/digital/pages/welc...	Digital Evidence and Forensics | National Institute of Justice	Chrome	nij.gov	c
otFoundError.aspx?requestUrl...	NIJ Home Page Page not found (404 Error)	Chrome	nij.gov	c
cs/evidence/digital/pages/welc...	Digital Evidence and Forensics | National Institute of Justice	Chrome	nij.gov	c
cs/evidence/digital/analysis/pa...	Digital Evidence Analysis Tools | National Institute of Justice	Chrome	nij.gov	c

arch?q=information+leakage+...	how to delete data - Google Search	Chrome	www.google.com	c
arch?q=information+leakage+...	anti-forensics - Google Search	Chrome	www.google.com	c
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
Anti-forensic_techniques	Anti-forensic techniques - ForensicsWiki	Chrome	forensicswiki.org	c
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
efcon-20/dc-20-presentations...		Chrome	defcon.org	c
arch?q=information+leakage+...		Chrome	www.google.com	c
arch?q=information+leakage+...		Chrome	www.google.com	c
arch?q=information+leakage+...	how to recover data - Google Search	Chrome	www.google.com	c
arch?q=information+leakage+...		Chrome	www.google.com	c
arch?q=information+leakage+...		Chrome	www.google.com	c
arch?q=information+leakage+...	information leakage cases - Google Search	Chrome	www.google.com	c
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
List_of_data_recovery_software	List of data recovery software - Wikipedia, the free encycl...	Chrome	en.wikipedia.org	c
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	c
g/wiki/Tools:Data_Recovery	Tools:Data Recovery - ForensicsWiki	Chrome	www.forensicswiki.org	c
arch?q=information+leakage+...	information leakage cases - Google Search	Chrome	www.google.com	c

)/DL1455	iCloud for Windows	Chrome	support.apple.com	
:b/DL1455	iCloud for Windows	Chrome	support.apple.com	
)/DL1455?locale=en_US	iCloud for Windows	Chrome	support.apple.com	
:b/DL1455?locale=en_US	iCloud for Windows	Chrome	support.apple.com	
ebhp?hl=en#hl=	http://support.apple.com/kb/DL1455?locale=en_US	Chrome	www.google.com	
l?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	
ive/	Google Drive - Cloud Storage & File Backup for Photos, Doc...	Chrome	www.google.com	
ive/download/	Download Google Drive - Free Cloud Storage	Chrome	www.google.com	
)age/drive/index.html?hl=en#e...	Download Google Drive Now – For Free	Chrome	tools.google.com	
)age/drive/thankyou.html?hl=en	Google Drive	Chrome	tools.google.com	
ebhp?hl=en	Google	Chrome	www.google.com	
	Bing	Chrome	www.bing.com	
ebhp?hl=en	Google	Chrome	www.google.com	
	Bing	Chrome	www.bing.com	
ebhp?hl=en	Google	Chrome	www.google.com	
vshp?hl=en&tab=wn&ei=xnAR...	Google News	Chrome	news.google.com	
ews/section?pz=1&cf=all&ned...	World	Chrome	news.google.com	
List_of_data_recovery_software	List of data recovery software - Wikipedia, the free encycl...	Chrome	en.wikipedia.org	
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	
g/wiki/Tools:Data_Recovery	Tools:Data Recovery - ForensicsWiki	Chrome	www.forensicswiki.org	
arch?q=information+leakage+...	information leakage cases - Google Search	Chrome	www.google.com	
	Bing	Chrome	www.bing.com	
ebhp?hl=en	Google	Chrome	www.google.com	
ebhp?hl=en#hl=en&q=google		Chrome	www.google.com	
ebhp?hl=en	Google	Chrome	www.google.com	
ebhp?hl=en#hl=en&q=apple+i...	apple icloud - Google Search	Chrome	www.google.com	
?sa=t&rct=j&q=&esrc=s&sour...		Chrome	www.google.com	
ud/	Apple - iCloud - Everything you love, everywhere you go.	Chrome	www.apple.com	
ud/setup/pc.html	Apple - iCloud - Learn how to set up iCloud on all your devi...	Chrome	www.apple.com	
dcontrolpanel	iCloud	Chrome	www.icloud.com	
udcontrolpanel	iCloud	Chrome	www.icloud.com	
dcontrolpanel/	iCloud	Chrome	www.icloud.com	

The second column shows the search keywords used in web browsers. (The time stamp is also shown along with those, but my screenshots could not fit the tampstamp)

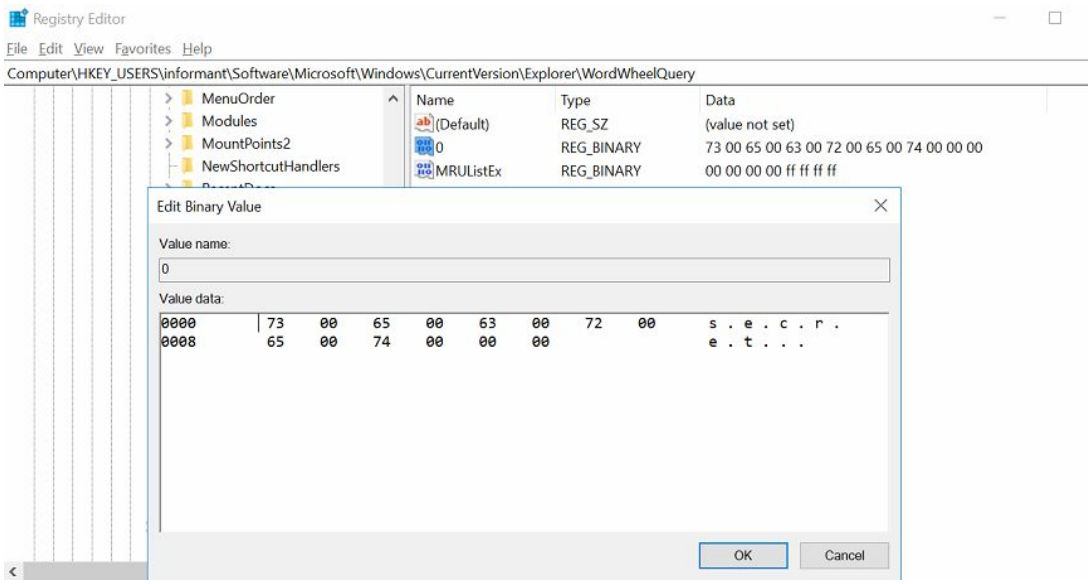
17. List all user keywords at the search bar in Windows Explorer.

Secret

Loading the registry hive "*pc_vol3.ntfs\Windows\Users\informant*" in a VM as *HKU\informant.*

Looking into HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

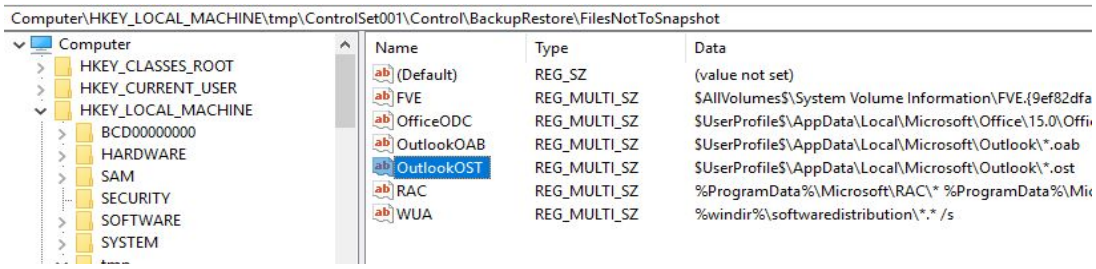
Select the the first key '0'. It shows the word secret.



18. What application is used for e-mail communication?

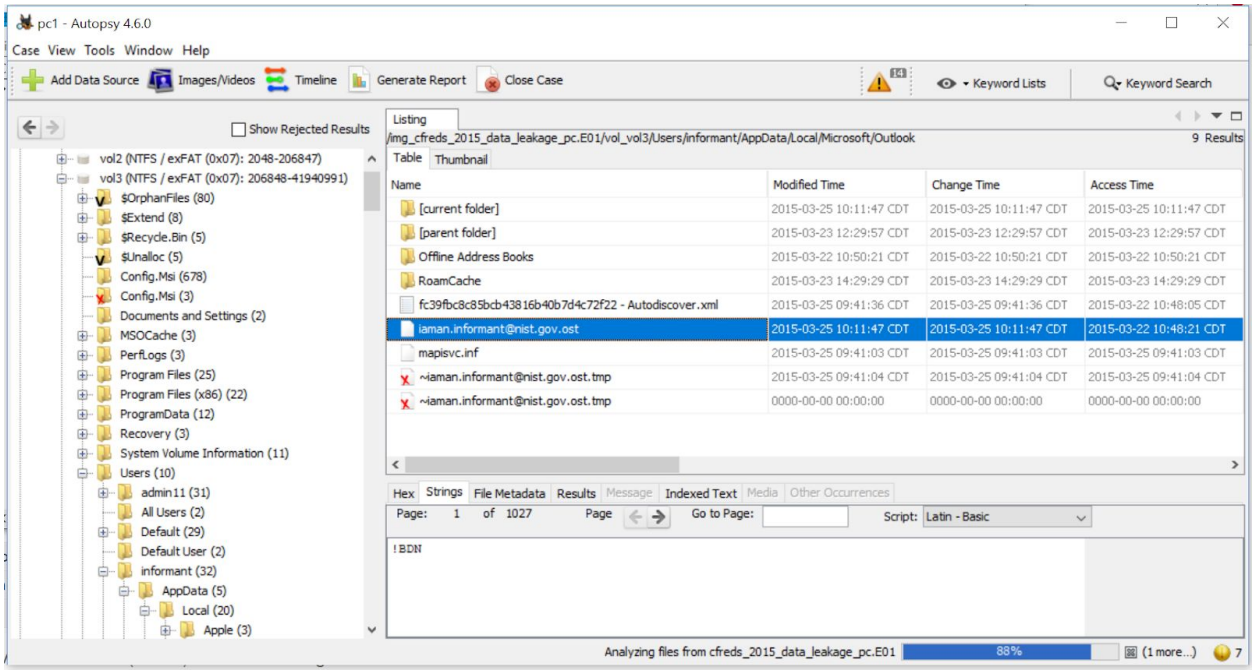
Loading the registry hive "*pc_vol3.ntfs\Windows\System32\config\SYSTEM*" in a VM as *HKLM\tmp*.

Looking into HKLM\tmp\ControlSet001\Control\BackupRestore\FilesNotToSnapshot, shows there is a outlook ost folder.



Microsoft Outlook is used for email communication.

19. Where is the email file located?



C:\Users\informant\appData\Local\Microsoft\Outlook\iaman.inofrmant@nist.gov.ost

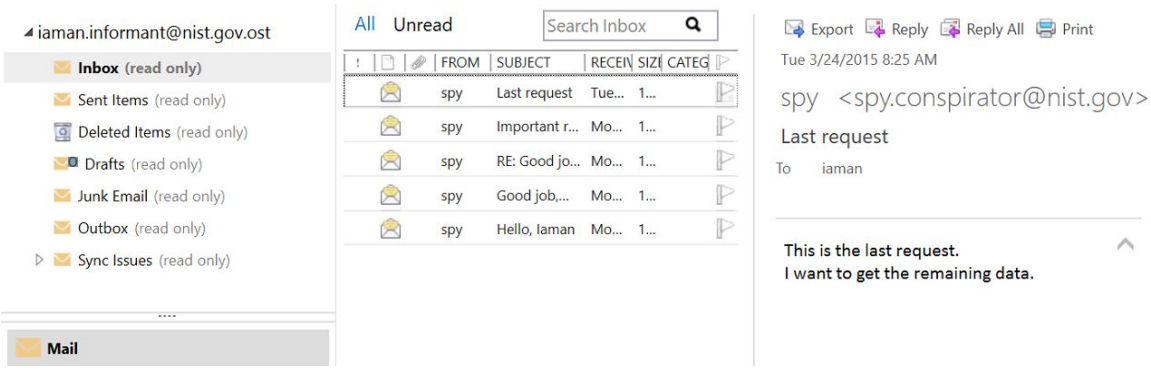
20. What is the e-mail account used by the suspect

From Q.19, the email account used by suspect is **iaman.informant@nist.gov**

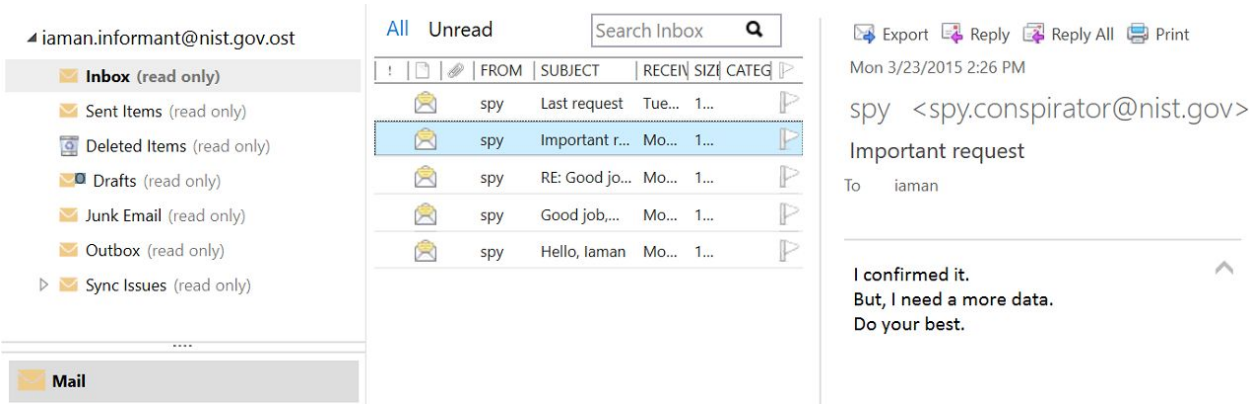
21. List all e-mails of the suspect. If possible, identify deleted e-mails.

The iaman.informant@nist.gov.ost file is opened and viwed in a ost viewer.

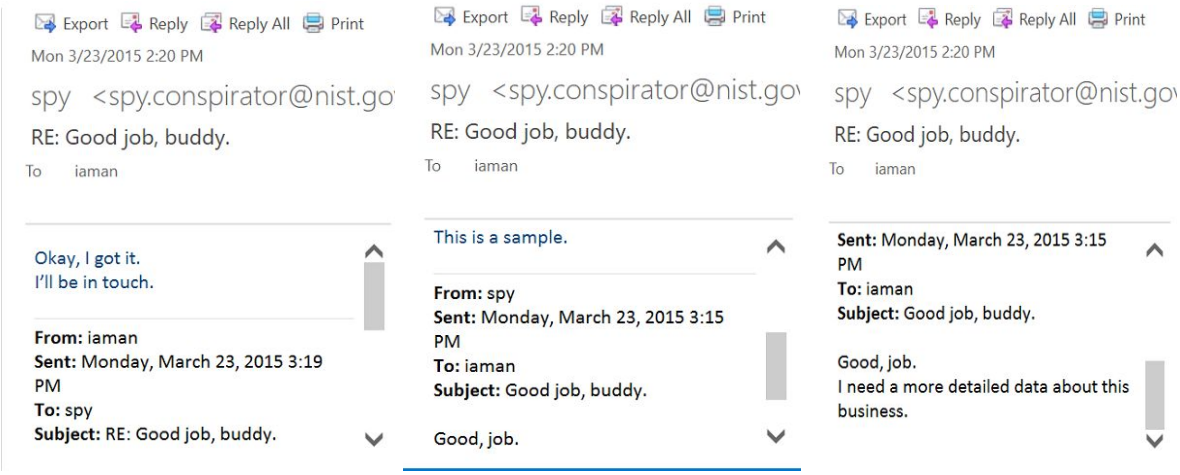
There are 5 emails in inbox.



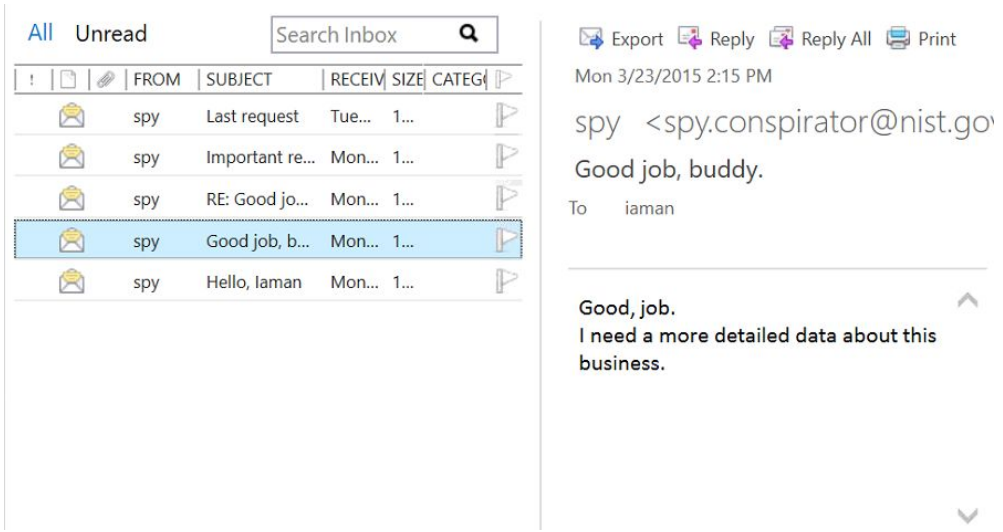
Inbox 2



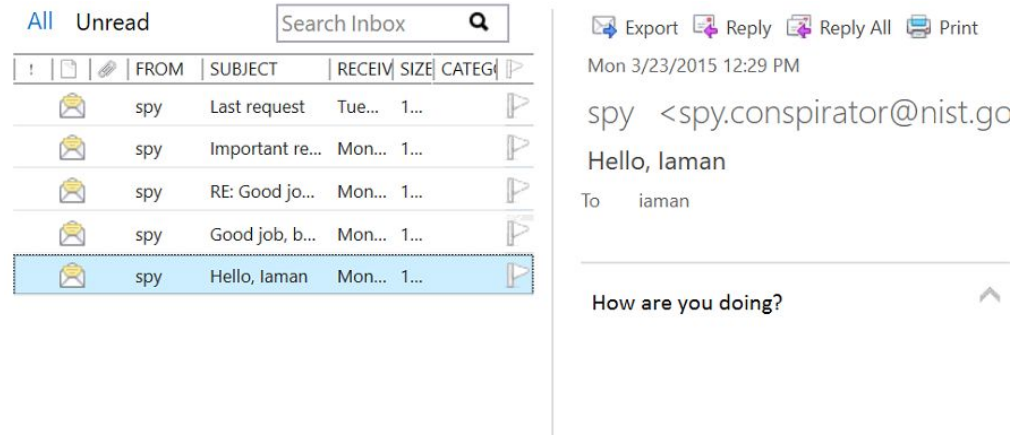
Inbox 3



Inbox 4

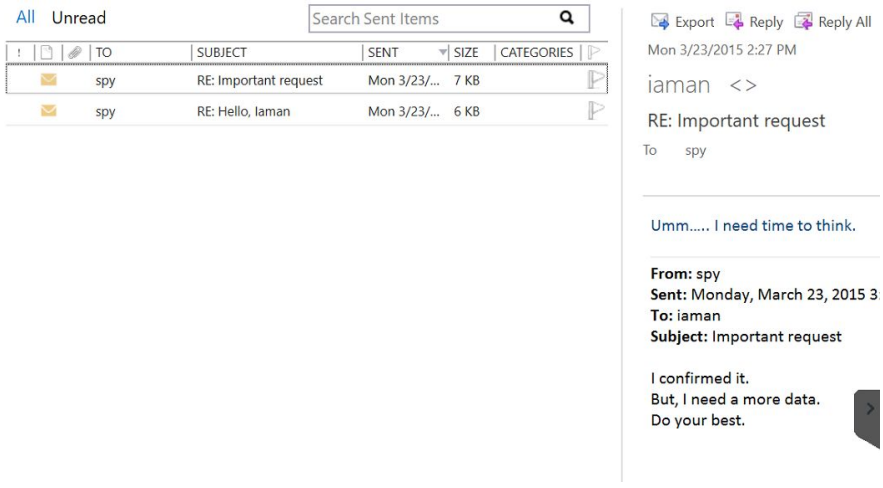


Inbox 5

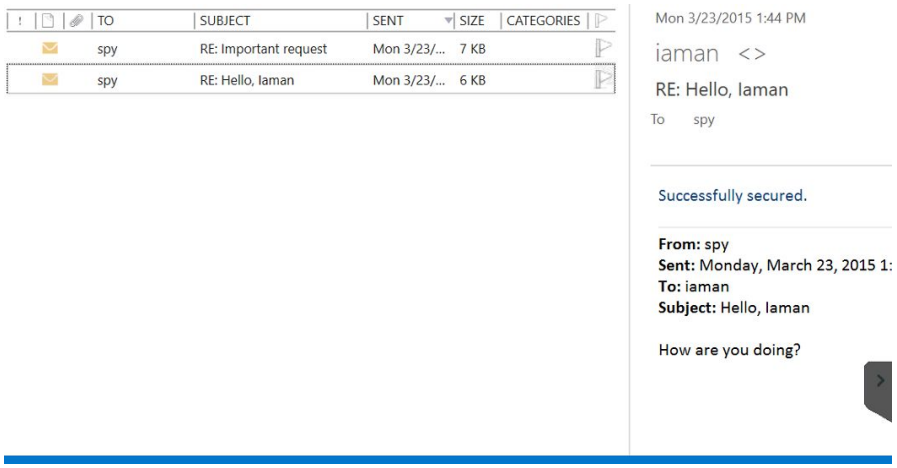


There are 2 sent emails.

Sent 1

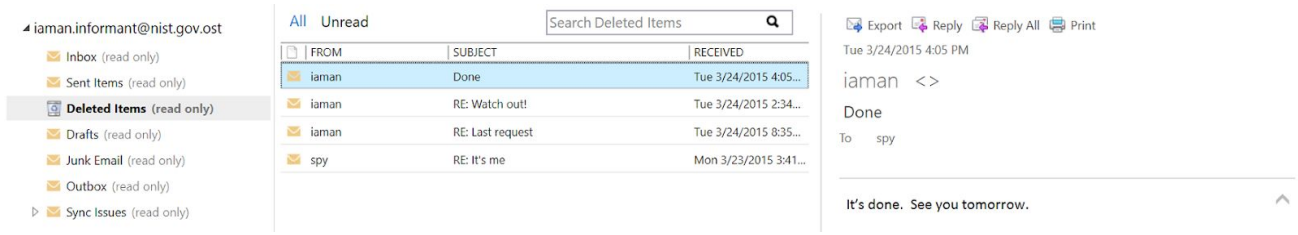


Sent 2

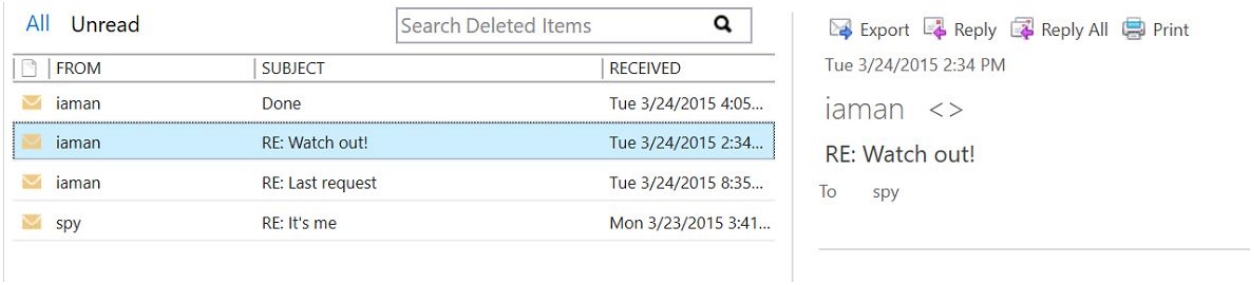


There are 4 emails in deleted emails folder

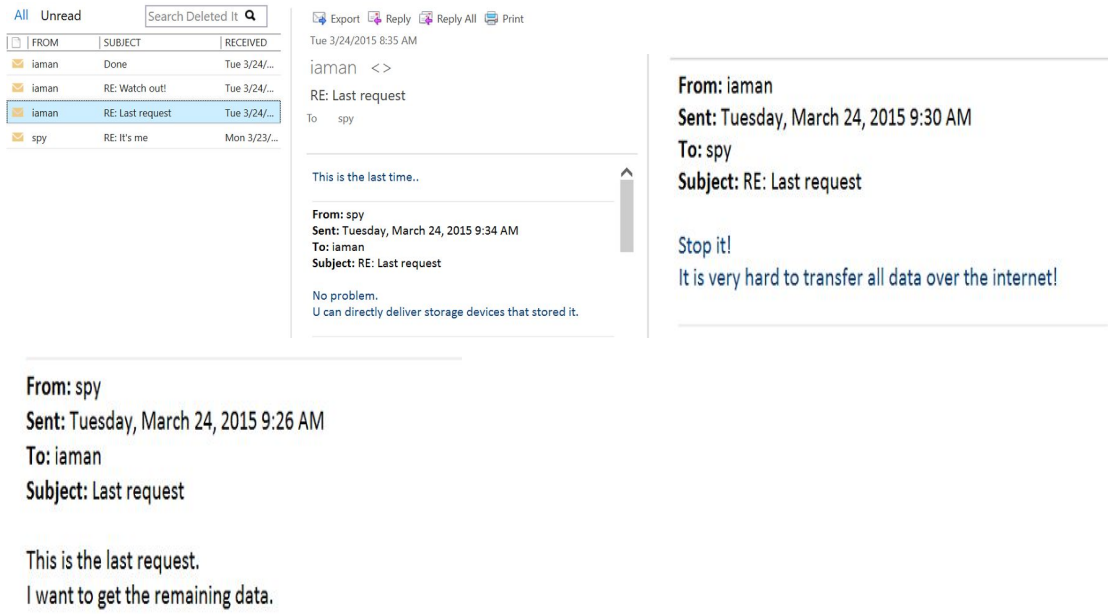
Deleted Item 1



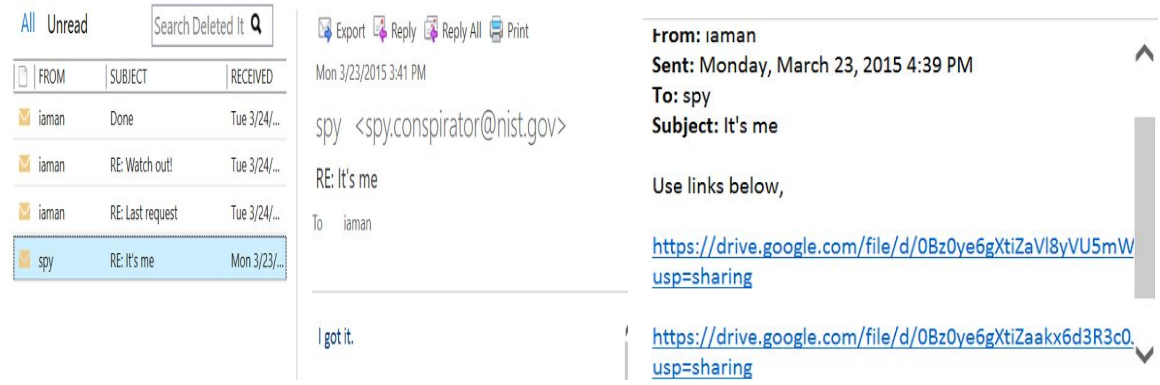
Deleted Item 2



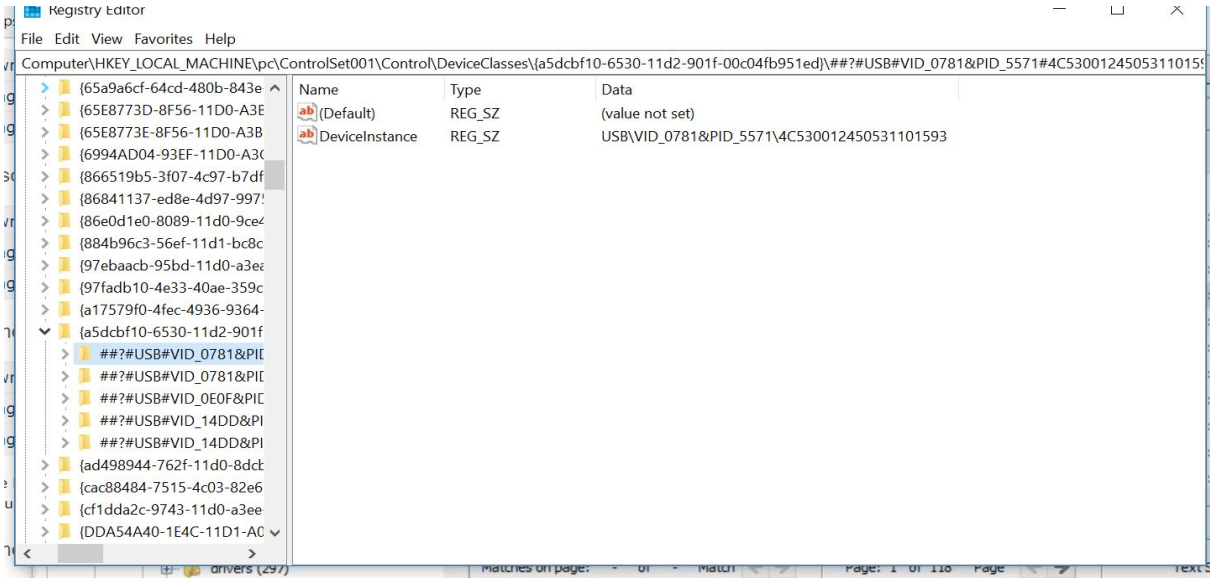
Deleted Item 3

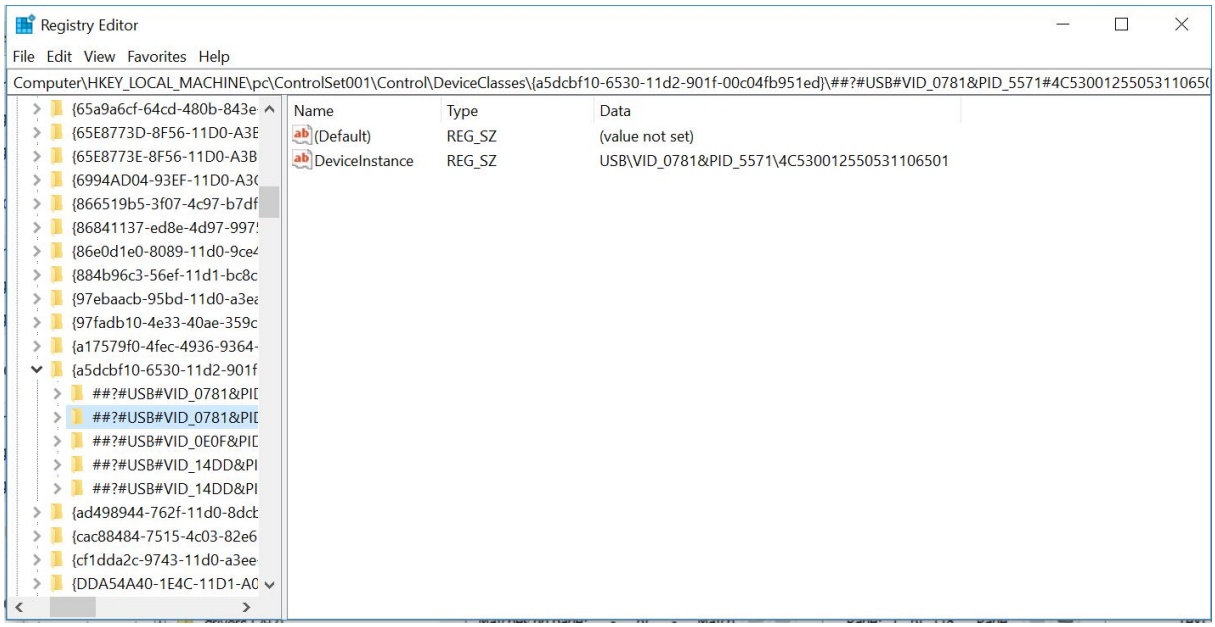


Deleted item 4



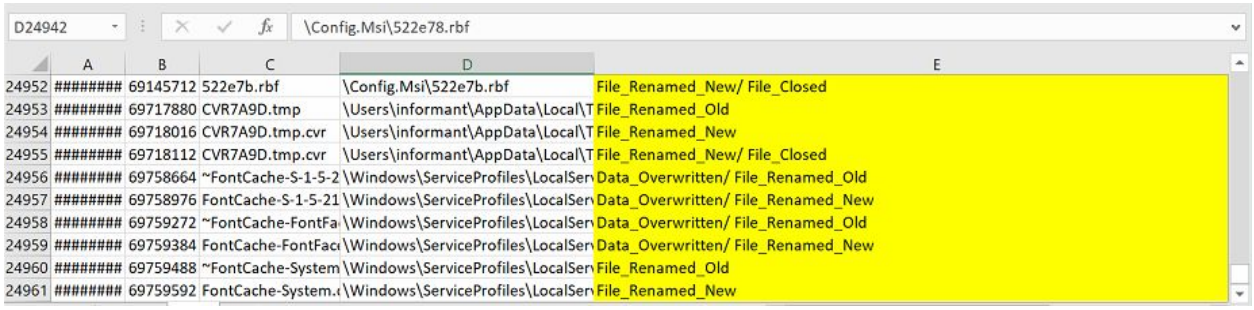
22. List external storage devices attached to PC.
Loading the registry hive "*pc_vol3.ntfs\Windows\System32\config\SYSTEM*" in a VM as *HKLM\pc*





23. Identify all traces related to ‘renaming’ of files in Windows Desktop.
NTFS jounal contains $UsnJrnl·$J .
Also, extract $MFT.
Using NTFS log tracker, give the path of extracted $MFT and $UsnJrnl·$J and then parse it. The result is exported to a .csv file.

After analyzing the .csv file, there is a total of 24,961 records that show the files which are renamed.



	A	B	C	D	E
24952	########	69145712	522e7b.rbf	\Config.Msi\522e7b.rbf	File_Renamed_New/ File_Closed
24953	########	69717880	CVR7A9D.tmp	\Users\informant\AppData\Local\T	File_Renamed_Old
24954	########	69718016	CVR7A9D.tmp.cvr	\Users\informant\AppData\Local\T	File_Renamed_New
24955	########	69718112	CVR7A9D.tmp.cvr	\Users\informant\AppData\Local\T	File_Renamed_New/ File_Closed
24956	########	69758664	~FontCache-S-1-5-2	\Windows\ServiceProfiles\LocalSer	Data_Overwritten/ File_Renamed_Old
24957	########	69758976	FontCache-S-1-5-21	\Windows\ServiceProfiles\LocalSer	Data_Overwritten/ File_Renamed_New
24958	########	69759272	~FontCache-FontFa	\Windows\ServiceProfiles\LocalSer	Data_Overwritten/ File_Renamed_Old
24959	########	69759384	FontCache-FontFac	\Windows\ServiceProfiles\LocalSer	Data_Overwritten/ File_Renamed_New
24960	########	69759488	~FontCache-System	\Windows\ServiceProfiles\LocalSer	File_Renamed_Old
24961	########	69759592	FontCache-System.d	\Windows\ServiceProfiles\LocalSer	File_Renamed_New

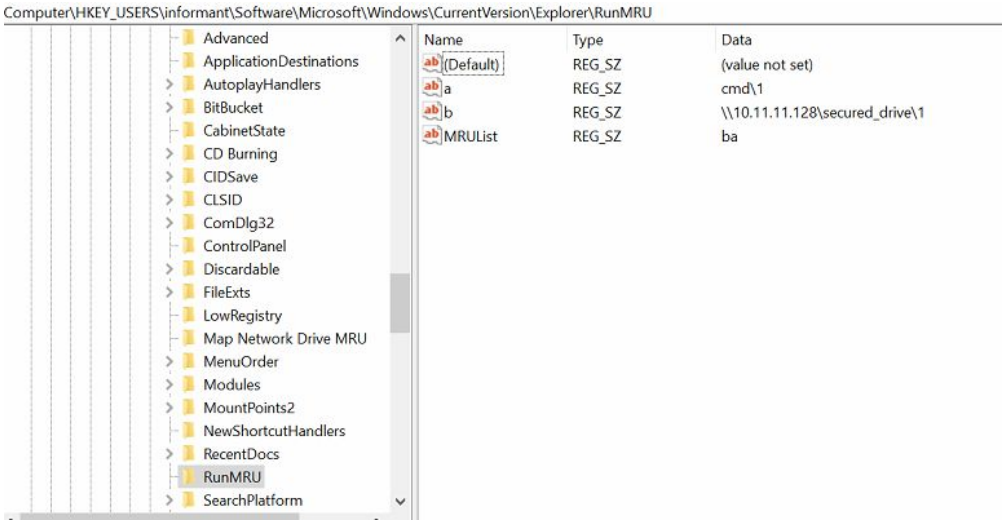
24. What is the ip address of company's shared network drive?

10.11.11.128

Extract the informant and load this hive in the registry.

Look into HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

Key 'b' shows the required ip address.



Questions 25 - 36

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

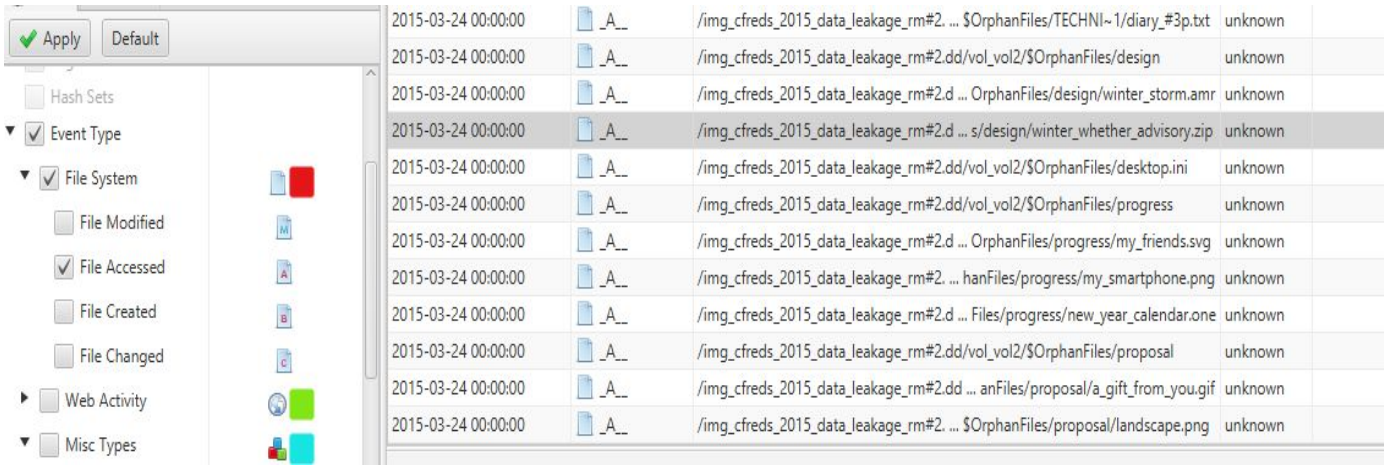
- TECHNI
- proposal
- progress

are frequently accessed directories

2015-03-24 09:59:39	___B	/img_cfreds_2015_data_leakage_rm#2.d ... iles/PRICIN~1/my_favorite_movies.7z	unknown		
2015-03-24 09:59:39	___B	/img_cfreds_2015_data_leakage_rm#2. ... hanFiles/PRICIN~1/new_years_day.jpg	unknown		
2015-03-24 09:59:40	___B	/img_cfreds_2015_data_leakage_rm#2.d ... OrphanFiles/PRICIN~1/super_bowl.avi	unknown		
2015-03-24 09:59:43	___B	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/progress	unknown		
2015-03-24 09:59:43	___B	/img_cfreds_2015_data_leakage_rm#2.d ... OrphanFiles/progress/my_friends.svg	unknown		
2015-03-24 09:59:43	___B	/img_cfreds_2015_data_leakage_rm#2. ... hanFiles/progress/my_smartphone.png	unknown		
2015-03-24 09:59:44	___B	/img_cfreds_2015_data_leakage_rm#2.d ... Files/progress/new_year_calendar.one	unknown		
2015-03-24 09:59:44	___B	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/proposal	unknown		
2015-03-24 09:59:44	___B	/img_cfreds_2015_data_leakage_rm#2.dd ... anFiles/proposal/a_gift_from_you.gif	unknown		
2015-03-24 10:00:06	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/proposal/landscape.png	unknown		
2015-03-24 10:00:12	___B	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/TECHNI~1	unknown		
2015-03-24 10:00:12	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#1d.txt	unknown		

2015-03-24 09:59:44	___B	/img_cfreds_2015_data_leakage_rm#2.dd ... anFiles/proposal/a_gift_from_you.gif	unknown		
2015-03-24 10:00:06	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/proposal/landscape.png	unknown		
2015-03-24 10:00:12	___B	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/TECHNI~1	unknown		
2015-03-24 10:00:12	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#1d.txt	unknown		
2015-03-24 10:00:12	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#1p.txt	unknown		
2015-03-24 10:00:13	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#2d.txt	unknown		
2015-03-24 10:00:14	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#2p.txt	unknown		
2015-03-24 10:00:15	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#3d.txt	unknown		
2015-03-24 10:00:18	___B	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#3p.txt	unknown		
2015-03-24 15:51:47	___B	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/desktop.ini	unknown		
2015-03-24 15:51:48	M___	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/desktop.ini	unknown		
2015-03-24 17:02:36	M___	/img_cfreds_2015_data_leakage_rm#2.d ... I2/IAMAN $_@ (Volume Label Entry)	unknown		

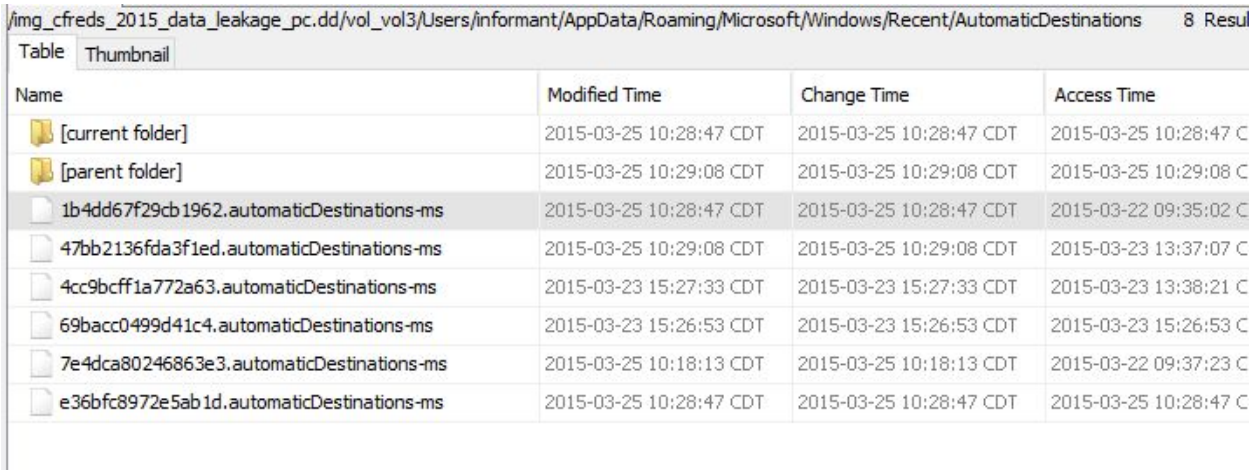
26. List all files that were opened in 'RM#2'.



2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/TECHNI~1/diary_#3p.txt	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/design	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.d ... OrphanFiles/design/winter_storm.amr	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.d ... s/design/winter_whether_advisory.zip	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/desktop.ini	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/progress	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.d ... OrphanFiles/progress/my_friends.svg	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2. ... hanFiles/progress/my_smartphone.png	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.d ... Files/progress/new_year_calendar.one	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$OrphanFiles/proposal	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2.dd ... anFiles/proposal/a_gift_from_you.gif	unknown
2015-03-24 00:00:00	_A__	/img_cfreds_2015_data_leakage_rm#2. ... $OrphanFiles/proposal/landscape.png	unknown

27. List all directories that were traversed in the company's network drive.

Looking into
\User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
and locations from question 8 reveal that
\\10.11.11.128\secured_drive\Secret Project Data
Directory folders are traversed.



/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations 8 Resul

Table | Thumbnail

Name	Modified Time	Change Time	Access Time
[current folder]	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 C
[parent folder]	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 C
1b4dd67f29cb1962.automaticDestinations-ms	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-22 09:35:02 C
47bb2136fda3f1ed.automaticDestinations-ms	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-23 13:37:07 C
4cc9bcff1a772a63.automaticDestinations-ms	2015-03-23 15:27:33 CDT	2015-03-23 15:27:33 CDT	2015-03-23 13:38:21 C
69bacc0499d41c4.automaticDestinations-ms	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 C
7e4dca80246863e3.automaticDestinations-ms	2015-03-25 10:18:13 CDT	2015-03-25 10:18:13 CDT	2015-03-22 09:37:23 C
e36bfc8972e5ab1d.automaticDestinations-ms	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 C

```
1SPSsC
\\10.11.11.128\secured_driveMicrosoft NetworkCompany's Secured Network Drive
SECRET~1
Secret Project Data
PRICIN~1
pricing decision
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision
WmcG
WmcG
Project Data\design\winter_whether_advisory.zip
WmcG
WmcG
V:\Secret Project Data\fL
/V:\
SECRET~1
Secret Project Data
final8
final
\\10.11.11.128\secured_driveV:Secret Project Data\final9
1SPSU(L
```

28. List all files that were opened in the company's network drive.

Date/Time	Event Type	Description	Kn
2015-03-23 13:26:53	Recent Doc...	\\10.11.11.128\SECURED_DRIVE\Secret Proje ... on\(secret_project)_pricing_decision.xlsx	unkno
2015-03-23 13:26:53	Recent Doc...	\\10.11.11.128\SECURED_DRIVE\Secret Proje ... on\(secret_project)_pricing_decision.xlsx	unkno
2015-03-23 13:26:54	Recent Doc...	\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision	unkno
2015-03-23 13:27:33	Recent Doc...	\\10.11.11.128\secured_drive\Secret Project Data\final	unkno
2015-03-23 13:27:33	Recent Doc...	\\10.11.11.128\secured_drive\Secret Project ... \final\[secret_project]_final_meeting.pptx	unkno
2015-03-23 13:27:37	Recent Doc...	\\10.11.11.128\secured_drive\Secret Project ... \final\[secret_project]_final_meeting.pptx	unkno

29. Find traces related to cloud services on PC.

Google Drive:

img_cfreds_2015_data_leakage_pc.dd/vol_vol3/ProgramData/Microsoft/Windows/Start Menu/Programs/Google Drive 6 Results

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	56
[parent folder]	2015-03-25 08:19:07 PDT	2015-03-25 08:19:07 PDT	2015-03-25 08:19:07 PDT	2009-07-13 20:20:08 PDT	56
Google Docs.lnk	2015-03-23 13:02:45 PDT	2015-03-24 08:16:26 PDT	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	2048
Google Drive.lnk	2015-03-23 13:02:45 PDT	2015-03-24 08:16:27 PDT	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	1080
Google Sheets.lnk	2015-03-23 13:02:45 PDT	2015-03-24 08:16:27 PDT	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	2058
Google Slides.lnk	2015-03-23 13:02:45 PDT	2015-03-24 08:16:27 PDT	2015-03-23 13:02:45 PDT	2015-03-23 13:02:45 PDT	2060

Apple iCloud:

img_cfreds_2015_data_leakage_pc.dd/vol_vol3/ProgramData/Microsoft/Windows/Start Menu/Programs/iCloud 10 Resu

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2015-03-25 08:19:07 PDT	2015-03-25 08:19:07 PDT	2015-03-25 08:19:07 PDT	2015-03-23 13:01:53 PDT	48
[parent folder]	2015-03-25 08:19:07 PDT	2015-03-25 08:19:07 PDT	2015-03-25 08:19:07 PDT	2009-07-13 20:20:08 PDT	56
Calendar.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:27 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2126
Contacts.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:27 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2126
Find My iPhone.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:27 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2126
iCloud Photos.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:28 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2179
iCloud.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:28 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2087
Mail.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:28 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2110
Notes.lnk	2015-03-23 13:01:53 PDT	2015-03-24 08:16:28 PDT	2015-03-23 13:01:53 PDT	2015-03-23 13:01:53 PDT	2114

Both:

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Downloads 7 R

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time
[current folder]	2015-03-23 12:56:53 PDT	2015-03-23 12:56:53 PDT	2015-03-23 12:56:53 PDT	2015-03-22 07:34:4
[parent folder]	2015-03-23 13:05:32 PDT	2015-03-23 13:05:32 PDT	2015-03-23 13:05:32 PDT	2015-03-22 07:34:3
desktop.ini	2015-03-22 07:34:59 PDT	2015-03-22 07:34:59 PDT	2015-03-22 07:34:55 PDT	2015-03-22 07:34:5
googledrivesync.exe	2015-03-23 12:56:33 PDT	2015-03-23 12:56:33 PDT	2015-03-23 12:56:30 PDT	2015-03-23 12:56:3
googledrivesync.exe:Zone.Identifier	2015-03-23 12:56:33 PDT	2015-03-23 12:56:33 PDT	2015-03-23 12:56:30 PDT	2015-03-23 12:56:3
icloudsetup.exe	2015-03-23 12:56:53 PDT	2015-03-23 12:56:53 PDT	2015-03-23 12:55:47 PDT	2015-03-23 12:55:4
icloudsetup.exe:Zone.Identifier	2015-03-23 12:56:53 PDT	2015-03-23 12:56:53 PDT	2015-03-23 12:55:47 PDT	2015-03-23 12:55:4

30. What files were deleted from Google Drive?

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Google Drive 6 Result

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2015-03-25 08:21:36 PDT	2015-03-25 08:21:36 PDT	2015-03-25 08:21:36 PDT	2015-03-23 13:05:32 PDT	152
[parent folder]	2015-03-23 13:05:32 PDT	2015-03-23 13:05:32 PDT	2015-03-23 13:05:32 PDT	2015-03-22 07:34:31 PDT	256
desktop.ini	2015-03-25 08:21:36 PDT	2015-03-25 08:21:36 PDT	2015-03-25 08:21:36 PDT	2015-03-23 13:05:32 PDT	180
desktop.ini	2015-03-23 13:05:32 PDT	2015-03-25 08:21:36 PDT	2015-03-23 13:05:32 PDT	2015-03-23 13:05:32 PDT	180
desktop.ini	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
happy_holiday.jpg	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

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Local/Google/Drive/user_default

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
CrashReports	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	48
cacerts	2015-03-25 08:21:34 PDT	2015-03-25 08:21:34 PDT	2015-03-25 08:21:34 PDT	2015-03-23 13:02:51 PDT	3245
cacerts	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	3245
com.google.drive.nativeproxy.json	2015-03-25 08:21:36 PDT	2015-03-25 08:21:36 PDT	2015-03-23 13:05:32 PDT	2015-03-23 13:05:32 PDT	294
lockfile	2015-03-25 08:21:34 PDT	2015-03-25 08:21:34 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	0
pid	2015-03-25 08:21:34 PDT	2015-03-25 08:21:34 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	4
run_dir	2015-03-25 08:21:34 PDT	2015-03-25 08:21:34 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	46
snapshot.db	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	20480
snapshot.db-shm	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:21:34 PDT	32768
snapshot.db-wal	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:21:34 PDT	33568
sync_config.db	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	11264
sync_config.db-shm	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:21:34 PDT	32768
sync_config.db-wal	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:22:48 PDT	2015-03-25 08:21:34 PDT	4224
sync_log.log	2015-03-25 08:23:00 PDT	2015-03-25 08:23:00 PDT	2015-03-23 13:02:51 PDT	2015-03-23 13:02:51 PDT	408238
sync_log.log	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

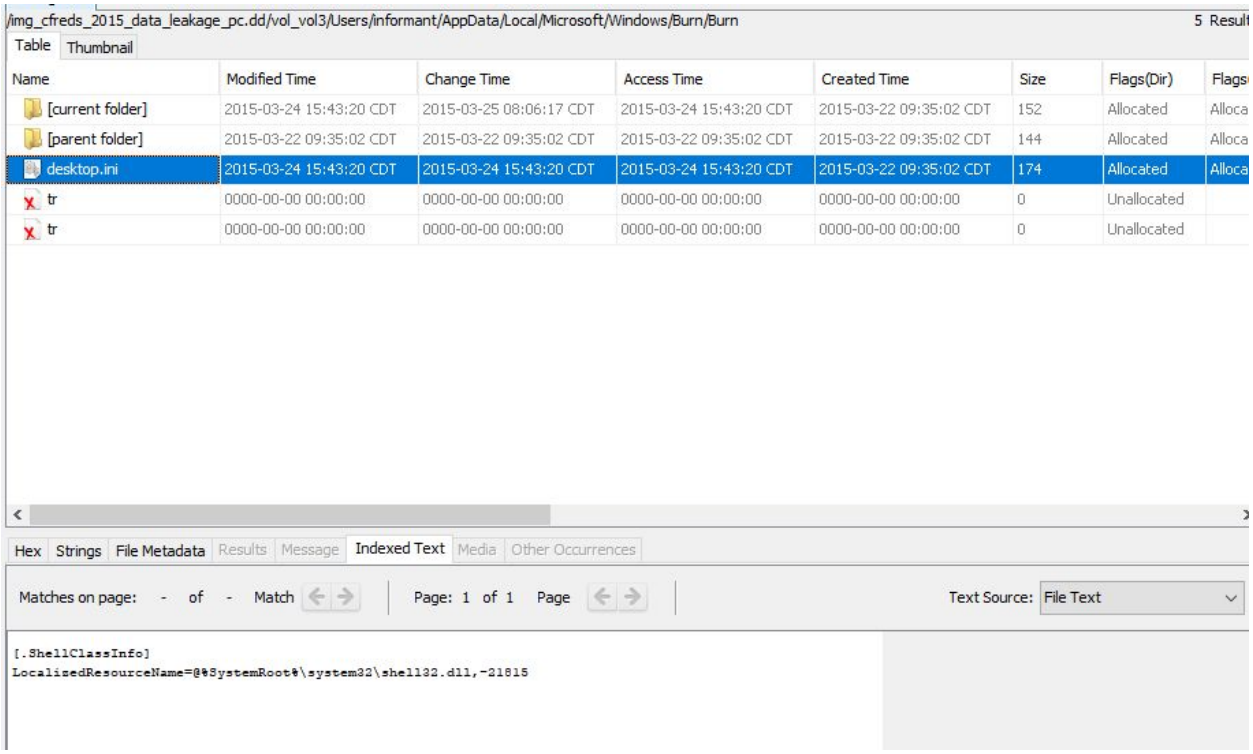
From *\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log*
We see that do_u_wanna_build_a_snow_man.mp3 is also deleted.

31. Identify account information for synchronizing Google Drive.
From *\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log* we can see the email and sync info:
Email: iaman.informant.personal@gmail.com

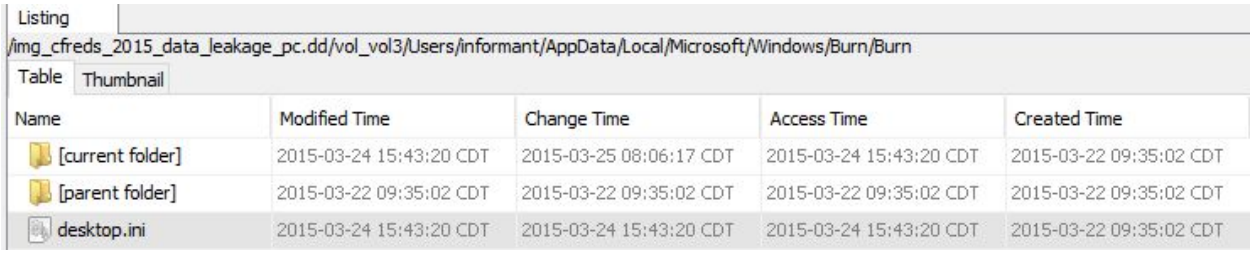
```
new_document_url='https://docs.google.com/document?usp=drive_sync',
new_presentation_url='https://docs.google.com/presentation?usp=drive_sync',
new_spreadsheet_url='https://docs.google.com/spreadsheets?usp=drive_sync',
num_workers=3,
only_rooted_items_in_cloud_graph=False,
open_url='https://docs.google.com/open?id={doc_id}',
overlays_enabled_finder_versions=['10.6.8', '10.7', '10.7.1', '10.7.2', '10.7.3', '10.7.5'
, '10.8', '10.8.1', '10.8.2', '10.8.3', '10.9', '10.9.1', '10.9.2', '10.9.3', '10.9.4'],
perf_throttle_percentage=100.0,
push_keepalive_interval=72000.0,
regular_polling_interval_secs=30,
selective_sub_folder_sync=False,
share_template_url='https://drive.google.com/sharing/share?subapp=10&shareProtocolVersion=
2&theme=2&command=settings&shareUiType=default&authuser=0&client=desktop',
show_confirmation_dialog_on_delete=True,
telemetry_enabled=True,
telemetry_upload_interval_secs=1800,
telemetry_url='https://drive.google.com/syncclient_impressions',
token_bucket_read_qps=10,
token_bucket_write_qps=3,)
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads   logging:1612 OS: Windows/
6.1.7601-SP1
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads   logging:1612 Google Drive
 (build 1.20.8672.3137)
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads   logging:1612 SSL: OpenSSL
 1.0.1i 6 Aug 2014
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads   common.sync_app:1162 Conf
ig:
Email: iaman.informant.personal@gmail.com
Sync root: \\?\C:\Users\informant\Google Drive
Sync collections: set([])
Upgrade number: 20
App version: 1.20.8672.3137
```

32. What a method (or software) was used for burning CD-R?

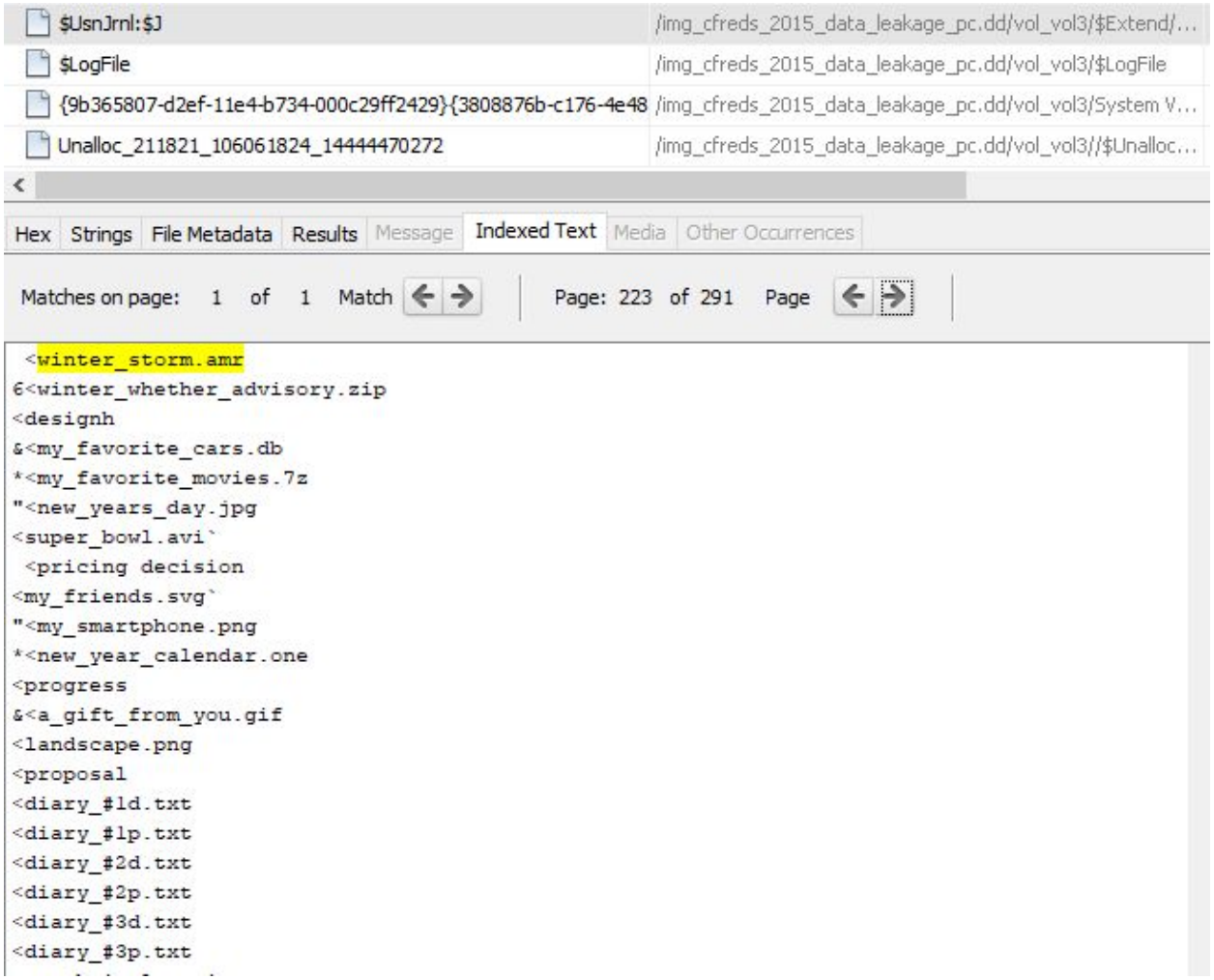
Local Burn directory shows that Windows default burning feature is used.



33. When did the suspect burn CD-R?



34. What files were copied from PC to CD-R?



35. What files were opened from CD-R?

From the location below:

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations 8 Results

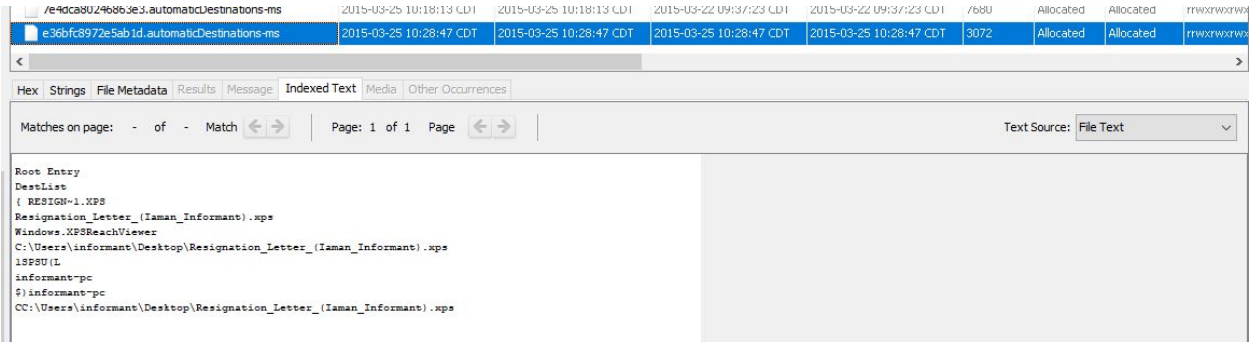
Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Si
[current folder]	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-22 09:35:02 CDT	56
[parent folder]	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-22 09:34:41 CDT	17
1b4dd67f29cb1962.automaticDestinations-ms	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-22 09:35:02 CDT	2015-03-22 09:35:02 CDT	17
47bb2136fda3f1ed.automaticDestinations-ms	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-23 13:37:07 CDT	2015-03-23 13:37:07 CDT	17
4cc9bcff1a772a63.automaticDestinations-ms	2015-03-23 15:27:33 CDT	2015-03-23 15:27:33 CDT	2015-03-23 13:38:21 CDT	2015-03-23 13:38:21 CDT	17
69bacc0499d41c4.automaticDestinations-ms	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT	46
7e4dca80246863e3.automaticDestinations-ms	2015-03-25 10:18:13 CDT	2015-03-25 10:18:13 CDT	2015-03-22 09:37:23 CDT	2015-03-22 09:37:23 CDT	76
e36bfc8972e5ab1d.automaticDestinations-ms	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	30

```
C:\Users\informant\Desktop
8:X]
C:\Users\informant\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms
1SPSU(L
informant-pc
GLsf
2D:\de\winter_whether_advisory.zip\ppt\slL
C:\Users\informant\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms
1SPSU(L
informant-pc
ideMasters
WKsf
,D:\de\winter_whether_advisory.zip\ppt\slidesy
C:\Users\informant\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms
1SPSU(L
informant-pc
@Ke0Jsf
0D:\de\winter_whether_advisory.zip\ppt
```

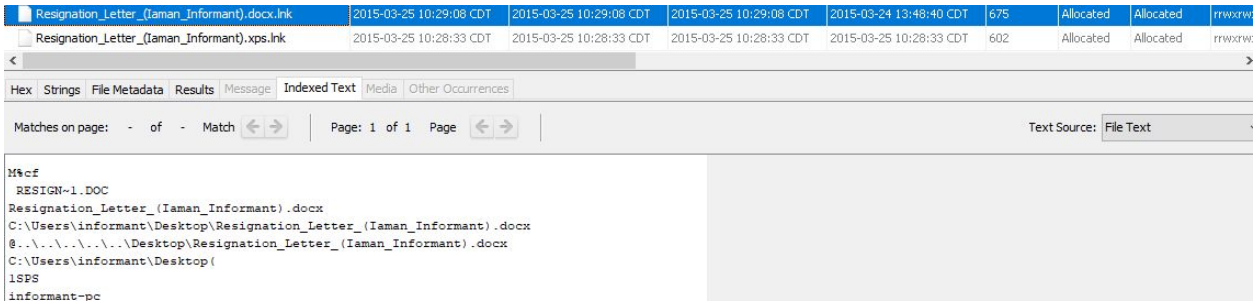
The user opened D:\de\winter_whether_advisory.zip\ and some other files within the directory.

36. Identify all timestamps related to a resignation file in Windows Desktop.



```
Root Entry
DestList
{ RESIGN~1.XPS
Resignation_Letter_(Iaman_Informant).xps
Windows.XPSReachViewer
C:\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps
1SPSU(L
informant-pc
$)informant-pc
CC:\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps
```

Modified Time	Change Time	Access Time	Created Time
2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-22 09:35:02 CDT
2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-22 09:34:41 CDT
2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-22 09:35:02 CDT	2015-03-22 09:35:02 CDT
2015-03-25 10:29:08 CDT	2015-03-25 10:29:08 CDT	2015-03-23 13:37:07 CDT	2015-03-23 13:37:07 CDT
2015-03-23 15:27:33 CDT	2015-03-23 15:27:33 CDT	2015-03-23 13:38:21 CDT	2015-03-23 13:38:21 CDT
2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT	2015-03-23 15:26:53 CDT
2015-03-25 10:18:13 CDT	2015-03-25 10:18:13 CDT	2015-03-22 09:37:23 CDT	2015-03-22 09:37:23 CDT
2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT	2015-03-25 10:28:47 CDT



Questions 37 - 48

37. How and when did the suspect print a resignation file?

Print to xps file

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Desktop 9 Res

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir
[current folder]	2015-03-25 11:29:08 EDT	2015-03-25 11:29:08 EDT	2015-03-25 11:29:08 EDT	2015-03-22 10:34:41 EDT	56	Allocatec
[parent folder]	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-22 10:34:31 EDT	256	Allocatec
[QAT	2076-11-29 03:54:34 EST	2015-03-25 11:13:49 EDT	2076-11-29 03:54:34 EST	2076-11-29 03:54:34 EST	48	Unallocat
Download	2015-03-25 11:15:45 EDT	2015-03-25 11:15:45 EDT	2015-03-25 11:15:45 EDT	2015-03-22 11:08:23 EDT	56	Allocatec
desktop.ini	2015-03-22 10:34:59 EDT	2015-03-22 10:34:59 EDT	2015-03-22 10:34:55 EDT	2015-03-22 10:34:55 EDT	282	Allocatec
Google Drive.lnk	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	1665	Unallocat
Resignation_Letter_(Iaman_Informant).docx	2015-03-24 14:59:30 EDT	2015-03-24 14:59:30 EDT	2015-03-24 14:59:30 EDT	2015-03-24 14:48:40 EDT	11893	Allocatec
Resignation_Letter_(Iaman_Informant).xps	2015-03-25 11:28:34 EDT	2015-03-25 11:28:47 EDT	2015-03-25 11:28:33 EDT	2015-03-25 11:28:33 EDT	178139	Allocatec
~$signation_Letter_(Iaman_Informant).docx	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	Unallocat

38. Where are ‘Thumbcache’ files located?

Listing

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Local/Microsoft/Windows/Explorer 10 Results

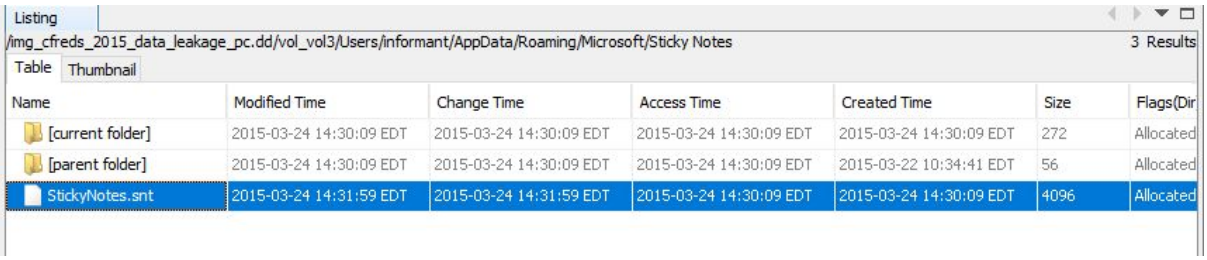
Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:34:42 EDT	56
[parent folder]	2015-03-23 14:35:59 EDT	2015-03-23 14:35:59 EDT	2015-03-23 14:35:59 EDT	2015-03-22 10:34:41 EDT	56
ExplorerStartupLog.etl	2015-03-22 10:35:07 EDT	2015-03-22 10:35:07 EDT	2015-03-22 10:34:42 EDT	2015-03-22 10:34:42 EDT	3276
ExplorerStartupLog_RunOnce.etl	2015-03-22 10:34:43 EDT	2015-03-22 10:34:43 EDT	2015-03-22 10:34:43 EDT	2015-03-22 10:34:43 EDT	1638
thumbcache_1024.db	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	24
thumbcache_256.db	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	5242
thumbcache_32.db	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	1048
thumbcache_96.db	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	4194
thumbcache_idx.db	2015-03-24 10:44:13 EDT	2015-03-24 10:44:13 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	1295
thumbcache_sr.db	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	2015-03-22 10:35:02 EDT	24

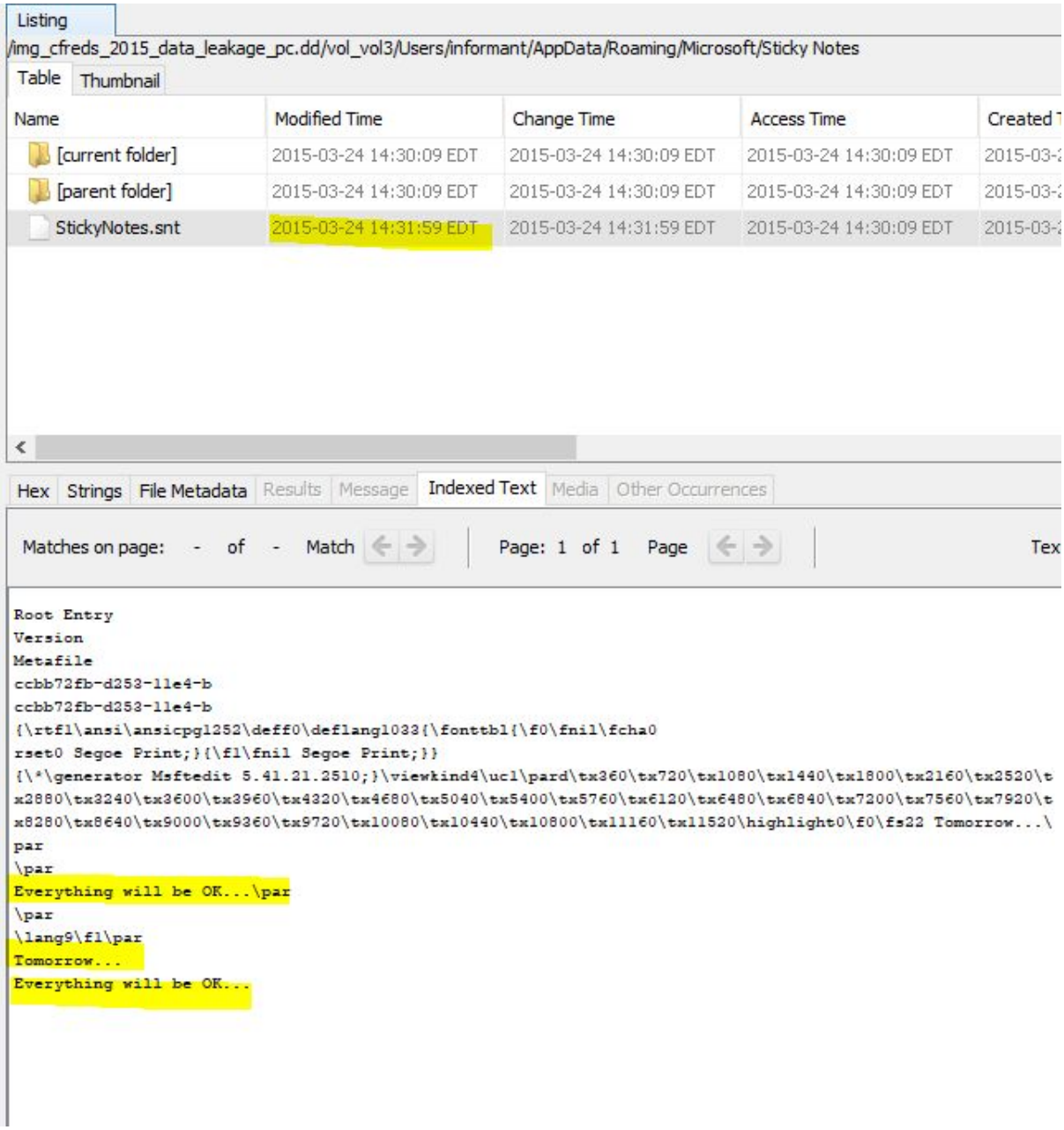
39. Identify traces related to confidential files stored in Thumbcache.
(Include ‘256’ only)

[secret_project]_proposal.lnk	E:\RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx	2015-03-23 14:37:20 EDT
[secret_project]_proposal.LNK	E:\RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx	2015-03-23 14:37:54 EDT
[secret_project]_final_meeting.pptx.lnk	\\10.11.11.128\secured_drive\Secret Project Data\final\[secret_project]_final_meeting.pptx	2015-03-23 16:27:33 EDT
[secret_project]_final_meeting.pptx.LNK	\\10.11.11.128\secured_drive\Secret Project Data\final\[secret_project]_final_meeting.pptx	2015-03-23 16:27:37 EDT
[secret_project]_design_concept.lnk	E:\RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt	2015-03-23 14:38:21 EDT
[secret_project]_design_concept.LNK	E:\RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt	2015-03-23 14:38:23 EDT

40. Where are Sticky Note files located?

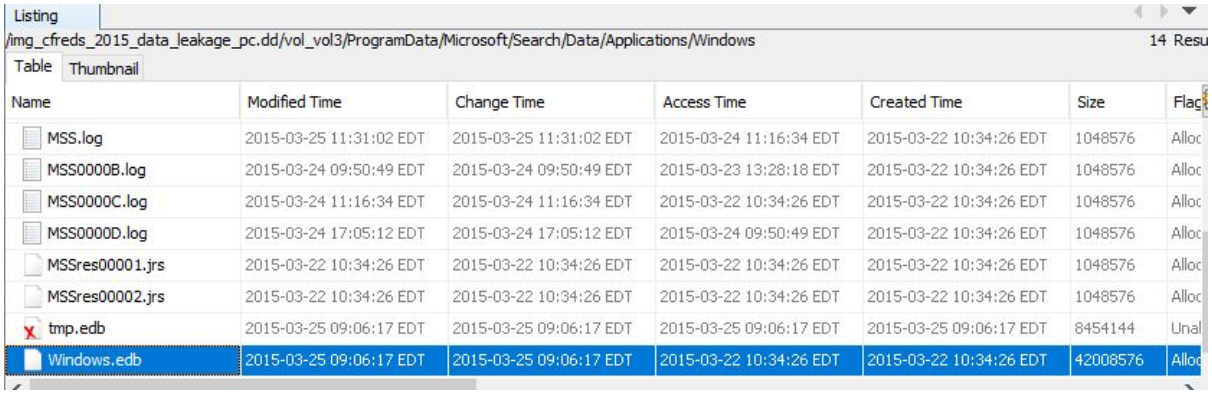


41. Identify notes stored in the Sticky Note file.



42. Was the ‘Windows Search and Indexing’ function enabled? How can you identify it? If it was enabled, what is a file path of the ‘Windows Search’ index database?

Windows Search was enabled



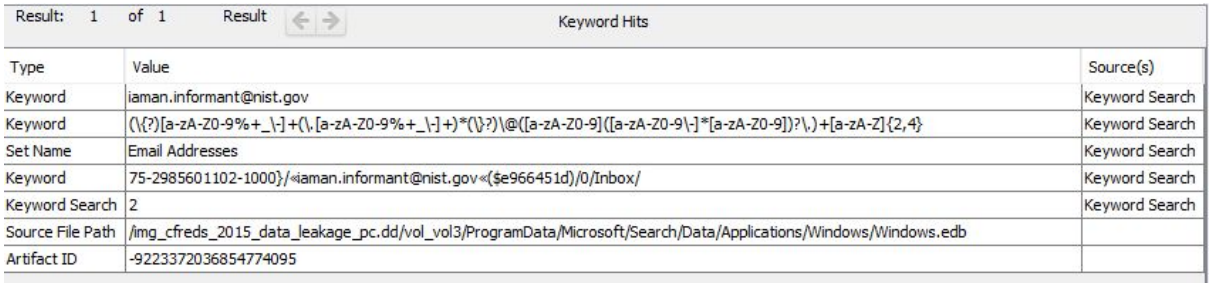
Listing

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/ProgramData/Microsoft/Search/Data/Applications/Windows 14 Resu

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flag
MSS.log	2015-03-25 11:31:02 EDT	2015-03-25 11:31:02 EDT	2015-03-24 11:16:34 EDT	2015-03-22 10:34:26 EDT	1048576	Alloc
MSS0000B.log	2015-03-24 09:50:49 EDT	2015-03-24 09:50:49 EDT	2015-03-23 13:28:18 EDT	2015-03-22 10:34:26 EDT	1048576	Alloc
MSS0000C.log	2015-03-24 11:16:34 EDT	2015-03-24 11:16:34 EDT	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	1048576	Alloc
MSS0000D.log	2015-03-24 17:05:12 EDT	2015-03-24 17:05:12 EDT	2015-03-24 09:50:49 EDT	2015-03-22 10:34:26 EDT	1048576	Alloc
MSSres00001.jrs	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	1048576	Alloc
MSSres00002.jrs	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	1048576	Alloc
tmp.edb	2015-03-25 09:06:17 EDT	2015-03-25 09:06:17 EDT	2015-03-25 09:06:17 EDT	2015-03-25 09:06:17 EDT	8454144	Unal
Windows.edb	2015-03-25 09:06:17 EDT	2015-03-25 09:06:17 EDT	2015-03-22 10:34:26 EDT	2015-03-22 10:34:26 EDT	42008576	Alloc

43. What kinds of data were stored in Windows Search database?



Result: 1 of 1 Result Keyword Hits

Type	Value	Source(s)
Keyword	iaman.informant@nist.gov	Keyword Search
Keyword	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}	Keyword Search
Set Name	Email Addresses	Keyword Search
Keyword	75-2985601102-1000}/«iaman.informant@nist.gov«($e966451d)/0/Inbox/	Keyword Search
Keyword Search	2	Keyword Search
Source File Path	/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.edb	
Artifact ID	-9223372036854774095	

44. Find traces of Internet Explorer usage stored in Windows Search database.
(It should be considered only during a date range between 2015-03-22 and 2015-03-23.)

index.dat	clients1.google.com	int	Internet Explorer	2015-03-22 04:09:43 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	www.google.com	internet explorer 11	Internet Explorer	2015-03-22 04:09:48 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	intern	Internet Explorer	2015-03-22 04:09:44 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	internet explorer 11	Internet Explorer	2015-03-22 04:09:46 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	internet e	Internet Explorer	2015-03-22 04:09:44 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	i	Internet Explorer	2015-03-22 04:09:43 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	interne	Internet Explorer	2015-03-22 04:09:44 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	internet ex	Internet Explorer	2015-03-22 04:09:44 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	internet explorer	Internet Explorer	2015-03-22 04:09:45 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	internet explorer 1	Internet Explorer	2015-03-22 04:09:46 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	inter	Internet Explorer	2015-03-22 04:09:43 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	inte	Internet Explorer	2015-03-22 04:09:43 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	in	Internet Explorer	2015-03-22 04:09:43 EDT	cfreds_2015_data_leakage_pc.dd
index.dat	clients1.google.com	internet	Internet Explorer	2015-03-22 04:09:44 EDT	cfreds_2015_data_leakage_pc.dd

45. List the e-mail communication stored in Windows Search database.
(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)

```
-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!
USB device may be easily detected.
So, try another method.
I am trying.
-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!
USB device may be easily detected.
So, try another method.
I am trying.
-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!
USB device may be easily detected.
So, try another method.
I am trying.
-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!
USB device may be easily detected.
So, try another method.
I am trying.
-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!
USB device may be easily detected.
So, try another method.
I am trying.
-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!
USB device may be easily detected.
So, try another method.
USB device may be easily detected.
```

46.List files and directories related to Windows Desktop stored in Windows Search database. (Windows Desktop directory: \Users\informant\Desktop\)

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Desktop 9 Res

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir
[current folder]	2015-03-25 11:29:08 EDT	2015-03-25 11:29:08 EDT	2015-03-25 11:29:08 EDT	2015-03-22 10:34:41 EDT	56	Allocatec
[parent folder]	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-22 10:34:31 EDT	256	Allocatec
[QAT	2076-11-29 03:54:34 EST	2015-03-25 11:13:49 EDT	2076-11-29 03:54:34 EST	2076-11-29 03:54:34 EST	48	Unallocat
Download	2015-03-25 11:15:45 EDT	2015-03-25 11:15:45 EDT	2015-03-25 11:15:45 EDT	2015-03-22 11:08:23 EDT	56	Allocatec
desktop.ini	2015-03-22 10:34:59 EDT	2015-03-22 10:34:59 EDT	2015-03-22 10:34:55 EDT	2015-03-22 10:34:55 EDT	282	Allocatec
Google Drive.lnk	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	1665	Unallocat
Resignation_Letter_(Iaman_Informant).docx	2015-03-24 14:59:30 EDT	2015-03-24 14:59:30 EDT	2015-03-24 14:59:30 EDT	2015-03-24 14:48:40 EDT	11893	Allocatec
Resignation_Letter_(Iaman_Informant).xps	2015-03-25 11:28:34 EDT	2015-03-25 11:28:47 EDT	2015-03-25 11:28:33 EDT	2015-03-25 11:28:33 EDT	178139	Allocatec
~$signation_Letter_(Iaman_Informant).docx	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	Unallocat

47. Where are Volume Shadow Copies stored? When were they created?

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2015-03-25 10:57:28 EDT	2015-03-25 10:57:28 EDT	2015-03-25 10:57:28 EDT	2015-03-25 06:15:18 EDT	56
[parent folder]	2015-03-25 11:19:05 EDT	2015-03-25 11:19:05 EDT	2015-03-25 11:19:05 EDT	2009-07-13 22:38:56 EDT	288
SPP	2015-03-25 10:57:24 EDT	2015-03-25 10:57:24 EDT	2015-03-25 10:57:24 EDT	2015-03-22 11:00:14 EDT	56
MountPointManagerRemoteDatabase	2015-03-25 06:15:18 EDT	2015-03-25 06:15:18 EDT	2015-03-25 06:15:18 EDT	2015-03-25 06:15:18 EDT	0
Syscache.hve	2015-03-25 11:31:05 EDT	2015-03-25 11:20:57 EDT	2015-03-25 11:31:05 EDT	2015-03-25 06:15:55 EDT	2883584
Syscache.hve.LOG1	2015-03-25 11:20:57 EDT	2015-03-25 11:20:57 EDT	2015-03-25 06:15:55 EDT	2015-03-25 06:15:55 EDT	262144
Syscache.hve.LOG2	2015-03-25 06:15:55 EDT	2015-03-25 06:15:55 EDT	2015-03-25 06:15:55 EDT	2015-03-25 06:15:55 EDT	0
tracking.log	2015-03-25 06:16:09 EDT	2015-03-25 06:16:09 EDT	2015-03-25 06:15:52 EDT	2015-03-25 06:15:52 EDT	20480
{3808876b-c176-4e48-b7ae-04046e6cc752}	2015-03-25 10:50:37 EDT	2015-03-25 10:50:37 EDT	2015-03-25 10:50:37 EDT	2015-03-25 10:50:37 EDT	65536
{9b365807-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-	2015-03-25 10:57:27 EDT	2015-03-25 10:57:27 EDT	2015-03-25 10:50:37 EDT	2015-03-25 10:50:37 EDT	94109696
{9b365826-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-	2015-03-25 10:57:24 EDT	2015-03-25 10:57:24 EDT	2015-03-25 10:57:24 EDT	2015-03-25 10:57:24 EDT	335544320

48. Find traces related to Google Drive service in Volume Shadow Copy.
What are the differences between the current system image (of Question 29 ~ 31) and its VSC?

/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Local/Google/Drive/user_default 18 R

Table Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-23 16:02:51 EDT	56	Allocated
[parent folder]	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:45 EDT	56	Allocated
cloud_graph	2015-03-25 11:22:47 EDT	2015-03-25 11:22:47 EDT	2015-03-25 11:22:47 EDT	2015-03-23 16:05:32 EDT	152	Allocated
CrashReports	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	48	Allocated
cacerts	2015-03-25 11:21:34 EDT	2015-03-25 11:21:34 EDT	2015-03-25 11:21:34 EDT	2015-03-23 16:02:51 EDT	3245	Unallocated
cacerts	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	3245	Unallocated
com.google.drive.nativeproxy.json	2015-03-25 11:21:36 EDT	2015-03-25 11:21:36 EDT	2015-03-23 16:05:32 EDT	2015-03-23 16:05:32 EDT	294	Allocated
lockfile	2015-03-25 11:21:34 EDT	2015-03-25 11:21:34 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	0	Allocated
pid	2015-03-25 11:21:34 EDT	2015-03-25 11:21:34 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	4	Allocated
run_dir	2015-03-25 11:21:34 EDT	2015-03-25 11:21:34 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	46	Allocated
snapshot.db	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	20480	Unallocated
snapshot.db-shm	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:21:34 EDT	32768	Unallocated
snapshot.db-wal	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:21:34 EDT	33568	Unallocated
sync_config.db	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	11264	Unallocated
sync_config.db-shm	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:21:34 EDT	32768	Unallocated
sync_config.db-wal	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:22:48 EDT	2015-03-25 11:21:34 EDT	4224	Unallocated
sync_log.log	2015-03-25 11:23:00 EDT	2015-03-25 11:23:00 EDT	2015-03-23 16:02:51 EDT	2015-03-23 16:02:51 EDT	408238	Allocated
sync_log.log	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

Questions 49 - 60

49. What files were deleted from Google Drive?

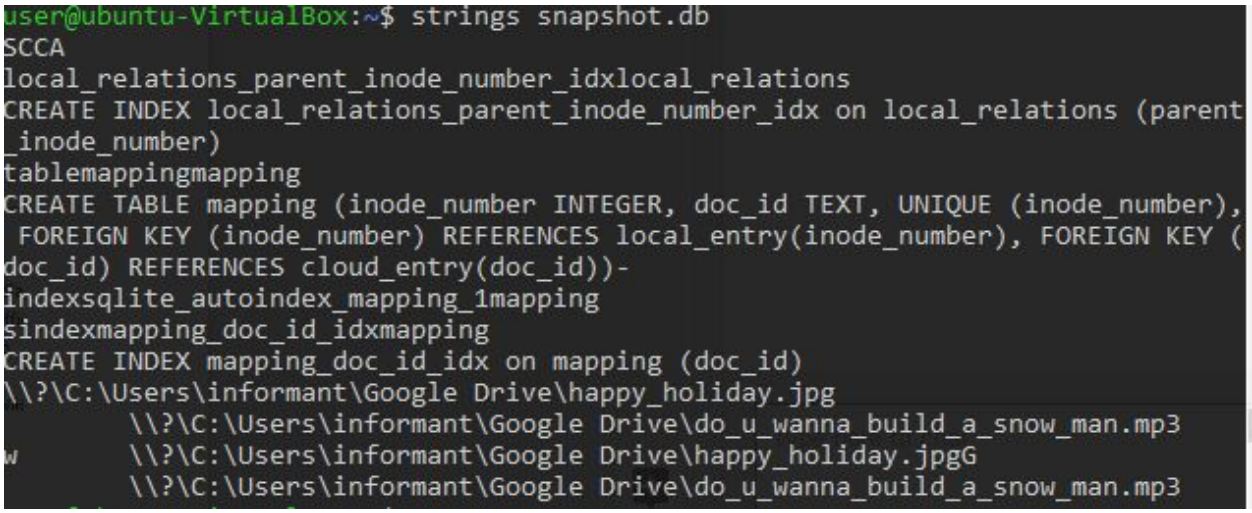
Taking the obvious path of using the (**not deleted**) log file *\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log* gives the deleted files

- How to get started with Drive
- happy_holiday.jpg
- Do_u_wanna_build_a_snow_man.mp3

after a few searches (/Action\.DELETE.*name=u'.*?'/).

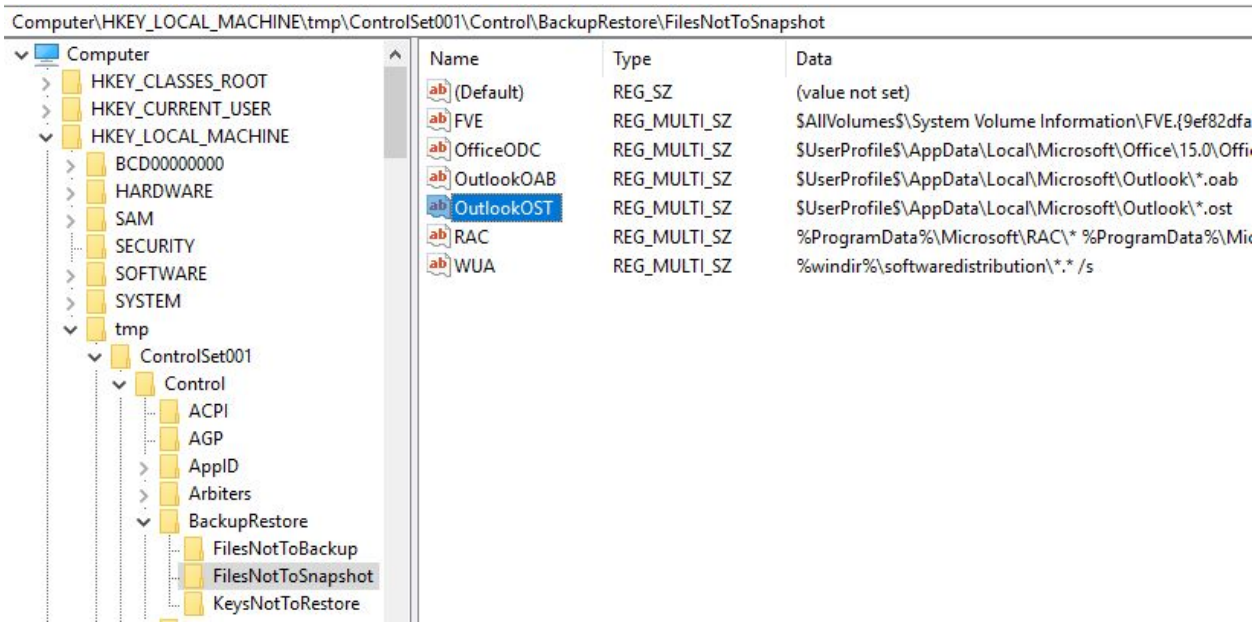
One *could* of course also take the painful path of restoring the deleted file *\Users\informant\AppData\Local\Google\Drive\user_default\snapshot.db* and try to restore deleted rows from it (SQLite).
Opening the DB in a couple of open source tools didn't work (or gave no output, but opening the (only 20kb) file in a hex viewer (or with *strings*) shows that the DB only contains two (distinct) file paths:

- C:\Users\informant\Google Drive\happy_holiday.jpg
- C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3



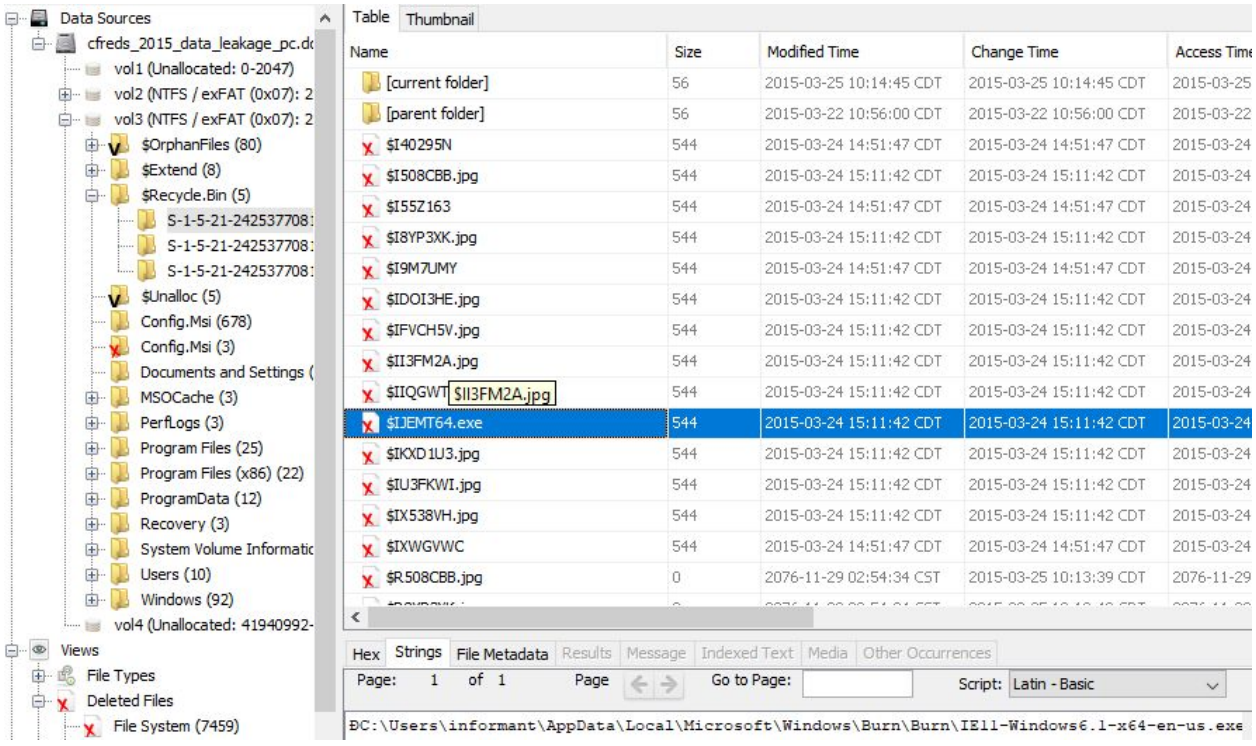
50. Why can't we find Outlook's e-mail data in Volume Shadow Copy?

Loading the registry hive "*1.ntfs\Windows\System32\config\SYSTEM*" in a VM (as *HKLM\tmp*) shows that "*HKLM\tmp\ControlSet001\Control\BackupRestore\FilesNotToSnapshot*" and "*HKLM\tmp\ControlSet002\Control\BackupRestore\FilesNotToSnapshot*" booth contain "*$UserProfile$\AppData\Local\Microsoft\Outlook*.ost*" which excludes the mails from the VSM:



51. Examine ‘Recycle Bin’ data in PC.

Opening the `.dd` image in 7-zip or mounting it in Windows shows the trash to be empty. *Autopsy* reveals, that there were a number of files. The *Strings* tab for each file shows the original file name:



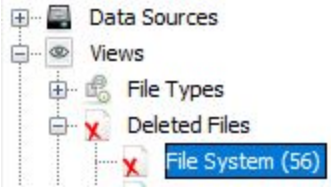
52. What actions were performed for anti-forensics on PC at the last day '2015-03-25'?

BLOCKED: I don’t think I will actually do this, as it depends on all kinds of previous questions:
- *See Question 10 and 11 for identifying application usage logs.*
- *See Question 15, 16 and 44 for identifying web history.*
- *See Question 30 and 49 for identifying cloud storage drive history.*

And this goes hand in hand with questions 58 to 60.

53. Recover deleted files from USB drive ‘RM#2’.

Image loaded in Autopsy:



Name	Size
design	4096
[current folder]	4096
winter_storm.amr	14547968
winter_whether_advisory.zip	16381123
PRICIN~1	4096
[current folder]	4096
my_favorite_cars.db	1260544
my_favorite_movies.7z	100078
new_years_day.jpg	10237535
super_bowl.avi	10289152
progress	4096
[current folder]	4096
my_friends.svg	58368
my_smartphone.png	4440235
new_year_calendar.one	27414
proposal	4096
[current folder]	4096
a_gift_from_you.gif	35226880
landscape.png	6484502
TECHNI~1	4096
[current folder]	4096
diary_#1d.txt	121441
diary_#1p.txt	458267

Name	Size
diary_#2d.txt	658922
diary_#2p.txt	1154560
diary_#3d.txt	2360832
diary_#3p.txt	325120
desktop.ini	129
amalfi.bmp	921654
BAMBOO~1.GIF	6717692
barn.gif	3352929
blini.gif	2125114
boudicca.bmp	8798374
cactus.png	6164389
cave.png	8182655
CUTTY-~1.JPG	1625241
eggs.gif	2284125
FORSYT~1.PNG	8107995
injera.gif	34480
JACK-O~1.TIF	7545856
jump.jpg	2015880
leaf.jpg	798064
oak-snow.jpg	1370140
orchid.png	8455527
PIAZZA~1.JPG	1267394
pisa.JPG	847709

54. What actions were performed for anti-forensics on USB drive ‘RM#2’?

Current FS is empty, but has a number of deleted files → quick format.

55. What files were copied from PC to USB drive ‘RM#2’?

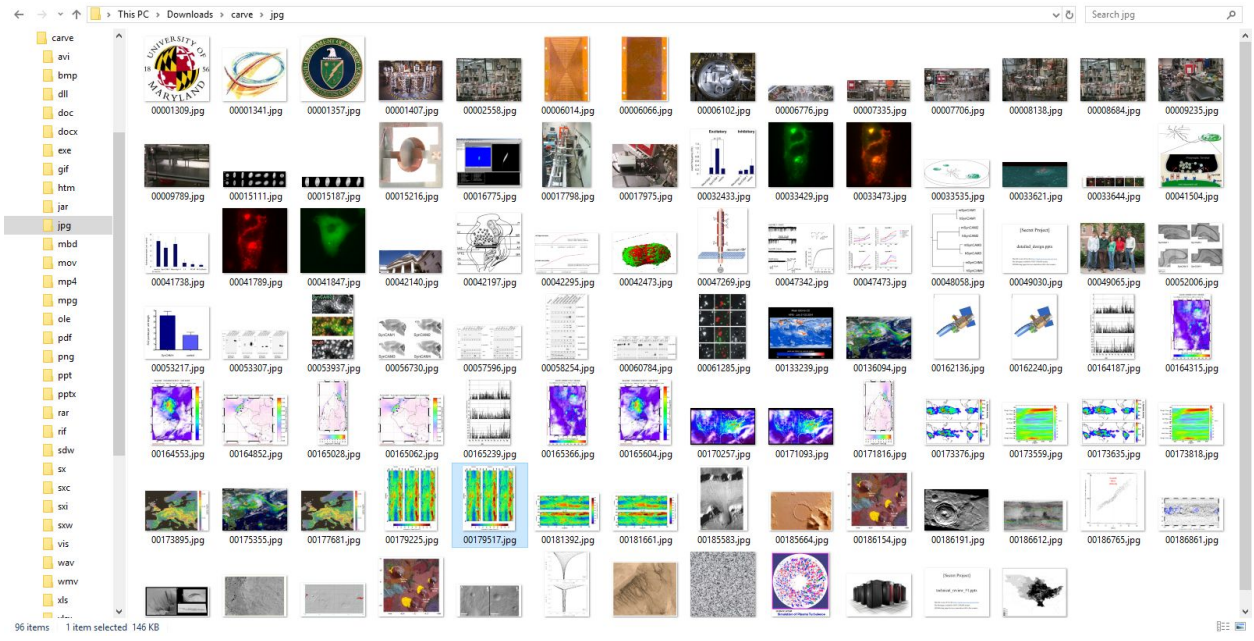
I think they are getting at file names that appear in questions 25 or 26 *and* question 53. The only on is “*winter_whether_advisory.zip*”.

56. Recover hidden files from the CD-R ‘RM#3’. How to determine proper filenames of the original files prior to renaming tasks?

Current files:

```
user@ubuntu-VirtualBox:~$ sudo mount -o loop cfreds-cd-r.dd /mnt/tmp/
mount: /dev/loop0 is write-protected, mounting read-only
user@ubuntu-VirtualBox:~$ ll /mnt/tmp/
total 2136
drwxrwxrwx 2 nobody nogroup    668 Mar 24  2015 ./
drwxr-xr-x 3 root   root      4096 Mar 16 19:10 ../
-rwxrwxrwx 1 nobody nogroup 780831 Jul 14  2009 Koala.jpg*
-rwxrwxrwx 1 nobody nogroup 777835 Jul 14  2009 Penguins.jpg*
-rwxrwxrwx 1 nobody nogroup 620888 Jul 14  2009 Tulips.jpg*
```

Autopsy couldn’t recognize the file system, but *foremost* works on any raw file buffer by pattern recognizing the content of certain file types.
foremost -t all -i cfreds-cd-r.dd -o carve/ -v produces a flat file structure sorted by file type. The names are unrelated to the original names. E.g. for *jpeg* files:



Something like *strings -n 40* could be used to extract all intelligible text (and xml-based) files from the raw image.

The solution says that "*Filename can be inferred from the first page [...]*". But manual inspection of the image shows that the beginning of the file contains littel other than null bytes. This can be demonstrated by running *head -600k cfreds-cd-r.dd | strings -n 1* which shows any single byte in the first 600kb if the image that can be interpreted as a character. The output is less than 1kb, and even that mostly repeats itself.

57. What actions were performed for anti-forensics on CD-R 'RM#3'?

The original file system of the CD was obviously removed and replaced with one containing only the three image files in the fist screenshot of *56*.
Also, we are told by the solution, that a lot of unrelated (image) files were added, but on first glance (without knowing what is actually being leaked), the images don't seem to be unrelated. They are photographies and charts of … scientific stuff.
The most obvious solution for destroying the data on an optical disk (physically shredding it) was not taken.

58. Create a detailed timeline of data leakage processes.
59. List and explain methodologies of data leakage performed by the suspect.
60. Create a visual diagram for a summary of results.

BLOCKED: These three depend on *ALL* previous questions.