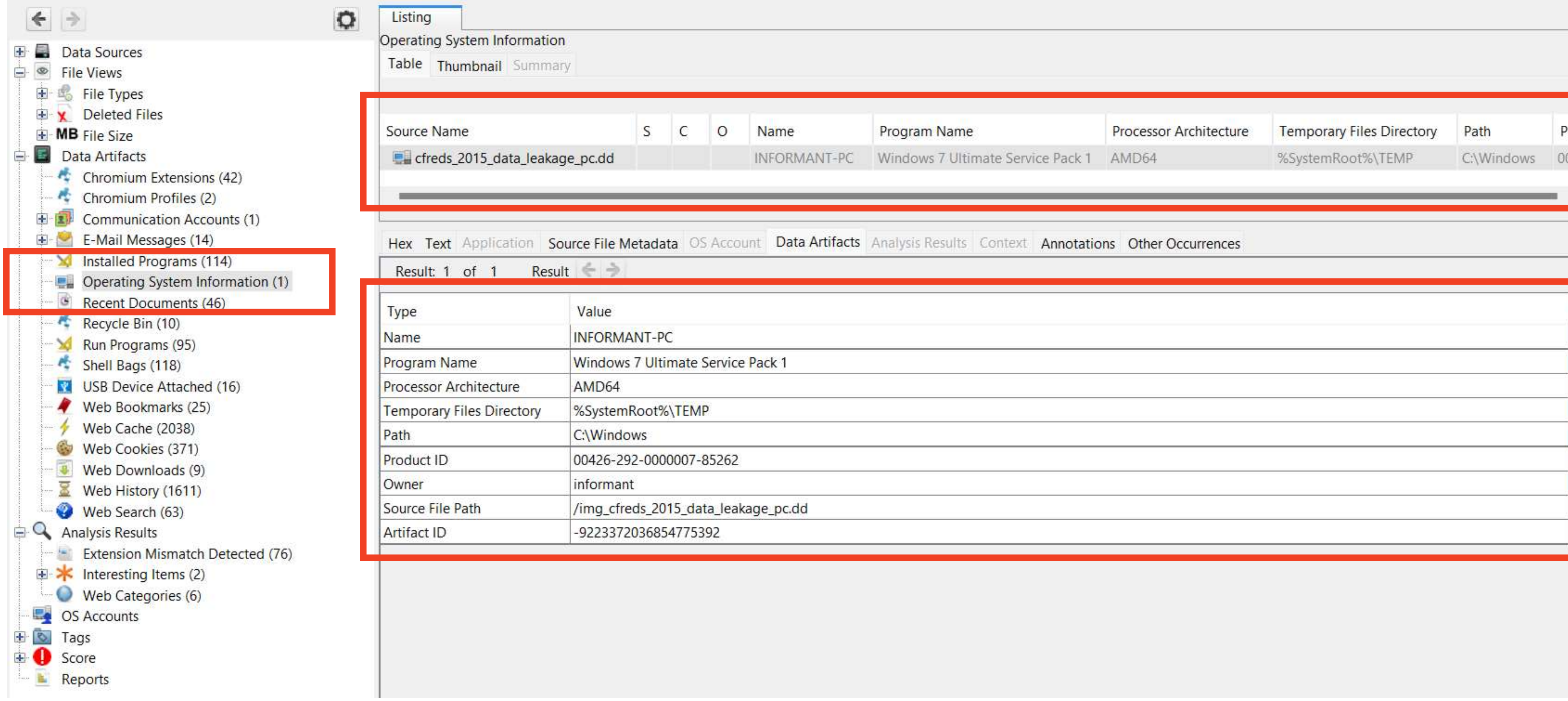
[Exercise] Answer these questions

1. Explain installed OS information in detail. (OS name, install date, registered c
2. List all user accounts in OS.
3. What applications were installed by the suspect after installing OS?
4. List application execution logs. (Executable path, execution time, execution c
5. List recent opened documents (File path, last accessed...)
6. Examine ‘Recycle Bin’ data in PC.
7. What websites were the suspect accessing? (Timestamp, URL...)
8. List all e-mails of the suspect. If possible, identify deleted e-mails.
9. List external storage devices attached to PC.
10. What actions were performed for anti-forensics on PC at the last day '2015-0

Autopsy User's Guide: http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/

1) System Information



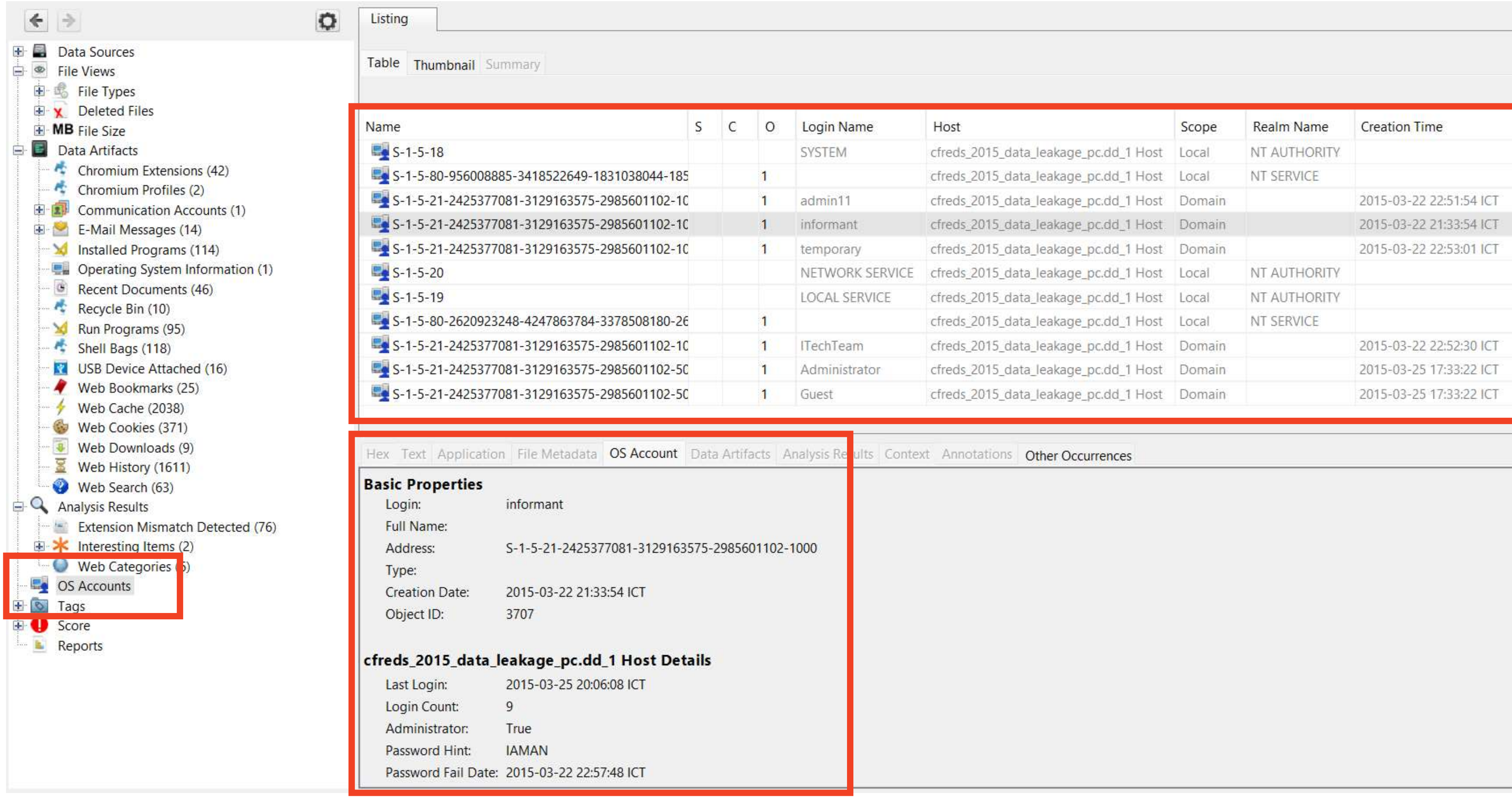
Operating System Information

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	P
cfreds_2015_data_leakage_pc.dd				INFORMANT-PC	Windows 7 Ultimate Service Pack 1	AMD64	%SystemRoot%\TEMP	C:\Windows	0(

Result: 1 of 1 Result

Type	Value
Name	INFORMANT-PC
Program Name	Windows 7 Ultimate Service Pack 1
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00426-292-0000007-85262
Owner	informant
Source File Path	/img_cfreds_2015_data_leakage_pc.dd
Artifact ID	-9223372036854775392

2) User accounts



Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	cfreds_2015_data_leakage_pc.dd_1 Host	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-185			1		cfreds_2015_data_leakage_pc.dd_1 Host	Local	NT SERVICE	
S-1-5-21-2425377081-3129163575-2985601102-10			1	admin11	cfreds_2015_data_leakage_pc.dd_1 Host	Domain		2015-03-22 22:51:54 ICT
S-1-5-21-2425377081-3129163575-2985601102-10			1	informant	cfreds_2015_data_leakage_pc.dd_1 Host	Domain		2015-03-22 21:33:54 ICT
S-1-5-21-2425377081-3129163575-2985601102-10			1	temporary	cfreds_2015_data_leakage_pc.dd_1 Host	Domain		2015-03-22 22:53:01 ICT
S-1-5-20				NETWORK SERVICE	cfreds_2015_data_leakage_pc.dd_1 Host	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	cfreds_2015_data_leakage_pc.dd_1 Host	Local	NT AUTHORITY	
S-1-5-80-2620923248-4247863784-3378508180-26			1		cfreds_2015_data_leakage_pc.dd_1 Host	Local	NT SERVICE	
S-1-5-21-2425377081-3129163575-2985601102-10			1	ITechTeam	cfreds_2015_data_leakage_pc.dd_1 Host	Domain		2015-03-22 22:52:30 ICT
S-1-5-21-2425377081-3129163575-2985601102-50			1	Administrator	cfreds_2015_data_leakage_pc.dd_1 Host	Domain		2015-03-25 17:33:22 ICT
S-1-5-21-2425377081-3129163575-2985601102-50			1	Guest	cfreds_2015_data_leakage_pc.dd_1 Host	Domain		2015-03-25 17:33:22 ICT

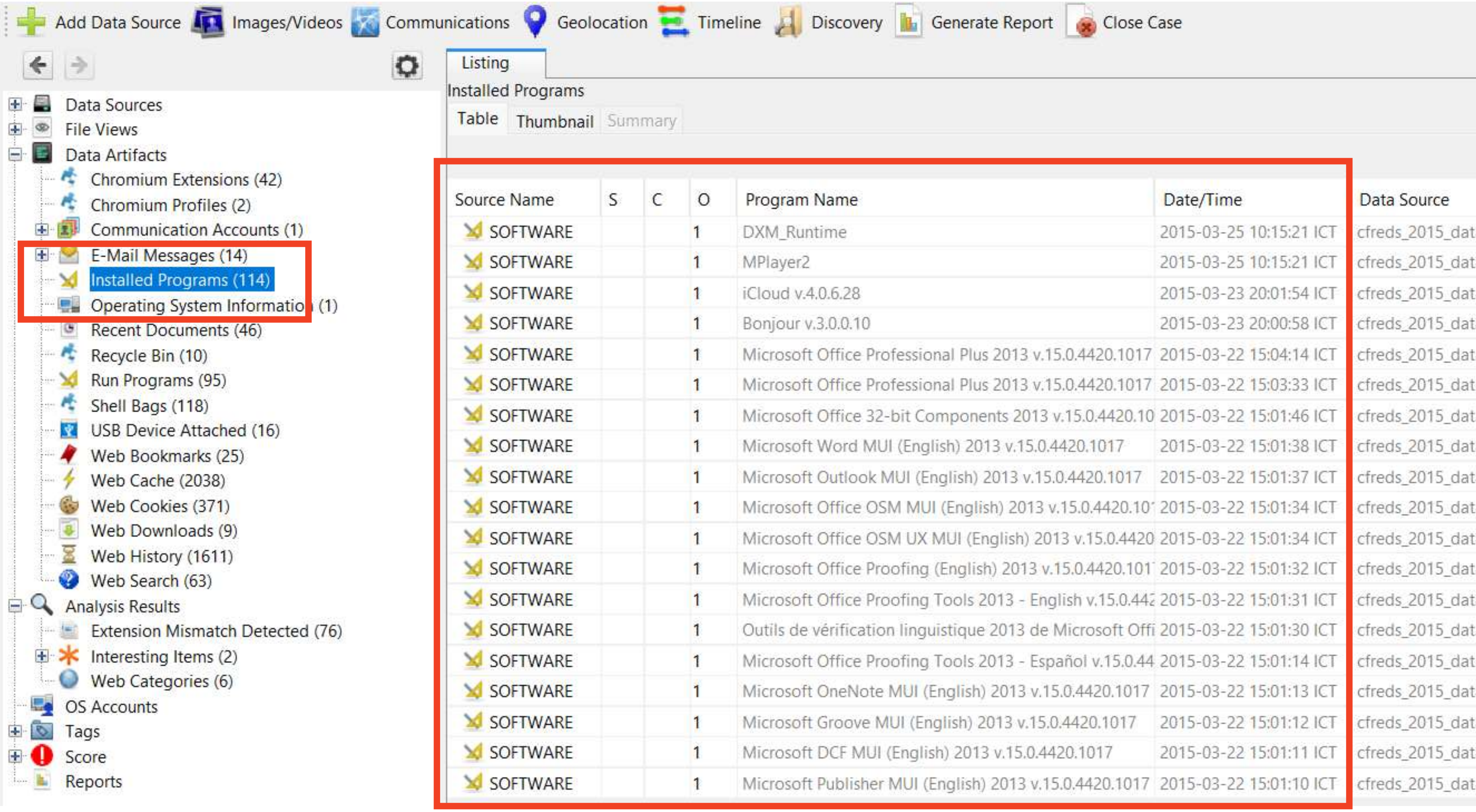
Basic Properties

Login:	informant
Full Name:	
Address:	S-1-5-21-2425377081-3129163575-2985601102-1000
Type:	
Creation Date:	2015-03-22 21:33:54 ICT
Object ID:	3707

cfreds_2015_data_leakage_pc.dd_1 Host Details

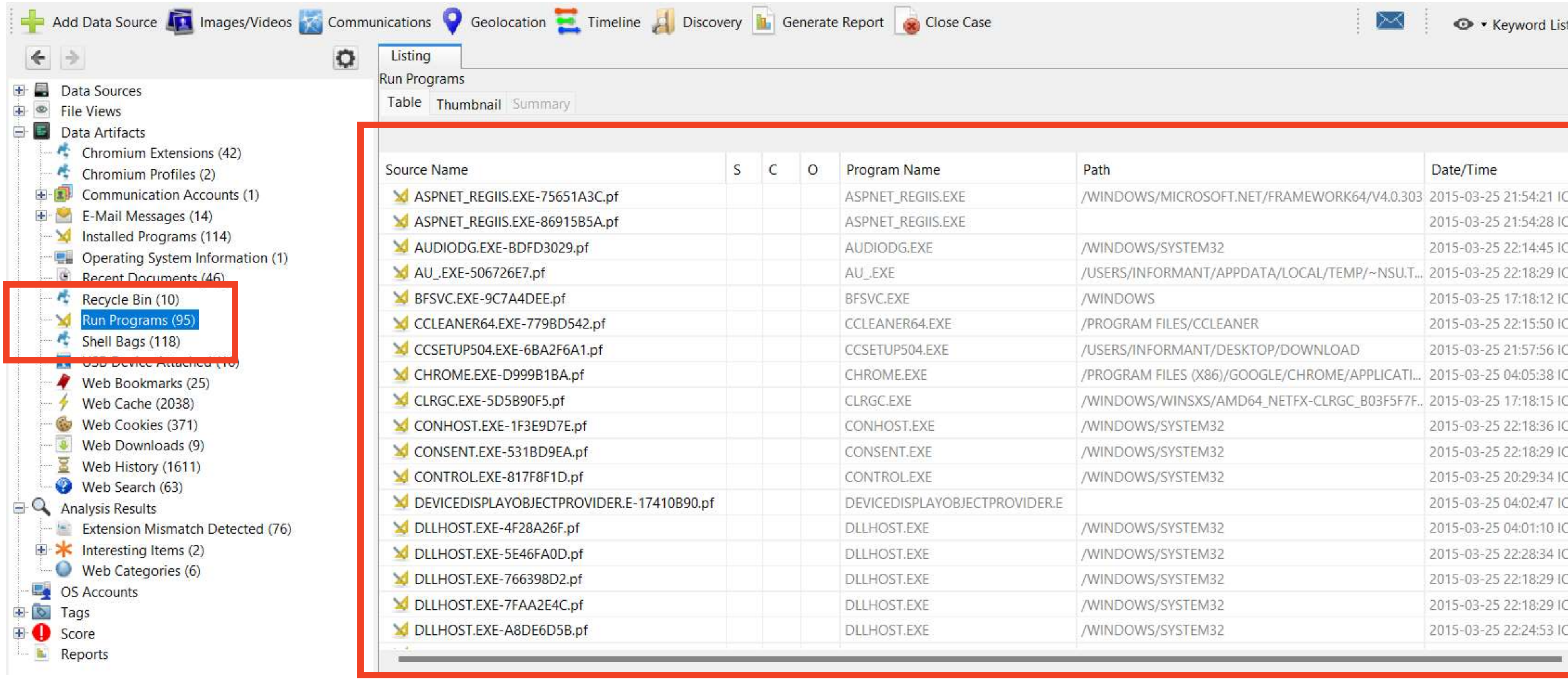
Last Login:	2015-03-25 20:06:08 ICT
Login Count:	9
Administrator:	True
Password Hint:	IAMAN
Password Fail Date:	2015-03-22 22:57:48 ICT

3) Installed programs



Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			1	DXM_Runtime	2015-03-25 10:15:21 ICT	cfreds_2015_dat
SOFTWARE			1	MPlayer2	2015-03-25 10:15:21 ICT	cfreds_2015_dat
SOFTWARE			1	iCloud v.4.0.6.28	2015-03-23 20:01:54 ICT	cfreds_2015_dat
SOFTWARE			1	Bonjour v.3.0.0.10	2015-03-23 20:00:58 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 15:04:14 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 15:03:33 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office 32-bit Components 2013 v.15.0.4420.10	2015-03-22 15:01:46 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Word MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:38 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Outlook MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:37 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office OSM MUI (English) 2013 v.15.0.4420.10	2015-03-22 15:01:34 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office OSM UX MUI (English) 2013 v.15.0.4420	2015-03-22 15:01:34 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office Proofing (English) 2013 v.15.0.4420.101	2015-03-22 15:01:32 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office Proofing Tools 2013 - English v.15.0.44	2015-03-22 15:01:31 ICT	cfreds_2015_dat
SOFTWARE			1	Outils de vérification linguistique 2013 de Microsoft Offi	2015-03-22 15:01:30 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Office Proofing Tools 2013 - Español v.15.0.44	2015-03-22 15:01:14 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft OneNote MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:13 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Groove MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:12 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft DCF MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:11 ICT	cfreds_2015_dat
SOFTWARE			1	Microsoft Publisher MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:10 ICT	cfreds_2015_dat

4) Program execution



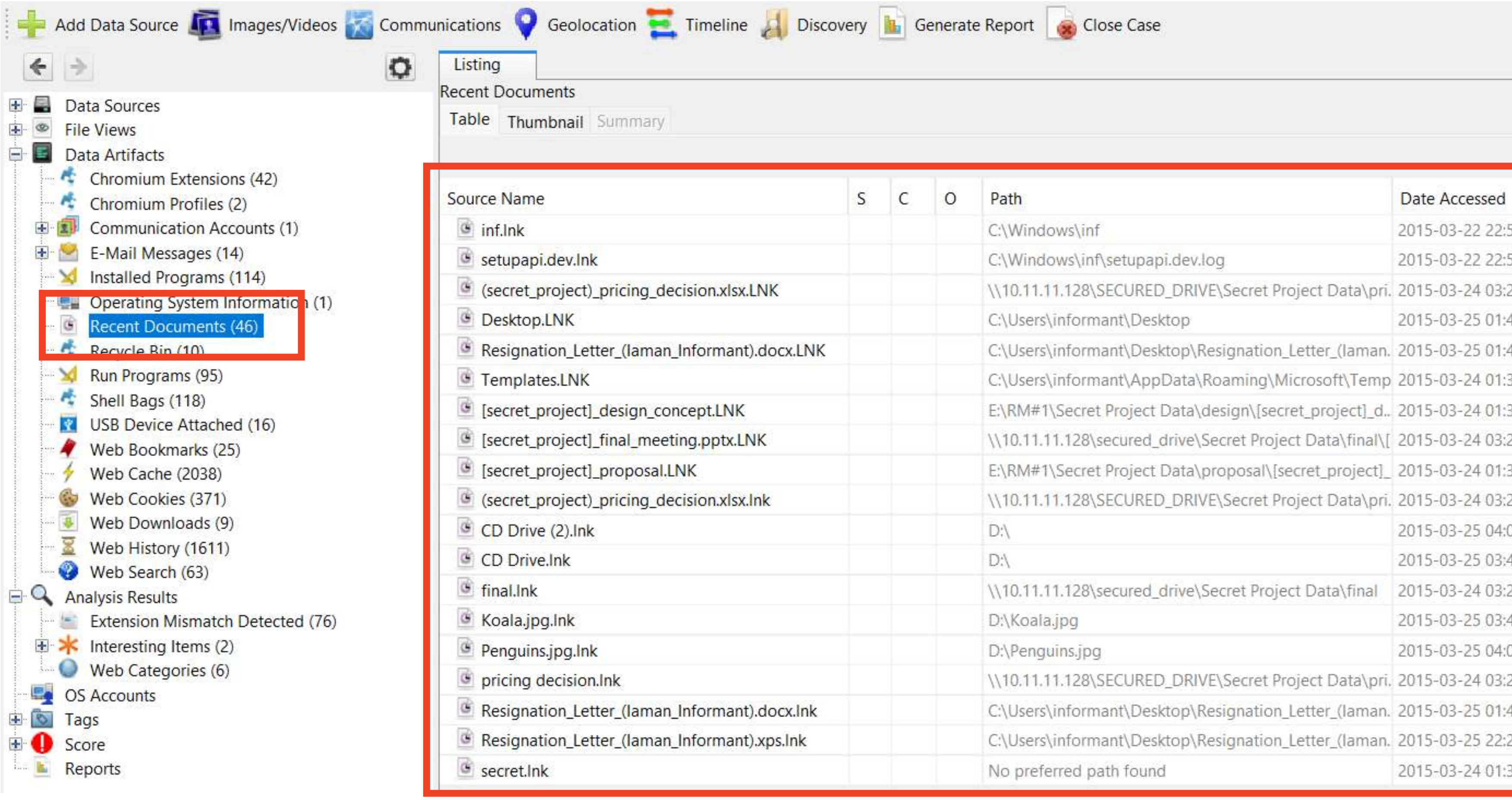
- Data Sources
- File Views
- Data Artifacts
  - Chromium Extensions (42)
  - Chromium Profiles (2)
  - Communication Accounts (1)
  - E-Mail Messages (14)
  - Installed Programs (114)
  - Operating System Information (1)
  - Recent Documents (46)
  - Recycle Bin (10)
  - Run Programs (95)
  - Shell Bags (118)
  - USB Device Attached (10)
  - Web Bookmarks (25)
  - Web Cache (2038)
  - Web Cookies (371)
  - Web Downloads (9)
  - Web History (1611)
  - Web Search (63)
- Analysis Results
  - Extension Mismatch Detected (76)
  - Interesting Items (2)
  - Web Categories (6)
- OS Accounts
- Tags
- Score
- Reports

Listing
Run Programs

Table | Thumbnail | Summary

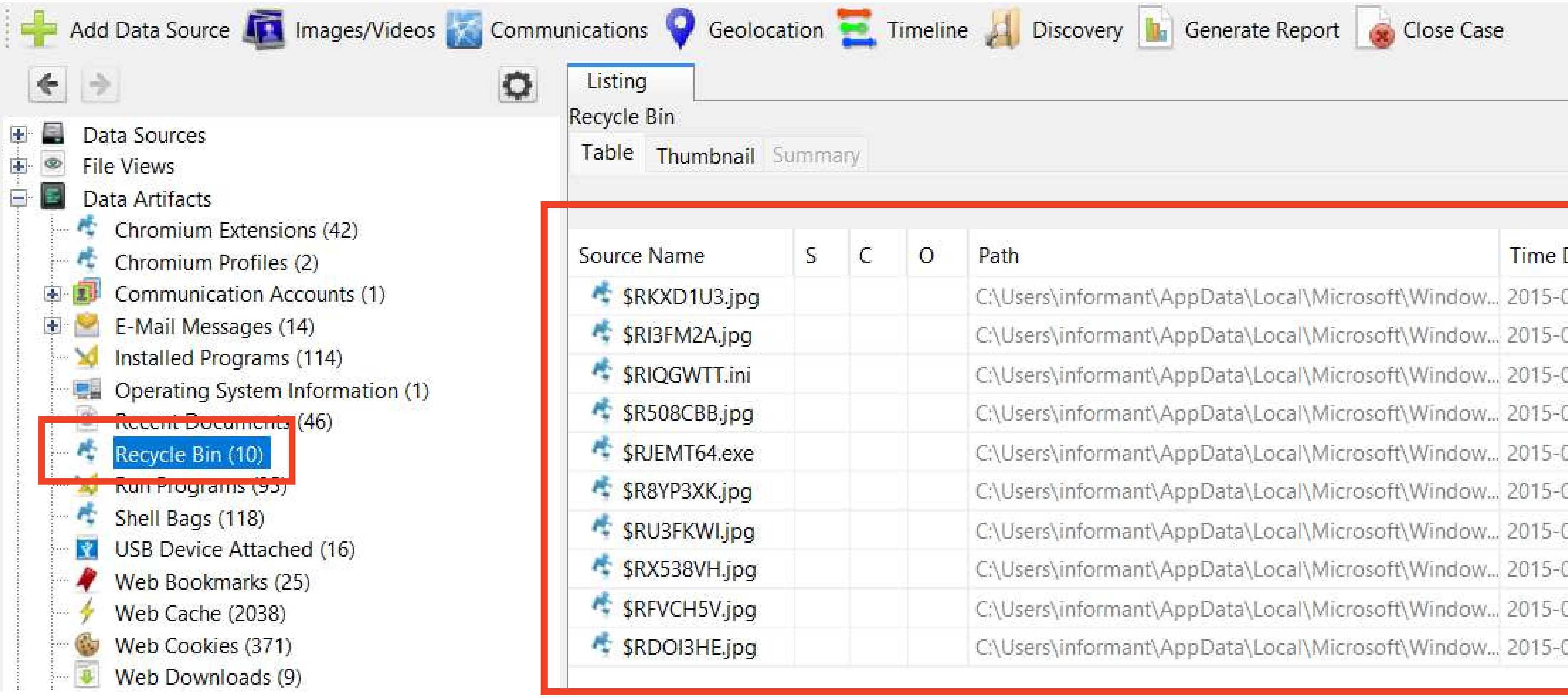
Source Name	S	C	O	Program Name	Path	Date/Time
ASPNET_REGIIS.EXE-75651A3C.pf				ASPNET_REGIIS.EXE	/WINDOWS/MICROSOFT.NET/FRAMEWORK64/V4.0.303	2015-03-25 21:54:21 IC
ASPNET_REGIIS.EXE-86915B5A.pf				ASPNET_REGIIS.EXE		2015-03-25 21:54:28 IC
AUDIODG.EXE-BDFD3029.pf				AUDIODG.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:14:45 IC
AU_.EXE-506726E7.pf				AU_.EXE	/USERS/INFORMANT/APPDATA/LOCAL/TEMP/~NSU.T...	2015-03-25 22:18:29 IC
BFSVC.EXE-9C7A4DEE.pf				BFSVC.EXE	/WINDOWS	2015-03-25 17:18:12 IC
CCLEANER64.EXE-779BD542.pf				CCLEANER64.EXE	/PROGRAM FILES/CCLEANER	2015-03-25 22:15:50 IC
CCSETUP504.EXE-6BA2F6A1.pf				CCSETUP504.EXE	/USERS/INFORMANT/DESKTOP/DOWNLOAD	2015-03-25 21:57:56 IC
CHROME.EXE-D999B1BA.pf				CHROME.EXE	/PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICATI...	2015-03-25 04:05:38 IC
CLRGC.EXE-5D5B90F5.pf				CLRGC.EXE	/WINDOWS/WINSXS/AMD64_NETFX-CLRGC_B03F5F7F...	2015-03-25 17:18:15 IC
CONHOST.EXE-1F3E9D7E.pf				CONHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:18:36 IC
CONSENT.EXE-531BD9EA.pf				CONSENT.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:18:29 IC
CONTROL.EXE-817F8F1D.pf				CONTROL.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:29:34 IC
DEVICEDISPLAYOBJECTPROVIDER.E-17410B90.pf				DEVICEDISPLAYOBJECTPROVIDER.E		2015-03-25 04:02:47 IC
DLLHOST.EXE-4F28A26F.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 04:01:10 IC
DLLHOST.EXE-5E46FA0D.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:28:34 IC
DLLHOST.EXE-766398D2.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:18:29 IC
DLLHOST.EXE-7FAA2E4C.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:18:29 IC
DLLHOST.EXE-A8DE6D5B.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 22:24:53 IC

5) Recent documents



Source Name	S	C	O	Path	Date Accessed
inf.lnk				C:\Windows\inf	2015-03-22 22:5
setupapi.dev.lnk				C:\Windows\inf\setupapi.dev.log	2015-03-22 22:5
(secret_project)_pricing_decision.xlsx.LNK				\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pri.	2015-03-24 03:2
Desktop.LNK				C:\Users\informant\Desktop	2015-03-25 01:4
Resignation_Letter_(laman_Informant).docx.LNK				C:\Users\informant\Desktop\Resignation_Letter_(laman.	2015-03-25 01:4
Templates.LNK				C:\Users\informant\AppData\Roaming\Microsoft\Temp	2015-03-24 01:3
[secret_project]_design_concept.LNK				E:\RM#1\Secret Project Data\design\[secret_project]_d..	2015-03-24 01:3
[secret_project]_final_meeting.pptx.LNK				\\10.11.11.128\secured_drive\Secret Project Data\final\[	2015-03-24 03:2
[secret_project]_proposal.LNK				E:\RM#1\Secret Project Data\proposal\[secret_project]_	2015-03-24 01:3
(secret_project)_pricing_decision.xlsx.lnk				\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pri.	2015-03-24 03:2
CD Drive (2).lnk				D:\	2015-03-25 04:0
CD Drive.lnk				D:\	2015-03-25 03:4
final.lnk				\\10.11.11.128\secured_drive\Secret Project Data\final	2015-03-24 03:2
Koala.jpg.lnk				D:\Koala.jpg	2015-03-25 03:4
Penguins.jpg.lnk				D:\Penguins.jpg	2015-03-25 04:0
pricing decision.lnk				\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pri.	2015-03-24 03:2
Resignation_Letter_(laman_Informant).docx.lnk				C:\Users\informant\Desktop\Resignation_Letter_(laman.	2015-03-25 01:4
Resignation_Letter_(laman_Informant).xps.lnk				C:\Users\informant\Desktop\Resignation_Letter_(laman.	2015-03-25 22:2
secret.lnk				No preferred path found	2015-03-24 01:3

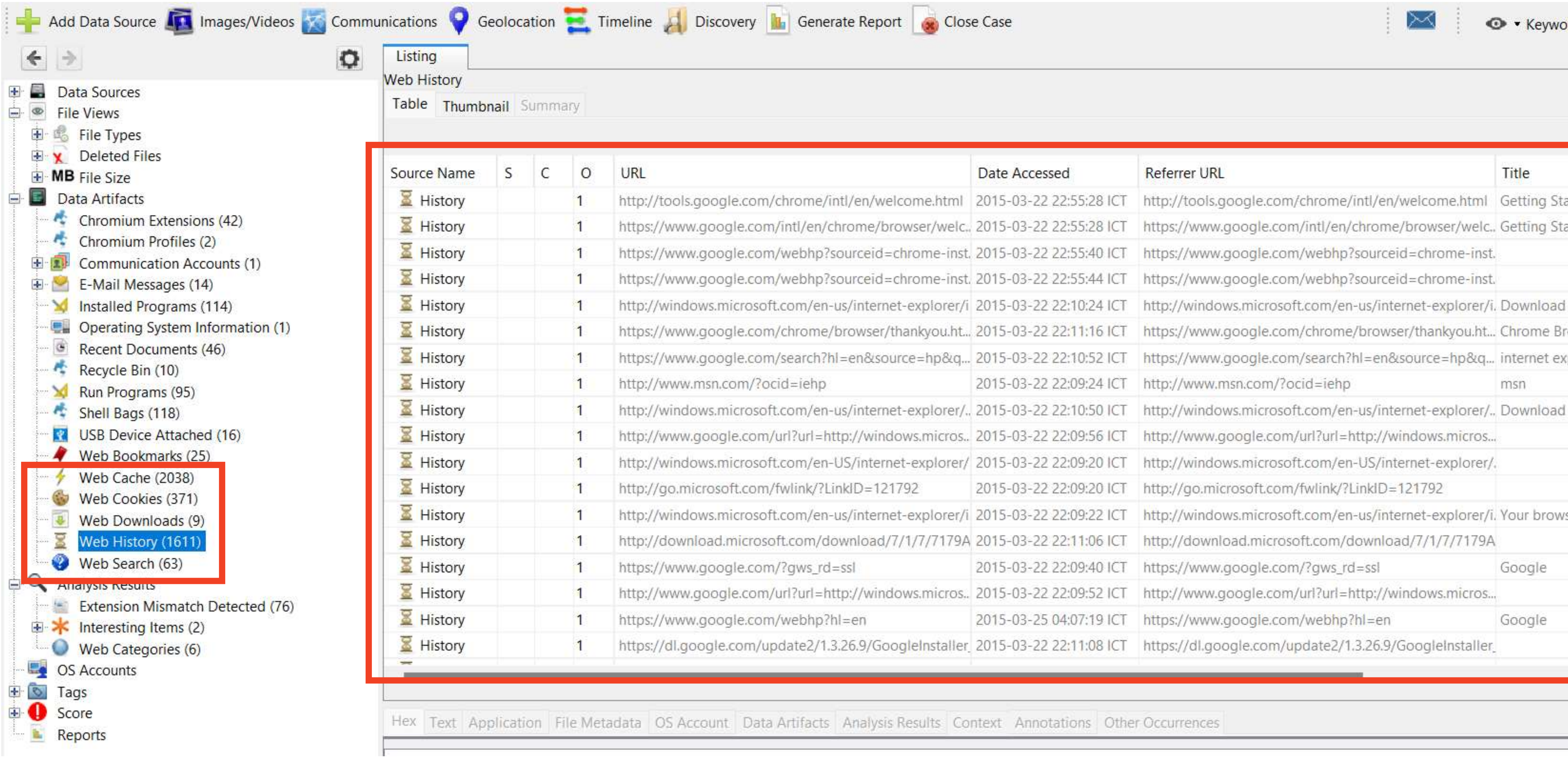
6) Recycle Bin



Recycle Bin

Source Name	S	C	O	Path	Time D
$RKXD1U3.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RI3FM2A.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RIQGWTT.ini				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$R508CBB.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RJEMT64.exe				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$R8YP3XK.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RU3FKWI.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RX538VH.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RFVCH5V.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0
$RDOI3HE.jpg				C:\Users\informant\AppData\Local\Microsoft\Window...	2015-0

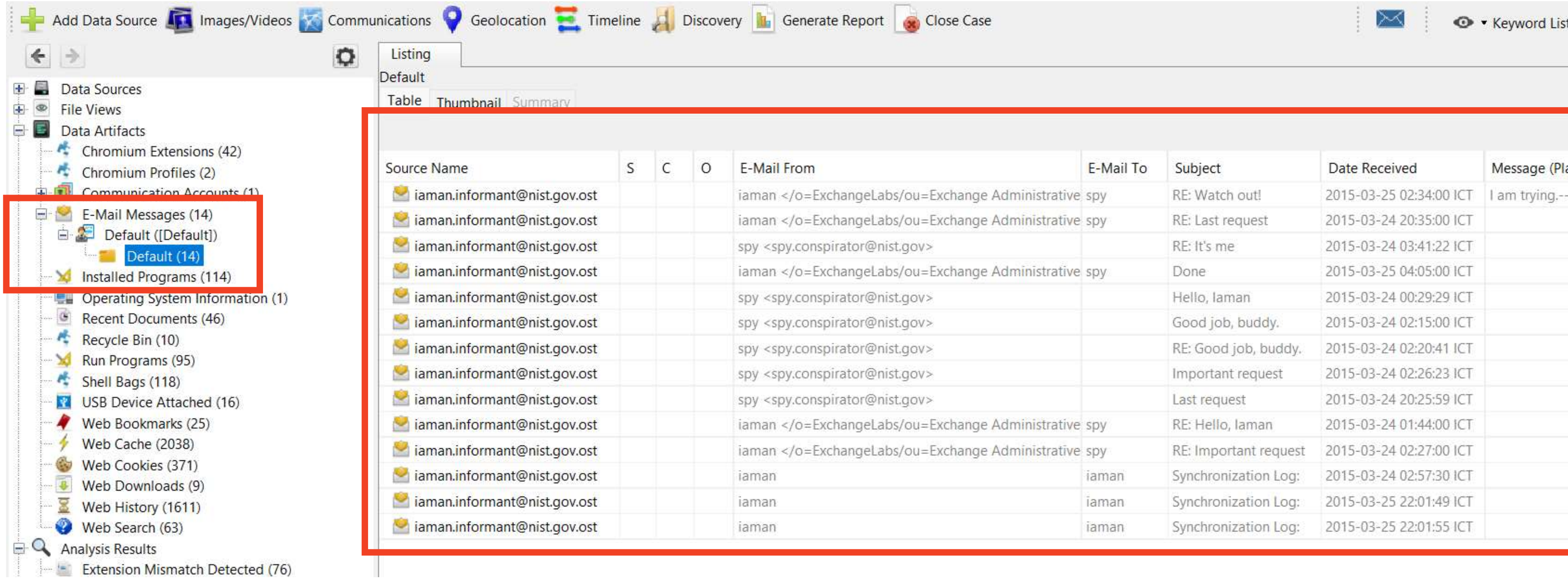
7) Browser history



- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Chromium Extensions (42)
  - Chromium Profiles (2)
  - Communication Accounts (1)
  - E-Mail Messages (14)
  - Installed Programs (114)
  - Operating System Information (1)
  - Recent Documents (46)
  - Recycle Bin (10)
  - Run Programs (95)
  - Shell Bags (118)
  - USB Device Attached (16)
  - Web Bookmarks (25)
  - Web Cache (2038)
  - Web Cookies (371)
  - Web Downloads (9)
  - Web History (1611)
  - Web Search (63)
- Analysis Results
  - Extension Mismatch Detected (76)
  - Interesting Items (2)
  - Web Categories (6)
- OS Accounts
- Tags
- Score
- Reports

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History			1	http://tools.google.com/chrome/intl/en/welcome.html	2015-03-22 22:55:28 ICT	http://tools.google.com/chrome/intl/en/welcome.html	Getting Sta
History			1	https://www.google.com/intl/en/chrome/browser/welc..	2015-03-22 22:55:28 ICT	https://www.google.com/intl/en/chrome/browser/welc..	Getting Sta
History			1	https://www.google.com/webhp?sourceid=chrome-inst.	2015-03-22 22:55:40 ICT	https://www.google.com/webhp?sourceid=chrome-inst.	
History			1	https://www.google.com/webhp?sourceid=chrome-inst.	2015-03-22 22:55:44 ICT	https://www.google.com/webhp?sourceid=chrome-inst.	
History			1	http://windows.microsoft.com/en-us/internet-explorer/i	2015-03-22 22:10:24 ICT	http://windows.microsoft.com/en-us/internet-explorer/i.	Download
History			1	https://www.google.com/chrome/browser/thankyou.ht...	2015-03-22 22:11:16 ICT	https://www.google.com/chrome/browser/thankyou.ht...	Chrome Br
History			1	https://www.google.com/search?hl=en&source=hp&q...	2015-03-22 22:10:52 ICT	https://www.google.com/search?hl=en&source=hp&q...	internet ex
History			1	http://www.msn.com/?ocid=iehp	2015-03-22 22:09:24 ICT	http://www.msn.com/?ocid=iehp	msn
History			1	http://windows.microsoft.com/en-us/internet-explorer/..	2015-03-22 22:10:50 ICT	http://windows.microsoft.com/en-us/internet-explorer/..	Download
History			1	http://www.google.com/url?url=http://windows.micros..	2015-03-22 22:09:56 ICT	http://www.google.com/url?url=http://windows.micros...	
History			1	http://windows.microsoft.com/en-US/internet-explorer/	2015-03-22 22:09:20 ICT	http://windows.microsoft.com/en-US/internet-explorer/.	
History			1	http://go.microsoft.com/fwlink/?LinkID=121792	2015-03-22 22:09:20 ICT	http://go.microsoft.com/fwlink/?LinkID=121792	
History			1	http://windows.microsoft.com/en-us/internet-explorer/i	2015-03-22 22:09:22 ICT	http://windows.microsoft.com/en-us/internet-explorer/i.	Your brows
History			1	http://download.microsoft.com/download/7/1/7/7179A	2015-03-22 22:11:06 ICT	http://download.microsoft.com/download/7/1/7/7179A	
History			1	https://www.google.com/?gws_rd=ssl	2015-03-22 22:09:40 ICT	https://www.google.com/?gws_rd=ssl	Google
History			1	http://www.google.com/url?url=http://windows.micros..	2015-03-22 22:09:52 ICT	http://www.google.com/url?url=http://windows.micros...	
History			1	https://www.google.com/webhp?hl=en	2015-03-25 04:07:19 ICT	https://www.google.com/webhp?hl=en	Google
History			1	https://dl.google.com/update2/1.3.26.9/GoogleInstaller_	2015-03-22 22:11:08 ICT	https://dl.google.com/update2/1.3.26.9/GoogleInstaller_	

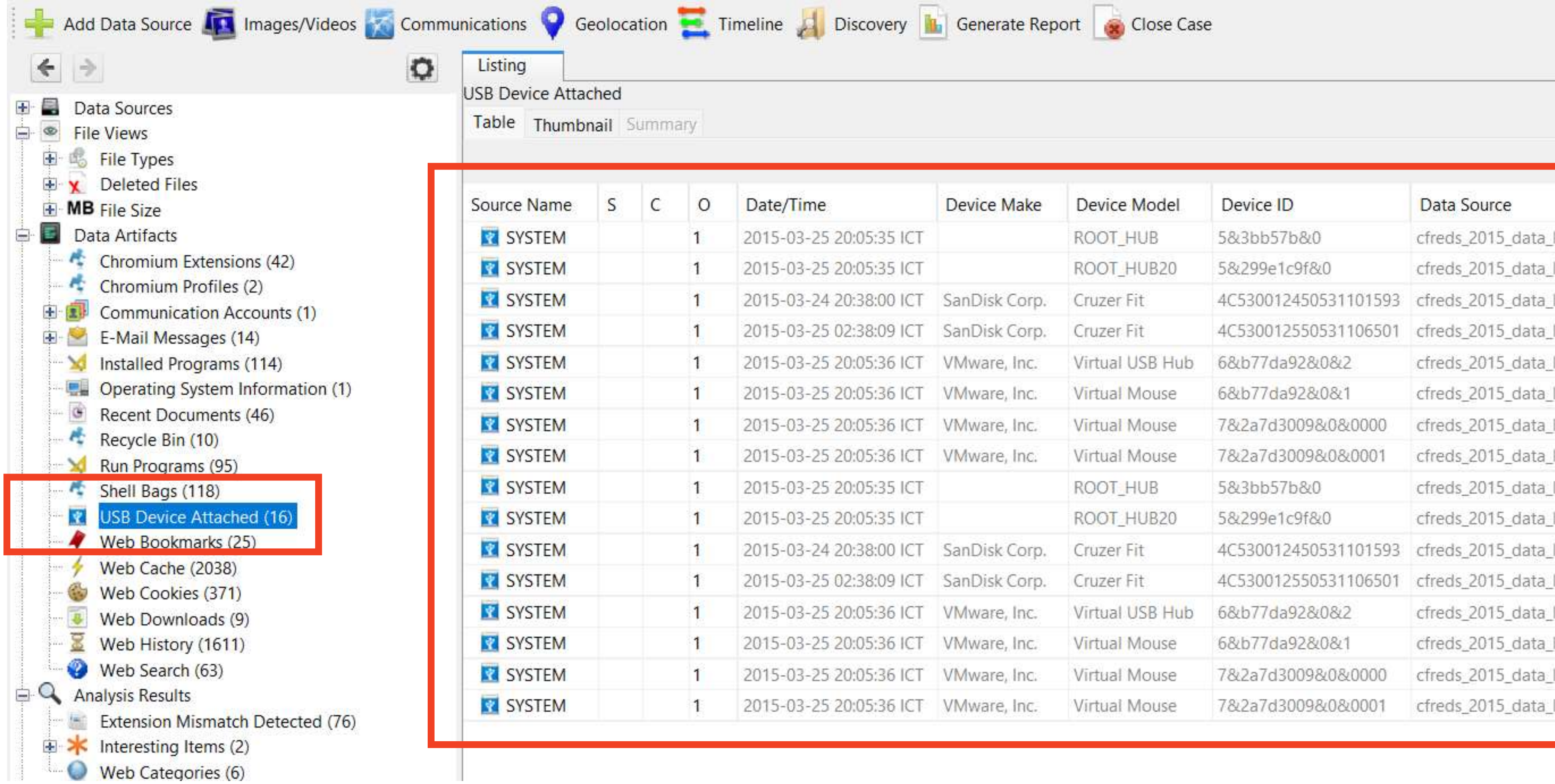
8) Email activities



- Data Sources
- File Views
- Data Artifacts
  - Chromium Extensions (42)
  - Chromium Profiles (2)
  - Communication Accounts (1)
  - E-Mail Messages (14)
    - Default ([Default])
      - Default (14)
  - Installed Programs (114)
  - Operating System Information (1)
  - Recent Documents (46)
  - Recycle Bin (10)
  - Run Programs (95)
  - Shell Bags (118)
  - USB Device Attached (16)
  - Web Bookmarks (25)
  - Web Cache (2038)
  - Web Cookies (371)
  - Web Downloads (9)
  - Web History (1611)
  - Web Search (63)
- Analysis Results
  - Extension Mismatch Detected (76)

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Pla
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	RE: Watch out!	2015-03-25 02:34:00 ICT	I am trying.--
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	RE: Last request	2015-03-24 20:35:00 ICT	
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		RE: It's me	2015-03-24 03:41:22 ICT	
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	Done	2015-03-25 04:05:00 ICT	
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Hello, Iaman	2015-03-24 00:29:29 ICT	
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Good job, buddy.	2015-03-24 02:15:00 ICT	
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		RE: Good job, buddy.	2015-03-24 02:20:41 ICT	
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Important request	2015-03-24 02:26:23 ICT	
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Last request	2015-03-24 20:25:59 ICT	
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	RE: Hello, Iaman	2015-03-24 01:44:00 ICT	
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	RE: Important request	2015-03-24 02:27:00 ICT	
iaman.informant@nist.gov.ost				iaman	iaman	Synchronization Log:	2015-03-24 02:57:30 ICT	
iaman.informant@nist.gov.ost				iaman	iaman	Synchronization Log:	2015-03-25 22:01:49 ICT	
iaman.informant@nist.gov.ost				iaman	iaman	Synchronization Log:	2015-03-25 22:01:55 ICT	

9) External storage devices



USB Device Attached

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			1	2015-03-25 20:05:35 ICT		ROOT_HUB	5&3bb57b&0	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:35 ICT		ROOT_HUB20	5&299e1c9f&0	cfreds_2015_data_
SYSTEM			1	2015-03-24 20:38:00 ICT	SanDisk Corp.	Cruzer Fit	4C530012450531101593	cfreds_2015_data_
SYSTEM			1	2015-03-25 02:38:09 ICT	SanDisk Corp.	Cruzer Fit	4C530012550531106501	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual USB Hub	6&b77da92&0&2	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual Mouse	6&b77da92&0&1	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0000	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0001	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:35 ICT		ROOT_HUB	5&3bb57b&0	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:35 ICT		ROOT_HUB20	5&299e1c9f&0	cfreds_2015_data_
SYSTEM			1	2015-03-24 20:38:00 ICT	SanDisk Corp.	Cruzer Fit	4C530012450531101593	cfreds_2015_data_
SYSTEM			1	2015-03-25 02:38:09 ICT	SanDisk Corp.	Cruzer Fit	4C530012550531106501	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual USB Hub	6&b77da92&0&2	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual Mouse	6&b77da92&0&1	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0000	cfreds_2015_data_
SYSTEM			1	2015-03-25 20:05:36 ICT	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0001	cfreds_2015_data_

10) Anti-forensics

- Using files cleaner tool and secure delete tool for anti-forensic
- CCleaner
  - https://www.synacktiv.com/en/publications/ccleaner-forensics
- Eraser
  - https://eraser.heidi.ie/forum/threads/how-could-eraser-be-a-better-anti-forensic-