Forensics and eDiscovery

Project Report (Continuous Assessment)

for
Mark Monaghan

by
Rohan Bhangale (x18147119)

Computer Forensics Report

Future Holdings LTD (Limited)

Investigator: Rohan Bhangale
x18147119@student.ncirl.ie
11th August 2018

Contents

Investigator: *Rohan Bhangale*
Address: *Executive Suite 2, School of Business,*
National College of Ireland, Mayor Square, IFSC
Dublin 1
Ireland

Client: *Future Holdings LTD*
Address: *Dublin, Ireland*

Date of Report: 11 August 2019

Report on the analysis of Computer found under floorboard from the CFO office, during the renovation of the office.

Dear Mr. Bernard Rug,
This report entails on the findings from forensic analysis on the computer found under the floorboard from the former CFO's office, during the renovation of the office of former CFO's office. The renovation of the office took place after the dismissal of the former CFO for gross misconduct. At the time of renovating the office the operating carpenter found a sword and computer under the floorboard. Investigator Rohan Bhangale was engaged by the CEO of Future Holdings LTD Mr. Bernard Rug to carry out a forensic analysis on the found computer. For the analysis, investigator received drive image of the found computer.

Case Description

Laptop and Sword found in Future Holdings LTD's Former CFO William Rapp's office is being investigated under his dismissal over gross misconduct.

Computer Image and Forensics Tool Statistics

The laptop found under floorboard at Future Holdings LTD office was imaged for its harddrive contents for forensics lab to initiate with the research and testing. The image of hard drive was tested using forensics application FTK Imager and Registry Viewer by AccessData. This program has been demonstrated to be valid and precise when scanning and evaluating a system in the court of law.

Investigator Information

The following report was conducted by Rohan Bhangale. My task is to take the proof that I have received and provide facts that seem relevant to the situation. The evidence being reviewed has been collected by Future Holdings and verified to be unaltered. Any questions or concerns pertaining to the acquisition of the evidence can be gathered from the individual who took possession of the laptop after its discovery by the carpenter.

Investigation

Case Summary

Future Holdings and Investigator Rohan Bhangale established on working for the outcome a forensics investigation on a suspect device and reporting the findings from the investigation

Conclusion Summary

The report tells about the information on the linkage between the former Future Holdings CFO’s laptop and sword.On the analysis of the device hard drive image it was concluded that the suspect purchased the *Batleth* Sword on the basis of the user activity, such as email conversation, photos and browsing history.

Investigations of the Facts

Based on the Electronic Discovery Reference Model, the investigation was conducted and reported

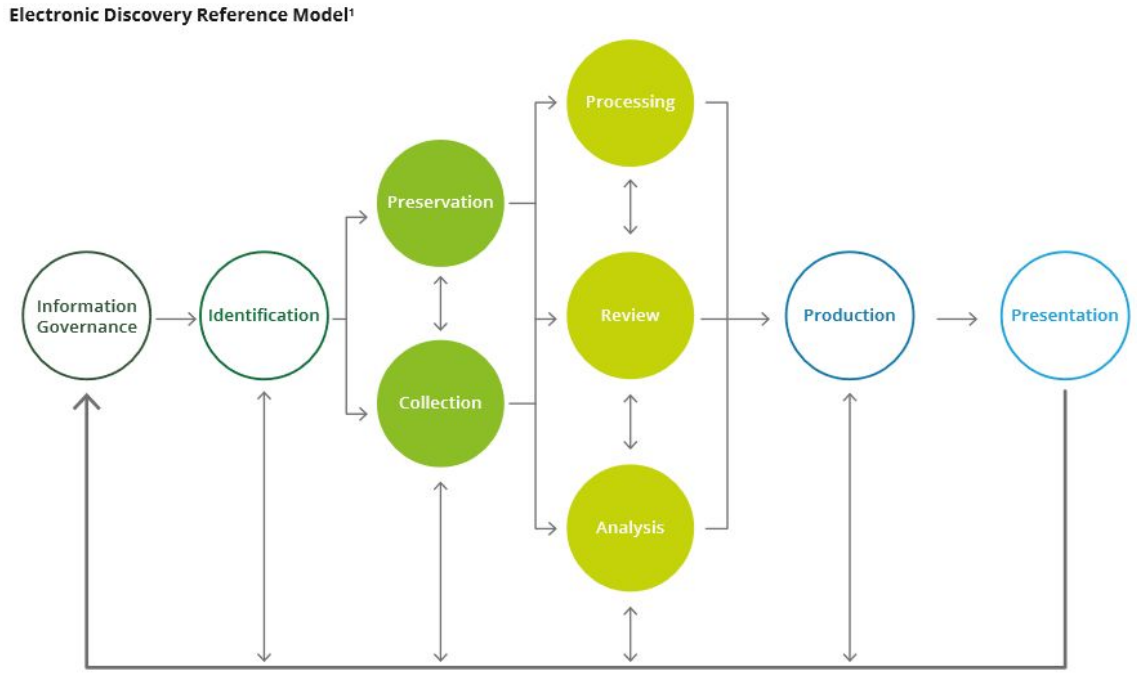


Figure: EDRM; Source: Deloitte

- Identification: Identifying relevant data(suspect data) and where it might be located and determining the nature
- Collection:Gathering the required evidence for further use in Forensics and eDiscovery without contamination of the evidence gathered.
- Preservation: Ensuring that the evidence is safe, saving the evidence by creating an image of it for forensics analysis
- Process:Reducing the volume of the data by removing duplicates and irrelevant data.
- Review and Analysis: Evaluation of the relevance of the evidence and for content to be discussed by people(criminal lawyers,experts,etc.)
- Produce and Report: Delivering the outcomes in appropriate form and presenting it for legal authority for the outcome.

Findings

Provided disk image "***Image.ad1***" of size **195 MB** was analysed using FTK Imager which gave the following information on the evidence

Personal Computer	HW	Type	Virtual System	VMWare v9.2.2
	SW (OS)	Operating System	Microsoft Windows 7 Ultimate SP1	English (64 bits)
	SW (Apps)	Web	- MS Internet Explorer	Version 8.0.7600
		E-mail	Microsoft Outlook	
Removable Media #1	HW	Type	USB removable mouse	
		Mfg.	-	Vendor ID = 0x0781
		Serial No.	7&2a63cead&0&0001	Unique serial number
Removable Media #2	HW	Type	Virtual USB Hub	
		Serial No.	6&b25d31b&0&2	Unique serial number

- Hash Values

MD5 HASH: 024f0e46fe76f6c645e2e0cb5e10bdaa
SHA1 HASH: 1e192283e06f20cb5c9b1023407d01d441b5aec0

- Partition Information

The disk image is of NTFS file system based on the version of Windows NTFS 3.1 with cluster count of 15,728,127

- Operating System Information

OS Name	Windows 7 Ultimate
Version	6.1
Build Number	7600
Registered Owner	Windows User

System Root	C:\Windows
Install Date	Tue Apr 30 18:34:15 2013

Above details were gathered using FTK registry viewer and Autopsy, screenshot of the gathered information can be found in the appendix

- Following accounts were available in the system apart from the 2 system accounts

User	ID	Number of Logins	Last Access
Admin	S-1-5-21-3981241421-3166723359-794646137-**1000**	7	2013-07-30 17:35:55
Jack	S-1-5-21-3981241421-3166723359-794646137-**1003**	1	2013-07-30 16:18:22
PepBoyz	S-1-5-21-3981241421-3166723359-794646137-**1004**	2	2013-07-30 17:22:08
Manny	S-1-5-21-3981241421-3166723359-794646137-**1001**	2	2013-07-30 16:42:12
Moe	S-1-5-21-3981241421-3166723359-794646137-**1002**	2	2013-07-30 17:15:43

Source: Autopsy

Based on the above information, considering the access date, Admin was the last one to access the system

- Shutdown recorded last was at July 30 14:19:46 2013, gathered using Registry Viewer, later the hex values were converted to human readable using regripper tool
- Programs installed on the system

AccessData FTK Imager v.3.1.3.2 2013-07-30 20:06:49 BST LogicalFileSet1

AddressBook 2009-07-14 04:53:25 BST LogicalFileSet1

Connection Manager 2009-07-14 04:53:26 BST LogicalFileSet1

DXM_Runtime 2013-04-30 21:30:00 BST LogicalFileSet1

DirectDrawEx 2009-07-14 04:53:26 BST LogicalFileSet1

Fontcore 2009-07-14 04:53:26 BST LogicalFileSet1

IE40 2009-07-14 04:53:26 BST LogicalFileSet1

IE4Data 2009-07-14 04:53:26 BST LogicalFileSet1

IE5BAKEX 2009-07-14 04:53:26 BST LogicalFileSet1

IEData 2009-07-14 04:53:26 BST LogicalFileSet1

MPlayer2 2013-04-30 21:30:00 BST LogicalFileSet1

Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161 2013-04-30 18:36:06 BST LogicalFileSet1

MobileOptionPack 2009-07-14 04:53:26 BST LogicalFileSet1

SchedulingAgent 2009-07-14 04:53:26 BST LogicalFileSet1

VMware Tools v.9.2.2.18018 2013-04-30 18:37:53 BST LogicalFileSet1

WIC 2009-07-14 04:53:26 BST LogicalFileSet1

- Traces about the system on/off and the user logon/logoff could not be retrieved as the concerning registry was missing
- Application user log can be seen with the registry viewer (Sec Appendix d.10)

- After analysing the media found on the disk image, from the retrieved images, strange looking swords were present in the images, which raises suspicion as a sword was found with the laptop at the time of discovery. After looking into the metadata of the image it was seen that the image belonged to user **Manny**

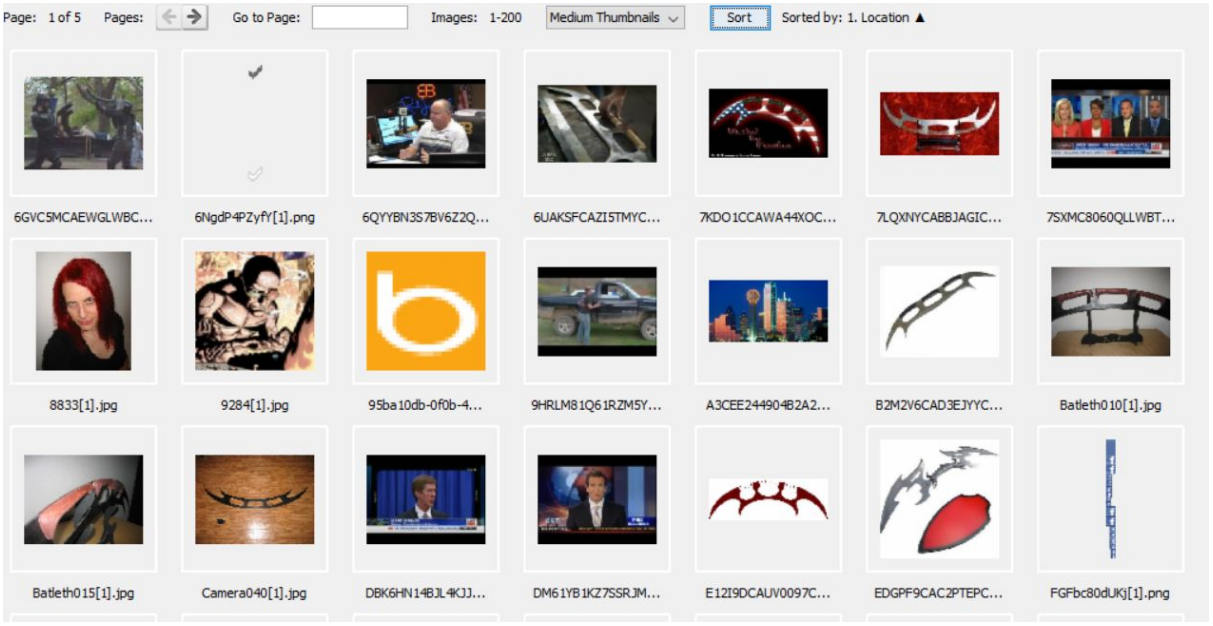


Figure: Swords Images; Source: Autopsy

- In order to dig further, investigation was led into analysing user activity of the user Manny, it was observed that Manny has been using Microsoft Internet Browser, for more details, the browser history was analysed of the user Manny.
- From BrowseHistoryTool it was observed that suspect user Manny was looking for a sword named **batleth** based on the table mentioned below. Furthermore searches were made for terms as **Zachary Quinto**, **batle, batleth**, and **google images batleth**

index.dat www.bing.com google images Internet Explorer 2013-07-30 15:47:33 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:51:11 BST LogicalFileSet1

index.dat www.bing.com google images batleth Internet Explorer 2013-07-30 15:47:51 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:51:11 BST LogicalFileSet1

index.dat www.bing.com google images batleth Internet Explorer 2013-07-30 15:47:51 BST LogicalFileSet1

index.dat www.bing.com google images Internet Explorer 2013-07-30 15:47:33 BST LogicalFileSet1

index.dat clients1.google.com batle Internet Explorer 2013-07-30 15:47:59 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:49:12 BST LogicalFileSet1

index.dat clients1.google.com bat Internet Explorer 2013-07-30 15:47:58 BST LogicalFileSet1

index.dat clients1.google.com ba Internet Explorer 2013-07-30 15:47:58 BST LogicalFileSet1

index.dat www.google.com Zachary Quinto Internet Explorer 2013-07-30 15:48:42 BST LogicalFileSet1

index.dat clients1.google.com b Internet Explorer 2013-07-30 15:47:58 BST LogicalFileSet1

index.dat clients1.google.com batleth Internet Explorer 2013-07-30 15:48:00 BST LogicalFileSet1

index.dat clients1.google.com batl Internet Explorer 2013-07-30 15:47:59 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:50:48 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:51:10 BST LogicalFileSet1

index.dat www.bing.com google images Internet Explorer 2013-07-30 15:47:33 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:50:36 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:48:20 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:48:30 BST LogicalFileSet1

index.dat clients1.google.com batlet Internet Explorer 2013-07-30 15:47:59 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:49:41 BST LogicalFileSet1

index.dat images.google.com batleth Internet Explorer 2013-07-30 15:51:20 BST LogicalFileSet1

- The suspect was using Windows Mail Client with the account brapp@ENRON.com and the backup of which was found in the location

```
/LogicalFileSet1/C___NONAME/[NTFS]/[root]/Users/Admin/Downloads/bill_rapp_000_1.pst
```

- Also it was found that external devices were used looking at the USB registry

```
SYSTEM  2013-07-30 15:20:05 BST   VMware, Inc.    Product: 0008
000650268328    LogicalFileSet1
SYSTEM  2013-07-30 15:20:03 BST   ROOT_HUB        5&17df1c1b&0
LogicalFileSet1
SYSTEM  2013-07-30 15:20:04 BST   VMware, Inc.    Virtual Mouse
6&b25d31b&0&1    LogicalFileSet1
SYSTEM 2013-07-30 15:20:04 BST    VMware, Inc.    Virtual USB Hub
6&b25d31b&0&2    LogicalFileSet1
```

Recommendations

Here it shows that the employee of Future Holdings was abusing the fair use policy for the internet and accessed content which was not supposed to be accessed, the evidence found incriminates the suspect for the wrong doing. Based on that here are some recommendations for the Future Holdings LTD.

- Network monitoring: analysing incoming and outgoing data, using deep packet inspection or sniffing the packets using tools like Wireshark
- Disabling Input/Output devices which enable users to copy data on/from remote media for avoiding leakage/malware importation
- Role Based Policies should be implemented and least privilege policy should be implemented.

Signature

R. Bhangale

Appendix

a. Experience and Qualifications

Investigator Rohan Bhangale, is a master's student majoring in Cybersecurity with specialization in forensics and ediscovery at National College of Ireland.

b. Items Examined

Disk Image "Image.ad1"

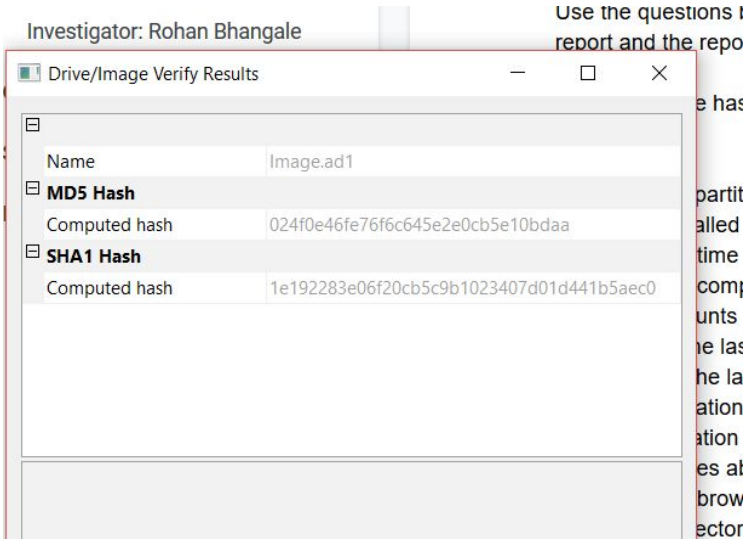
c. Forensic Tools

Autopsy
FTK Imager
FTK Registry Viewer
Reg Ripper
Browser History View

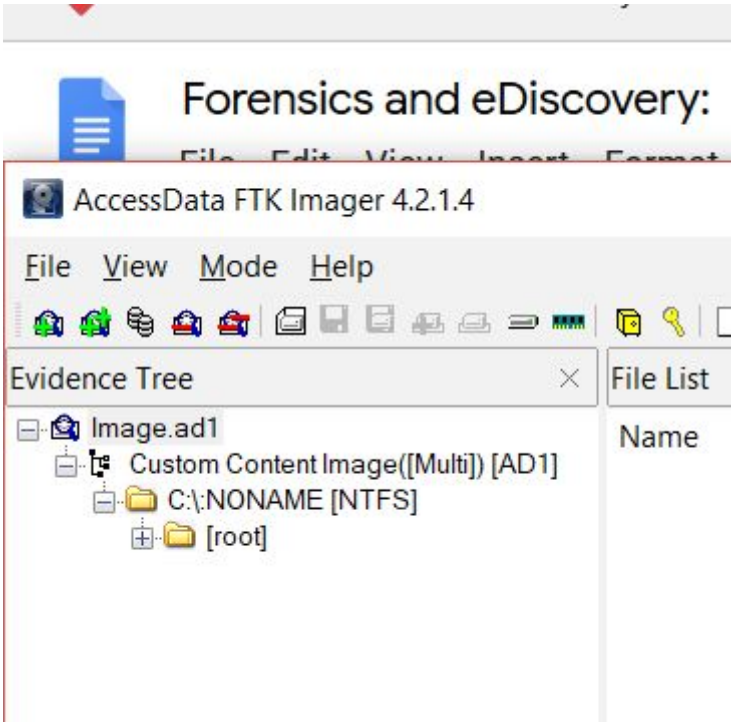
d. Photographs and Diagrams

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

MD5 HASH: 024f0e46fe76f6c645e2e0cb5e10bdaa
SHA1 HASH: 1e192283e06f20cb5c9b1023407d01d441b5aec0

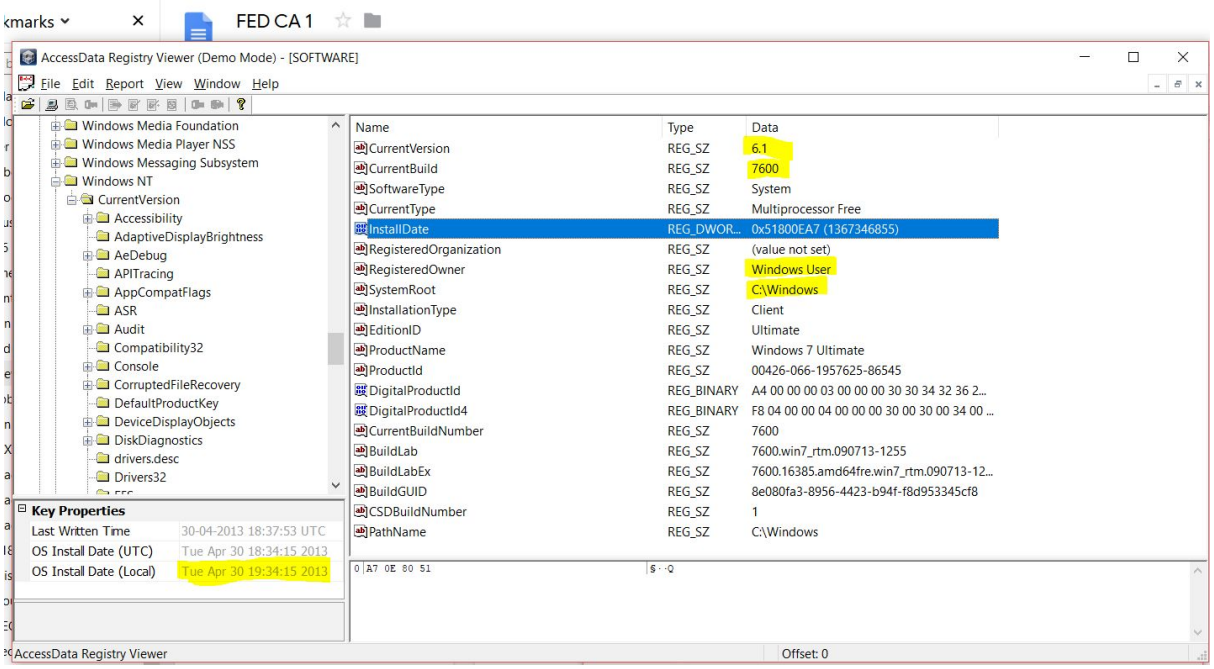


2. Identify the partition information of PC image.



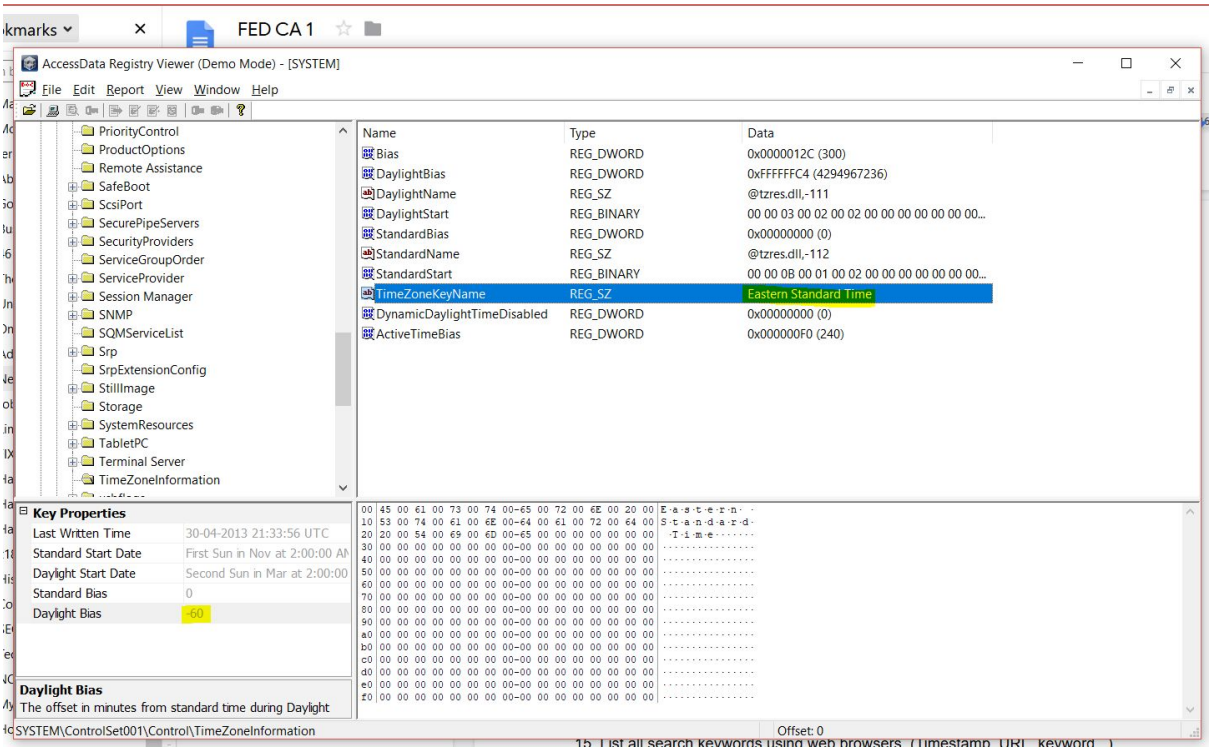
3. Explain installed OS information in detail. (OS name, install date, registered owner…)

Possible Answer	OS Name	Windows 7 Ultimate
	Version	6.1
	Build Number	7600
	Registered Owner	Windows User
	System Root	C:\Windows
	Install Date	Tue Apr 30 18:34:15 2013
Considerations	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	



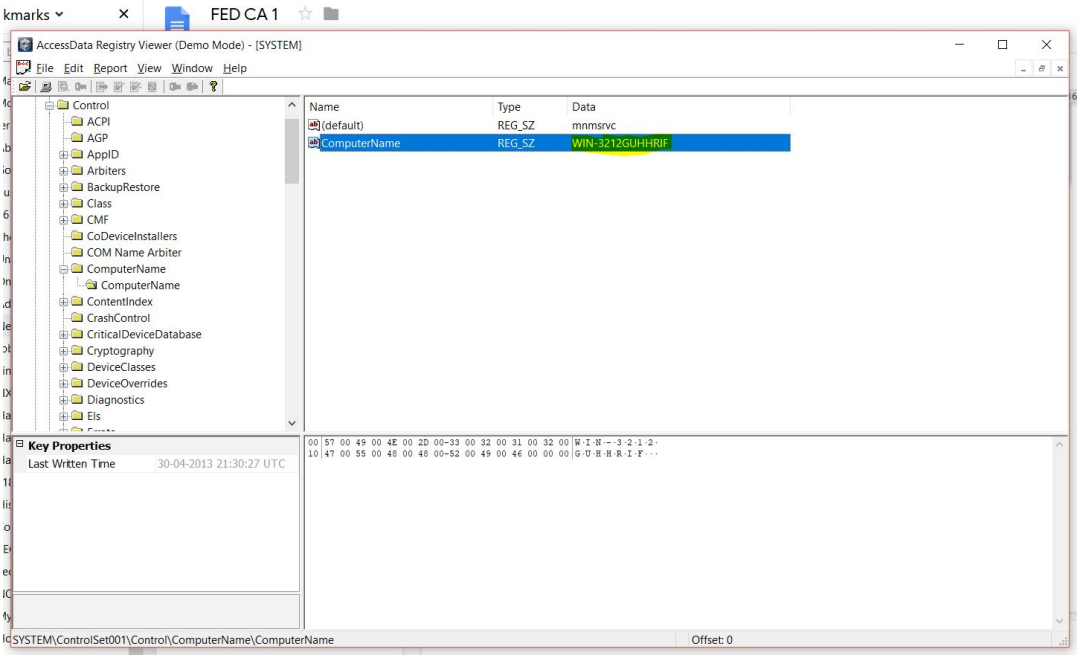
4. What is the time zone setting?

Possible Answer	Timezone	Eastern Time (US & Canada) (UTC-05:00)
	Daylight Time Bias	+1
Considerations	HKLM\SYSTEM\ControlSet###\Control\TimeZoneInformation	

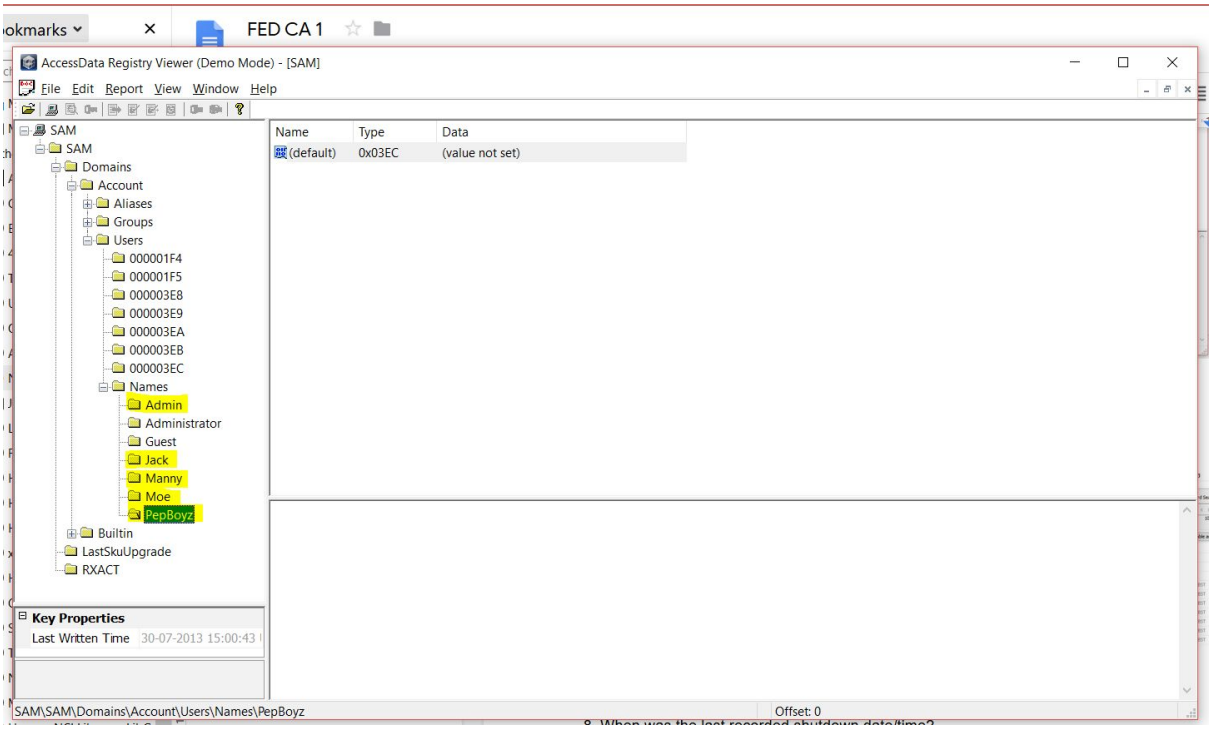


5. What is the computer name?

Possible Answer	WIN-3212GUHHRIF
Considerations	HKLM\SYSTEM\ControlSet###\Control\ComputerName\ComputerName (value: ComputerName) HKLM\SYSTEM\ControlSet###\Services\Tcpip\Parameters (value: Hostname) ……

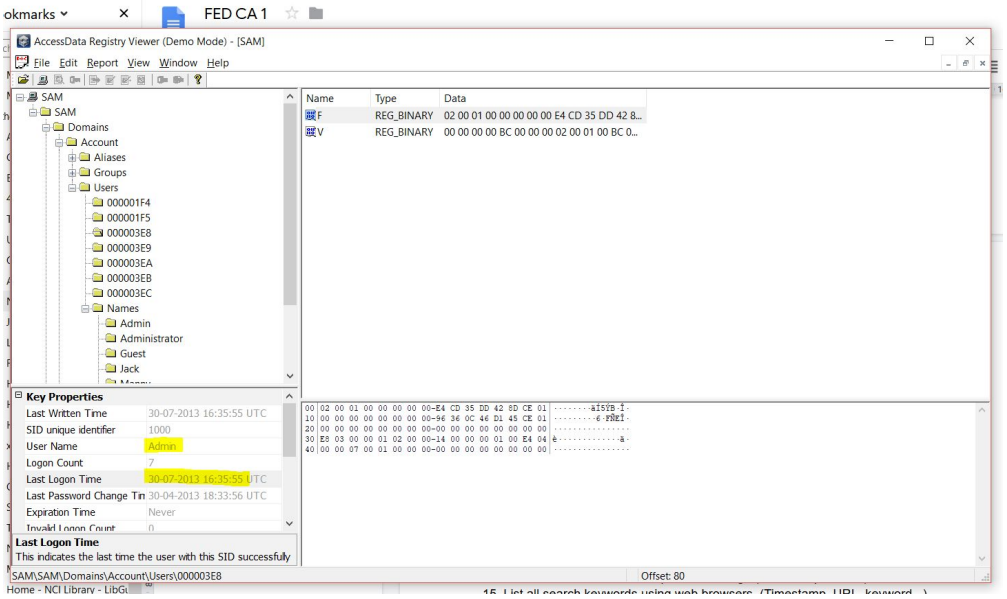


6. List all accounts in OS except the system accounts:

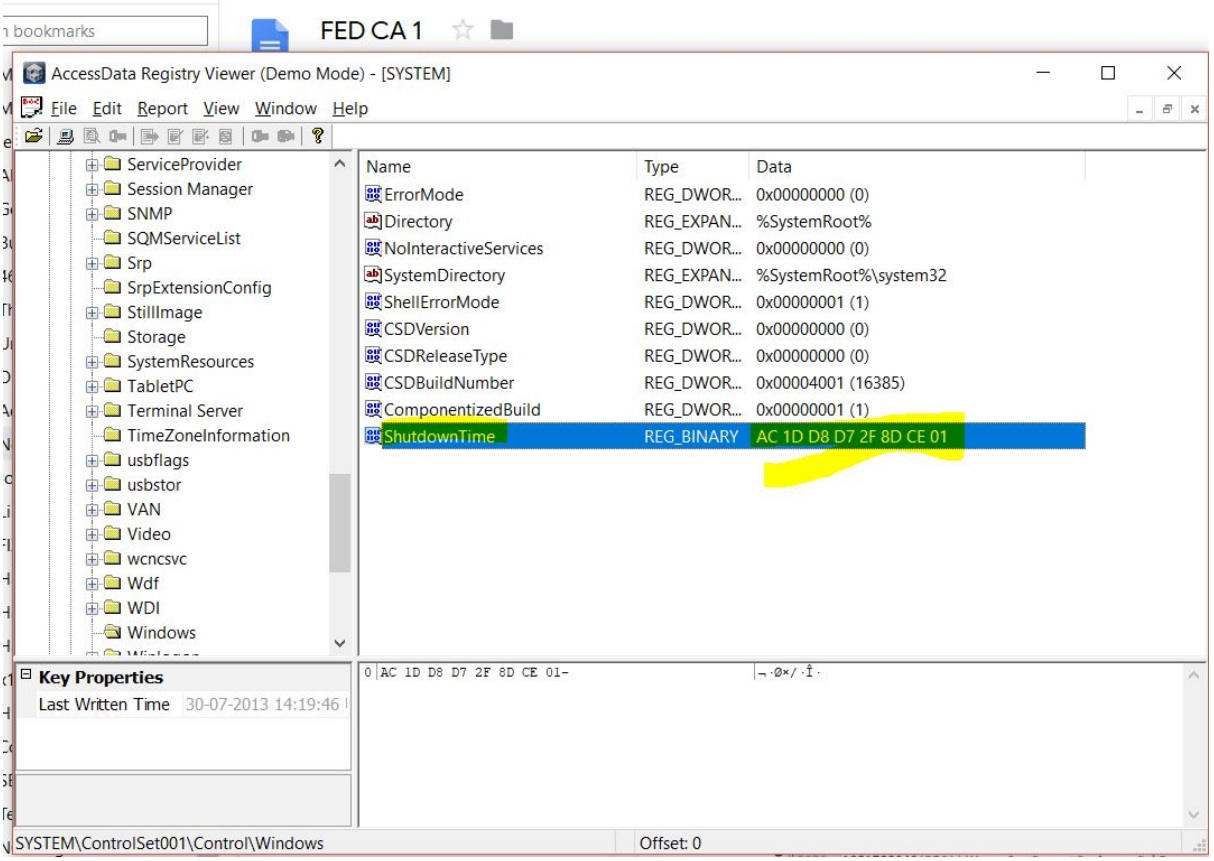


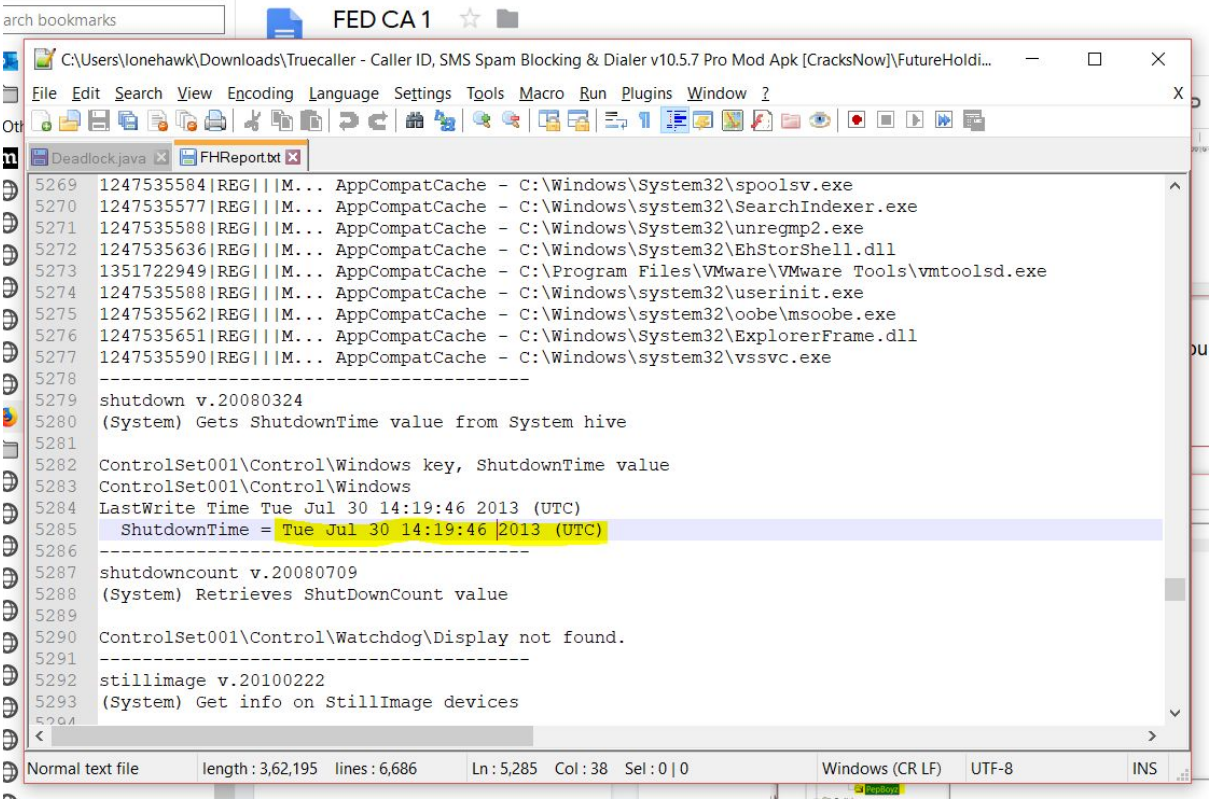
7. Who was the last user to logon into PC?

Possible Answer	Admin
Considerations	HKLM\SAM\Domains\Account\Users\F KeyBytes



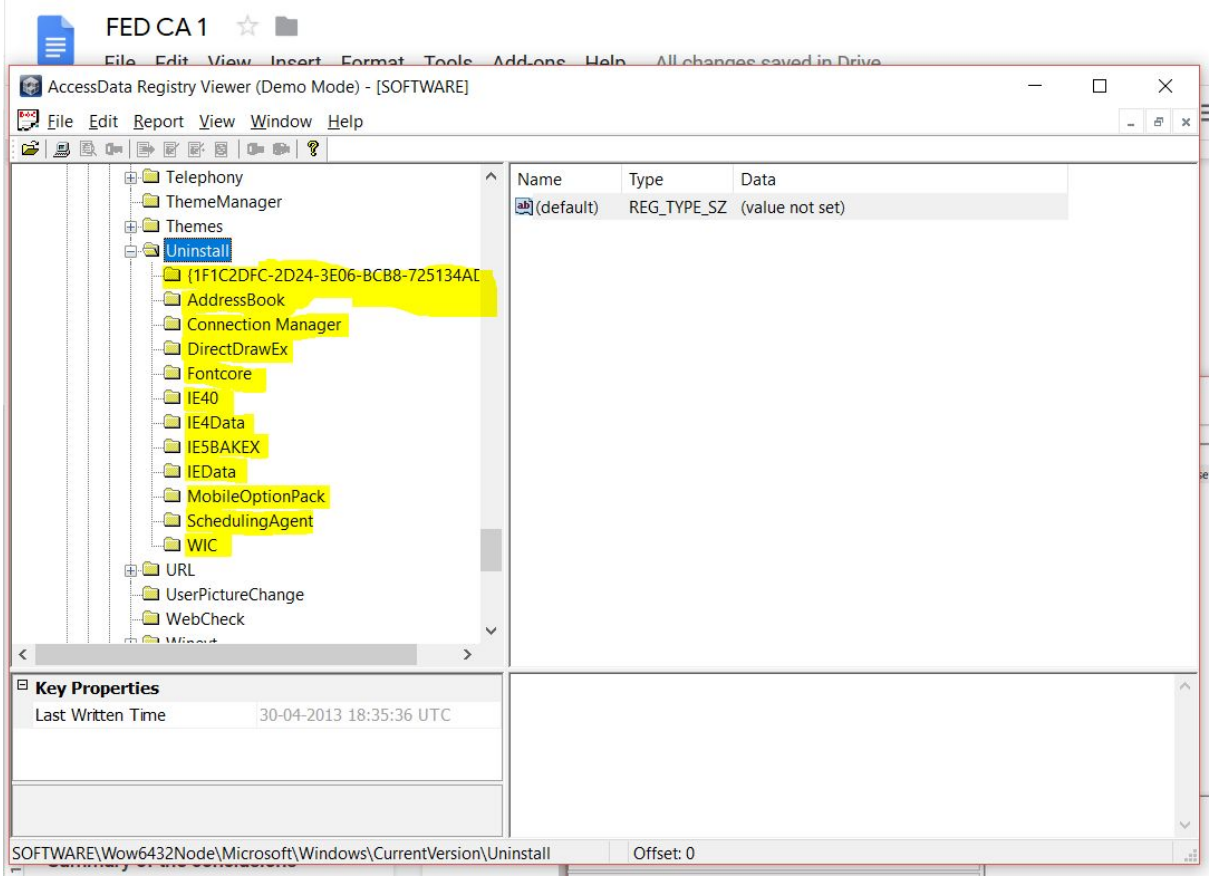
8. When was the last recorded shutdown date/time?





	Possible Answer	Tue Jul 30 14:19:46 2013 (UTC)
	Considerations	HKLM\SYSTEM\ControlSet###\Control\Windows (value: ShutdownTime)

9. What applications were installed?



Timestamp	Program Name & Version	Installation Path
2013-04-30 21:30:00 BST	DXM_Runtime	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 21:30:00 BST	MPlayer2	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE

2013-04-30 18:37:53 BST	VMware Tools v.9.2.2.18018	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 18:36:06 BST	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	AddressBook	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	Connection Manager	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	DirectDrawEx	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	Fontcore	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IE40	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IE4Data	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IE5BAKEX	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IEData	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	MobileOptionPack	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	SchedulingAgent	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE

2009-07-14 04:53:26 BST	WIC	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 18:35:36 BST	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	AddressBook	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	Connection Manager	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	DirectDrawEx	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	Fontcore	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IE40	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IE4Data	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IE5BAKEX	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IEData	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	MobileOptionPack	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	SchedulingAgent	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE

2009-07-14 04:53:25 BST	WIC	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-07-30 19:51:21 BST	MPlayer2	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 21:30:00 BST	DXM_Runtime	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 18:37:53 BST	VMware Tools v.9.2.2.18018	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 18:36:06 BST	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	AddressBook	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	Connection Manager	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	DirectDrawEx	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	Fontcore	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IE40	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IE4Data	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	IE5BAKEX	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE

2009-07-14 04:53:26 BST	IEData	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	MobileOptionPack	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	SchedulingAgent	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:26 BST	WIC	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-07-30 20:06:49 BST	AccessData FTK Imager v.3.1.3.2	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2013-04-30 18:35:36 BST	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	AddressBook	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	Connection Manager	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	DirectDrawEx	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	Fontcore	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IE40	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IE4Data	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE

2009-07-14 04:53:25 BST	IE5BAKEX	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	IEData	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	MobileOptionPack	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	SchedulingAgent	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
2009-07-14 04:53:25 BST	WIC	/LogicalFileSet1/C___NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE

Considerations: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\~
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\~

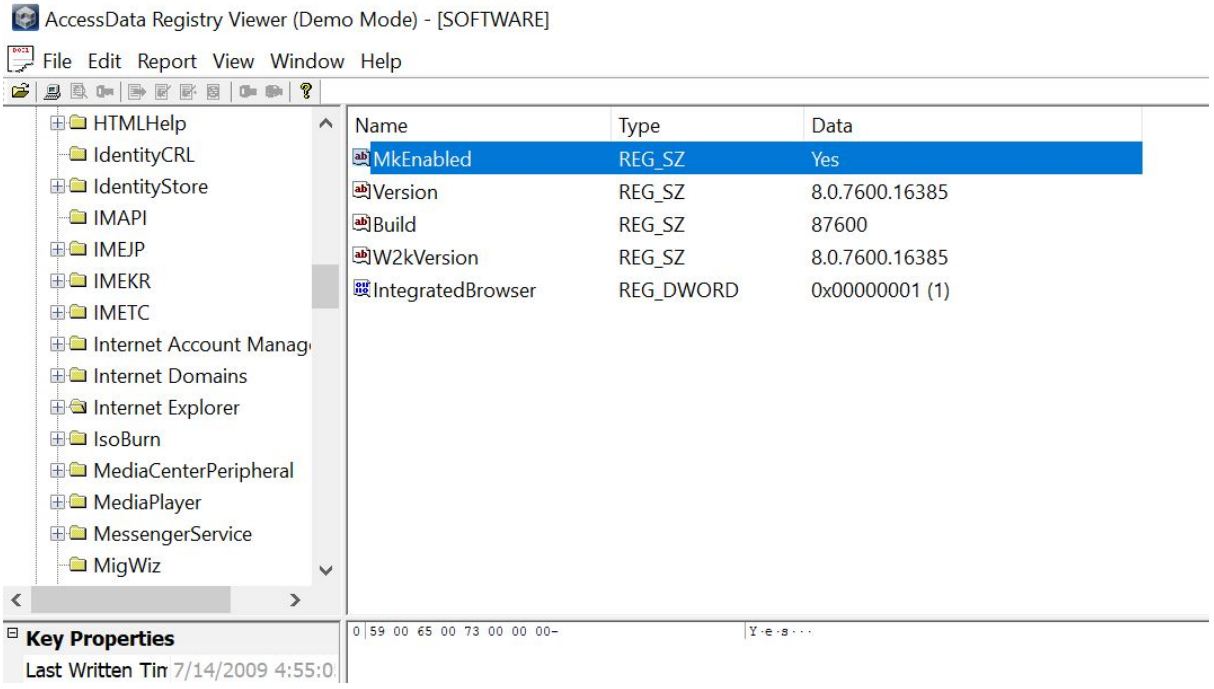
10. List application execution logs. (Executable path, execution time, execution count...)

```
C:\Windows\system32\msiexec.exe  Tue Jul 14 01:39:21 2009 Z  Executed
C:\Windows\System32\msdtc.exe  Tue Jul 14 01:39:21 2009 Z  Executed
C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe  Tue May  1 17:12:56 2012 Z  Executed
C:\Users\Admin\AppData\Local\Temp\unattend.cmd  Tue Apr 30 18:22:30 2013 Z
C:\Windows\System32\networkexplorer.dll  Tue Jul 14 01:41:52 2009 Z
C:\Windows\System32\ieframe.dll  Tue Jul 14 01:41:06 2009 Z
C:\Windows\System32\wsqmcons.exe  Tue Jul 14 01:39:57 2009 Z  Executed
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe  Wed Jun 10 21:23:09 2009 Z  Executed
C:\Users\Admin\AppData\Local\Temp\{44D55920-B223-4702-81D9-4C07108A3C27}~setup\vcredist_x86.exe  Tue Apr 30 18:35:15 2013 Z  Executed
C:\Windows\System32\fontext.dll  Tue Jul 14 01:40:54 2009 Z
C:\Program Files\VMware\VMware Tools\TPVCGateway.exe  Tue May  1 17:12:56 2012 Z  Executed
C:\Windows\syswow64\MsiExec.exe  Tue Jul 14 01:14:25 2009 Z  Executed
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe  Wed Jun 10 20:39:58 2009 Z  Executed
c:\030743edcff2699d20616e2e\install.exe  Sun Jul 12 07:55:40 2009 Z  Executed
c:\144dd22db986c04925ead27956\MpSigStub.exe  Tue Mar 12 05:10:55 2013 Z  Executed
C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat  Wed Oct 31 22:35:35 2012 Z
C:\Windows\WinSxS\amd64_netfx-clrgc_b03f5f7f11d50a3a_6.1.7600.16385_none_ada52b8ba0da82ba\clrgc.exe  Wed Jun 10 20:39:44 2009 Z  Executed
C:\Windows\system32\odbcad32.exe  Tue Jul 14 01:39:26 2009 Z
C:\Windows\system32\lsm.exe  Tue Jul 14 01:39:16 2009 Z  Executed
C:\Windows\System32\syncui.dll  Tue Jul 14 01:41:54 2009 Z
C:\Windows\System32\regsvr32.exe  Tue Jul 14 01:39:29 2009 Z  Executed
C:\Windows\system32\runonce.exe  Tue Jul 14 01:39:31 2009 Z  Executed
C:\Windows\System32\vds.exe  Tue Jul 14 01:39:49 2009 Z  Executed
C:\Windows\system32\services.exe  Tue Jul 14 01:39:37 2009 Z  Executed
C:\Windows\System32\prnfldr.dll  Tue Jul 14 01:41:53 2009 Z
C:\Windows\system32\mstsc.exe  Tue Jul 14 01:39:24 2009 Z
C:\Windows\System32\sbe.dll  Tue Jul 14 01:41:53 2009 Z
C:\Windows\System32\wpdshext.dll  Tue Jul 14 01:41:57 2009 Z
C:\Windows\system32\rstrui.exe  Tue Jul 14 01:39:31 2009 Z  Executed
C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe  Wed Oct 31 22:35:49 2012 Z  Executed
C:\Windows\SysWOW64\ie4uinit.exe  Tue Jul 14 01:14:21 2009 Z  Executed
C:\Windows\system32\UserAccountControlSettings.exe  Tue Jul 14 01:39:48 2009 Z  Executed
C:\Windows\SoftwareDistribution\Download\Install\mpas-fe.exe  Tue Apr 30 05:36:10 2013 Z  Executed
C:\Windows\system32\wuapp.exe  Tue Jul 14 01:39:58 2009 Z  Executed
C:\Windows\syswow64\WOWReg32.exe  Mon Jul 13 23:16:09 2009 Z  Executed
C:\Windows\system32\wermgr.exe  Tue Jul 14 01:39:51 2009 Z  Executed
C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe  Tue May  1 17:12:56 2012 Z  Executed
```

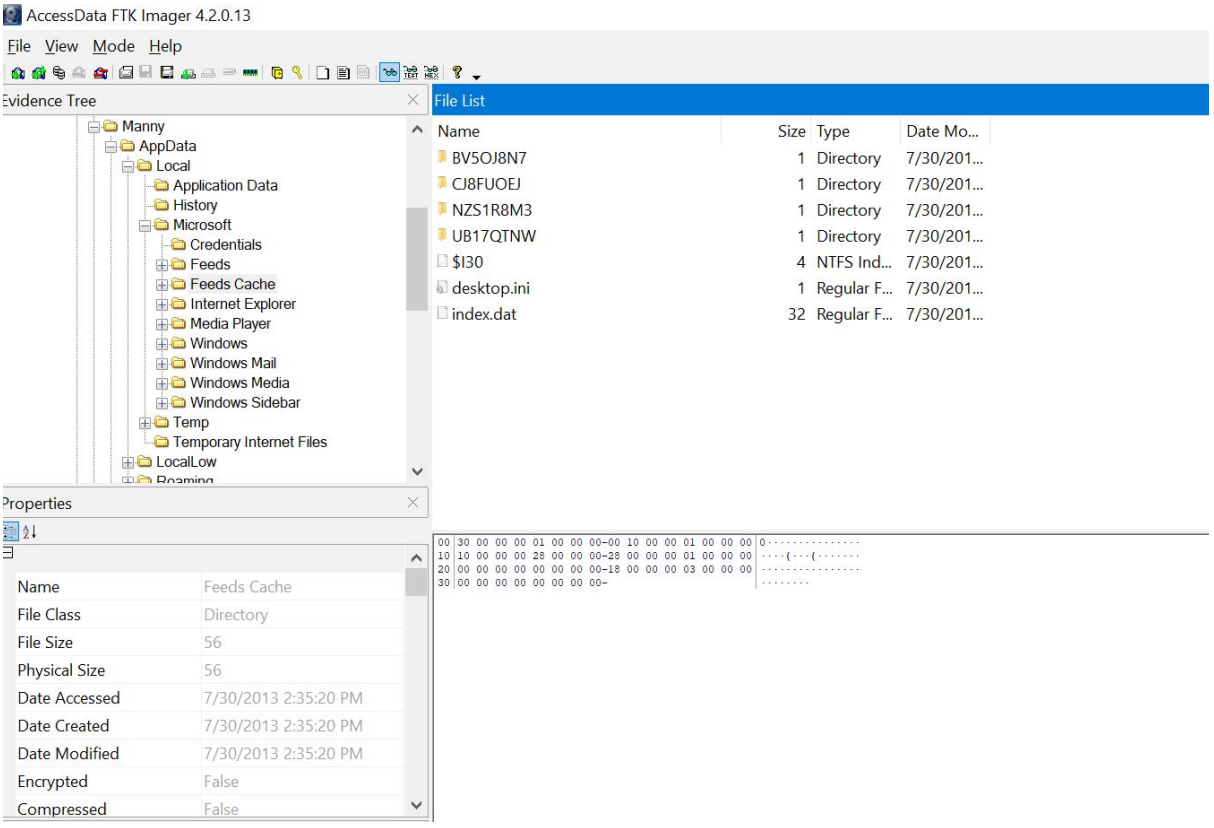
11. List all traces about the system on/off and the user logon/logoff.

The registry is missing for power functions.

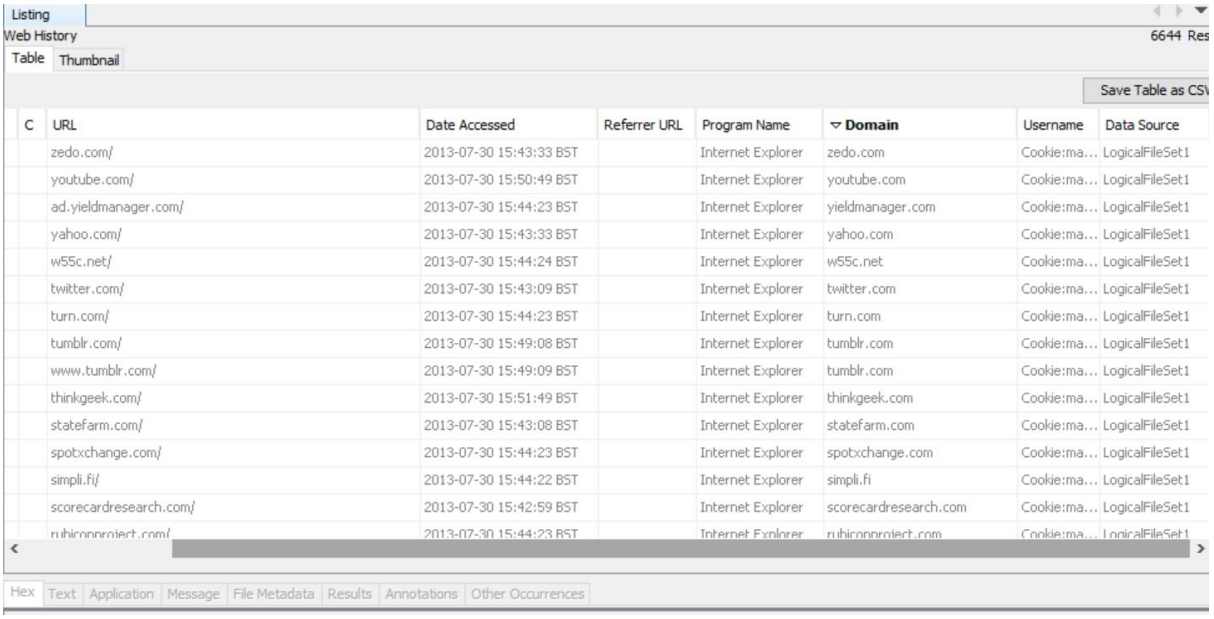
12. What web browsers were used?



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



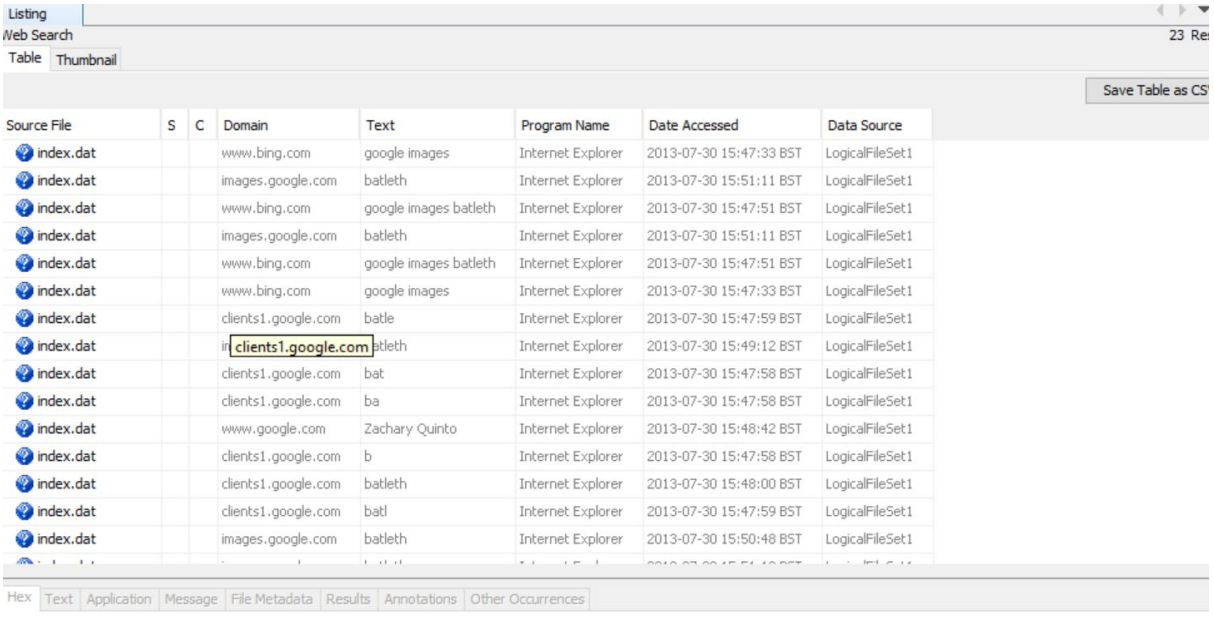
14. What websites were the suspect accessing? (Timestamp, URL...)



C	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source
	zedo.com/	2013-07-30 15:43:33 BST		Internet Explorer	zedo.com	Cookie:ma...	LogicalFileSet1
	youtube.com/	2013-07-30 15:50:49 BST		Internet Explorer	youtube.com	Cookie:ma...	LogicalFileSet1
	ad.yieldmanager.com/	2013-07-30 15:44:23 BST		Internet Explorer	yieldmanager.com	Cookie:ma...	LogicalFileSet1
	yahoo.com/	2013-07-30 15:43:33 BST		Internet Explorer	yahoo.com	Cookie:ma...	LogicalFileSet1
	w55c.net/	2013-07-30 15:44:24 BST		Internet Explorer	w55c.net	Cookie:ma...	LogicalFileSet1
	twitter.com/	2013-07-30 15:43:09 BST		Internet Explorer	twitter.com	Cookie:ma...	LogicalFileSet1
	turn.com/	2013-07-30 15:44:23 BST		Internet Explorer	turn.com	Cookie:ma...	LogicalFileSet1
	tumblr.com/	2013-07-30 15:49:08 BST		Internet Explorer	tumblr.com	Cookie:ma...	LogicalFileSet1
	www.tumblr.com/	2013-07-30 15:49:09 BST		Internet Explorer	tumblr.com	Cookie:ma...	LogicalFileSet1
	thinkgeek.com/	2013-07-30 15:51:49 BST		Internet Explorer	thinkgeek.com	Cookie:ma...	LogicalFileSet1
	statefarm.com/	2013-07-30 15:43:08 BST		Internet Explorer	statefarm.com	Cookie:ma...	LogicalFileSet1
	spotxchange.com/	2013-07-30 15:44:23 BST		Internet Explorer	spotxchange.com	Cookie:ma...	LogicalFileSet1
	simpli.fi/	2013-07-30 15:44:22 BST		Internet Explorer	simpli.fi	Cookie:ma...	LogicalFileSet1
	scorecardresearch.com/	2013-07-30 15:42:59 BST		Internet Explorer	scorecardresearch.com	Cookie:ma...	LogicalFileSet1
	rubiconproject.com/	2013-07-30 15:44:23 BST		Internet Explorer	rubiconproject.com	Cookie:ma...	LogicalFileSet1

Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

15. List all search keywords using web browsers. (Timestamp, URL, keyword...)

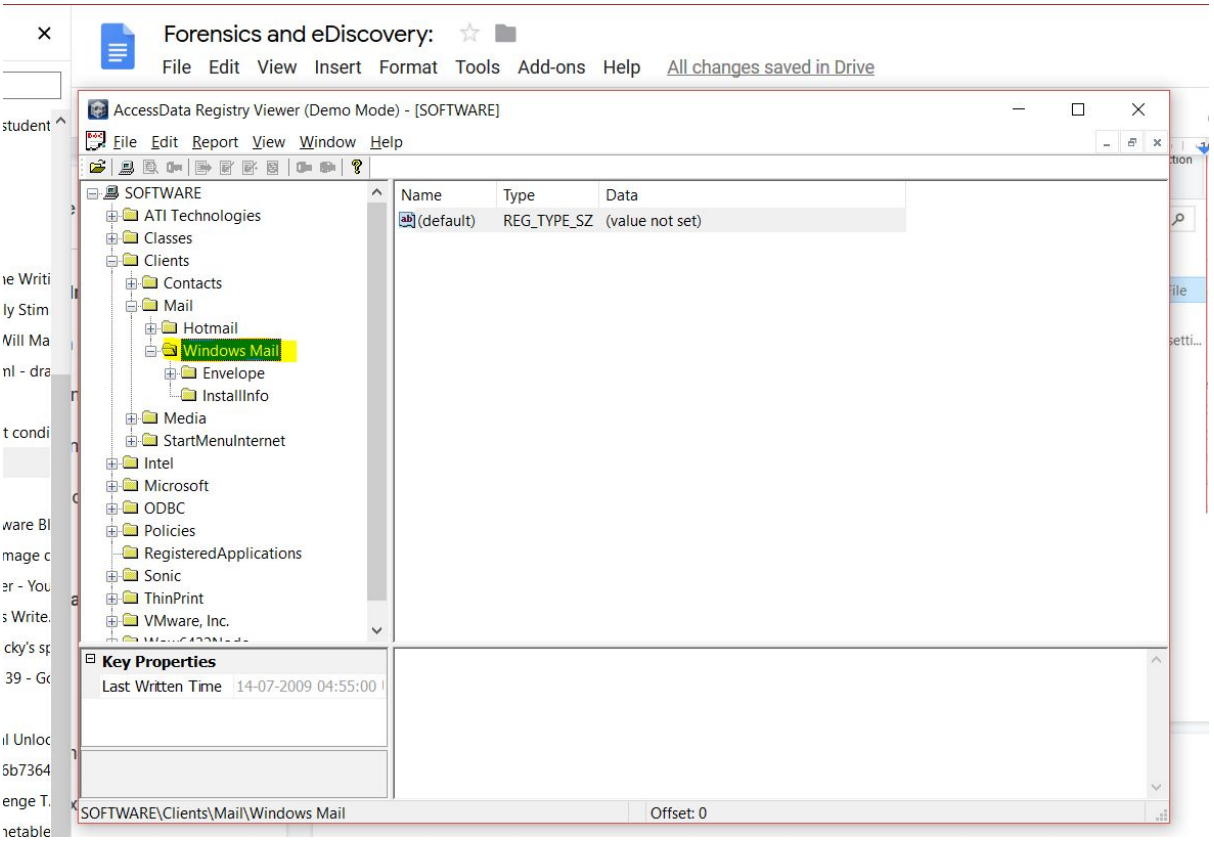


Source File	S	C	Domain	Text	Program Name	Date Accessed	Data Source
index.dat			www.bing.com	google images	Internet Explorer	2013-07-30 15:47:33 BST	LogicalFileSet1
index.dat			images.google.com	batleth	Internet Explorer	2013-07-30 15:51:11 BST	LogicalFileSet1
index.dat			www.bing.com	google images batleth	Internet Explorer	2013-07-30 15:47:51 BST	LogicalFileSet1
index.dat			images.google.com	batleth	Internet Explorer	2013-07-30 15:51:11 BST	LogicalFileSet1
index.dat			www.bing.com	google images batleth	Internet Explorer	2013-07-30 15:47:51 BST	LogicalFileSet1
index.dat			www.bing.com	google images	Internet Explorer	2013-07-30 15:47:33 BST	LogicalFileSet1
index.dat			clients1.google.com	batle	Internet Explorer	2013-07-30 15:47:59 BST	LogicalFileSet1
index.dat			clients1.google.com	batleth	Internet Explorer	2013-07-30 15:49:12 BST	LogicalFileSet1
index.dat			clients1.google.com	bat	Internet Explorer	2013-07-30 15:47:58 BST	LogicalFileSet1
index.dat			clients1.google.com	ba	Internet Explorer	2013-07-30 15:47:58 BST	LogicalFileSet1
index.dat			www.google.com	Zachary Quinto	Internet Explorer	2013-07-30 15:48:42 BST	LogicalFileSet1
index.dat			clients1.google.com	b	Internet Explorer	2013-07-30 15:47:58 BST	LogicalFileSet1
index.dat			clients1.google.com	batleth	Internet Explorer	2013-07-30 15:48:00 BST	LogicalFileSet1
index.dat			clients1.google.com	batl	Internet Explorer	2013-07-30 15:47:59 BST	LogicalFileSet1
index.dat			images.google.com	batleth	Internet Explorer	2013-07-30 15:50:48 BST	LogicalFileSet1

Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

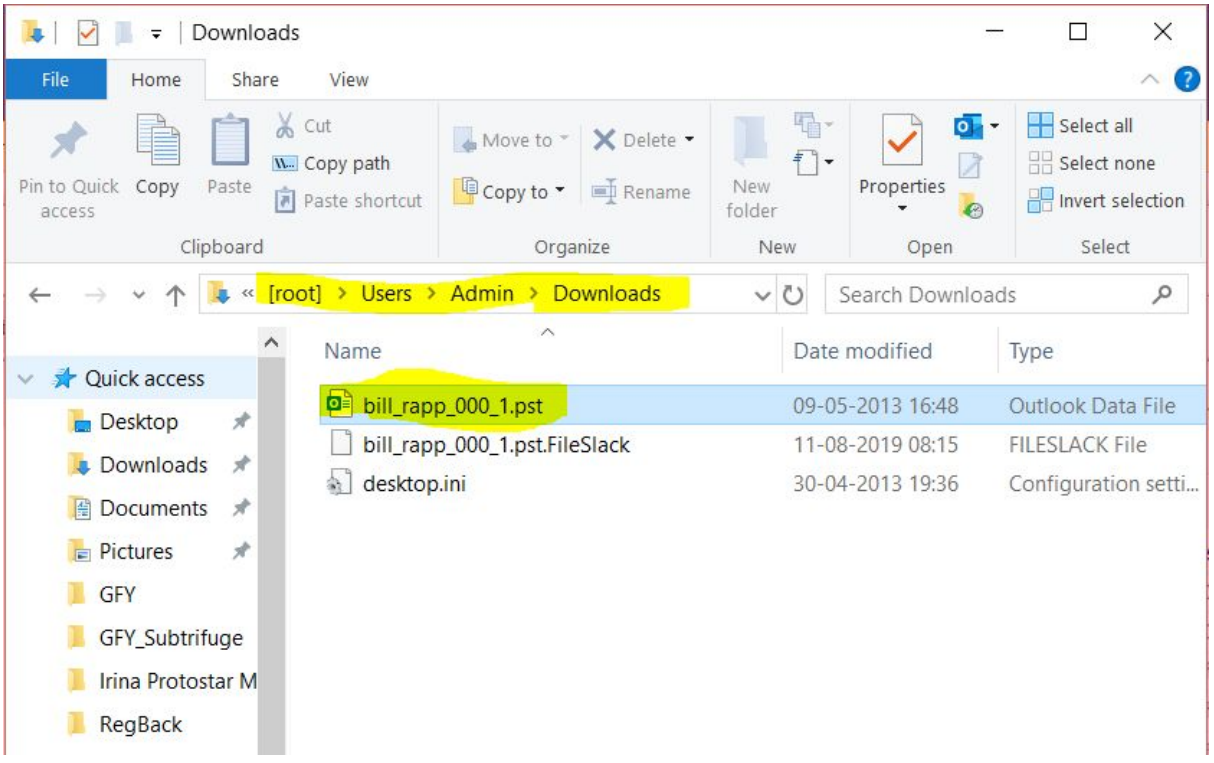
16. List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)
Unable to recover

17. What application was used for e-mail communication?

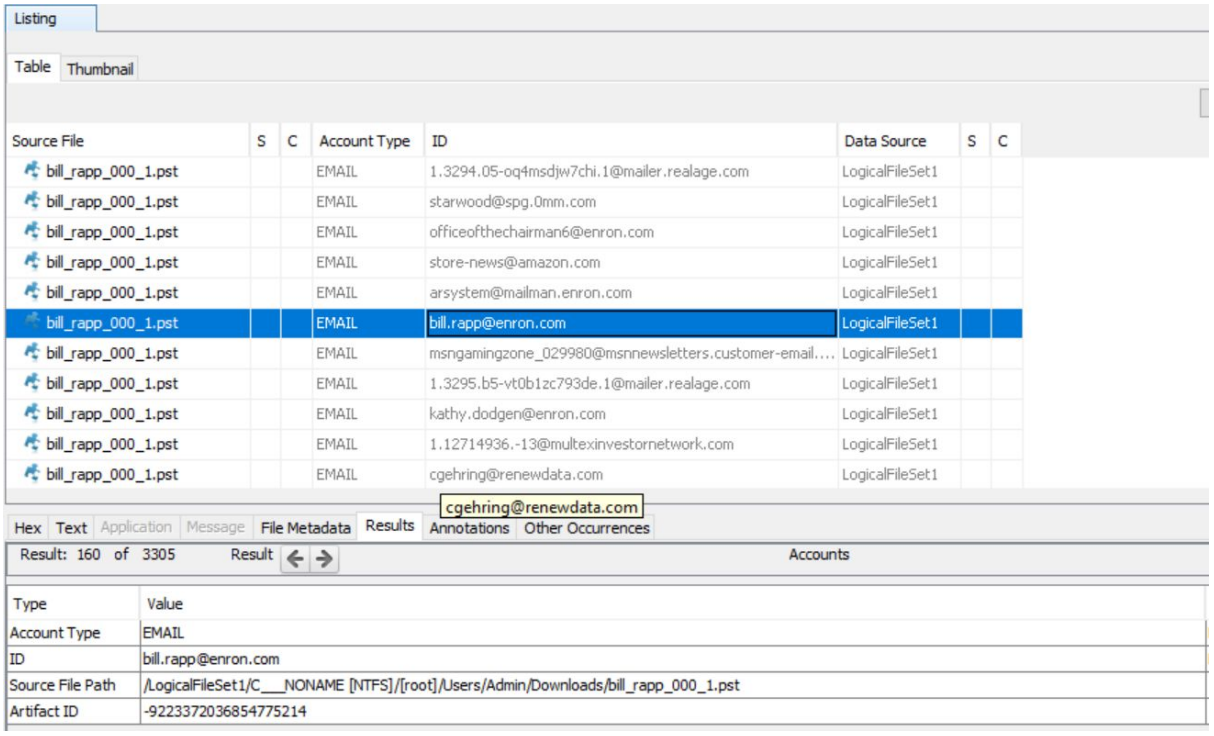


Rasphone.exe

18. Where is the e-mail file located?



19. What was the e-mail account used by the suspect?



20. List all the e-mails of the suspect. If possible, identify deleted e-mails. (You can identify the following items: Timestamp, From, To, Subject, Body, and Attachment)

Unable to recover

21. List external storage devices attached to PC.