



# Digital Forensics Report

Luís Aguiar 80950 & Jorge Pereira 81428 & Filipe Azevedo 82468

## Index

1	Objectives of the investigation .....	1
2	Artifacts for analysis .....	1
3	Evidence to look for.....	1
4	Examination Details .....	2
5	Analysis Results .....	38
6	Conclusions .....	38
7	Appendix - Tools Used .....	38

## 1 Objectives of the investigation

In this case we were given artifacts collected from Mr. Iaman Informant, who is suspected of leaking information about the famous international company OOO to Mr. Spy Conspirator, who works for a rival company. Our job is to collect evidences of the data leakage, and any data that might have been generated from the suspect's electronic devices.

## 2 Artifacts for analysis

In this case, we were given an image of a hard drive, an image of a USB removable storage device, and an image of a CD-R, collected from Mr. Iaman Informant himself.

## 3 Evidence to look for

The three images that were given to us contained a lot of information, not just information relevant to the investigation. With this in mind, we set out to find proof in the artifacts that were given to us about the leakage of data from Mr. Iaman Informant.

## 4 Examination Details

- 1) The MD5 hashes of the images are:

File name	MD5 - Acquisition	MD5 - Verification
cfreds_2015_data_leakage_pc.dd	a49d1254c873808c58e6f1bcd60b5bde	a49d1254c873808c58e6f1bcd60b5bde
cfreds_2015_data_leakage_rm#2.dd	b4644902acab4583a1d0f9f1a08faa77	b4644902acab4583a1d0f9f1a08faa77
cfreds_2015_data_leakage_rm#3_type2.dd	858c7250183a44dd83eb706f3f178990	858c7250183a44dd83eb706f3f178990

So, yes, they match.

- 2) The PC image has 4 volumes, with 2 partitions. The information about them is in the image below.

Name	ID	Starting Sector	Length in Sectors	Description	Flags
 vol1 (Unallocated: 0-1048575)	1	0	2048	Unallocated	Unallocated
 vol2 (NTFS / exFAT (0x07): 2048-104859647)	2	2048	204800	NTFS / exFAT (0x07)	Allocated
 vol3 (NTFS / exFAT (0x07): 206848-21368088575)	3	206848	41734144	NTFS / exFAT (0x07)	Allocated
 vol4 (Unallocated: 41940992-42989567)	4	41940992	2048	Unallocated	Unallocated

Figure 1 - Information about the PC image

- 3) After consulting the following registry file, it is possible to obtain the following information [1]:

**\Windows\System32\Config\SOFTWARE\Microsoft\WindowsNT\CurrentVersion**

<b>OS Name</b>	Windows 7 Ultimate Service Pack 1
<b>Product ID</b>	00426-292-0000007-85262
<b>Installation date</b>	2015-03-22 14:34:26 GMT
<b>System Root</b>	C:\Windows
<b>Build Number</b>	7601
<b>Version Number</b>	6.1
<b>Registered Owner</b>	informant

- 4) After consulting the following registry file, it is possible to obtain the following information [1]:

**\Windows\System32\Config\SYSTEM\ControlSet00X\Control\TimeZoneInformation**

<b>Time Zone Key Name</b>	Eastern Standard Time
<b>Bias</b>	- 300 (minutes) = - 5 (hours)

- 5) The name of the computer is "INFORMANT-PC", as it is possible to prove with the following image [2]:



Source File	Name
 SYSTEM	INFORMANT-PC
 SYSTEM	INFORMANT-PC

Figure 2 - Name of the PC

- 6) All accounts in the OS are in the table below. This information was obtained from the following hive [3]:

**\Windows\System32\Config\SAM**

User Name	Account Type	Account Created	Password Hint	Last Login Date	Password Reset Date	Password Fail Date	Login Count
informant	Default Admin User	Sun Mar 22 09:33:54 2015	IAMAN	Wed Mar 25 09:45:59 2015	Sun Mar 22 09:33:54 2015	Wed Mar 25 09:45:43 2015	10
admin11	Default Admin User	Sun Mar 22 10:51:54 2015	----	Sun Mar 22 10:57:02 2015	Sun Mar 22 10:52:10 2015	Sun Mar 22 10:53:02 2015	2
ITechTeam	Default Admin User	Sun Mar 22 10:52:30 2015	----	Never	Sun Mar 22 10:52:45 2015	Sun Mar 22 10:53:02 2015	0
temporary	Custom Limited Acct	Sun Mar 22 10:53:01 2015	----	Sun Mar 22 10:55:57 2015	Sun Mar 22 10:53:11 2015	Sun Mar 22 10:56:37 2015	1

- 7) After consulting the answer to question (6) it is easy to verify that the last logged in user was:

**informant at Wed Mar 25 09:45:59 2015 (EST)**

- 8) After consulting the SYSTEM hive, it's trivial to see that the last shutdown was at [4]:

**Wed Mar 25 10:31:05 2015 (EST)**

- 9) Again, after consulting the same SYSTEM hive, we obtained the following information [4]:

<b>Adapter</b>	Intel(R) PRO/1000 MT Network Connection
<b>DHCP Enabled</b>	Yes
<b>DHCP IP Address</b>	10.11.11.129
<b>DHCP Subnet Mask</b>	255.255.255.0
<b>DHCP Server</b>	10.11.11.254
<b>DHCP Name Server</b>	10.11.11.2
<b>DHCP Default Gateway</b>	10.11.11.2
<b>DHCP Domain</b>	localdomain

- 10) The list of the installed programs can be obtained by analyzing the content of the SOFTWARE hive, using a specialized tool [3]. After analyzing the output of that tool, we obtained the following results:

Installation Date (EST)	Name	Version
10:04:14 - 2015-03-22	Microsoft Office Professional Plus 2013	15.0.4420.1017
10:11:52 - 2015-03-22	Google Chrome	41.0.2272.101
10:16:03 - 2015-03-22	Google Update Helper	1.3.26.9
15:00:45 - 2015-03-23	Apple Application Support	3.0.6
15:00:58 - 2015-03-23	Bonjour	3.0.0.10
15:01:01 - 2015-03-23	Apple Software Update	2.1.3.127
15:02:46 - 2015-03-23	Google Drive	1.20.8672.3137
09:51:39 - 2015-03-25	Microsoft .NET Framework 4	4.0.30319
09:57:31 - 2015-03-25	Eraser	6.2.0.2962

- 11) After analyzing the NTUSER.DAT hive [3] of the **informant** user, and consulting the Prefetch [1], it's possible to obtain the following execution log:

Last Execution Time (EST)	Name	Count	Source
10:12:32 - 2015-03-22	IE11-Windows6.1-x64-en-us.exe	1	User Assist
15:26:50 - 2015-03-23	EXCEL.EXE	1	User Assist
16:27:33 - 2015-03-23	POWERPNT.EXE	2	User Assist
13:29:07 - 2015-03-24	SOLITAIRE.EXE	1	Prefetch
13:31:55 - 2015-03-24	StickyNotes	13	User Assist
16:05:38 - 2015-03-24	CHROME.EXE	71	Prefetch
09:41:03 - 2015-03-25	OUTLOOK.EXE	1	Prefetch
09:50:14 - 2015-03-25	ERASER 6.2.0.2962.EXE	1	Prefetch
09:57:56 - 2015-03-25	CCSETUP504.EXE	1	Prefetch
10:13:30 - 2015-03-25	ERASER.EXE	2	Prefetch
10:15:50 - 2015-03-25	CCLEANER64.EXE	2	Prefetch
10:16:00 - 2015-03-25	GOOGLEUPDATE.EXE	38	Prefetch
10:18:29 - 2015-03-25	UNINST.EXE (CCleaner)	1	Prefetch
10:21:31 - 2015-03-25	GOOGLEDRIVESYNC.EXE	2	Prefetch
10:22:06 - 2015-03-25	IEXPLORE.EXE	2	Prefetch
10:22:07 - 2015-03-25	IEXPLORE.EXE	14	Prefetch

10:24:48 - 2015-03-25	WINWORD.EXE	3	Prefetch
10:28:47 - 2015-03-25	XPSRCHVW.EXE	1	Prefetch

Some interesting logs without timestamps			
No timestamp	icloudsetup.exe	-	User Assist
No timestamp	dotNetFx40_Full_setup.exe	-	User Assist
No timestamp	icloudsetup.exe	-	User Assist

12) If we look at the Windows Event Log using a specialized tool [5], we can look at all the traces about the system on/off and the user logon/logoff.

Event	Event Description	Timestamp (EST)
4624	Log On	09:34:24 – 2015-03-22
4624	Log On	09:34:28 – 2015-03-22
4624	Log On	09:34:49 – 2015-03-22
1100	Shutting Down	09:38:16 – 2015-03-22
4608	Starting Up	09:51:14 – 2015-03-22
4624	Log On	09:51:14 – 2015-03-22
4624	Log On	09:51:15 – 2015-03-22
4624	Log On	09:51:16 – 2015-03-22
4624	Log On	09:51:20 – 2015-03-22
4624	Log On	09:51:27 – 2015-03-22
4624	Log On	09:53:30 – 2015-03-22
4624	Log On	09:53:31 – 2015-03-22
4624	Log On	09:53:39 – 2015-03-22
4624	Log On	10:00:08 – 2015-03-22
4624	Log On	10:00:18 – 2015-03-22
4624	Log On	10:04:33– 2015-03-22
4624	Log On	10:12:37– 2015-03-22
4624	Log On	10:13:22– 2015-03-22
4624	Log On	10:16:01– 2015-03-22
1100	Shutting Down	10:19:42 – 2015-03-22
4624	Log On	10:19:42– 2015-03-22
4624	Log On	10:22:31– 2015-03-22
4608	Starting Up	10:22:31 – 2015-03-22

4624	Log On	10:22:54- 2015-03-22
4624	Log On	10:22:56- 2015-03-22
4624	Log On	10:23:02- 2015-03-22
4624	Log On	10:23:12- 2015-03-22
4624	Log On	10:24:03- 2015-03-22
4624	Log On	10:25:04- 2015-03-22
1100	Shutting Down	10:28:28 - 2015-03-22
4608	Starting Up	10:43:36 - 2015-03-22
4624	Log On	10:43:36 - 2015-03-22
4624	Log On	10:43:37 - 2015-03-22
4624	Log On	10:43:38 - 2015-03-22
4624	Log On	10:43:43 - 2015-03-22
4624	Log On	10:45:16 - 2015-03-22
4624	Log On	10:45:31 - 2015-03-22
4624	Log On	10:45:45 - 2015-03-22
4624	Log On	10:47:37 - 2015-03-22
4624	Log On	10:52:10 - 2015-03-22
4624	Log On	10:52:45 - 2015-03-22
4624	Log On	10:53:11 - 2015-03-22
4624	Log On	10:53:44 - 2015-03-22
4624	Log On	10:55:57 - 2015-03-22
4634	Log Off	10:56:45 - 2015-03-22
4624	Log On	10:57:02 - 2015-03-22
4624	Log On	10:57:54 - 2015-03-22
4634	Log Off	10:57:55 - 2015-03-22
4634	Log Off	10:57:56 - 2015-03-22
4634	Log Off	10:58:26 - 2015-03-22
1100	Shutting Down	11:00:09 - 2015-03-22
4624	Log On	12:24:23 - 2015-03-23
4624	Log On	12:24:24 - 2015-03-23
4624	Log On	12:24:25 - 2015-03-23
4624	Log On	12:24:26 - 2015-03-23
4624	Log On	12:24:28 - 2015-03-23
4624	Log On	12:24:41 - 2015-03-23

4624	Log On	12:24:53 – 2015-03-23
4624	Log On	12:26:34 – 2015-03-23
4624	Log On	13:36:07 – 2015-03-23
4624	Log On	15:00:22 – 2015-03-23
4624	Log On	15:00:45 – 2015-03-23
4624	Log On	15:01:01 – 2015-03-23
4624	Log On	15:01:02 – 2015-03-23
1100	Shutting Down	16:02:59 – 2015-02-23
4624	Log On	10:14:30 – 2015-03-24
4624	Log On	10:21:38 – 2015-03-24
4624	Log On	10:22:39 – 2015-03-24
4624	Log On	10:46:14 – 2015-03-24
4634	Log Off	13:28:38 – 2015-03-24
4624	Log On	13:28:38 – 2015-03-24
4624	Log On	15:58:52 – 2015-03-24
1100	Shutting Down	16:07:26 – 2015-02-24
4624	Log On	09:31:53 – 2015-03-25
4624	Log On	09:45:59 – 2015-03-25
4634	Log Off	09:45:59 – 2015-03-25
4624	Log On	09:50:50 – 2015-03-25
4624	Log On	09:50:30 – 2015-03-25
4624	Log On	09:50:50 – 2015-03-25
4624	Log On	09:56:55 – 2015-03-25
4624	Log On	09:57:18 – 2015-03-25
4624	Log On	10:18:54 – 2015-03-25

13) After analyzing the SOFTWARE hive [3], we discovered that the suspect contained the following browsers installed on his computer:

```
[Sun Mar 22 15:11:52 2015 (UTC)] StartMenuInternet
VALUE: (default) -> IEXPLORE.EXE
SUBKEY: [Sun Mar 22 15:11:52 2015 (UTC)] Google Chrome
SUBKEY: [Sun Mar 22 15:19:29 2015 (UTC)] IEXPLORE.EXE
```

*Figure 3 - Browsers installed*

- 14) The history, cache and cookies of the previously referred browsers can be found at.

<b>Google Chrome</b>	C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\~
<b>Internet Explorer</b>	C:\Users\informant\AppData\Local\Microsoft\Windows\History\~ C:\Users\informant\AppData\Local\Microsoft\Windows\Temporary Internet Files\~ C:\Users\informant\AppData\Roaming\Microsoft\Windows\Cookies\~ C:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

- 15) After consulting the content of the files of the previous answer [6], it's possible to find the following history:

<b>Timestamp (EST)</b>	<b>URL</b>
10:09:01 - 2015-03-22	<a href="http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome">http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome</a>
10:09:47 - 2015-03-22	<a href="https://www.google.com/">https://www.google.com/</a>
10:10:50 - 2015-03-22	<a href="http://windows.microsoft.com/en-us/internet-explorer/download-ie">http://windows.microsoft.com/en-us/internet-explorer/download-ie</a>
10:11:04 - 2015-03-22	<a href="http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe">http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe</a>
10:11:06 - 2015-03-22	<a href="https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D%7B8A69D345-D564-463C-AFF1-">https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D%7B8A69D345-D564-463C-AFF1-</a>
10:11:58 - 2015-03-22	<a href="https://www.google.com/intl/en/chrome/browser/welcome.html">https://www.google.com/intl/en/chrome/browser/welcome.html</a>
10:27:59 - 2015-03-22	<a href="https://www.google.com/#q=outlook+2013+settings">https://www.google.com/#q=outlook+2013+settings</a>
10:28:13 - 2015-03-22	<a href="https://support.office.com/en-nz/article/Set-up-email-in-Outlook-2010-or-Outlook-2013-for-Office-365-or-Exchange-based-accounts-6e27792a-9267-4aa4-8bb6-c84ef146101b">https://support.office.com/en-nz/article/Set-up-email-in-Outlook-2010-or-Outlook-2013-for-Office-365-or-Exchange-based-accounts-6e27792a-9267-4aa4-8bb6-c84ef146101b</a>
12:26:58 - 2015-03-23	<a href="http://www.bing.com/">http://www.bing.com/</a>
12:26:58 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en">https://www.google.com/webhp?hl=en</a>
12:27:05 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en#q=Emmy+Noether&amp;oi=ddle&amp;ct=emmy-noethers-133rd-birthday-5681045017985024-hp&amp;hl=en">https://www.google.com/webhp?hl=en#q=Emmy+Noether&amp;oi=ddle&amp;ct=emmy-noethers-133rd-birthday-5681045017985024-hp&amp;hl=en</a>
12:27:36 - 2015-03-23	<a href="http://go.microsoft.com/fwlink/?LinkId=69157">http://go.microsoft.com/fwlink/?LinkId=69157</a>
12:27:49 - 2015-03-23	<a href="http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie">http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie</a>
13:02:09 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en#hl=en&amp;q=data+leakage+methods">https://www.google.com/webhp?hl=en#hl=en&amp;q=data+leakage+methods</a>
13:02:18 - 2015-03-23	<a href="http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation_1931">http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation_1931</a>
13:02:44 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en#hl=en&amp;q=leaking+confidential+information">https://www.google.com/webhp?hl=en#hl=en&amp;q=leaking+confidential+information</a>
13:03:40 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en#hl=en&amp;q=information+leakage+cases">https://www.google.com/webhp?hl=en#hl=en&amp;q=information+leakage+cases</a>
13:04:54 - 2015-03-23	<a href="http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-data-2015-03-13-1.584027">http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-data-2015-03-13-1.584027</a>



13:05:48 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=intellectual+property+theft">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=intellectual+property+theft</a>
13:05:55 - 2015-03-23	<a href="http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr">http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr</a>
13:06:01 - 2015-03-23	<a href="http://en.wikipedia.org/wiki/Intellectual_property">http://en.wikipedia.org/wiki/Intellectual_property</a>
13:06:27 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=how+to+leak+a+secret">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=how+to+leak+a+secret</a>
13:06:53 - 2015-03-23	<a href="http://research.microsoft.com/en-us/um/people/yael/publications/2001-leak_secret.pdf">http://research.microsoft.com/en-us/um/people/yael/publications/2001-leak_secret.pdf</a>
13:07:58 - 2015-03-23	<a href="http://www.bing.com/news/search?q=file+sharing+and+tethering&amp;FORM=HDRSC6">http://www.bing.com/news/search?q=file+sharing+and+tethering&amp;FORM=HDRSC6</a>
13:08:18 - 2015-03-23	<a href="http://sysinfotools.com/blog/tethering-internet-files-sharing/">http://sysinfotools.com/blog/tethering-internet-files-sharing/</a>
13:08:31 - 2015-03-23	<a href="http://www.bing.com/search?q=DLP%20DRM&amp;qsn=n&amp;form=QBRE&amp;pq=dlp%20drm&amp;sc=8-7&amp;sp=-1&amp;sk=&amp;cvid=6e206ee8751e4ad89f882ed52daf3aea&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=0">http://www.bing.com/search?q=DLP%20DRM&amp;qsn=n&amp;form=QBRE&amp;pq=dlp%20drm&amp;sc=8-7&amp;sp=-1&amp;sk=&amp;cvid=6e206ee8751e4ad89f882ed52daf3aea&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=0</a>
13:08:54 - 2015-03-23	<a href="http://www.bing.com/search?q=e-mail%20investigation&amp;qsn=n&amp;form=QBRE&amp;pq=e-mail%20investigation&amp;sc=8-7&amp;sp=-1&amp;sk=&amp;cvid=fe1c3738d8c7471284731724166959af&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=1">http://www.bing.com/search?q=e-mail%20investigation&amp;qsn=n&amp;form=QBRE&amp;pq=e-mail%20investigation&amp;sc=8-7&amp;sp=-1&amp;sk=&amp;cvid=fe1c3738d8c7471284731724166959af&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=1</a>
13:10:03 - 2015-03-23	<a href="http://www.bing.com/search?q=Forensic+Email+Investigation&amp;FORM=QSRE1&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=3">http://www.bing.com/search?q=Forensic+Email+Investigation&amp;FORM=QSRE1&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=3</a>
13:10:27 - 2015-03-23	<a href="http://www.bing.com/search?q=what%20is%20windows%20system%20artifacts&amp;qsn=n&amp;form=QBRE&amp;pq=what%20is%20windows%20system%20artifacts&amp;sc=0-27&amp;sp=-1&amp;sk=&amp;cvid=1ef4ace146854d97acf263b53bf97b8c&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=4">http://www.bing.com/search?q=what%20is%20windows%20system%20artifacts&amp;qsn=n&amp;form=QBRE&amp;pq=what%20is%20windows%20system%20artifacts&amp;sc=0-27&amp;sp=-1&amp;sk=&amp;cvid=1ef4ace146854d97acf263b53bf97b8c&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=4</a>
13:11:12 - 2015-03-23	<a href="http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/">http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/</a>
13:11:50 - 2015-03-23	<a href="http://www.bing.com/search?q=investigation%20on%20windows%20machine&amp;qsn=n&amp;form=QBRE&amp;pq=investigation%20on%20windows%20machine&amp;sc=8-4&amp;sp=-1&amp;sk=&amp;cvid=eb73de7f523c48769d56201379f55e67&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=5">http://www.bing.com/search?q=investigation%20on%20windows%20machine&amp;qsn=n&amp;form=QBRE&amp;pq=investigation%20on%20windows%20machine&amp;sc=8-4&amp;sp=-1&amp;sk=&amp;cvid=eb73de7f523c48769d56201379f55e67&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=5</a>
13:12:07 - 2015-03-23	<a href="https://technet.microsoft.com/en-us/library/cc162846.aspx">https://technet.microsoft.com/en-us/library/cc162846.aspx</a>
13:12:35 - 2015-03-23	<a href="http://www.bing.com/search?q=windows%20event%20logs&amp;qsn=n&amp;form=QBRE&amp;pq=windows%20event%20logs&amp;sc=0-32&amp;sp=-1&amp;sk=&amp;cvid=36b33ac5151246398f7dc1ca79de069c&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=6">http://www.bing.com/search?q=windows%20event%20logs&amp;qsn=n&amp;form=QBRE&amp;pq=windows%20event%20logs&amp;sc=0-32&amp;sp=-1&amp;sk=&amp;cvid=36b33ac5151246398f7dc1ca79de069c&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=6</a>
13:12:45 - 2015-03-23	<a href="https://support.microsoft.com/en-us/kb/308427">https://support.microsoft.com/en-us/kb/308427</a>
13:12:52 - 2015-03-23	<a href="http://en.wikipedia.org/wiki/Event_Viewer">http://en.wikipedia.org/wiki/Event_Viewer</a>
13:13:20 - 2015-03-23	<a href="http://www.bing.com/search?q=cd%20burning%20method&amp;qsn=n&amp;form=QBRE&amp;pq=cd%20burning%20method&amp;sc=8-2&amp;sp=-1&amp;sk=&amp;cvid=b7dbe6fb67424c578172ba57330a0894&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=7">http://www.bing.com/search?q=cd%20burning%20method&amp;qsn=n&amp;form=QBRE&amp;pq=cd%20burning%20method&amp;sc=8-2&amp;sp=-1&amp;sk=&amp;cvid=b7dbe6fb67424c578172ba57330a0894&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=7</a>

13:13:37 - 2015-03-23	<a href="http://www.bing.com/search?q=cd%20burning%20method%20in%20windows&amp;qs=n&amp;form=QBRE&amp;pq=cd%20burning%20method%20in%20windows&amp;sc=0-0&amp;sp=-1&amp;sk=&amp;cvid=acec9b1dcb8146c58258ad65c770d76e&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=8">http://www.bing.com/search?q=cd%20burning%20method%20in%20windows&amp;qs=n&amp;form=QBRE&amp;pq=cd%20burning%20method%20in%20windows&amp;sc=0-0&amp;sp=-1&amp;sk=&amp;cvid=acec9b1dcb8146c58258ad65c770d76e&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=8</a>
13:13:57 - 2015-03-23	<a href="https://msdn.microsoft.com/en-us/library/windows/desktop/dd562212(v=vs.85).aspx">https://msdn.microsoft.com/en-us/library/windows/desktop/dd562212(v=vs.85).aspx</a>
13:14:11 - 2015-03-23	<a href="http://www.bing.com/search?q=external%20device%20and%20forensics&amp;qs=n&amp;form=QBRE&amp;pq=external%20device%20and%20forensics&amp;sc=8-9&amp;sp=-1&amp;sk=&amp;cvid=c30c4b1f36114b1c9bc683838c69823a&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=9">http://www.bing.com/search?q=external%20device%20and%20forensics&amp;qs=n&amp;form=QBRE&amp;pq=external%20device%20and%20forensics&amp;sc=8-9&amp;sp=-1&amp;sk=&amp;cvid=c30c4b1f36114b1c9bc683838c69823a&amp;sid=BE5E388F8757406CAA32E58334719A20&amp;format=jsonv2&amp;jsoncbid=9</a>
13:14:24 - 2015-03-23	<a href="http://www.forensicswiki.org/wiki/USB_History_Viewing">http://www.forensicswiki.org/wiki/USB_History_Viewing</a>
13:14:50 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=cloud+storage">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=cloud+storage</a>
13:15:09 - 2015-03-23	<a href="http://en.wikipedia.org/wiki/Cloud_storage">http://en.wikipedia.org/wiki/Cloud_storage</a>
13:15:32 - 2015-03-23	<a href="http://www.pcadvisor.co.uk/test-centre/internet/3506734/best-cloud-storage-dropbox-google-drive-onedrive-icloud/">http://www.pcadvisor.co.uk/test-centre/internet/3506734/best-cloud-storage-dropbox-google-drive-onedrive-icloud/</a>
13:15:44 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=digital+forensics">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=digital+forensics</a>
13:15:49 - 2015-03-23	<a href="http://en.wikipedia.org/wiki/Digital_forensics">http://en.wikipedia.org/wiki/Digital_forensics</a>
13:16:06 - 2015-03-23	<a href="http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx">http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx</a>
13:16:55 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=how+to+delete+data">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=how+to+delete+data</a>
13:17:14 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=anti-forensics">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=anti-forensics</a>
13:17:19 - 2015-03-23	<a href="http://forensicswiki.org/wiki/Anti-forensic_techniques">http://forensicswiki.org/wiki/Anti-forensic_techniques</a>
13:18:00 - 2015-03-23	<a href="https://defcon.org/images/defcon-20/dc-20-presentations/Perklin/DEFCON-20-Perklin-AntiForensics.pdf">https://defcon.org/images/defcon-20/dc-20-presentations/Perklin/DEFCON-20-Perklin-AntiForensics.pdf</a>
13:18:10 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=system+cleaner">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=system+cleaner</a>
13:18:30 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=how+to+recover+data">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=how+to+recover+data</a>
13:19:03 - 2015-03-23	<a href="https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=data+recovery+tools">https://www.google.com/search?q=information+leakage+cases&amp;hl=en&amp;biw=950&amp;bih=499&amp;site=webhp&amp;tbm=vid&amp;source=lnms&amp;sa=X&amp;ei=3VUQVYH3FMO1sQTf1YGwBw&amp;ved=0CAoQ_AUoBA&amp;dpr=1#hl=en&amp;q=data+recovery+tools</a>
13:19:17 - 2015-03-23	<a href="http://en.wikipedia.org/wiki/List_of_data_recovery_software">http://en.wikipedia.org/wiki/List_of_data_recovery_software</a>
13:19:21 - 2015-03-23	<a href="http://www.forensicswiki.org/wiki/Tools:Data_Recovery">http://www.forensicswiki.org/wiki/Tools:Data_Recovery</a>
14:55:09 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en#hl=en&amp;q=apple+icloud">https://www.google.com/webhp?hl=en#hl=en&amp;q=apple+icloud</a>
14:55:28 - 2015-03-23	<a href="https://www.apple.com/icloud/setup/pc.html">https://www.apple.com/icloud/setup/pc.html</a>
14:56:04 - 2015-03-23	<a href="https://www.google.com/webhp?hl=en#hl=en&amp;q=google+drive">https://www.google.com/webhp?hl=en#hl=en&amp;q=google+drive</a>

14:56:15 - 2015-03-23	<a href="https://www.google.com/drive/download/">https://www.google.com/drive/download/</a>
15:43:52 - 2015-03-23	<a href="http://www.bing.com/news?FORM=Z9LH3">http://www.bing.com/news?FORM=Z9LH3</a>
15:45:30 - 2015-03-23	<a href="http://www.bing.com/news?q=Soccer+News&amp;FORM=NSBABR">http://www.bing.com/news?q=Soccer+News&amp;FORM=NSBABR</a>
15:53:46 - 2015-03-23	<a href="http://www.bing.com/news?q=top+stories&amp;FORM=NWRFSH">http://www.bing.com/news?q=top+stories&amp;FORM=NWRFSH</a>
15:55:10 - 2015-03-23	<a href="http://www.bing.com/news?q=world+news&amp;FORM=NSBABR">http://www.bing.com/news?q=world+news&amp;FORM=NSBABR</a>
15:55:18 - 2015-03-23	<a href="http://www.bing.com/news?q=entertainment+news&amp;FORM=NSBABR">http://www.bing.com/news?q=entertainment+news&amp;FORM=NSBABR</a>
15:55:54 - 2015-03-23	<a href="http://www.bing.com/news?q=business+news&amp;FORM=NSBABR">http://www.bing.com/news?q=business+news&amp;FORM=NSBABR</a>
10:22:46 - 2015-03-24	<a href="https://news.google.com/news/section?pz=1&amp;cf=all&amp;ned=us&amp;topic=w&amp;siidp=0b2226a6a5dab3b27ee85fc5e8d21f28f01e">https://news.google.com/news/section?pz=1&amp;cf=all&amp;ned=us&amp;topic=w&amp;siidp=0b2226a6a5dab3b27ee85fc5e8d21f28f01e</a>
10:23:16 - 2015-03-24	<a href="https://news.google.com/news/section?pz=1&amp;cf=all&amp;ned=us&amp;topic=tc&amp;siidp=e6116f8175cb189b8dd7fd58ef6bc922ec04&amp;ar=1427212899">https://news.google.com/news/section?pz=1&amp;cf=all&amp;ned=us&amp;topic=tc&amp;siidp=e6116f8175cb189b8dd7fd58ef6bc922ec04&amp;ar=1427212899</a>
13:59:52 - 2015-03-24	<a href="https://news.google.com/news?pz=1&amp;cf=all&amp;ned=us&amp;siidp=0c33ef04190b3734a22c5bae18801ff1041e">https://news.google.com/news?pz=1&amp;cf=all&amp;ned=us&amp;siidp=0c33ef04190b3734a22c5bae18801ff1041e</a>
15:00:27 - 2015-03-24	<a href="https://news.google.com/news/section?pz=1&amp;cf=all&amp;ned=us&amp;topic=w&amp;siidp=538c61c825aba06be7485be747a619778015">https://news.google.com/news/section?pz=1&amp;cf=all&amp;ned=us&amp;topic=w&amp;siidp=538c61c825aba06be7485be747a619778015</a>
16:06:50 - 2015-03-24	<a href="https://www.google.com/#q=security+checkpoint+cd-r">https://www.google.com/#q=security+checkpoint+cd-r</a>
09:46:44 - 2015-03-25	<a href="http://www.bing.com/search?q=anti-forensic+tools&amp;qsn=&amp;form=QLH&amp;pq=anti-forensic+tools&amp;sc=8-13&amp;sp=-1&amp;sk=&amp;cvid=e799e715fa2244a5a7967675bdcca9d3">http://www.bing.com/search?q=anti-forensic+tools&amp;qsn=&amp;form=QLH&amp;pq=anti-forensic+tools&amp;sc=8-13&amp;sp=-1&amp;sk=&amp;cvid=e799e715fa2244a5a7967675bdcca9d3</a>
09:46:54 - 2015-03-25	<a href="http://www.bing.com/search?q=eraser&amp;qsn=&amp;form=QBRE&amp;pq=eraser&amp;sc=8-6&amp;sp=-1&amp;sk=&amp;cvid=e3b983fe889944179093ff5199b2eac4&amp;sid=C7E8F3776E804120B57C623F21EF33C4&amp;format=jsonv2&amp;jsoncbid=0">http://www.bing.com/search?q=eraser&amp;qsn=&amp;form=QBRE&amp;pq=eraser&amp;sc=8-6&amp;sp=-1&amp;sk=&amp;cvid=e3b983fe889944179093ff5199b2eac4&amp;sid=C7E8F3776E804120B57C623F21EF33C4&amp;format=jsonv2&amp;jsoncbid=0</a>
09:46:59 - 2015-03-25	<a href="http://eraser.heidi.ie/">http://eraser.heidi.ie/</a>
09:47:34 - 2015-03-25	<a href="http://iweb.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2962.exe">http://iweb.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2962.exe</a>
09:47:51 - 2015-03-25	<a href="http://www.bing.com/search?q=ccleaner&amp;qsn=&amp;form=QBRE&amp;pq=ccleaner&amp;sc=8-8&amp;sp=-1&amp;sk=&amp;cvid=d434736d4e514ad497f68734a6779104&amp;sid=C7E8F3776E804120B57C623F21EF33C4&amp;format=jsonv2&amp;jsoncbid=1">http://www.bing.com/search?q=ccleaner&amp;qsn=&amp;form=QBRE&amp;pq=ccleaner&amp;sc=8-8&amp;sp=-1&amp;sk=&amp;cvid=d434736d4e514ad497f68734a6779104&amp;sid=C7E8F3776E804120B57C623F21EF33C4&amp;format=jsonv2&amp;jsoncbid=1</a>
09:48:12 - 2015-03-25	<a href="http://www.piriform.com/ccleaner/download">http://www.piriform.com/ccleaner/download</a>

16) Using the same tool as before with the same history files, it's possible to see the following search history:

Timestamp (EST)	Keywords
12:27:05 - 2015-03-23	Emmy Noether
13:02:09 - 2015-03-23	data leakage method
13:02:44 - 2015-03-23	leaking confidential information
13:03:40 - 2015-03-23	information leakage cases
13:05:22 - 2015-03-23	intellectual property theft
13:05:48 - 2015-03-23	how to leak a secret

13:06:53 - 2015-03-23	cloud storage
13:07:48 - 2015-03-23	file sharing and tethering
13:08:31 - 2015-03-23	DLP DRM
13:08:54 - 2015-03-23	e-mail investigation
13:10:03 - 2015-03-23	Forensic Email Investigation
13:10:27 - 2015-03-23	what is windows system artifacts
13:11:50 - 2015-03-23	investigation on windows machine
13:12:35 - 2015-03-23	windows event logs
13:13:20 - 2015-03-23	cd burning method
13:13:37 - 2015-03-23	cd burning method in windows
13:14:11 - 2015-03-23	external device and forensics
13:15:44 - 2015-03-23	digital forensics
13:16:55 - 2015-03-23	how to delete data
13:17:14 - 2015-03-23	anti-forensics
13:18:18 - 2015-03-23	system cleaner
13:18:30 - 2015-03-23	how to recover data
13:18:30 - 2015-03-23	data recovery tools
14:55:09 - 2015-03-23	apple icloud
14:56:04 - 2015-03-23	google drive
16:06:50 - 2015-03-24	security checkpoint cd-r
09:46:44 - 2015-03-25	anti-forensic tools
09:46:54 - 2015-03-25	eraser
09:47:51 - 2015-03-25	ccleaner

- 17) After consulting again the USER.NAT hive, and inspecting the wordwheelquery [3], we obtained the following information about the searches:

Keyword	Timestamp (EST)
secret	Mon Mar 23 13:40:17 2015

- 18) After consulting SOFTWARE hive [3] it's possible to find the default email application.

```
[Sun Mar 22 15:19:29 2015 (UTC)] Mail
VALUE: (default) -> Microsoft Outlook
SUBKEY: [Sun Mar 22 15:03:50 2015 (UTC)] Microsoft Outlook
SUBKEY: [Tue Jul 14 04:55:00 2009 (UTC)] Windows Mail
```

Figure 4 - Default Email Application

- 19) After consulting the manual of Microsoft Outlook (<https://goo.gl/ExXiaT>), it's possible to find that it stores the email file at: *drive:\Users\user\AppData\Local\Microsoft\Outlook*. And after going to that directory in the disk it was possible to find the following email file:

**C:\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost**

- 20) The email used by the suspect, as you can confirm by looking at the answer of question 19, is:

**[iaman.informant@nist.gov](mailto:iaman.informant@nist.gov)**

- 21) After using a specialized tool [7] to open the file referred to in the answer to question 19, it is possible to obtain the following information:

Timestamp (EST)	Source	Mail	
2015-03-23 12:29	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Hello, Iaman
		Body	How are you doing?
		Attachment	No
	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Hello, Iaman
		Body	Successfully secured. ----- From: spy Sent: Monday, March 23, 2015 1:29 PM To: iaman Subject: Hello, Iaman
		Attachment	No
2015-03-23 14:15	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Good job, buddy.
		Body	Good, job. I need a more detailed data about this business.
		Attachment	No

2015-03-23 14:20	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	RE: Good job, buddy.
		Body	Okay, I got it. I'll be in touch.  -----  From: iaman Sent: Monday, March 23, 2015 3:19 PM To: spy Subject: RE: Good job, buddy.  This is a sample.  -----  From: spy Sent: Monday, March 23, 2015 3:15 PM To: iaman Subject: Good job, buddy.  Good, job.  I need a more detailed data about this business.
		Attachment	Yes
2015-03-23 14:26	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Important request
		Body	I confirmed it. But, I need a more data. Do your best.
	Attachment	No	
2015-03-23 14:27	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Important request

		Body	Umm..... I need time to think.  ----- From: spy Sent: Monday, March 23, 2015 3:26 PM To: iaman Subject: Important request  I confirmed it.  But, I need a more data.  Do your best.
		Attachment	No
2015-03-23 15:38	Deleted Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	It's me
		Body	Use links below, <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing</a>  <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing</a>
		Attachment	No
2015-03-23 15:41	Deleted Items	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	RE: It's me
		Body	I got it.  -----  From: iaman Sent: Monday, March 23, 2015 4:39 PM To: spy Subject: It's me  Use links below, <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing</a>  <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing</a>
		Attachment	No

2015-03-24 09:25	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Last request
		Body	This is the last request. I want to get the remaining data.
		Attachment	No
2015-03-24 09:35	Deleted Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Last request
		Body	This is the last time.. -----  From: spy Sent: Tuesday, March 24, 2015 9:34 AM To: iaman Subject: RE: Last request No problem. U can directly deliver storage devices that stored it. -----  From: iaman Sent: Tuesday, March 24, 2015 9:30 AM To: spy Subject: RE: Last request Stop it!  It is very hard to transfer all data over the internet! -----  From: spy Sent: Tuesday, March 24, 2015 9:26 AM To: iaman Subject: Last request  This is the last request. I want to get the remaining data.
		Attachment	No



2015-03-24 14:34	Deleted Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Watch out!
		Body	I am trying.  -----  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.
		Attachment	No
2015-03-24 16:05	Deleted Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	Done
		Body	It's done. See you tomorrow.
		Attachment	No

- 22) The list of the attached devices can be easily obtained by seeing the tab “Devices attached”, by using a specialized forensics tool [2].

Device Maker	Device Model	Device ID	Volume Name
SanDisk Corp.	Cruzer Fit	4C530012550531106501	IAMAN \$_@
SanDisk Corp.	Cruzer Fit	4C530012450531101593	

- 23) Using a specialized forensics tool [8], to open with the \$UsnJrnl:\$J (Journal of the file system), and the \$MFT file, plus the information from the Windows.edb it's possible to see the following information:

Timestamp (EST)	Change	Name (\Users\informant\Desktop)
2015-03-23 13:41:40	From	\S data\[secret_project]_detailed_proposal.docx
	To	\S data\landscape.png
2015-03-23 13:41:55	From	\S data\[secret_project]_design_concept.ppt
	To	\S data\space_and_earth.mp4
2015-03-23	From	\S data\[secret_project]_pricing_decision.xlsx

15:30:44	<b>To</b>	\\S data\\happy_holiday.jpg
2015-03-23 15:31:02	<b>From</b>	\\S data\\[secret_project]_final_meeting.pptx
	<b>To</b>	\\S data\\do_u_wanna_build_a_snow_man.mp3
2015-03-24 08:49:51	<b>From</b>	\\S data\\Secret Project Data\\design\\[secret_project]_detailed_design.pptx
	<b>To</b>	\\S data\\Secret Project Data\\design\\winter_whether_advisory.zip
2015-03-24 08:50:08	<b>From</b>	\\S data\\Secret Project Data\\design\\[secret_project]_revised_points.ppt
	<b>To</b>	\\S data\\Secret Project Data\\design\\winter_storm.amr
2015-03-24 08:50:49	<b>From</b>	\\S data\\Secret Project Data\\design\\[secret_project]_design_concept.ppt
	<b>To</b>	\\S data\\Secret Project Data\\design\\space_and_earth.mp4
2015-03-24 08:52:35	<b>From</b>	\\S data\\Secret Project Data\\final\\[secret_project]_final_meeting.pptx
	<b>To</b>	\\S data\\Secret Project Data\\final\\do_u_wanna_build_a_snow_man.mp3
2015-03-24 08:52:56	<b>From</b>	\\S data\\Secret Project Data\\pricing decision\\(secret_project)_market_analysis.xlsx
	<b>To</b>	\\S data\\Secret Project Data\\pricing decision\\new_years_day.jpg
2015-03-24 08:53:08	<b>From</b>	\\S data\\Secret Project Data\\pricing decision\\(secret_project)_market_shares.xls
	<b>To</b>	\\S data\\Secret Project Data\\pricing decision\\super_bowl.avi
2015-03-24 08:53:38	<b>From</b>	\\S data\\Secret Project Data\\pricing decision\\(secret_project)_price_analysis_#1.xlsx
	<b>To</b>	\\S data\\Secret Project Data\\pricing decision\\my_favorite_movies.7z
2015-03-24 08:53:52	<b>From</b>	\\S data\\Secret Project Data\\pricing decision\\(secret_project)_price_analysis_#2.xls
	<b>To</b>	\\S data\\Secret Project Data\\pricing decision\\my_favorite_cars.db
2015-03-24 08:54:05	<b>From</b>	\\S data\\Secret Project Data\\pricing decision\\(secret_project)_pricing_decision.xlsx
	<b>To</b>	\\S data\\Secret Project Data\\pricing decision\\happy_holiday.jpg
2015-03-24 08:54:23	<b>From</b>	\\S data\\Secret Project Data\\progress\\[secret_project]_progress_#1.docx
	<b>To</b>	\\S data\\Secret Project Data\\progress\\my_smartphone.png
2015-03-24 08:54:43	<b>From</b>	\\S data\\Secret Project Data\\progress\\[secret_project]_progress_#2.docx
	<b>To</b>	\\S data\\Secret Project Data\\progress\\new_year_calendar.one
2015-03-24 08:54:52	<b>From</b>	\\S data\\Secret Project Data\\progress\\[secret_project]_progress_#3.doc
	<b>To</b>	\\S data\\Secret Project Data\\progress\\my_friends.svg
2015-03-24 08:55:08	<b>From</b>	\\S data\\Secret Project Data\\proposal\\[secret_project]_detailed_proposal.docx
	<b>To</b>	\\S data\\Secret Project Data\\proposal\\a_gift_from_you.gif
2015-03-24 08:55:17	<b>From</b>	\\S data\\Secret Project Data\\proposal\\[secret_project]_proposal.docx
	<b>To</b>	\\S data\\Secret Project Data\\proposal\\landscape.png
2015-03-24 08:55:32	<b>From</b>	\\S data\\Secret Project Data\\technical review\\[secret_project]_technical_review_#1.docx
	<b>To</b>	\\S data\\Secret Project Data\\technical review\\diary_#1d.txt
2015-03-24	<b>From</b>	\\S data\\Secret Project Data\\technical review\\[secret_project]_technical_review_#1.pptx

08:55:42	<b>To</b>	\S data\Secret Project Data\technical review\diary_#1p.txt
2015-03-24 08:55:53	<b>From</b>	\S data\Secret Project Data\technical review\[secret_project]_technical_review_#2.docx
	<b>To</b>	\S data\Secret Project Data\technical review\diary_#2d.txt
2015-03-24 08:56:09	<b>From</b>	\S data\Secret Project Data\technical review\[secret_project]_technical_review_#2.ppt
	<b>To</b>	\S data\Secret Project Data\technical review\diary_#2p.txt
2015-03-24 08:56:14	<b>From</b>	\S data\Secret Project Data\technical review\[secret_project]_technical_review_#3.doc
	<b>To</b>	\S data\Secret Project Data\technical review\diary_#3d.txt
2015-03-24 08:56:20	<b>From</b>	\S data\Secret Project Data\technical review\[secret_project]_technical_review_#3.ppt
	<b>To</b>	\S data\Secret Project Data\technical review\diary_#3p.txt

24) After consulting the NTUSER hive, with a specialized tool [3], it's easy to find the information bellow:

```
Map Network Drive MRU
Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
LastWrite Time Mon Mar 23 20:26:04 2015 (UTC)
MRUList = a
a \\10.11.11.128\secured_drive
```

Figure 5 - Network Device

25) With the information in the question 24, and using a specialized tool [9] to analyze the shell bag information from the UsrClass.DAT of the **informant** user is possible to see the following folders:

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Miscellaneous
▼ a:c	No i...	a:c	=	=	=	=	=	=	a:c
▶ technical review	📁	Directory	4	2015-03-24 10:00:14	2015-03-24 09:56:22	2015-03-24 00:00:00	2015-03-24 10:01:11		FAT file system
proposal	📁	Directory	3	2015-03-24 09:59:46	2015-03-24 09:55:18	2015-03-24 00:00:00	2015-03-24 10:01:14		FAT file system
progress	📁	Directory	0	2015-03-24 09:59:44	2015-03-24 09:54:54	2015-03-24 00:00:00	2015-03-24 10:01:15	2015-03-24 16:54:07	FAT file system
pricing decision	📁	Directory	2	2015-03-24 09:59:40	2015-03-24 09:57:32	2015-03-24 00:00:00	2015-03-24 10:01:17		FAT file system
design	📁	Directory	1	2015-03-24 09:59:28	2015-03-24 09:57:14	2015-03-24 00:00:00			FAT file system

Figure 6 - Directories traversed in 'RM#2'

26) Using again the same tool [9] used in question 25, it's possible to see that the files opened are the following:

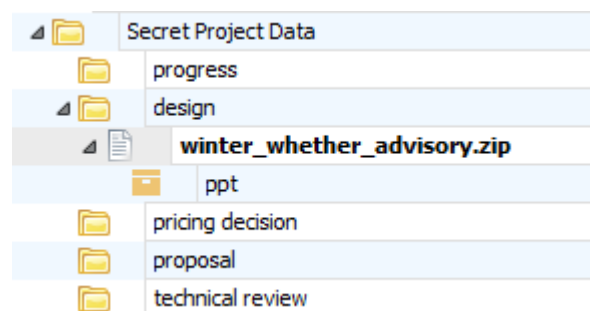


Figure 7 - Files opened in 'RM#2'

27) The directories traversed in the company's network drive are the following [9]:

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Miscellaneous
▼ c:	No i...	c:	=	=	=	=	=	=	c:
▶ Secret Project Data		Directory	2	2015-03-22 10:52:22	2015-03-22 10:52:24	2015-03-22 10:52:24			NTFS file system
Past Projects		Directory	0	2015-03-22 10:52:22	2015-02-05 13:06:32	2015-03-22 10:52:22	2015-03-23 16:24:08	2015-03-24 09:47:54	NTFS file system
Common Data		Directory	1	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-23 16:24:01		NTFS file system

Figure 9 - Directories traversed in the company's network drive (part1)

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Miscellaneous
▼ c:	No i...	c:	=	=	=	=	=	=	c:
▶ technical review		Directory	4	2015-03-22 10:52:24	2015-03-22 10:52:24	2015-03-22 10:52:24	2015-03-23 16:24:18		NTFS file system
progress		Directory	2	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-23 16:24:27		NTFS file system
proposal		Directory	3	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-23 16:24:20		NTFS file system
final		Directory	1	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-23 16:24:16		NTFS file system
pricing decision		Directory	0	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-23 16:24:15	2015-03-23 16:28:17	NTFS file system
design		Directory	5	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-22 10:52:22	2015-03-23 16:24:12		NTFS file system

Figure 8 - Directories traversed in the company's network drive (part2)

28) Using a specialized tool [5], we went to the directory where the JumpList is stored, and we found files that had the IP of the network in their path.

**Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations**

Timestamp (EST)	File	Source
15:26 - 2015-03-23	"\10.11.11.128\SECURED_DRIVE Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx"	JumpList
15:26 - 2015-03-23	"\10.11.11.128\SECURED_DRIVE Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx"	.LNK (Windows)

29) As stated early, the user downloaded Google Drive and iCloud, which suggests that he used cloud services.

Cloud Service	Downloaded Installer
Google Drive	\User\informant\Downloads\googledrivesync.exe
iCloud	\User\informant\Downloads\icloudsetup.exe

However, only traces of usage of the Google Drive were found, like the following:

Type of Evidence	Trace of Usage
Directory	\User\informant\AppData\Google\Drive\user_default\
Directory	\Program Files (x86)\Google\Drive\
Registry	\informant\Software\Google\Drive

- 30) After extracting the log file of the Google Drive - **sync\_log.log** - from the directory **\User\informant\AppData\Google\Drive\user\_default** and searching for “**Action.Delete**”, it’s possible to see that the following files have been deleted:

Delete Time (EST)	File Name	Modified Time (EST)
15:42:17 - 2015-03-23	happy_holiday.jpg	11:49:20 - 2015-01-30
15:42:17 - 2015-03-23	do_u_wanna_build_a_snow_man.mp3	15:35:14 - 2015-01-29

- 31) Again, after consulting the **sync\_log.log** it’s possible to know the account information of Google Drive.

```
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads common.service.user:64 Initializing User instance with new credentials. iaman.informant.personal@gmail.com
```

*Figure 10 - Credentials of Google Drive*

- 32) Windows default CD/DVD burning feature was used. No traces of other software installed on the computer that allows the recording of CD/DVD were found.

- 33) After analyzing the System Log, using a specialized tool [5], it’s possible to obtain the following information. Note that the times in the screenshot are in GMT (+ 5 over the EST).

Type	Date	Time	Source <sup>a)</sup>	Category	Event ID	User	Computer
Information	03/24/2015	07:47:47 PM	cdrom		133		informant-PC
Information	03/24/2015	08:41:21 PM	cdrom		133		informant-PC
Information	03/24/2015	08:24:46 PM	cdrom		133		informant-PC
Information	03/24/2015	07:56:11 PM	cdrom		133		informant-PC

*Figure 11 - Information Related to the CD in the System Log*

- 34) After consulting the logs of the NTFS file system [8] it’s possible to check the files that the suspect recorded on the CD.

File Name
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\de\winter_storm.amr
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\de\winter_whether_advisory.zip
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd\my_favorite_cars.db
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd\my_favorite_movies.7z
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd\new_years_day.jpg
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd\super_bowl.avi
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog\my_friends.svg
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog\my_smartphone.png
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog\new_year_calendar.one
\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop\a_gift_from_you.gif

\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\prop\\landscape.png
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\tr\\diary_#1d.txt
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\tr\\diary_#1p.txt
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\tr\\diary_#2d.txt
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\tr\\diary_#2p.txt
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\tr\\diary_#3d.txt
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\tr\\diary_#3p.txt
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\Penguins.jpg
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\Koala.jpg
\\Users\\informant\\AppData\\Local\\Microsoft\\Windows\\Burn\\Burn\\Tulips.jpg

35) It is possible to verify that the suspect has opened the following files (using the Jump List and the .LNK):

Timestamp (EST)	File Name
15:44:13 - 2015-03-24	D:\\de\\winter_whether_advisory.zip\\
15:44:14 - 2015-03-24	D:\\de\\winter_whether_advisory.zip\\ppt\\
15:44:16 - 2015-03-24	D:\\de\\winter_whether_advisory.zip\\ppt\\slides\\
15:44:18 - 2015-03-24	D:\\de\\winter_whether_advisory.zip\\ppt\\slideMasters\\
15:44:18 - 2015-03-24	D:\\de\\winter_whether_advisory.zip
16:01:10 - 2015-03-24	D:\\Penguins.jpg
16:01:12 - 2015-03-24	D:\\Koala.jpg
16:01:14 - 2015-03-24	D:\\Tulips.jpg

36) Using a tool to explore [2] the suspect's hard disk's, at the Desktop you can check the following. Note that the times in the screenshot are in GMT (+ 5 over the EST).

Name	Modified Time	Change Time	Access Time	Created Time
Resignation_Letter_(Iaman_Informant).xps	2015-03-25 15:28:34 GMT	2015-03-25 15:28:47 GMT	2015-03-25 15:28:33 GMT	2015-03-25 15:28:33 GMT
Resignation_Letter_(Iaman_Informant).docx	2015-03-24 18:59:30 GMT	2015-03-24 18:59:30 GMT	2015-03-24 18:59:30 GMT	2015-03-24 18:48:40 GMT

Figure 12 - Resignation Letter

37) There are no physical printers attached to the computer. However, next to the DOCX file it is possible to find an XPS file. This suggests that it was printed using Microsoft XPS Document Writer. Note that the times in the screenshot are in GMT (+ 5 over the EST).

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Resignation_Letter_(Iaman_Informant).xps	2015-03-25 15:28:34 GMT	2015-03-25 15:28:47 GMT	2015-03-25 15:28:33 GMT	2015-03-25 15:28:33 GMT	178139	Allocated
Resignation_Letter_(Iaman_Informant).docx	2015-03-24 18:59:30 GMT	2015-03-24 18:59:30 GMT	2015-03-24 18:59:30 GMT	2015-03-24 18:48:40 GMT	11893	Allocated

Figure 13 - DOCX file printed to XPS file

38) The Thumbcache files are located at:

C:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_32.db  
C:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_96.db  
C:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_256.db  
C:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_1024.db  
C:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_idx.db  
C:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_sr.db

39) Using a specialized tool [10] to open the **thumbcache\_256.db** file previously extracted, it was possible to view the following Thumbnails that contained a tag saying, "Secret Project":



40) The sticky notes file is stored in the following location:

C:\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt

41) The content of the Sticky Notes file is the following (after extract the file, and change the extension to rtf).

Tomorrow...

Everything will be OK...



- 42) After consulting the **SOFTWARE\Microsoft\Windows Search** registry file, it is possible to check that Windows Search and Indexing is active. The Windows Search index database is located at:

**C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb**

- 43) "By default, Windows 10/8 will index your documents for faster searches. As a result, all the data relating to the indexes is stored in this **Windows.edb** file. In Windows Vista, Windows 7 and Windows 8/10, in some cases this **Windows.edb** file tends to become huge or large in size. While a size of a couple of GB's can be considered normal, there have been reports of the size growing to even 100's of GBs!".

- 44) Using the **Windows.edb**, with a proper tool [1] it's possible to see the following web's history of the suspect:

Timestamp (EST)	Webpage (From System_ItemPathDisplay)
10:09:22 - 2015-03-22	<a href="http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome">http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome</a>
10:09:23 - 2015-03-22	<a href="http://www.msn.com/?ocid=iehp">http://www.msn.com/?ocid=iehp</a>
10:09:40 - 2015-03-22	<a href="https://www.google.com/?gws_rd=ssl">https://www.google.com/?gws_rd=ssl</a>
10:09:50 - 2015-03-22	<a href="https://www.google.com/search?hl=en&amp;source=hp&amp;q=internet+explorer+11&amp;gbv=2&amp;oq=internet+explorer+11&amp;gs_l=heirloomhp.3..0l10.5163.7893.0.9562.20.13.0.7.7.0.156.1110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv5w">https://www.google.com/search?hl=en&amp;source=hp&amp;q=internet+explorer+11&amp;gbv=2&amp;oq=internet+explorer+11&amp;gs_l=heirloomhp.3..0l10.5163.7893.0.9562.20.13.0.7.7.0.156.1110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv5w</a>
10:09:52 - 2015-03-22	<a href="http://www.google.com/url?url=http://windows.microsoft.com/en-us/internetexplorer/downloadie&amp;rct=j&amp;frm=1&amp;q=&amp;esrc=s&amp;sa=U&amp;ei=6ykQVZWLGbeJsQT7goDACg&amp;ved=0CB8QFjAA&amp;usg=AFQjCNEwslz17kY-jTXbaWPcQDfBbVEi7A">http://www.google.com/url?url=http://windows.microsoft.com/en-us/internetexplorer/downloadie&amp;rct=j&amp;frm=1&amp;q=&amp;esrc=s&amp;sa=U&amp;ei=6ykQVZWLGbeJsQT7goDACg&amp;ved=0CB8QFjAA&amp;usg=AFQjCNEwslz17kY-jTXbaWPcQDfBbVEi7A</a>
10:09:54 - 2015-03-22	<a href="http://windows.microsoft.com/en-us/internet-explorer/download-ie">http://windows.microsoft.com/en-us/internet-explorer/download-ie</a>
10:09:56 - 2015-03-22	<a href="http://www.google.com/url?url=http://windows.microsoft.com/en-us/internetexplorer/ie-11-worldwidelanguages&amp;rct=j&amp;frm=1&amp;q=&amp;esrc=s&amp;sa=U&amp;ei=6ykQVZWLGbeJsQT7goDACg&amp;ved=0CCoQFjAB&amp;usg=AFQjCNE7UKIWEBiWO2N96IFeo6ZywhRLfw">http://www.google.com/url?url=http://windows.microsoft.com/en-us/internetexplorer/ie-11-worldwidelanguages&amp;rct=j&amp;frm=1&amp;q=&amp;esrc=s&amp;sa=U&amp;ei=6ykQVZWLGbeJsQT7goDACg&amp;ved=0CCoQFjAB&amp;usg=AFQjCNE7UKIWEBiWO2N96IFeo6ZywhRLfw</a>
10:10:24 - 2015-03-22	<a href="http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwidelanguages">http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwidelanguages</a>
10:10:54 - 2015-03-22	<a href="https://www.google.com/webhp?hl=en">https://www.google.com/webhp?hl=en</a>
10:10:58 - 2015-03-22	<a href="https://www.google.com/chrome/index.html?hl=en&amp;brand=CHNG&amp;utm_source=en-hpp&amp;utm_medium=hpp&amp;utm_campaign=en">https://www.google.com/chrome/index.html?hl=en&amp;brand=CHNG&amp;utm_source=en-hpp&amp;utm_medium=hpp&amp;utm_campaign=en</a>
10:11:06 - 2015-03-22	<a href="http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe">http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe</a>
10:11:16 - 2015-03-22	<a href="https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&amp;platform=win&amp;clickonceinstalled=1">https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&amp;platform=win&amp;clickonceinstalled=1</a>
12:26:33 - 2015-03-23	<a href="https://odc.officeapps.live.com/odc/emailhrd?lcid=1033&amp;syslcid=1033&amp;uilcid=1033&amp;app=5&amp;ver=15&amp;build=15.0.4420&amp;p=0&amp;a=1&amp;hm=1&amp;sp=0">https://odc.officeapps.live.com/odc/emailhrd?lcid=1033&amp;syslcid=1033&amp;uilcid=1033&amp;app=5&amp;ver=15&amp;build=15.0.4420&amp;p=0&amp;a=1&amp;hm=1&amp;sp=0</a>
12:27:49 - 2015-03-23	<a href="http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie">http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie</a>
12:27:49 - 2015-03-23	<a href="http://www.bing.com/search">http://www.bing.com/search</a>
12:27:49 - 2015-03-23	<a href="http://go.microsoft.com/fwlink/?LinkId=69157">http://go.microsoft.com/fwlink/?LinkId=69157</a>



12:28:19 - 2015-03-23	<a href="http://www.bing.com/">http://www.bing.com/</a>
13:07:52 - 2015-03-23	<a href="http://www.bing.com/news/search?q=Top+Stories&amp;FORM=NSBABR">http://www.bing.com/news/search?q=Top Stories&amp;FORM=NSBABR</a>
13:07:55 - 2015-03-23	<a href="http://www.bing.com/search?q=Top+Stories&amp;FORM=HDRSC1">http://www.bing.com/search?q=Top+Stories&amp;FORM=HDRSC1</a>
13:07:58 - 2015-03-23	<a href="http://www.bing.com/news/search?q=file+sharing+and+tethering&amp;FORM=HDRSC6">http://www.bing.com/news/search?q=file+sharing+and+tethering&amp;FORM=HDRSC6</a>
13:08:00 - 2015-03-23	<a href="http://www.bing.com/search?q=file+sharing+and+tethering&amp;qs=n&amp;form=QBLH&amp;pq=file+sharing+and+tethering&amp;sc=0-18&amp;sp=-1&amp;sk=&amp;cvid=171b77e4ffd54b2a92c4e97abf995fe1">http://www.bing.com/search?q=file+sharing+and+tethering&amp;qs=n&amp;form=QBLH&amp;pq=file+sharing+and+tethering&amp;sc=0-18&amp;sp=-1&amp;sk=&amp;cvid=171b77e4ffd54b2a92c4e97abf995fe1</a>
13:08:18 - 2015-03-23	<a href="http://sysinfotools.com/blog/tethering-internet-files-sharing/">http://sysinfotools.com/blog/tethering-internet-files-sharing/</a>
13:11:13 - 2015-03-23	<a href="http://resources.infosecinstitute.com/windows-systems-and-artifacts-indigital-forensics-part-i-registry/">http://resources.infosecinstitute.com/windows-systems-and-artifacts-indigital-forensics-part-i-registry/</a>
13:12:08 - 2015-03-23	<a href="https://technet.microsoft.com/en-us/library/cc162846.aspx">https://technet.microsoft.com/en-us/library/cc162846.aspx</a>
13:12:45 - 2015-03-23	<a href="https://support.microsoft.com/en-us/kb/308427">https://support.microsoft.com/en-us/kb/308427</a>
13:12:52 - 2015-03-23	<a href="http://en.wikipedia.org/wiki/Event_Viewers">http://en.wikipedia.org/wiki/Event_Viewers</a>
13:13:58 - 2015-03-23	<a href="https://msdn.microsoft.com/enus/library/windows/desktop/dd562212(v=vs.85).aspx">https://msdn.microsoft.com/enus/library/windows/desktop/dd562212(v=vs.85).aspx</a>
13:14:25 - 2015-03-23	<a href="http://www.forensicswiki.org/wiki/USB_History_Viewing">http://www.forensicswiki.org/wiki/USB_History_Viewing</a>
15:43:48 - 2015-03-23	<a href="http://www.bing.com/search?q=external%20device%20and%20forensics&amp;qs=n&amp;form=QBRE&amp;pq=external%20device%20and%20forensics&amp;sc=8-9&amp;sp=-1&amp;sk=&amp;cvid=c30c4b1f36114b1c9bc683838c69823a">http://www.bing.com/search?q=external%20device%20and%20forensics&amp;qs=n&amp;form=QBRE&amp;pq=external%20device%20and%20forensics&amp;sc=8-9&amp;sp=-1&amp;sk=&amp;cvid=c30c4b1f36114b1c9bc683838c69823a</a>
15:43:50 - 2015-03-23	<a href="http://www.bing.com/?FORM=Z9FD1">http://www.bing.com/?FORM=Z9FD1</a>
15:43:52 - 2015-03-23	<a href="http://www.bing.com/news?FORM=Z9LH3">http://www.bing.com/news?FORM=Z9LH3</a>
15:44:58 - 2015-03-23	<a href="http://www.bing.com/news?q=science+technology+news&amp;FORM=NWBTCB">http://www.bing.com/news?q=science+technology+news&amp;FORM=NWBTCB</a>
15:45:22 - 2015-03-23	<a href="http://www.wired.com/?p=1756538">http://www.wired.com/?p=1756538</a>
15:45:30 - 2015-03-23	<a href="http://www.bing.com/news?q=Soccer+News&amp;FORM=NSBABR">http://www.bing.com/news?q=Soccer+News&amp;FORM=NSBABR</a>
15:53:47 - 2015-03-23	<a href="http://www.bing.com/news?q=top+stories&amp;FORM=NWRFSH">http://www.bing.com/news?q=top+stories&amp;FORM=NWRFSH</a>
15:55:09 - 2015-03-23	<a href="http://www.bing.com/news?q=us+news&amp;FORM=NSBABR">http://www.bing.com/news?q=us+news&amp;FORM=NSBABR</a>
15:55:10 - 2015-03-23	<a href="http://www.bing.com/news?q=world+news&amp;FORM=NSBABR">http://www.bing.com/news?q=world+news&amp;FORM=NSBABR</a>
15:55:17 - 2015-03-23	<a href="http://www.bing.com/news?q=local&amp;FORM=NSBABR">http://www.bing.com/news?q=local&amp;FORM=NSBABR</a>
15:55:18 - 2015-03-23	<a href="http://www.bing.com/news?q=entertainment+news&amp;FORM=NSBABR">http://www.bing.com/news?q=entertainment+news&amp;FORM=NSBABR</a>
15:55:29 - 2015-03-23	<a href="http://www.bing.com/news?q=science+technology+news&amp;FORM=NSBABR">http://www.bing.com/news?q=science+technology+news&amp;FORM=NSBABR</a>
15:55:55 - 2015-03-23	<a href="http://www.bing.com/news?q=business+news&amp;FORM=NSBABR">http://www.bing.com/news?q=business+news&amp;FORM=NSBABR</a>
15:55:56 - 2015-03-23	<a href="http://www.bing.com/news?q=political+news&amp;FORM=NSBABR">http://www.bing.com/news?q=political+news&amp;FORM=NSBABR</a>
15:55:57 - 2015-03-23	<a href="http://www.bing.com/news?q=sports+news&amp;FORM=NSBABR">http://www.bing.com/news?q=sports+news&amp;FORM=NSBABR</a>
15:55:59 - 2015-03-23	<a href="http://www.bing.com/news?q=health+news&amp;FORM=NSBABR">http://www.bing.com/news?q=health+news&amp;FORM=NSBABR</a>
15:56:09 - 2015-03-23	<a href="http://www.bing.com/news?q=top+stories&amp;FORM=NSBABR">http://www.bing.com/news?q=top+stories&amp;FORM=NSBABR</a>
15:56:33 - 2015-03-23	<a href="http://www.wired.com/2015/03/stealing-data-computers-using-heat/">http://www.wired.com/2015/03/stealing-data-computers-using-heat/</a>

- 45) In addition to the mails found in the question 21, some emails are only recorded on the Windows Search database (**Windows.edb**). So, the full timeline of emails changed is the following (the emails that only appear in the Windows Search there have the blue timestamp [1]).

Timestamp (EST)	Source	Mail	
2015-03-23 12:29	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Hello, Iaman
		Body	How are you doing?
		Attachment	No
2015-03-23 13:44	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Hello, Iaman
		Body	Successfully secured. ----- From: spy Sent: Monday, March 23, 2015 1:29 PM To: Iaman Subject: Hello, Iaman
		Attachment	No
2015-03-23 14:15	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Good job, buddy.
		Body	Good, job. I need a more detailed data about this business.
		Attachment	No
2015-03-15 14:19	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Good job, buddy.

		Body	<p>This is a sample.</p> <p>-----</p> <p>From: spy</p> <p>Sent: Monday, March 23, 2015 3:15 PM</p> <p>To: iaman</p> <p>Subject: Good job, buddy.</p> <p>Good, job.</p> <p>I need a more detailed data about this business.</p>
		Attachment	space_and_earth.mp4
2015-03-23 14:20	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	RE: Good job, buddy.
		Body	<p>Okay, I got it.</p> <p>I'll be in touch.</p> <p>-----</p> <p>From: iaman</p> <p>Sent: Monday, March 23, 2015 3:19 PM</p> <p>To: spy</p> <p>Subject: RE: Good job, buddy.</p> <p>This is a sample.</p> <p>-----</p> <p>From: spy</p> <p>Sent: Monday, March 23, 2015 3:15 PM</p> <p>To: iaman</p> <p>Subject: Good job, buddy.</p> <p>Good, job.</p> <p>I need a more detailed data about this business.</p>
		Attachment	Yes
2015-03-23 14:26	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Important request

		Body	I confirmed it. But, I need a more data. Do your best.
		Attachment	No
2015-03-23 14:27	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Important request
		Body	Umm..... I need time to think. ----- From: spy Sent: Monday, March 23, 2015 3:26 PM To: iaman Subject: Important request I confirmed it. But, I need a more data. Do your best.
		Attachment	No
2015-03-23 15:38	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	It's me
		Body	Use links below, <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing</a> <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing</a>
		Attachment	No
2015-03-23 15:41	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	RE: It's me

		Body	I got it. ----- From: iaman Sent: Monday, March 23, 2015 4:39 PM To: spy Subject: It's me Use links below, <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing</a> <a href="https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing">https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0ImM1U/view?usp=sharing</a>
		Attachment	No
2015-03-24 08:25	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Last request
		Body	This is the last request. I want to get the remaining data.
		Attachment	No
2015-03-24 08:30	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Last request
		Body	Stop it! It is very hard to transfer all data over the internet! ----- From: spy Sent: Tuesday, March 24, 2015 9:26 AM To: iaman Subject: Last request This is the last request. I want to get the remaining data.
		Attachment	No
2015-03-24	Inbox	From	spy.conspirator@nist.gov

08:33		To	iaman.informant@nist.gov
		Subject	RE: Last request
		Body	<p>No problem.</p> <p>U can directly deliver storage devices that stored it.</p> <p>-----</p> <p>From: iaman</p> <p>Sent: Tuesday, March 24, 2015 9:30 AM</p> <p>To: spy</p> <p>Subject: RE: Last request</p> <p>Stop it!</p> <p>It is very hard to transfer all data over the internet!</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 9:26 AM</p> <p>To: iaman</p> <p>Subject: Last request</p> <p>This is the last request.</p> <p>I want to get the remaining data.</p>
		Attachment	No
2015-03-24 08:35	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Last request

		Body	<p>This is the last time..</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 9:34 AM</p> <p>To: iaman</p> <p>Subject: RE: Last request</p> <p>No problem.</p> <p>U can directly deliver storage devices that stored it.</p> <p>-----</p> <p>From: iaman</p> <p>Sent: Tuesday, March 24, 2015 9:30 AM</p> <p>To: spy</p> <p>Subject: RE: Last request</p> <p>Stop it!</p> <p>It is very hard to transfer all data over the internet!</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 9:26 AM</p> <p>To: iaman</p> <p>Subject: Last request</p> <p>This is the last request.</p> <p>I want to get the remaining data.</p>
		Attachment	No
2015-03-24 14:32	Inbox	From	spy.conspirator@nist.gov
		To	iaman.informant@nist.gov
		Subject	Watch out!
		Body	USB device may be easily detected. So, try another method.
		Attachment	No
2015-03-24 14:34	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	RE: Watch out!

		Body	<p>I am trying.</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 3:33 PM</p> <p>To: iaman</p> <p>Subject: Watch out!</p> <p>USB device may be easily detected.</p> <p>So, try another method.</p>
		Attachment	No
2015-03-24 16:05	Sent Items	From	iaman.informant@nist.gov
		To	spy.conspirator@nist.gov
		Subject	Done
		Body	It's done. See you tomorrow.
		Attachment	No

46) Continuing the inspection of the Windows Search database with the same tool as before [1], it's possible to see the following files related to the Desktop:

Timestamp (EST)	Filename (C:\Users\informant\Desktop\)
15:05:33 - 2015-03-23	Google Drive.lnk
08:40:09 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\design\space_and_earth.mp4
08:40:09 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\design\winter_whether_advisory.zip
08:40:10 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\design\winter_storm.amr
08:40:11 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx
08:47:13 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\proposal\[secret_project]_proposal.docx
08:47:58 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\design\[secret_project]_detailed_design.pptx
08:47:58 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\final\[secret_project]_final_meeting.pptx
08:47:58 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\pricing decision\[secret_project]_market_analysis.xlsx
08:47:58 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\pricing decision\[secret_project]_market_shares.xls
08:47:58 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\pricing decision\[secret_project]_price_analysis_#1.xlsx
08:47:59 - 2015-03-24	\S data\Secret Project Data\Secret Project Data\proposal
13:48:41 - 2015-03-24	Resignation_Letter_(Iaman_Informant).docx
14:52:06 - 2015-03-24	\temp
14:52:36 - 2015-03-24	\temp\IE11-Windows6.1-x64-en-us.exe
14:52:46 - 2015-03-24	\temp\Chrysanthemum.jpg



14:52:46 - 2015-03-24	\temp\Hydrangeas.jpg
14:52:46 - 2015-03-24	\temp\Desert.jpg
14:52:46 - 2015-03-24	\temp\Lighthouse.jpg
14:52:46 - 2015-03-24	\temp\Koala.jpg
14:52:46 - 2015-03-24	\temp\Jellyfish.jpg
14:52:46 - 2015-03-24	\temp\Tulips.jpg
14:52:46 - 2015-03-24	\temp\Penguins.jpg

47) After consulting the **ControlSet001\Control\BackupRestore\FilesNotToBackup** registry file and the value of the VSS Default Provider it's possible to know that exists a Volume Shadow Copy.

<b>Where</b>	\System Volume Information\{9b365826-d2ef-11e4-b734-000c29ff2429}\{3808876b-c176-4e48-b7ae-04046e6cc752}
<b>When</b>	09:57:24 - 2015-03-25

48) After analyzing the content of the Volume Shadow Copy [1], it's possible to find the following information about the Google Drive:

Creation Date (EST)	Modification Date (EST)	Path
15:02:51 - 2015-03-23	15:47:55 - 2015-03-23	\User\informant\AppData\Local\Google\Drive\user_default\snapshot.db
15:02:51 - 2015-03-23	15:47:55 - 2015-03-23	\User\informant\AppData\Local\Google\Drive\user_default\sync_config.db
15:02:51 - 2015-03-23	15:47:56 - 2015-03-23	\User\informant\AppData\Local\Google\Drive\user_default\sync_log.log

49) After analyzing the content of the Volume Shadow Copy and after using a hexadecimal editor to analyze the snapshot.db file, it's possible to collect the following information:

Information	Column	Size(bytes)	Data
File offset 0x702 RecordSize: 0x76 RowID: 0x03 HeaderSize: 0x0C	doc_id	28	0Bz0ye6gXtiZaVl8yVU5mWHlGbWc
	filename	31	do_u_wanna_build_a_snow_man.mp3
	modified	4	0x54CBB610
	created	4	0x5510786D
	acl_role	0	0
	doc_type	0	1
	removed	0	0
	size	3	0x686F86
	checksum	32	2c4553f99533d85adb104b3a5c38521a
	shared	0	1

	resource_type	4	file
File offset 0x77A First 4 bytes are overwritten RecordSize: N/A RowID: N/A HeaderSize: N/A	doc_id	28	0Bz0ye6gXtiZaakx6d3R3c0JmM1U
	filename	17	happy_holiday.jpg
	modified	4	0x54CA9982
	created	4	0x5510786A
	acl_role	0	0
	doc_type	0	1
	removed	0	0
	size	3	0x6B8C5
	checksum	32	0c77d6a2704155dbfdf29817769b7478
	shared	0	1
	resource_type	4	file

50) The Outlook OST files don't exist in the Volume Shadow Copy because that service is disabled, as you can confirm by checking the **\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** registry file.

51) After exploring the files at \$Recycle.Bin\S-1-5-21-2425377081-3129163575-2985601102-1000 folder [2] (SID of 'informant' account is 1000), it's possible to find the following deleted files.

Timestamp Deleted (EST)	Recycle Bin File Name	Original File Name
14:51:47 - 2015-03-24	\$I40295N	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop
14:51:47 - 2015-03-24	\$IXWGVWC	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog
14:51:47 - 2015-03-24	\$I55Z163	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd
14:51:47 - 2015-03-24	\$I9M7UMY	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr
15:11:42 - 2015-03-24	\$I508CBB.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg
15:11:42 - 2015-03-24	\$I8YP3XK.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg
15:11:42 - 2015-03-24	\$IDOI3HE.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg
15:11:42 - 2015-03-24	\$IFVCH5V.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg
15:11:42 - 2015-03-24	\$II3FM2A.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg
15:11:42 - 2015-03-24	\$IIQGWTT.ini	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini
15:11:42 - 2015-03-24	\$IJE6T4.exe	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\IE11-Windows6.1-x64-en-us.exe
15:11:42 - 2015-03-24	\$IKXD1U3.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg
15:11:42 - 2015-03-24	\$IU3FKWL.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg
15:11:42 - 2015-03-24	\$IX538VH.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg

52) The suspect, on 2015-03-25, performed the following anti-forensic activities:

Timestamp (EST)	Activity
09:46:44 - 2015-03-25	Search on the internet for: anti-forensic tools
09:47:34 - 2015-03-25	Downloaded: eraser
09:48:12 - 2015-03-25	Downloaded: ccleaner
09:50:14 - 2015-03-25	Installed: ERASER 6.2.0.2962.EXE
09:57:56 - 2015-03-25	Installed: CCSETUP504.EXE
10:13:30 - 2015-03-25	Run: ERASER.EXE
10:15:50 - 2015-03-25	Run: CCLEANER64.EXE
10:18:29 - 2015-03-25	Uninstalled : Ccleaner

53) Opening the image with an explorer tool [2] (without using any file carving tool) it is possible to find (although they were deleted) all the files that existed on the device. It was then possible to find the following files:

File Name	Format	Size (bytes)
design/winter_storm.arm	ppt	14547968
design/winter_wheter_advisory.zip	pptx	16381123
PRICIN~1/my_favorite_cars.db	xls	1260544
PRICIN~1/my_favorite_movies.7z	xlsx	100078
PRICIN~1/new_years_day.jpg	xlsx	10237535
PRICIN~1/super_bowl.avi	xls	10289152
progress/my_friends.svg	doc	58368
progress/my_smarthphone.png	docx	4440235
progress/new_year_calendar.one	docx	27414
proposal/a_gift_from_you.gif	docx	35226880
proposal/landscape.png	docx	6484502
TECHNI~1/diary_#1d.txt	docx	121441
TECHNI~1/ diary_#1p.txt	pptx	458267
TECHNI~1/ diary_#2d.txt	docx	658922
TECHNI~1/ diary_#2p.txt	ppt	1154560
TECHNI~1/ diary_#3d.txt	doc	2360832
TECHNI~1/ diary_#3p.txt	ppt	325120

- 54) As you can see from the answer to the previous question, all the metadata and the files themselves were still recoverable, so no special anti-forensic action was taken, only a simple formatting was performed.
- 55) As found in the answers to questions 25 and 26, in which only registry files on the image extracted from the suspect's computer were analyzed, it copied the files referred to in the reply to question 53, as a subsequent analysis of the same device revealed that there were still traces of them.
- 56) Unlike what happened with RM#2, it was not possible to mount the device in an explorer tool [2], so using a file carving tools [11][12] it was possible to find traces of the following files in the RM#3 device. Since the file's name can be induced from the title of the file, we didn't perform a metadata analysis.

File Name	Format	Size (bytes)
[secret_project]_revised_points.ppt	ppt	14547968
[secret_project]_detailed_design.pptx	pptx	16381123
[secret_project]_price_analysis_#1.xlsx	xlsx	100078
[secret_project]_price_analysis_#2.xls	xls	1260544
[secret_project]_market_analysis.xlsx	xlsx	10237535
[secret_project]_market_shares.xls	xls	10289152
[secret_project]_progress_#3.doc	doc	57344
[secret_project]_progress_#1.docx	docx	4440235
[secret_project]_progress_#2.docx	docx	27414
[secret_project]_technical_review_#3.doc	doc	2360832
[secret_project]_technical_review_#3.ppt	ppt	325120
[secret_project]_proposal.docx	docx	6484503
[secret_project]_detailed_proposal.docx	docx	35259649
[secret_project]_technical_review_#2.ppt	ppt	1156608
[secret_project]_technical_review_#2.docx	docx	658923
[secret_project]_technical_review_#1.docx	docx	121442
[secret_project]_technical_review_#1.pptx	pptx	458268

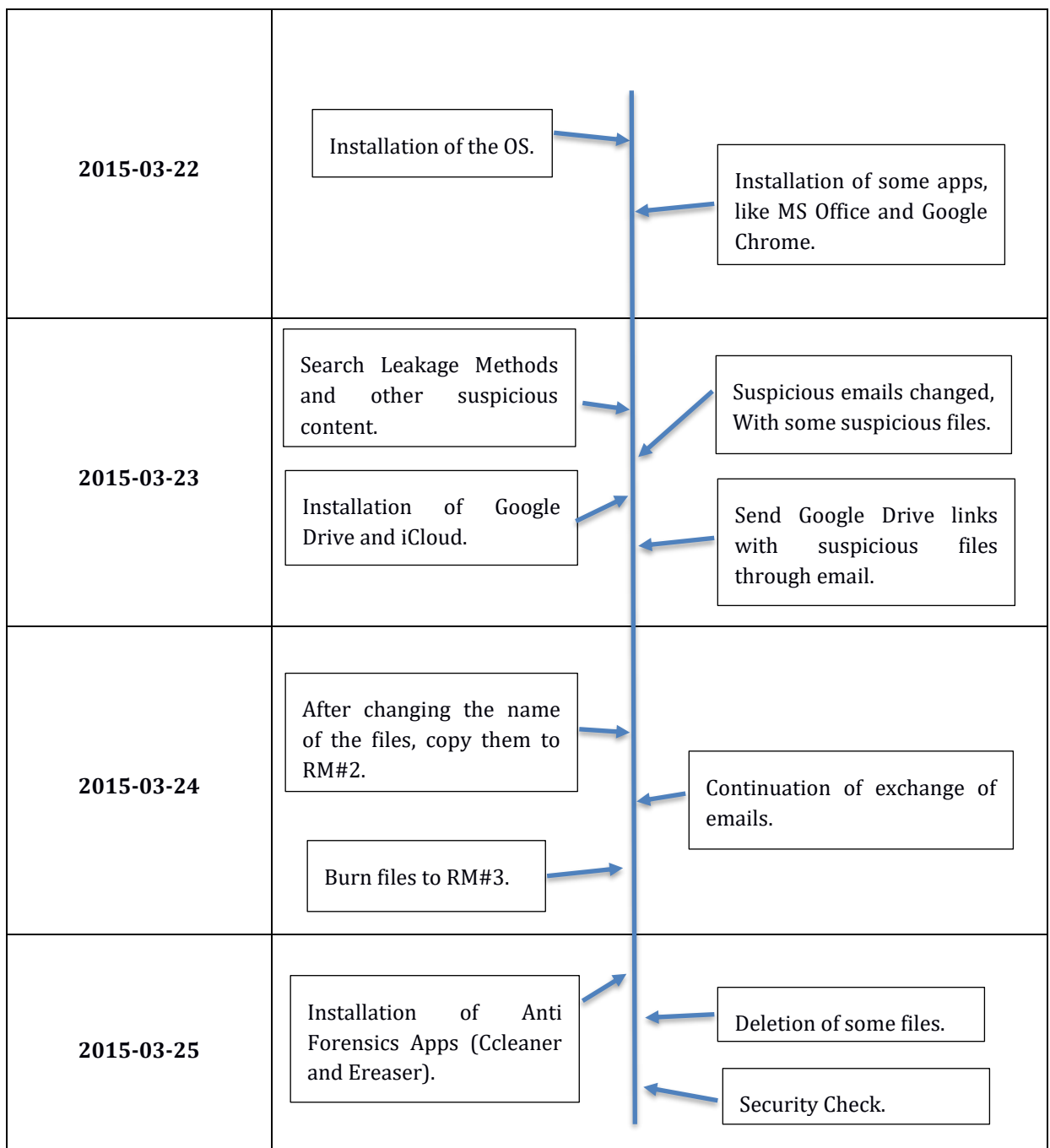
- 57) No special anti-forensic measures were taken, only the CD-R was recorded as if it were a USB stick, and then the confidential files copied to the pen were erased. However, as seen in the answer to the previous question, these files were still possible to recover.
- 58) It is possible to construct the following timeline for the activities of the suspect.

When?	What?
2015-03-22	Nothing suspicious happened. Only the Operating System was installed, and some applications for normal use.
2015-03-23	Exchange of emails with suspicious content. Some research on the internet also with suspicious content. Files sent by google drive.

2015-03-24	Continuation of exchange of suspicious emails. Recording of confidential information on external storage devices.
2015-03-25	Attempts (failed) to hide the vestiges of your activity, using tools like Ccleaner and Eraser.

59) The suspect tried to steal company information by using the internet and the physical devices to exchange files. The **space\_and\_earth.mp4** file and, as previously said, links to Google Drive containing the **happy\_holiday.jpg** and **do\_u\_wanna\_build\_a\_snow\_man.mp3** files were sent via email. In the physical devices, the files referred to in the answer to the question 53 and question 56 were found.

60) A summary of the events can be expressed in the following diagram:



## 5 Analysis Results

From the analysis of the files found on the artifacts that were delivered to us, we found some that are common in the directories that they were found in, but we also found some suspicious looking files. A more detailed analysis of this suspicious looking content, namely the google drive links, may be a starting point for future investigations. Overall, the content found looks to be used to leak data since the internet search history found in the computer contained searches such as “data leakage method” and “leaking confidential information”. The analysis of the removable media delivered to us also confirmed this claim.

## 6 Conclusions

In conclusion, we were able to find evidence connected to the data leakage of the company 000 in Mr. Iaman Informant's computer, by answering the 60 questions that were presented to us.

## 7 Appendix - Tools Used

- 1) OS Forensics – <https://www.osforensics.com/>
- 2) Autopsy – <http://www.sleuthkit.org/autopsy/>
- 3) Reg Ripper – <https://github.com/keydet89/RegRipper2.8>
- 4) MiTeC Windows Registry Recovery – <http://www.mitec.cz/wrr.html>
- 5) Pro Discover Basic – <https://www.arcgroupny.com/products/prodiscover-basic/~>
- 6) BrowsingHistoryView – [http://www.nirsoft.net/utils/browsing\\_history\\_view.html](http://www.nirsoft.net/utils/browsing_history_view.html)
- 7) OST Viewer Kernel – <https://www.nucleustechnologies.com/ost-viewer.html>
- 8) NTFS Log Tracker – <https://sites.google.com/site/forensicnote/ntfs-log-tracker>
- 9) ShellBags Explorer – <https://ericzimmerman.github.io/>
- 10) Thumbcache Viewer – <https://thumbcacheviewer.github.io/>
- 11) Foremost – <http://foremost.sourceforge.net/>
- 12) TestDisk & QPhotoRec – [http://www.cgsecurity.org/wiki/TestDisk\\_7.0\\_Release](http://www.cgsecurity.org/wiki/TestDisk_7.0_Release)

1st December 2017, Instituto Superior Técnico

Luís Aguiar - 80950

Jorge Pereira - 81428

Filipe Azevedo - 82468