

## Module 3 Test

## File System and OS Artifacts

Online monitoring of extremist websites has identified an individual that may be linked with possible extremist organizations. Subpoena requests to the internet service providers based on the suspect's IP address have lead investigators to a specific residence.

A team entered suspect's residence and found a powered down Dell laptop computer. The suspect was not present. Triage indicated that files of possible value might be found and that a full forensic exam would be beneficial.

They were able to create a forensic image on scene and bring it back for you to analyze. Your task is to analyze the forensic image file using any tools/techniques we have covered this semester, and answer the following questions. Please be specific and include where you found the answer. Use screenshots were appropriate or convenient.

Assume all the tools we have been using (either in assignments, or mentioned in lectures) have been validated and approved for use. When analyzing a multipart forensic image file, you typically only need to add/point to the first (\*.E01) file, and make sure all the image files are together in one folder.

Each question is worth 5 points.

1. What is the acquisition and verification hash value of the image?

Acquisition = a89e3c6dea879a7171c647598cef1d77

Verification = 9fd1a3bd0eac7e611a8b14569b74717

The screenshot shows the AccessData FTK Imager 3.40.1 interface. The Evidence Tree on the left lists the image file 'Laptop Image 1.E01' and its partitions. The File List on the right shows the contents of the image. The Hex Value Interpreter at the bottom displays the raw data of the image. The 'Drive/Image Verify Results' dialog box is open, showing the following verification details:

Name	Value
Name	Laptop Image 1.E01
Sector count	136301488
<b>MDS Hash</b>	
Computed hash	9f51a3bd0eac7e611a8b14569b74717
Stored verification hash	a89e3c6dea879a7171c647598cef1d77
Verify result	n/a - bad sectors found
<b>SHA1 Hash</b>	
Computed hash	4c43e13c053820d1a06c9f0117c9e994c
Stored verification hash	63e9e143a8f2b5661172e2a9b0421134
Verify result	n/a - bad sectors found
<b>Bad Sector List</b>	
Bad sector(s)	4657472-4660543
Bad sector(s)	12668312-12679423
<b>Stored verification hash</b>	
The hash computed during image acquisition and stored inside the image	

JOHN-PC

Registry Explorer v6.7.1.0

File
Tools
Options
Bookmarks (5/10)
View
Help

Registry hives (1)

Available bookmarks (5/10)

Key name	# values	Last write timestamp
C:\Users\Andres\Desktop\...		
ControlSet001	0	2/23/2012 11:36:50 PM +00:00
Control	8	2/23/2012 12:25:34 PM +00:00
ACPI	1	7/14/2009 4:37:09 AM +00:00
ADP	7	7/14/2009 4:41:46 AM +00:00
AppID	0	7/14/2009 4:42:10 AM +00:00
Arbiters	0	7/14/2009 4:37:09 AM +00:00
BackupRestore	0	7/14/2009 4:37:09 AM +00:00
Class	0	2/7/2012 6:00:25 PM +00:00
CHF	1	7/14/2009 4:37:09 AM +00:00
CoDeviceInstallers	17	2/7/2012 6:00:23 PM +00:00
COM Name Arbitrator	1	2/7/2012 5:58:50 PM +00:00
ComputerName	0	2/23/2012 12:25:34 PM +00:00
ComputerName	2	2/7/2012 6:10:14 PM +00:00
ContentIndex	0	7/14/2009 4:37:09 AM +00:00
CrashControl	8	7/14/2009 4:37:09 AM +00:00
CrashDeviceClass	0	2/7/2012 5:58:21 PM +00:00
Cryptography	0	7/14/2009 4:37:09 AM +00:00
DeviceClasses	0	2/18/2012 11:40:53 AM +00:00
DeviceOverrides	0	7/14/2009 4:37:09 AM +00:00
Diagnostics	0	7/14/2009 4:37:09 AM +00:00
Dm	0	7/14/2009 4:37:09 AM +00:00
Errata	1	7/14/2009 4:41:22 AM +00:00
FileSystem	20	7/14/2009 4:37:09 AM +00:00
FileSystemVolumes	1	7/14/2009 4:37:09 AM +00:00
GraphicsDrivers	2	2/7/2012 3:18:54 PM +00:00
GroupOrderList	48	2/7/2012 4:18:56 PM +00:00
HAL	16	2/23/2012 12:25:34 PM +00:00
IDConfigDB	2	2/23/2012 12:25:34 PM +00:00
KeyboardLayout	0	7/14/2009 4:37:09 AM +00:00
KeyboardLayouts	0	7/14/2009 4:37:09 AM +00:00
Lsa	18	2/22/2012 4:55:47 PM +00:00
LoadIntersectCo...	0	7/14/2009 4:37:09 AM +00:00
LoadIntersectCo...	1	7/14/2009 4:37:09 AM +00:00
MediaCategories	0	2/7/2012 5:58:12 PM +00:00
MediaDRM	0	4/12/2011 2:25:00 AM +00:00
MediaInterfaces	0	2/7/2012 5:58:32 PM +00:00
MediaTypes	0	7/14/2009 4:37:09 AM +00:00
MediaTypes	0	4/12/2011 2:25:00 AM +00:00
MobilePC	0	4/12/2011 2:25:00 AM +00:00
MPDEV	1	11/20/2010 9:32:38 PM +00:00
MSDTC	0	7/14/2009 4:37:09 AM +00:00
NLS	0	4/12/2011 2:26:04 AM +00:00
NetCfgJfx	0	7/14/2009 4:37:28 AM +00:00
NetTrace	0	7/14/2009 4:42:05 AM +00:00

Values

Drag a column header here to group by that column

Value name	Value type	Data	Value stack
(default)	RegDz	mmmmvc	00-00-00-00
ComputerName	RegDz	JOHN-PC	39-00-4D-00-44-00-54-00-4B-00-4D-00-31-03-00-00-00-00-00-00

Type viewer

Stack viewer

Value name	(default)
Value type	RegDz
Stack	00-00-00-00
Value	mmmmvc

Key: ControlSet001\Control\ComputerName\ComputerName

Value

Collapse all hives

Last write: 2/7/2012 6:10:14 PM +00:00

2 of 2 values shown (100.00%)

Load complete

Hidden keys 0

3. What version of Windows is this user running?

## Windows 7 Professional

Registry Explorer v6.7.1.0

File Tools Options Bookmarks (2/1) View Help

Registry hives (2) Available bookmarks (0/0)

Key name	# values	Last write timestamp
Sensors	1	4/12/2011 3:25:00 AM +00...
Shared	0	2/7/2012 3:23:49 PM +00...
Shared Tools	1	2/7/2012 3:23:03 PM +00...
Shared Tools Location	1	2/7/2012 3:54:30 PM +00...
SideShow	1	4/12/2011 3:25:00 AM +00...
Speech	0	4/12/2011 3:16:04 AM +00...
ISQNCient	1	2/7/2012 3:59:34 PM +00...
Sync Framework	0	7/14/2009 4:37:08 AM +00...
System	2	2/7/2012 3:55:48 PM +00...
SystemCertificates	0	2/7/2012 3:18:22 PM +00...
TabletService	0	7/14/2009 4:37:08 AM +00...
TabletTip	2	4/12/2011 2:25:13 AM +00...
Terminal	0	7/14/2009 4:39:42 AM +00...
Terminal Server Client	0	7/14/2009 4:37:08 AM +00...
TSF Shared	0	7/14/2009 4:37:08 AM +00...
TSM	1	2/7/2012 3:16:54 PM +00...
TPG	0	4/12/2011 3:25:00 AM +00...
Tpm	0	7/14/2009 4:37:08 AM +00...
Tracing	1	12/20/2012 3:13:39 PM +00...
Transaction Server	0	7/14/2009 4:37:08 AM +00...
TV System Services	0	7/14/2009 4:37:08 AM +00...
UDRM	1	7/14/2009 4:37:08 AM +00...
UPnP Device Host	0	2/7/2012 3:25:49 PM +00...
VBA	1	2/7/2012 3:23:07 PM +00...
Virtual Machine	0	4/12/2011 3:24:13 AM +00...
VisualStudio	0	2/7/2012 3:23:08 PM +00...
WAB	0	7/14/2009 4:37:08 AM +00...
WBEH	3	11/20/2010 9:35:23 PM +00...
WDMMount	0	7/14/2009 4:37:08 AM +00...
Windows	0	2/7/2012 3:18:33 PM +00...
Windows Defender	4	2/7/2012 4:22:32 PM +00...
Windows Desktop Search	1	2/7/2012 4:10:23 PM +00...
Windows Mail	5	11/20/2010 9:35:23 PM +00...
Windows Media Device Manager	1	7/14/2009 4:37:08 AM +00...
Windows Media Foundation	0	7/14/2009 4:37:08 AM +00...
Windows Media Player HGS	0	7/14/2009 4:37:08 AM +00...
Windows Messaging Subsystem	6	2/7/2012 3:19:40 PM +00...
Windows NT	4	7/14/2009 4:41:12 AM +00...
CurrentVersion	21	2/22/2012 9:09:56 PM +00...
Windows Photo Viewer	0	7/14/2009 4:37:08 AM +00...
Windows Portable Devices	0	7/14/2009 4:37:08 AM +00...
Windows Script Host	0	7/14/2009 4:37:08 AM +00...
Windows Search	9	2/7/2012 4:18:11 PM +00...
Wsp	0	7/14/2009 4:37:08 AM +00...
Wslmrc	3	2/7/2012 3:25:48 PM +00...
Workspaces	0	7/14/2009 4:37:08 AM +00...

Values

Drag a column header here to group by that column

Value name	Value type	Data	Value slack
CurrentBuildNumber	RegDword	7601	74-00
CurrentType	RegDword	Multiprocessor Free	65-06-64-00-00-00-00-0A-08-00
CurrentVersion	RegDword	6.1	33-00-32-00
DigitalProductId	RegBinary	A4-05-08-00-63-00-00-00-30-33-37-31-20-32-32-32-32-30-36-35-39-31-20-32-38-36-34-33-35-06-AC-00...	00-00-00-00
EditorId	RegDword	Professional	00-00-00-00
InstallerType	RegDword	Client	00-00-00-00-00-00
InstallDate	RegDword	1328627562	65-72-00-00-00-00
PathName	RegDword	C:\Windows	00-00-00-00-00-00
ProductId	RegDword	93371-222-083912-86421	00-00-00-00
ProductType	RegDword	Windows 7 Professional	2A-01-68-05-2A-01
RegisteredOrganization	RegDword		
RegisteredOwner	RegDword	John	77-00-75-00-20-55-00-75-00-65-00-72-00-00-00-64-0F
SoftwareType	RegDword	System	33-00-32-00-5C-00
SystemRoot	RegDword	C:\Windows	00-00-00-00-00-00

Type viewer

Value name

ProductType

Value type

RegDword

Slack

2A-01-68-05-2A-01

Value

Windows 7 Professional

Key: Microsoft\Windows NT\CurrentVersion

Last write: 2/22/2012 9:09:56 PM +00:00 21 of 21 values shown (100.0%) Load complete

Value: ProductName

Collapse all Hives

Hidden keys 0

4. When was this version of Windows installed?

Data = 1328627562

UNIX Numeric = Tue, 07 Feb 2012 15:12:42

**\*Same picture used in question 3\***

5. Who is the registered owner of this computer?

John

**\*Same picture used in question 3\***

6. When was this computer last shut down?

RegBinary = AC-AC-C1-BC-A6-F1-CC-01

Win 64Bit Little Endian = Wed, 22 Feb 2012 21:12:52

The screenshot shows the Windows Registry Editor with the following details:

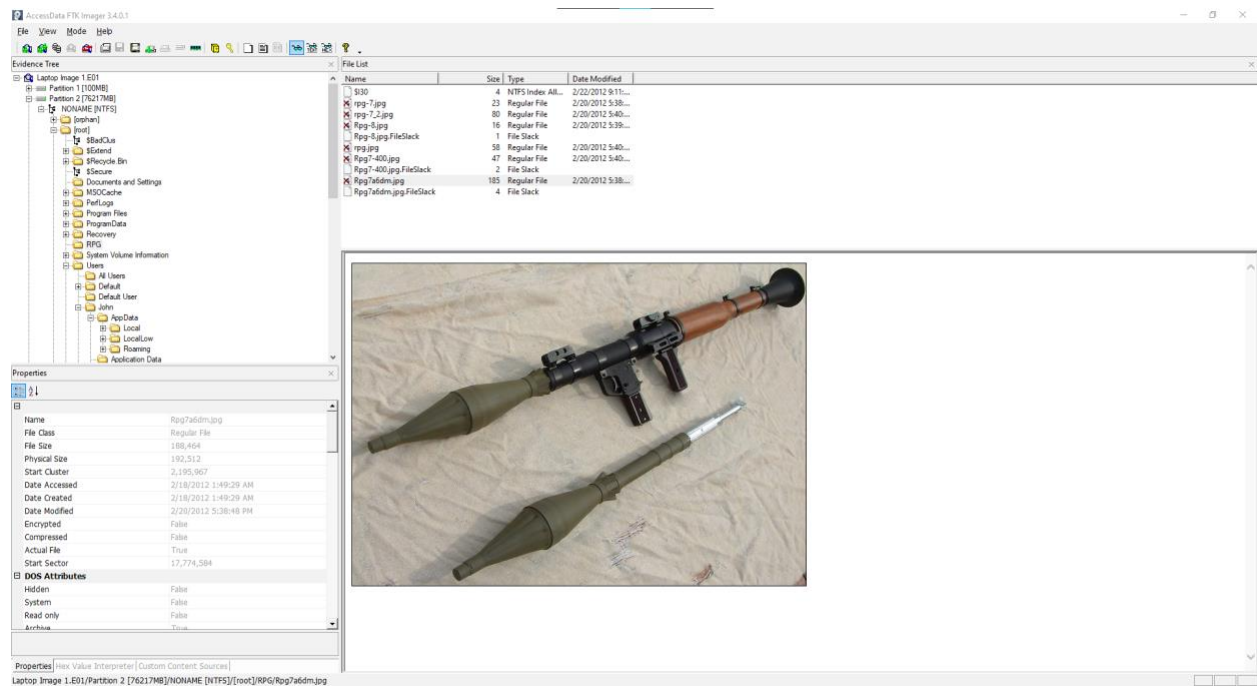
- Left pane (Tree view):** Expanded to `ControlSet001\Control\Windows`.
- Right pane (Values):** Shows the `ShutdownTime` value of type `RegBinary` with data `AC-AC-C1-BC-A6-F1-CC-01`.
- Bottom status bar:** Displays the key path `ControlSet001\Control\Windows`, the last write time `2/22/2012 9:12:52 PM +0000`, and the number of values shown (10 of 10).

7. When did the user last change their password?

25-32 Bytes = 46-8F-64-CC-FD-88-CB-01

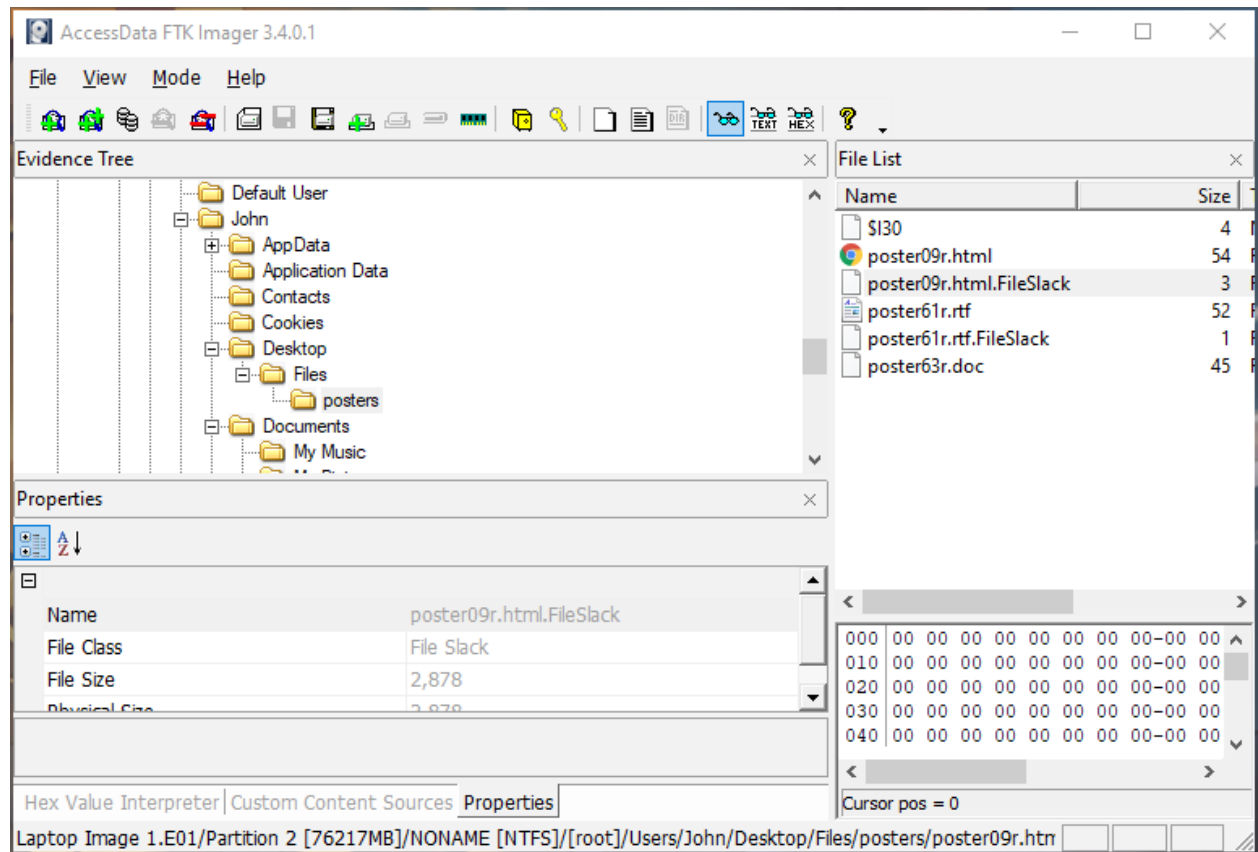
Win 64Bit Little Endian = Sat, 20 Nov 2010 21:56:34





10. Find the folder titled **posters**.

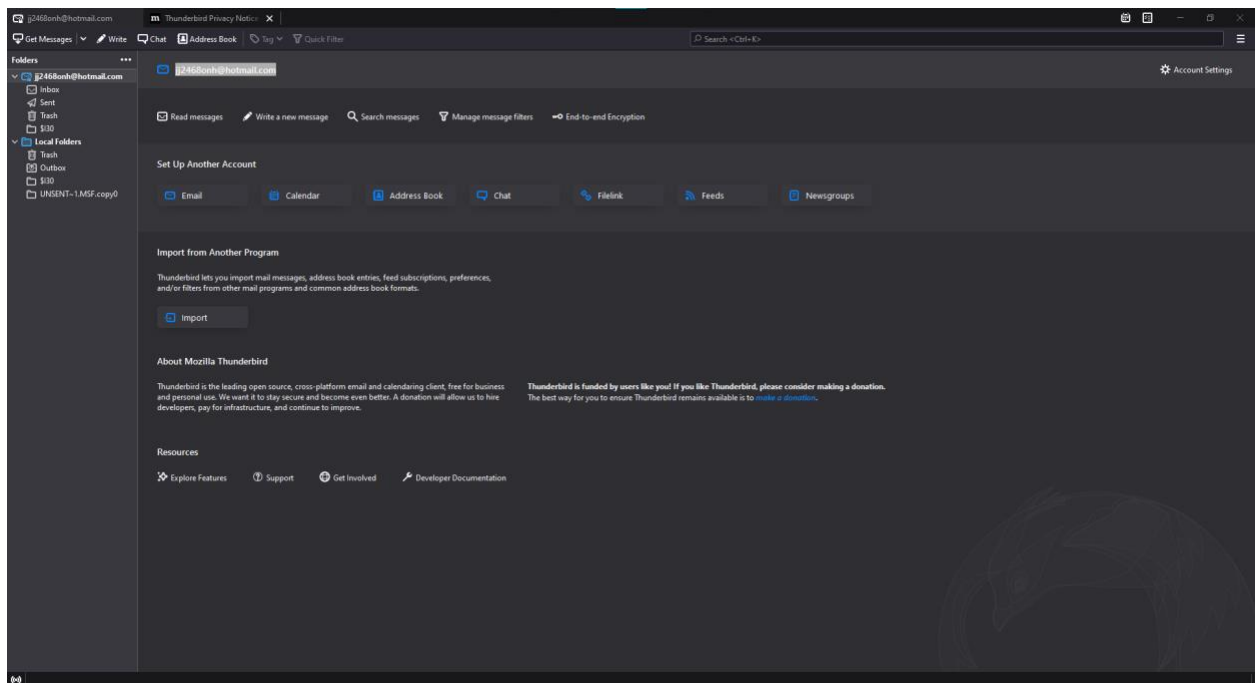
- What is the full path of this folder? (ie. C:\Windows\...)  
Users/John/Desktop/Files/posters



- b. Did the user try to hide the files in this folder? How?  
The user changed the file signatures of the files

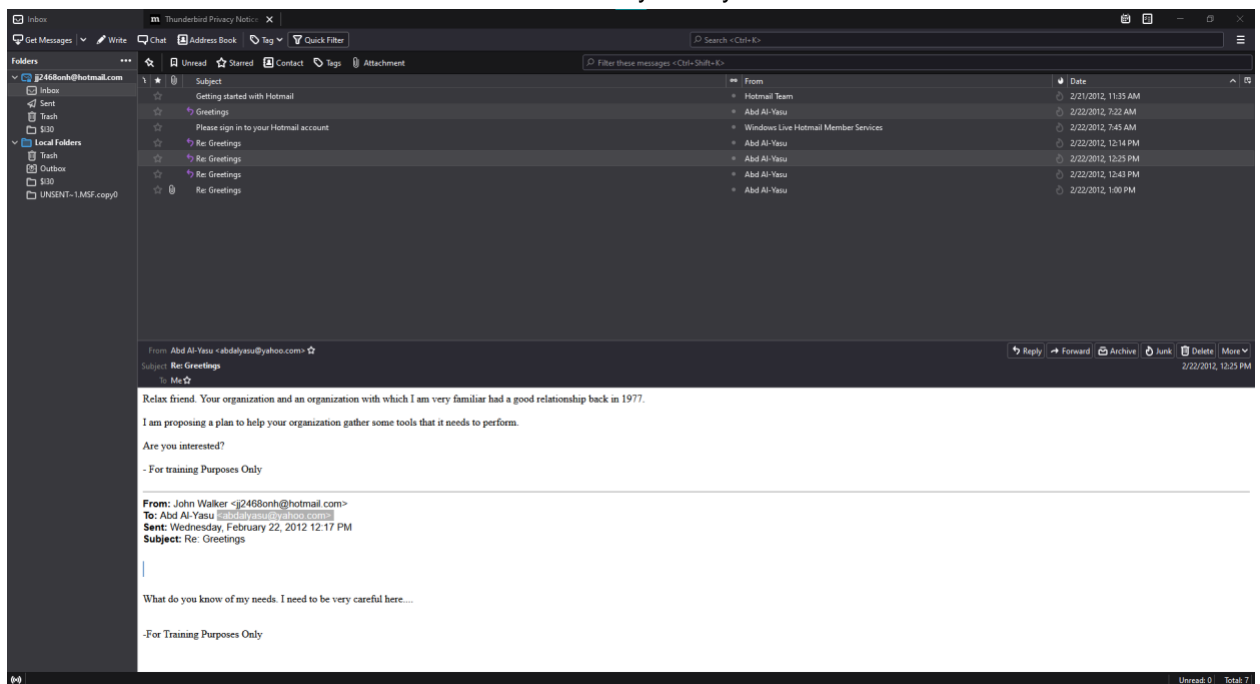
11. What is the users full email address?

jj2468onh@hotmail.com



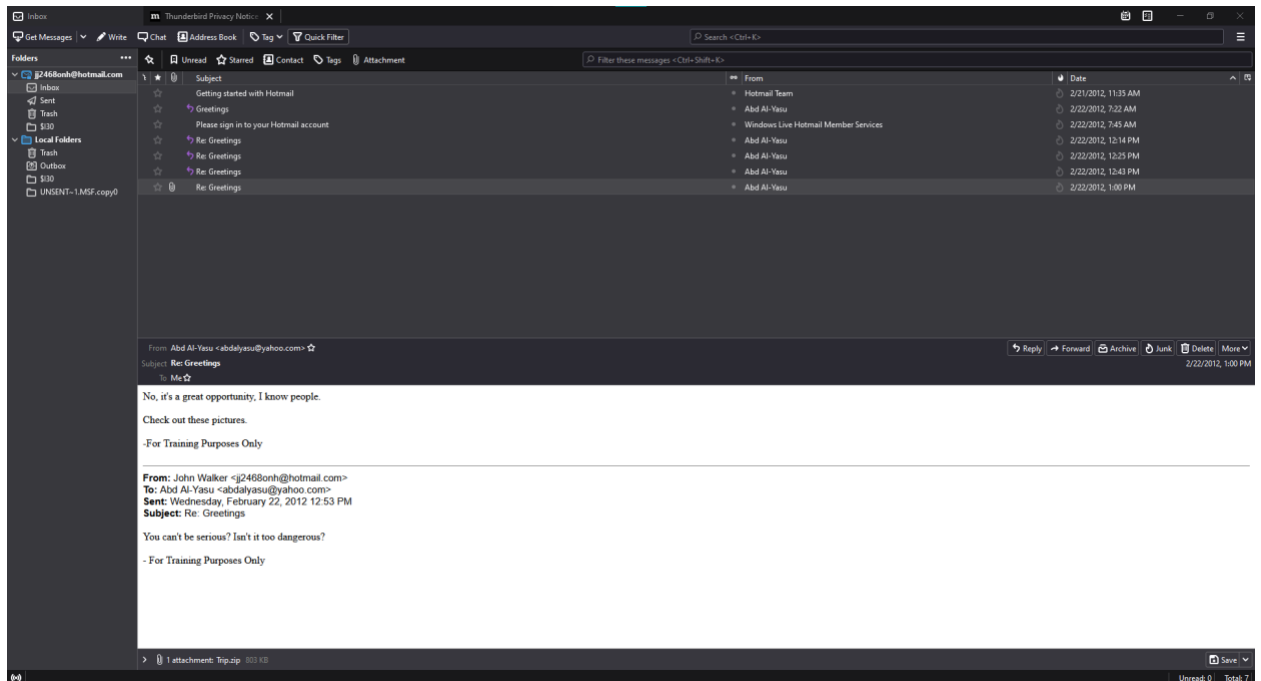
12. Who has the user been in contact with?

The user has been in contact with Abd Al-Yasu<abdalyasu@yahoo.com>



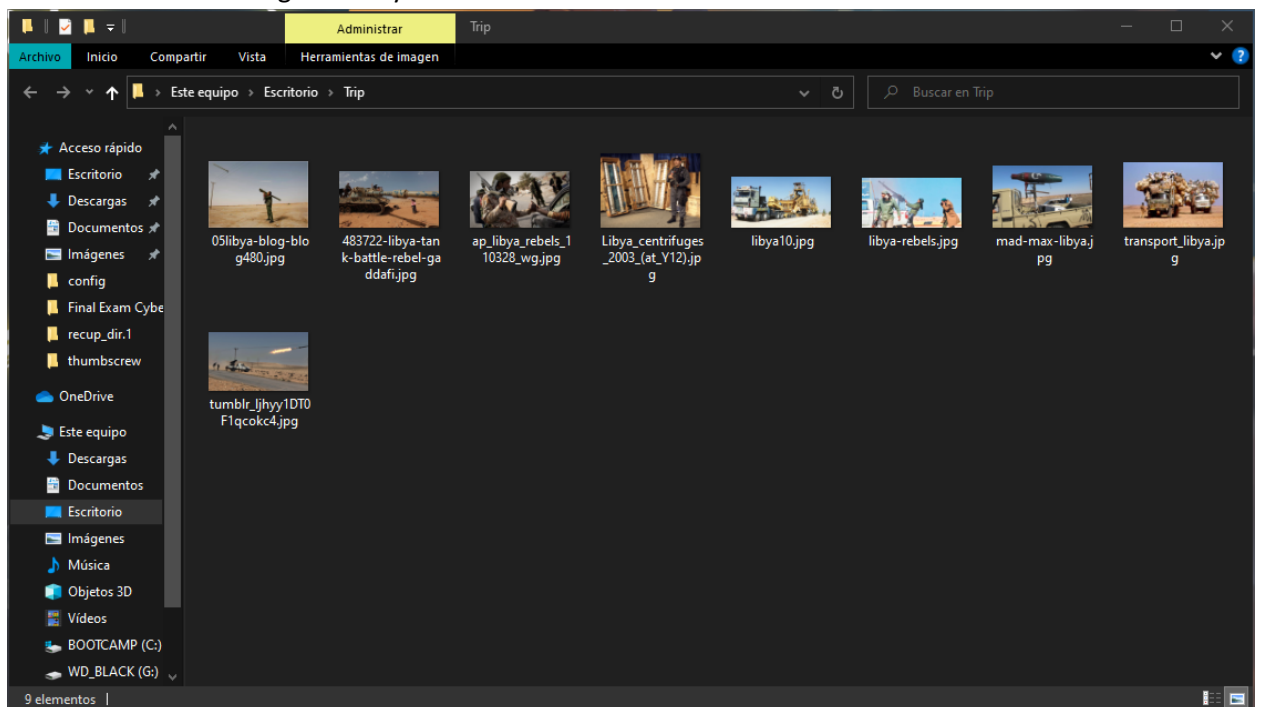
13. Where did the file Trip.zip come from?

The file Trip.zip came from an email sent by Abd Al-Yasu in 2/22/2012, 1:00PM



14. What does this file contain?

This file contains 9 images mostly about terrorist acts



15. What search terms has this user searched the Internet for? Using what search engine?

Ireland - Google Maps

microsoft security essentials - Bing

northern ireland conflict - Bing



high powered rifle - Google Search  
abd al-yasu - Google Search  
hotmail - Google Search  
hotmail for outlook - Google Search  
plo and ira connections? - Google Search  
plo - Google Search  
thunderbird email - Google Search  
Internet Explorer 9 - Microsoft Windows  
Provisional Irish Republican Army arms importation - Wikipedia, the free encyclopedia  
Palestine Liberation Organization - Wikipedia, the free encyclopedia

16. Did the user access the pictures of RPG launchers you found earlier? What proof do you have?

There is proof that he accessed the pictures as shown in the image below.

URL	Title	Visit Time	Visit Count	Visited From	Web Browser	User Profile	Browser Profile	URL Length	Typed Count
Host: Computer		2/22/2012 7:38:16 AM	1		Internet Explorer	John		15	
Host: go.microsoft.c...		2/17/2012 7:24:41 PM	2		Internet Explorer	John		23	
Host: internet.hiespre...		2/17/2012 7:24:57 PM	2		Internet Explorer	John		29	
Host: login.live.com		2/17/2012 7:25:14 PM	1		Internet Explorer	John		21	
Host: nimbos.chv.net		2/17/2012 7:24:47 PM	2		Internet Explorer	John		21	
Host: sn132w.ort132...		2/17/2012 7:36:15 PM	1		Internet Explorer	John		34	
Host: windows.micro...		2/7/2012 11:17:52 AM	1		Internet Explorer	John		28	
Host: www.bing.com		2/15/2012 9:04:04 PM	1		Internet Explorer	John		19	
Host: www.bing.com		2/7/2012 11:18:00 AM	1		Internet Explorer	John		19	
Host: www.google.co...		2/15/2012 8:54:28 PM	1		Internet Explorer	John		21	
Host: www.microsof...		2/7/2012 11:18:10 AM	1		Internet Explorer	John		24	
Host: www.mozilla.org		2/15/2012 8:54:53 PM	1		Internet Explorer	John		22	
Host: www.mon.com		2/15/2012 9:03:43 PM	1		Internet Explorer	John		18	
Host: www.mon.com		2/7/2012 11:17:45 AM	1		Internet Explorer	John		18	
about:blank		2/17/2012 7:36:37 PM	34		Internet Explorer	John		11	
about:blank		2/17/2012 7:37:03 PM	35		Internet Explorer	John		11	
file:///C:/RPG/48029.p...		2/22/2012 7:39:30 AM	2		Internet Explorer	John		28	
file:///C:/RPG/48029.p...		2/22/2012 7:39:30 AM	2		Internet Explorer	John		28	
file:///C:/RPG/ppg-16...		2/22/2012 7:38:29 AM	1		Internet Explorer	John		25	
file:///C:/RPG/ppg-16...		2/22/2012 7:38:29 AM	1		Internet Explorer	John		25	
file:///C:/RPG/ppg-7-L...	C:\RPG\ppg-7-launcher...	2/22/2012 7:38:50 AM	3		Internet Explorer	John		33	
file:///C:/RPG/ppg-7-L...		2/22/2012 7:38:49 AM	2		Internet Explorer	John		33	
file:///C:/RPG/ppg-7_2...		2/22/2012 7:39:16 AM	1		Internet Explorer	John		26	
file:///C:/RPG/ppg-7_2...		2/22/2012 7:39:18 AM	1		Internet Explorer	John		26	
file:///C:/RPG/ppg-8_j...		2/22/2012 7:38:38 AM	1		Internet Explorer	John		24	
file:///C:/RPG/ppg-8_j...		2/22/2012 7:38:38 AM	1		Internet Explorer	John		24	
file:///C:/RPG/ppg-7a...		2/22/2012 7:39:07 AM	2		Internet Explorer	John		27	
file:///C:/RPG/ppg-7a...		2/22/2012 7:39:07 AM	2		Internet Explorer	John		27	
file:///C:/Users/John/...		2/17/2012 8:50:25 PM	1		Internet Explorer	John		57	
file:///C:/Users/John/...		2/17/2012 8:50:25 PM	1		Internet Explorer	John		57	
file:///C:/Users/John/...		2/17/2012 8:50:33 PM	1		Internet Explorer	John		57	
file:///C:/Users/John/...		2/17/2012 8:50:33 PM	1		Internet Explorer	John		57	
file:///C:/Users/John/...		2/17/2012 8:50:37 PM	1		Internet Explorer	John		57	
file:///C:/Users/John/...		2/17/2012 8:50:37 PM	1		Internet Explorer	John		57	
file:///C:/Users/John/...		2/22/2012 2:05:01 PM	1		Internet Explorer	John		38	
file:///C:/Users/John/...		2/22/2012 2:05:01 PM	1		Internet Explorer	John		38	
file:///C:/Users/John/...		2/18/2012 7:17:37 AM	2		Internet Explorer	John		65	
file:///C:/Users/John/...		2/18/2012 7:17:37 AM	2		Internet Explorer	John		65	
file:///C:/Users/John/...		2/22/2012 12:13:36 PM	3		Internet Explorer	John		62	
file:///C:/Users/John/...		2/22/2012 12:13:31 PM	2		Internet Explorer	John		62	
file:///C:/Users/John/...		2/18/2012 7:15:05 AM	1		Internet Explorer	John		62	
file:///C:/Users/John/...		2/22/2012 12:13:36 PM	2		Internet Explorer	John		62	
file:///C:/Users/John/...		2/22/2012 2:04:18 PM	1		Internet Explorer	John		40	
file:///C:/Users/John/...		2/22/2012 2:04:18 PM	1		Internet Explorer	John		40	
file:///C:/Users/John/...		2/22/2012 12:41:43 PM	3		Internet Explorer	John		41	
file:///C:/Users/John/...		2/22/2012 12:41:43 PM	4		Internet Explorer	John		41	
file:///C:/Users/John/...		2/22/2012 4:12:05 PM	5		Internet Explorer	John		41	
file:///C:/Users/John/...		2/22/2012 4:12:05 PM	4		Internet Explorer	John		41	

17. Examine the MFT entry for the file **C\_ISC301.dll**

- According to the MFT entry what are the date/time stamps for Modified, Accessed and Created? Provide both the hex value as it is stored in the MFT and the decoded date/time.

Created - Hex = 38A0C90FDFEDCC01

Decoded = Sat, 18 Feb 2012 01:45:58

Accessed - Hex = 38A0C90FDFEDCC01

Decoded = Sat, 18 Feb 2012 01:45:58

### Modified - Standard Information Attribute

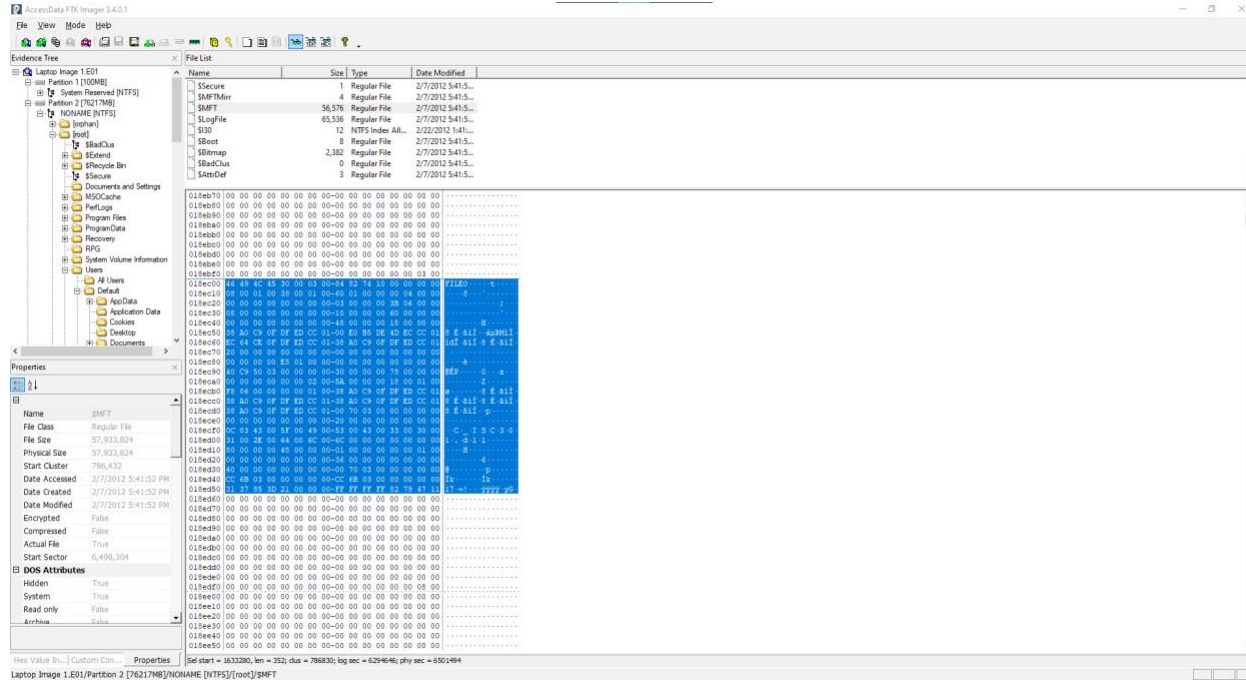
Hex = 00E0B5DE4DECCC01

Decoded = Thu, 16 Feb 2012 01:54:08

### - File Name Attribute

Hex = 38A0C90FD FEDCC01

Decoded = Sat, 18 Feb 2012 01:45:58



- b. What attribute did you recover this information from?  
Standard Information Attribute and File Name Attribute

- c. What is the MFT record number of this file?

Hex = 3B060000

Decimal = 1595

- d. What is the MFT record number of the parent directory?

Hex = F806000000000100

Decimal = 281474976712440

This file is located in Windows/System32.

- e. What type of file is this really?

jpg file



f. What is the MD5 hash value of this file?

1ecabdb8c35f88ca7115749b063442c7

18. Examine the MFT entry for the file **MSPUB20.BDR**

- a. According to the MFT entry what are the date/time stamps for Modified, Accessed and Created? Provide both the hex value as it is stored in the MFT and the decoded date/time.

Created - Hex = F115643BDFEDCC01

Decoded = Sat, 18 Feb 2012 01:47:11

Accessed - Hex = F115643BDFEDCC01

Decoded = Sat, 18 Feb 2012 01:47:11

Modified - **Standard Information Attribute**

Hex = 00D28ED74DECCC01

Decoded = Thu, 16 Feb 2012 01:53:56

- **File Name Attribute**

Hex = F115643BDFEDCC01

Decoded = Sat, 18 Feb 2012 01:47:11

The screenshot displays the AccessData FTK Imager 3.4.0.1 interface. The Evidence Tree on the left shows the file system structure, including Partition 1 (100MB) and Partition 2 (76217MB). The File List in the center shows the \$MFT file as a Regular File with a size of 56,576 bytes. The Properties pane on the right shows the details for the \$MFT file, including its size, physical size, start cluster, and date/time stamps for Accessed, Created, and Modified. The File Name Attribute is also visible in the Properties pane.

Name	Size	Type	Date Modified
\$Secure	1	Regular File	2/7/2012 5:41:52 PM
\$MFTMirr	4	Regular File	2/7/2012 5:41:52 PM
\$MFT	56,576	Regular File	2/7/2012 5:41:52 PM
\$LogFile	65,536	Regular File	2/7/2012 5:41:52 PM
\$Info	12	NTFS Index All...	2/22/2012 1:41:52 PM
\$Boot	8	Regular File	2/7/2012 5:41:52 PM
\$Bitmap	2,382	Regular File	2/7/2012 5:41:52 PM
\$BadClus	0	Regular File	2/7/2012 5:41:52 PM
\$AttrDef	3	Regular File	2/7/2012 5:41:52 PM

Name	\$MFT
File Class	Regular File
File Size	57,933,824
Physical Size	57,933,824
Start Cluster	786,432
Date Accessed	2/7/2012 5:41:52 PM
Date Created	2/7/2012 5:41:52 PM
Date Modified	2/7/2012 5:41:52 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	6,498,304
DOS Attributes	Hidden True

- b. What attribute did you recover this information from?

Standard Information Attribute and File Name Attribute

- c. What is the MFT record number of this file?

Hex = 46C10000

Decimal = 49478

- d. What is the MFT record number of the parent directory?

Hex = 4AB5000000000100

Decimal = 281474976757066

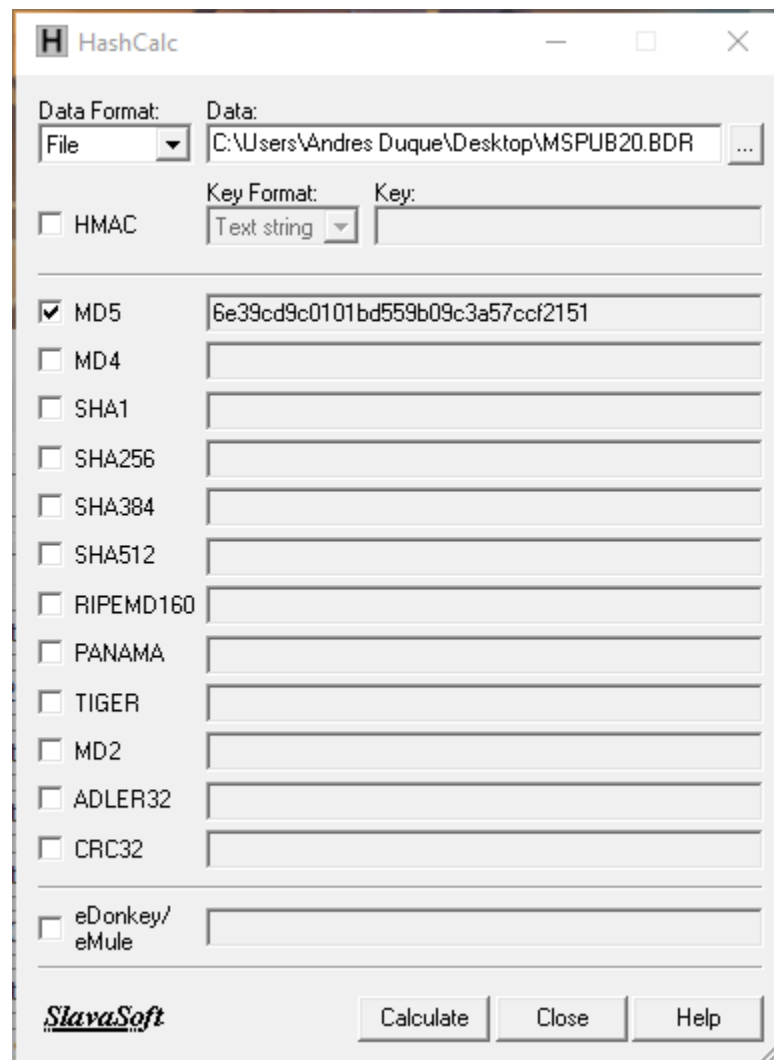
This file is located in Program Files/Microsoft Office/Office12/PUBBA

- e. What type of file is this really?

It is a jpg file

- f. What is the MD5 hash value of this file?

6e39cd9c0101bd559b09c3a57ccf2151



## 19. Examine the MFT entry for the file ilo[1].js

- a. According to the MFT entry what are the date/time stamps for Modified, Accessed and Created? Provide both the hex value as it is stored in the MFT and the decoded date/time.

Created - Hex = 0AC28759DFEDCC01

Decoded = Sat, 18 Feb 2012 01:48:02

Accessed - Hex = 0AC28759DFEDCC01

Decoded = Sat, 18 Feb 2012 01:48:02

Modified - **Standard Information Attribute**

Hex = 009B774E4DECCC01

Decoded = Thu, 16 Feb 2012 01:50:06

- **File Name Attribute**

Hex = 0AC28759DFEDCC01

Decoded = Sat, 18 Feb 2012 01:48:02

The screenshot displays the AccessData FTK Imager 3.4.0.1 interface. The Evidence Tree on the left shows the hierarchy: Laptop Image 1.E01 > Partition 2 [76217MB] > NONAME [NTFS] > [orphan] > [root] > \$BadClus > \$Extend > \$Recycle.Bin > \$Secure > Documents and Settings > MSOCache > PerfLogs > Program Files > Common Files > CONEXANT > DVD Maker > Internet Explorer > Microsoft Office > CLIPART > Document Themes > MEDIA.

The File List on the right shows the contents of the \$MFT file, including \$Volume, \$UpCase, \$TXF\_DATA, \$Secure, \$MFTMirr, \$LogFile, \$I30, \$Boot, and \$Bitman.

The Properties window at the bottom left shows the details for the selected \$MFT file:

Name	\$MFT
File Class	Regular File
File Size	57,933,824
Physical Size	57,933,824
Start Cluster	786,432
Date Accessed	2/7/2012 5:41:52 PM
Date Created	2/7/2012 5:41:52 PM
Date Modified	2/7/2012 5:41:52 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	6,498,304

The Hex Value In... Custom Con... Properties section at the bottom shows the hex value 009B774E4DECCC01 for the Modified date, which corresponds to the decoded date of Thu, 16 Feb 2012 01:50:06.

b. What attribute did you recover this information from?  
Standard Information Attribute and File Name Attribute

c. What is the MFT record number of this file?  
Hex = 76C20000  
Decimal = 49782

d. What is the MFT record number of the parent directory?  
Hex = 94D1000000000300  
Decimal = 844424930185620

This file is located in Users/John/AppData/Local/Temp/Low/TIF/Content.ie/G42QYY

e. What type of file is this really?  
This file is a jpg

f. What is the MD5 hash value of this file?  
c08fed3c02722d5e0cf24bcf385bf369

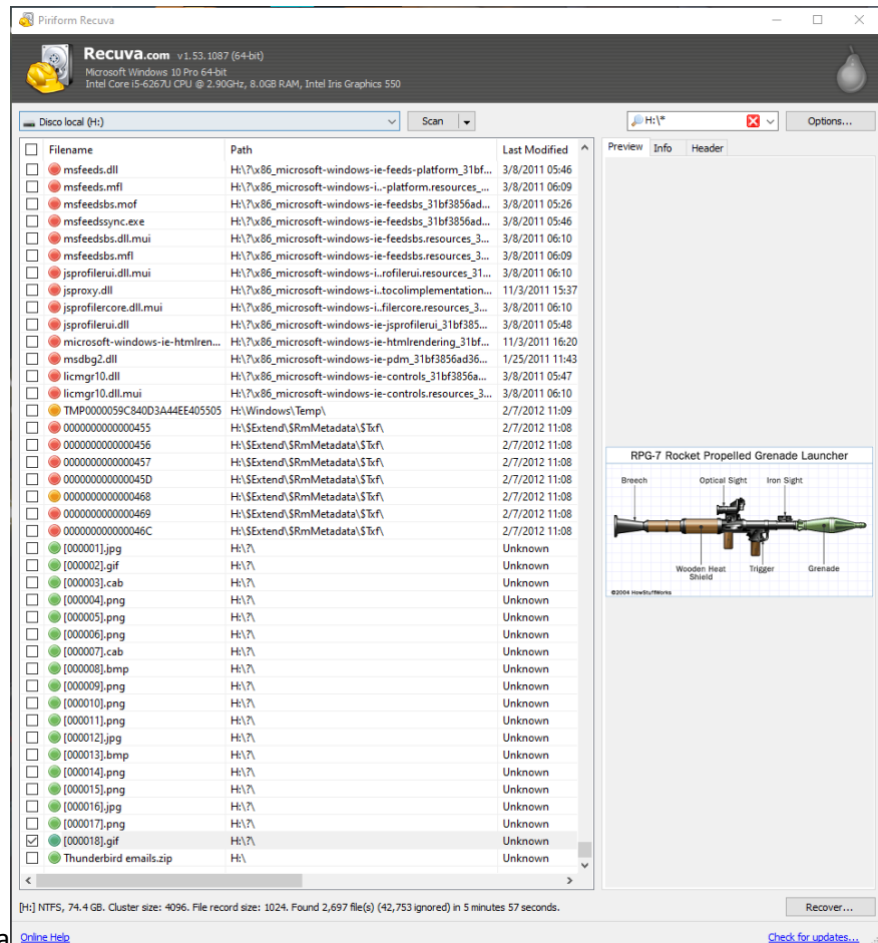
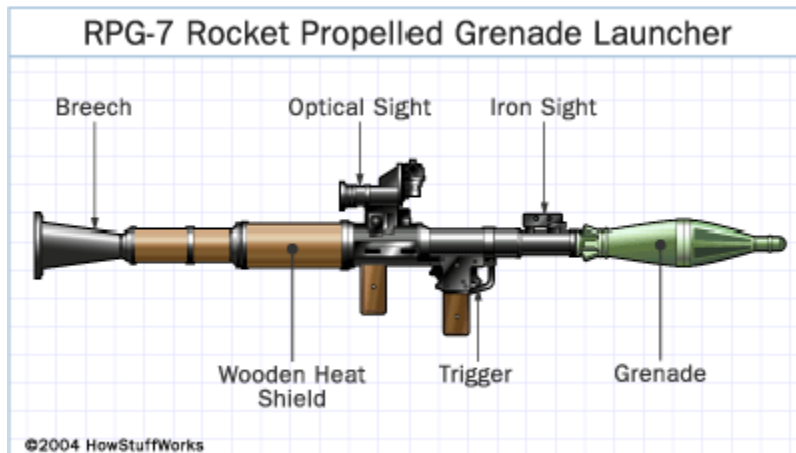
20. Give a brief case summary write-up. Include information on what organization the owner of the computer belongs to, who his "contact" is and what organization he belongs too and any other information you think may be relevant to the investigation.

In the information found we can clearly see that this guy is related to some kind of terrorism. It is not clear if he is related to IRA or PLO but we know for sure that he is one of them. His main contact is Abd Al-Yasu which is also a suspect of terrorism based on the emails found between him and John. His internet searches and the image files that he has been in contact with make John a suspect of terrorism. Also, a person with this kind of knowledge is not easy to find. The way that he tries to hide his traces makes him even more suspicious.



Extra Credit: +5

Can you find this picture on the image of the hard drive? If so, where and how did you find it?



I found this image using Recuva