CIS 4385 Name: Andres Duque

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.

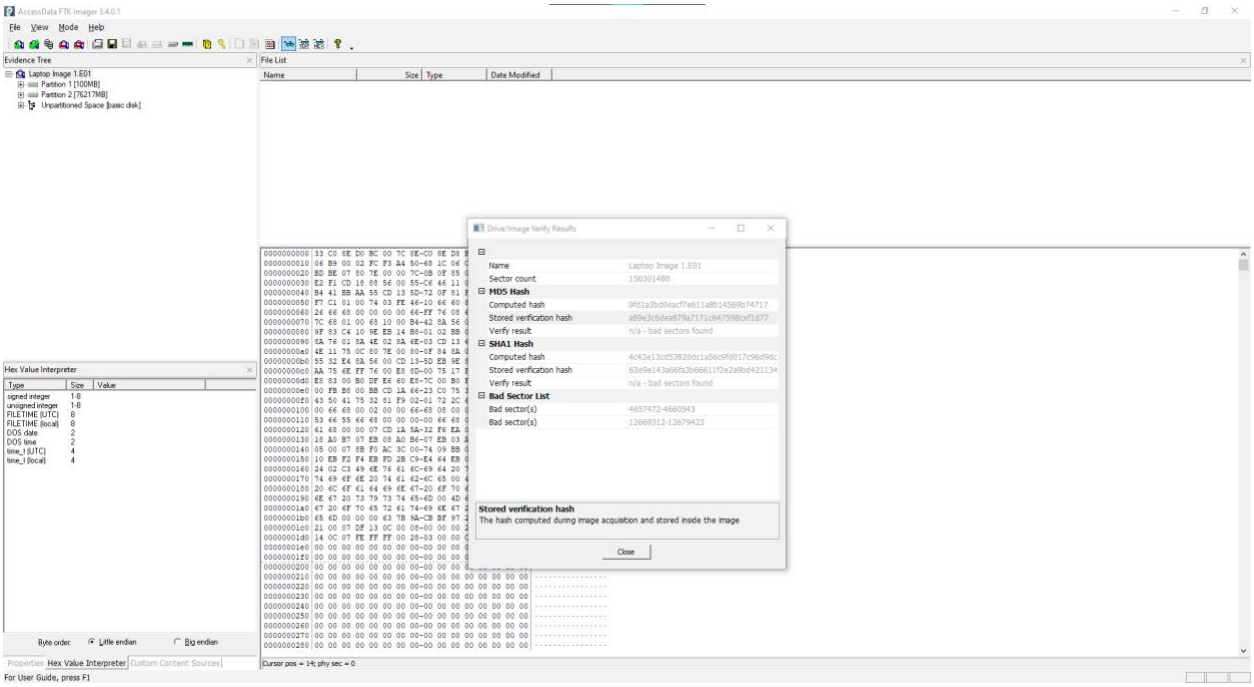
A team entered suspect's residence and found a powered down Dell laptop computer. The suspect was not present. Triage indicated that files of possible value might be found and that a full forensic exam would be beneficial.

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.

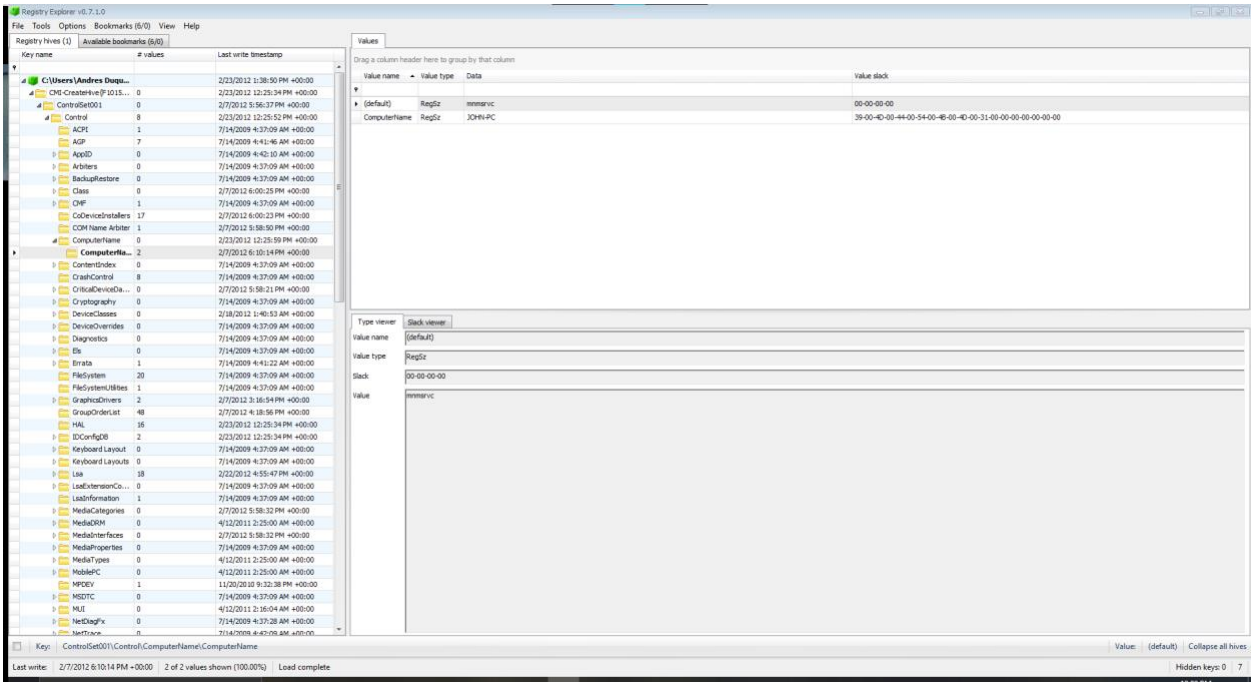
Each question is worth 5 points.

1. What is the acquisition and verification hash value of the image?
   Acquisition = a89e3c6dea879a7171c647598cef1d77
   Verification = 9fd1a3bd0eacf7e611a8b14569b74717



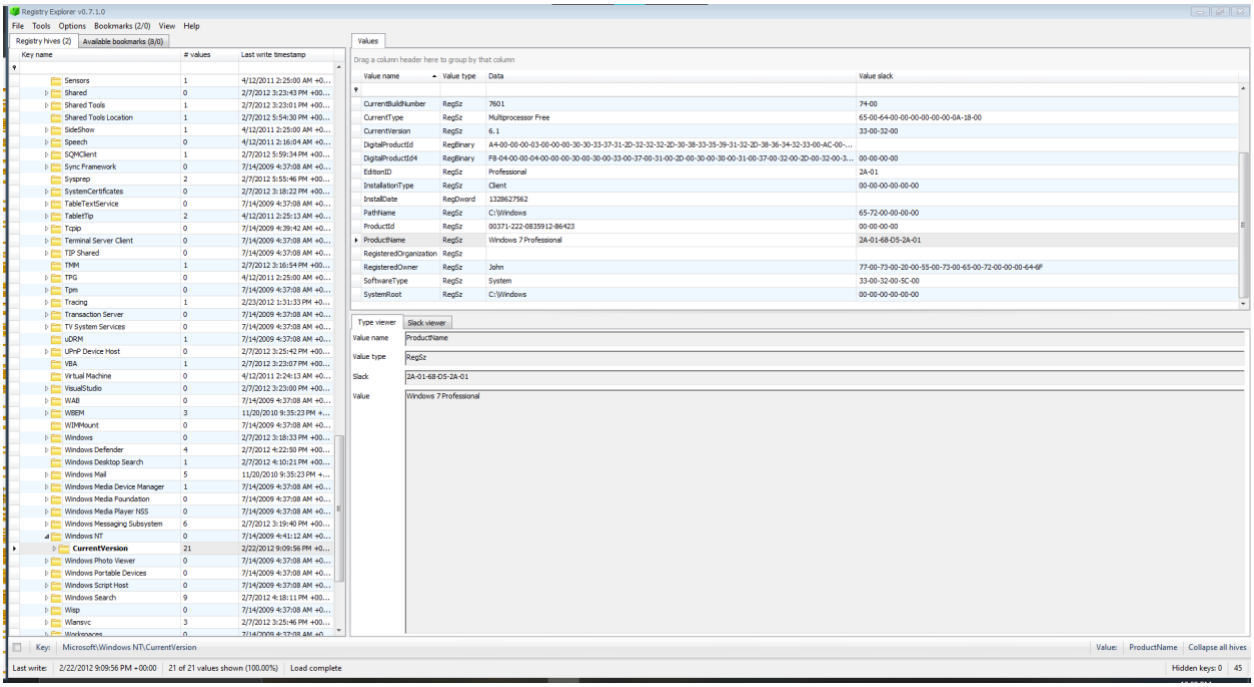
2. What is the Computer Name?

   JOHN-PC



3. What version of Windows is this user running?

   Windows 7 Professional



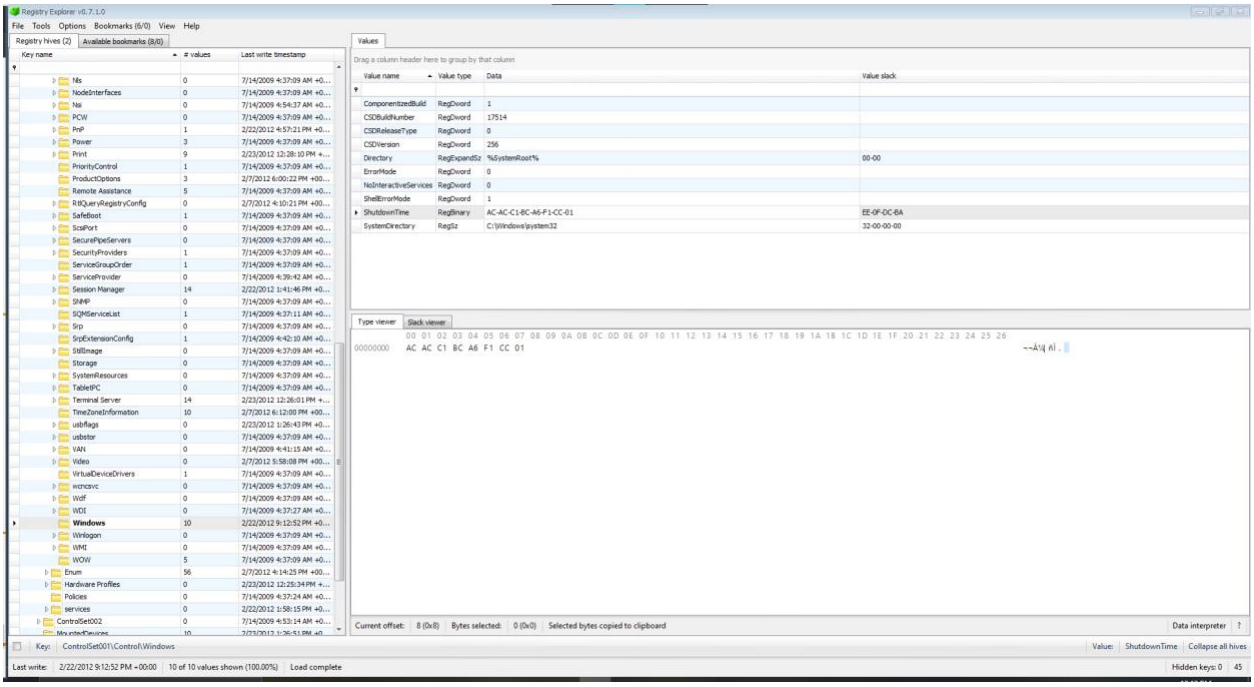
4. When was this version of Windows installed?

   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

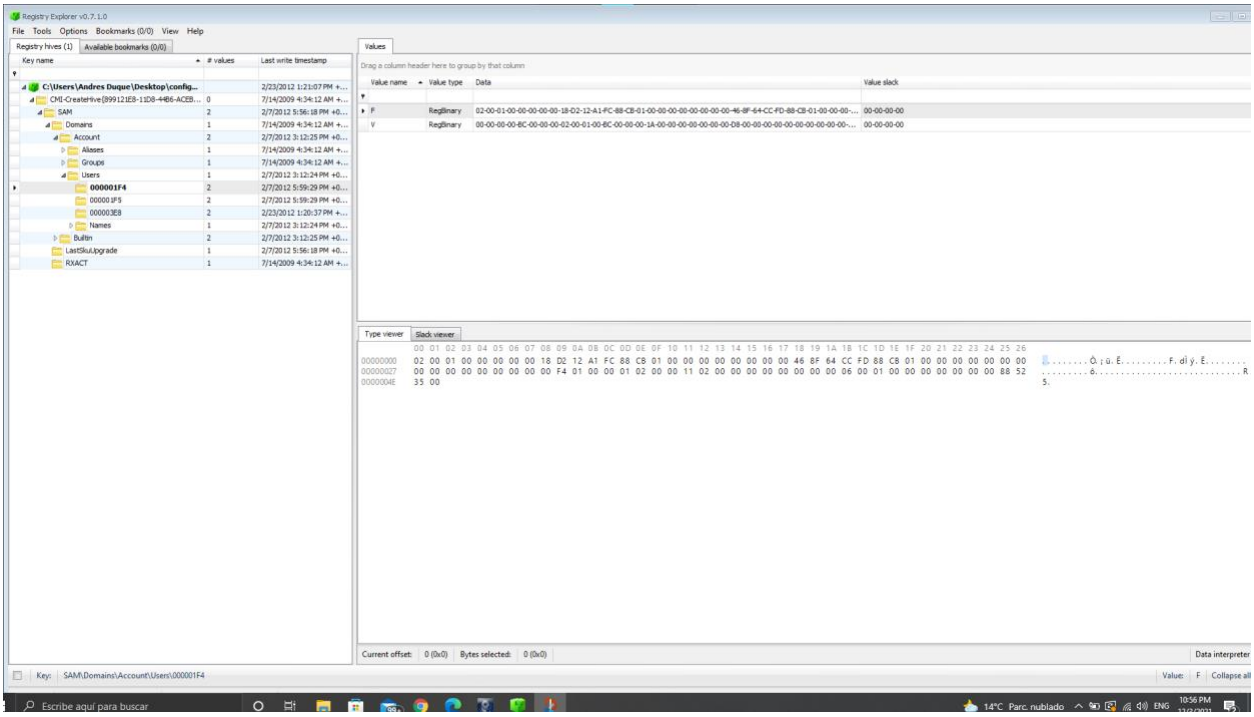
6. When was this computer last shut down?

   RegBinary = AC-AC-C1-BC-A6-F1-CC-01
   Win 64Bit Little Endian = Wed, 22 Feb 2012 21:12:52



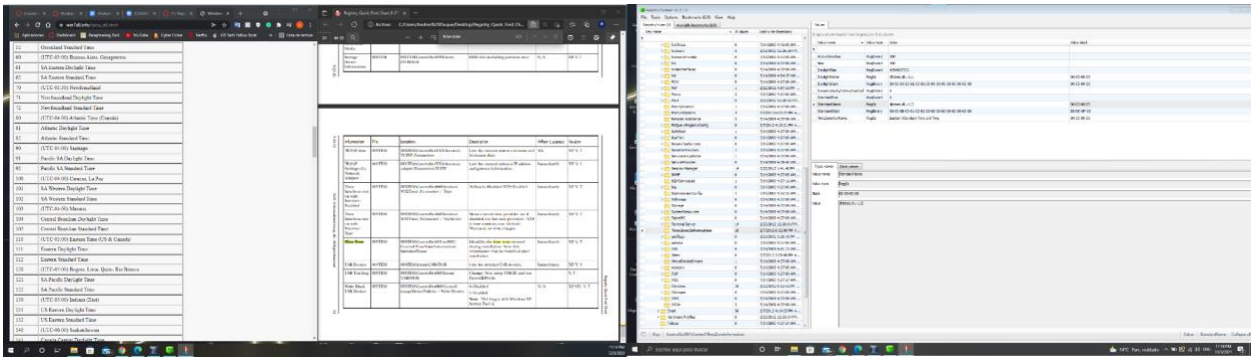
7. When did the user last change their password?

   25-32 Bytes = 46-8F-64-CC-FD-88-CB-01
   Win 64Bit Little Endian = Sat, 20 Nov 2010 21:56:34

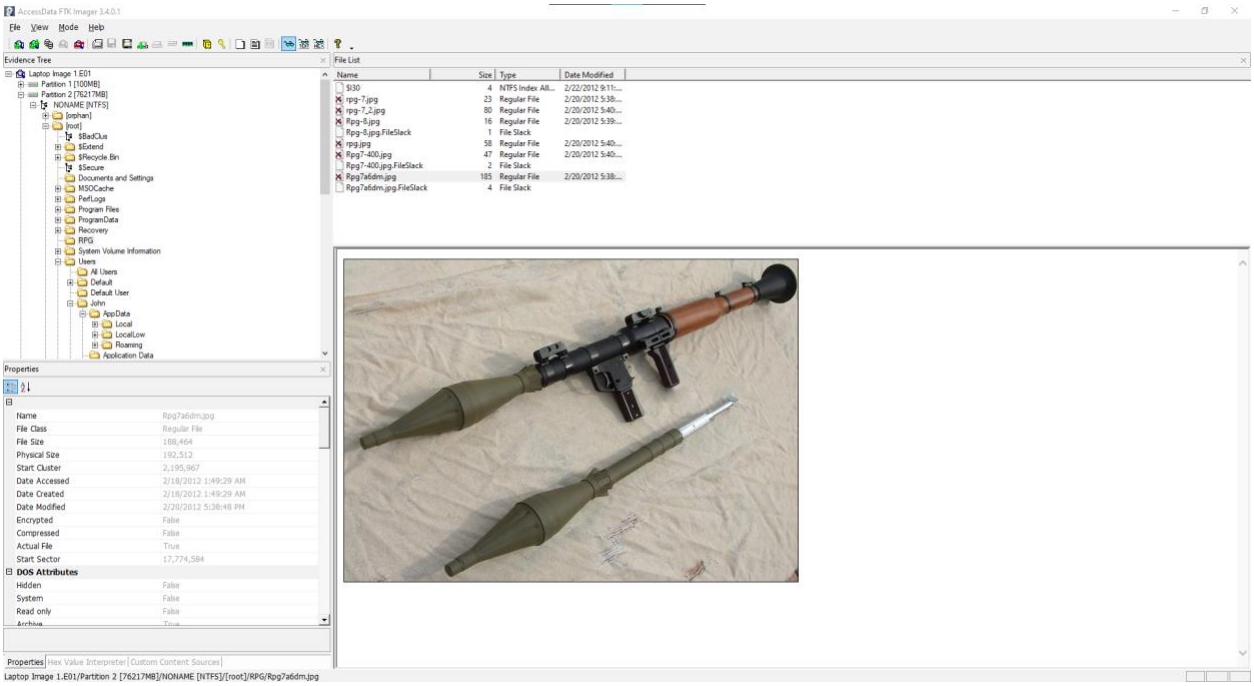


8. What is the time zone setting on this computer?

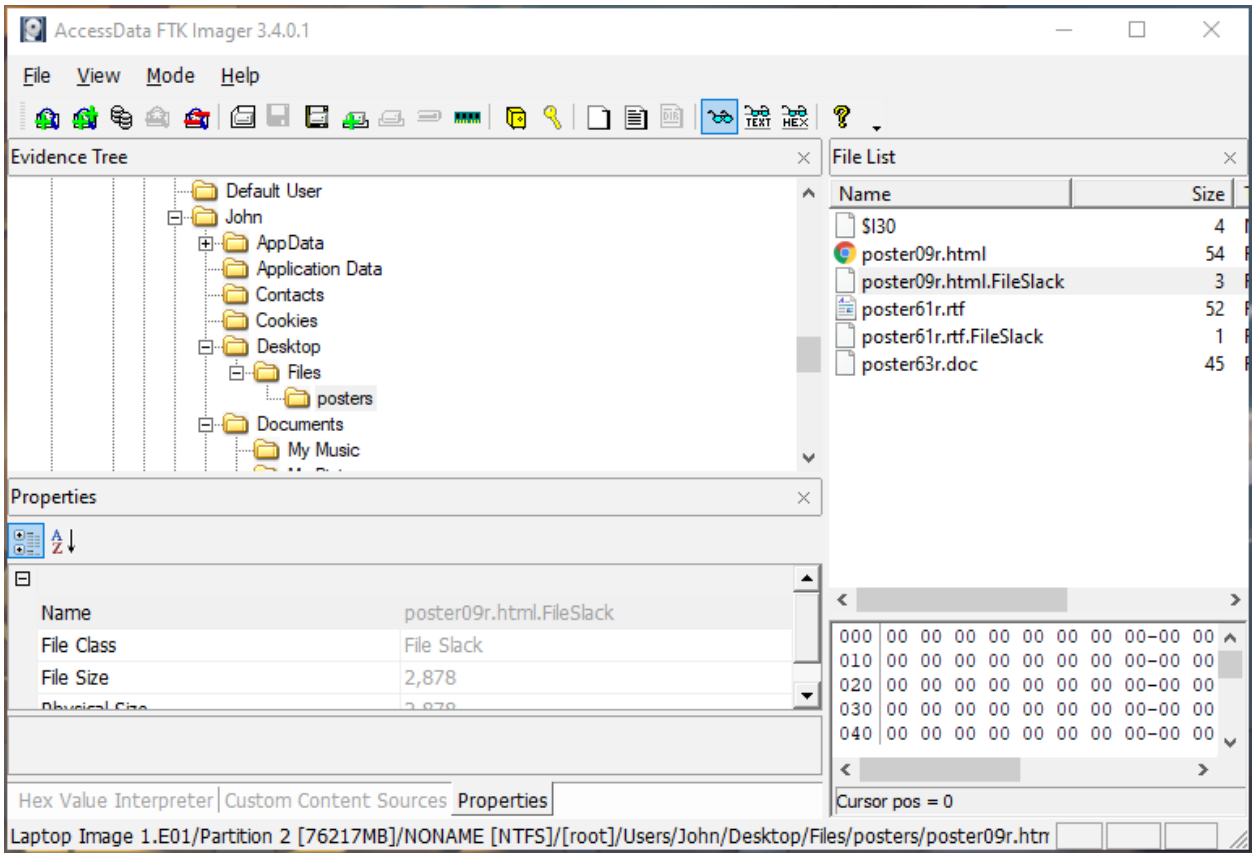
   Eastern Standard Time = @tzres.dll,-112



9. There are a series of pictures of Rocket Propelled Grenade launchers on this computer. Where are they located and what is the status of these pictures?
   These pictures are located in partition 2 in NONAME [NTFS] in the root folder and then the RPG folder. There are 6 pictures and they were deleted from the file as shown in the picture below.



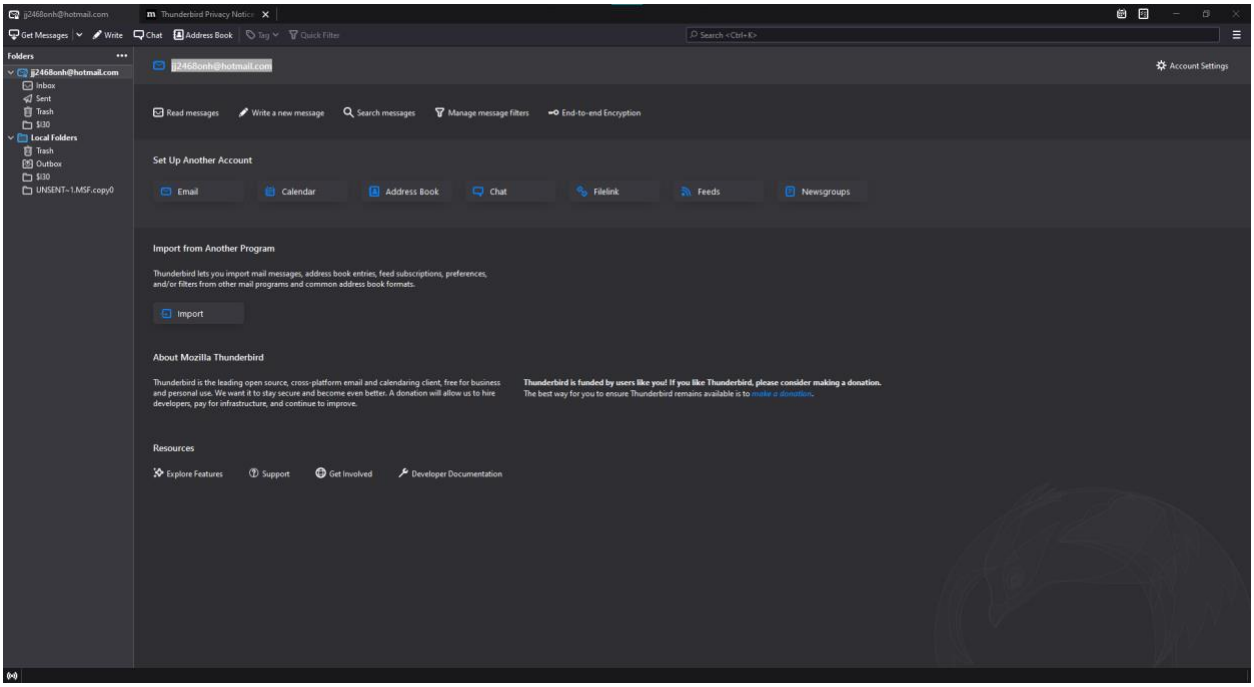
10. Find the folder titled **posters**.
    a. What is the full path of this folder? (ie. C:\Windows\...)
       Users/John/Desktop/Files/posters



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

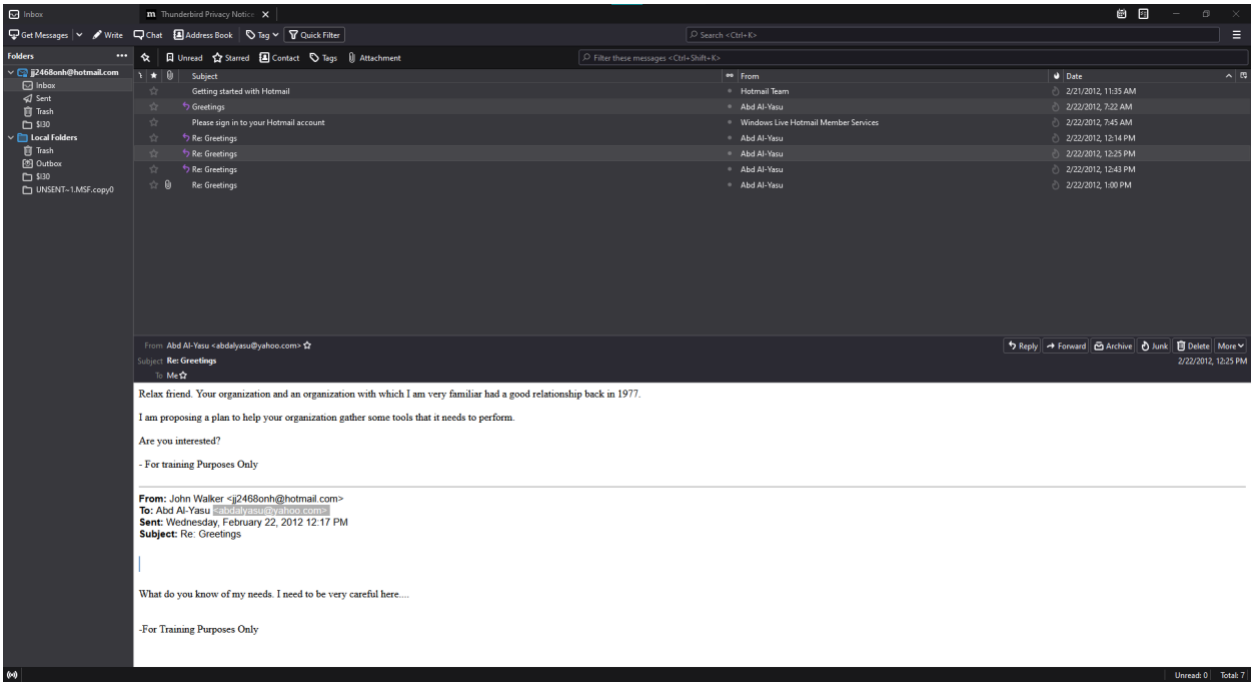
11. What is the users full email address?

jj2468onh@hotmail.com



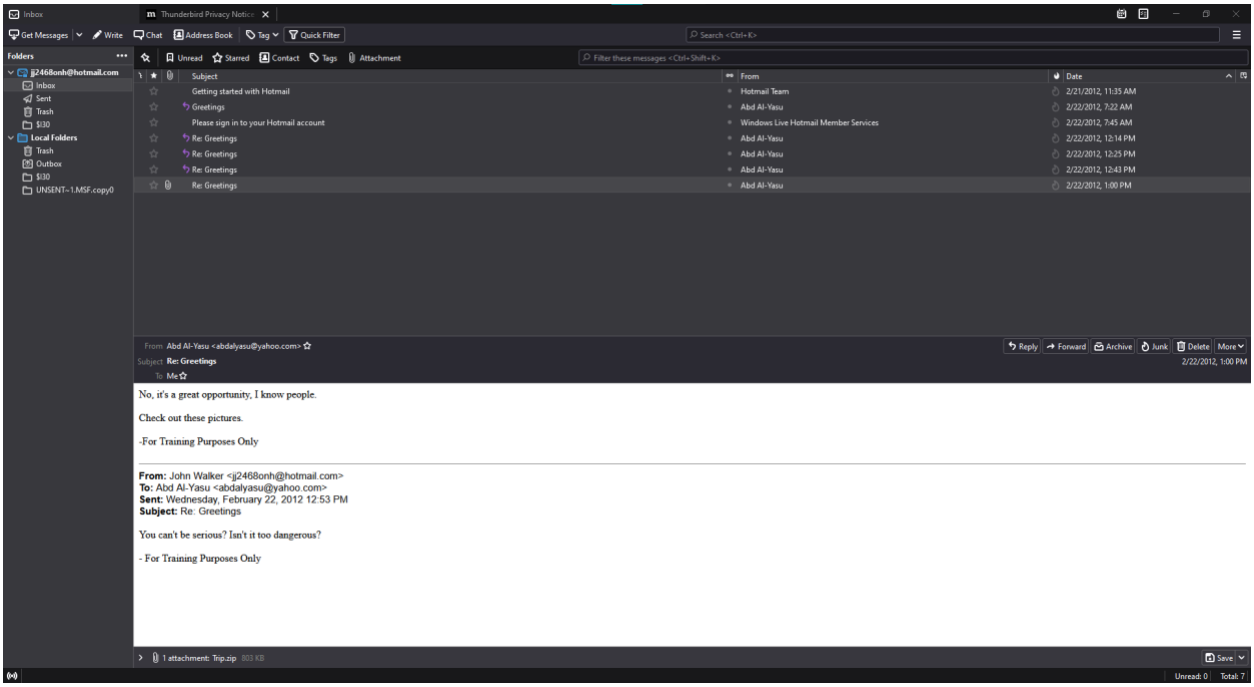
12. Who has the user been in contact with?

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

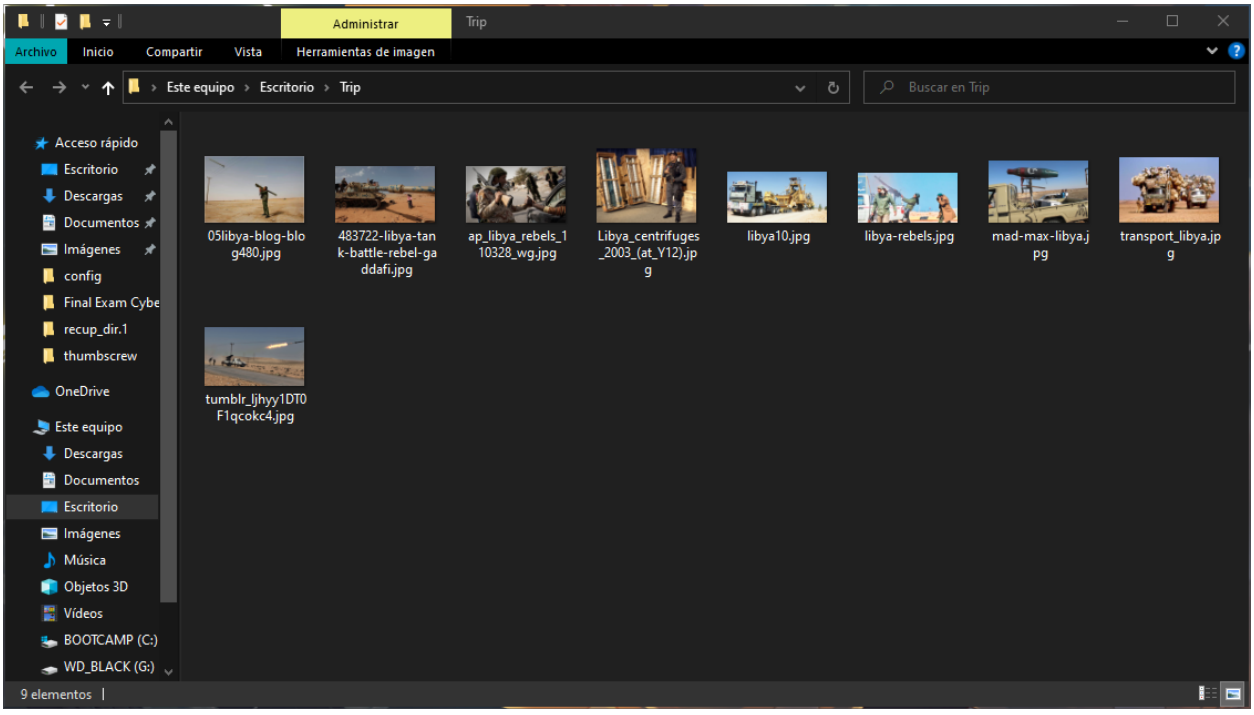


13. Where did the file Trip.zip come from?

    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

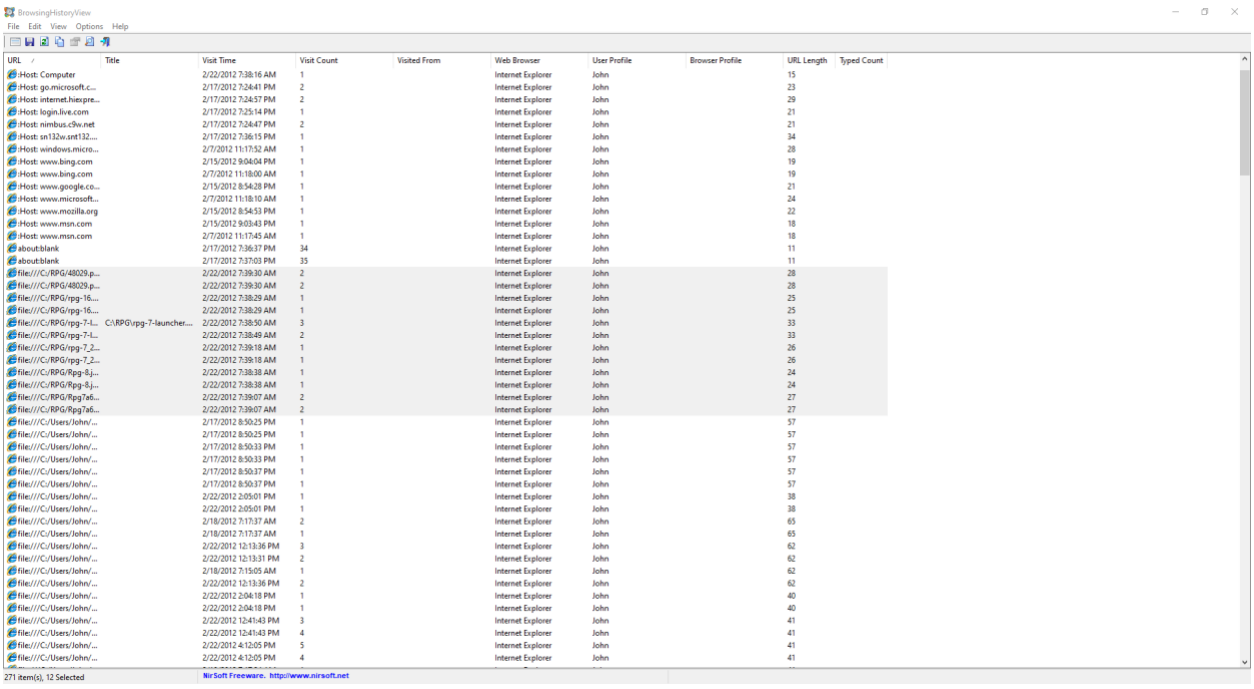


15. What search terms has this user searched the Internet for? Using what search engine?
    Ireland - Google Maps
    microsoft security essentials - Bing
    northern ireland conflict - Bing

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.



17. Examine the MFT entry for the file **C_ISC301.dll**

    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 = 38A0C90FDFEDCC01
    Decoded = Sat, 18 Feb 2012 01:45:58
    Accessed - Hex = 38A0C90FDFEDCC01
    Decoded = Sat, 18 Feb 2012 01:45:58

Modified **- Standard Information Attribute**

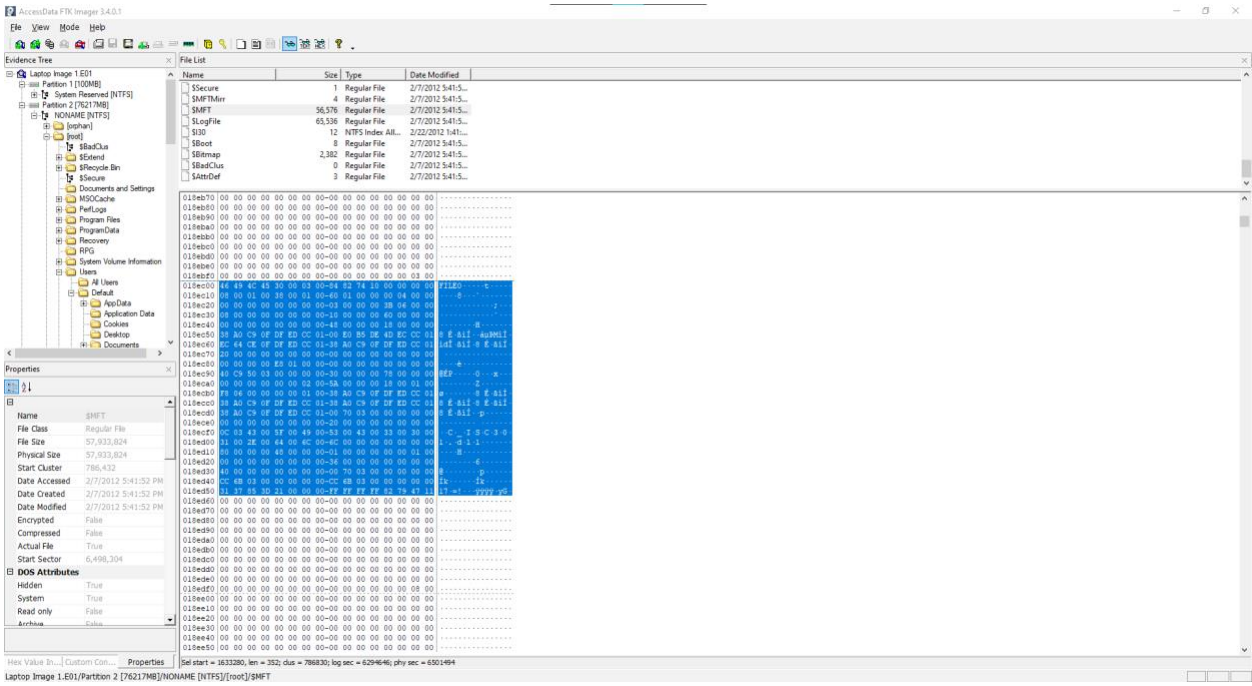
Hex = 00E0B5DE4DECCC01

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

- File Name Attribute

Hex = 38A0C90FDFEDCC01

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

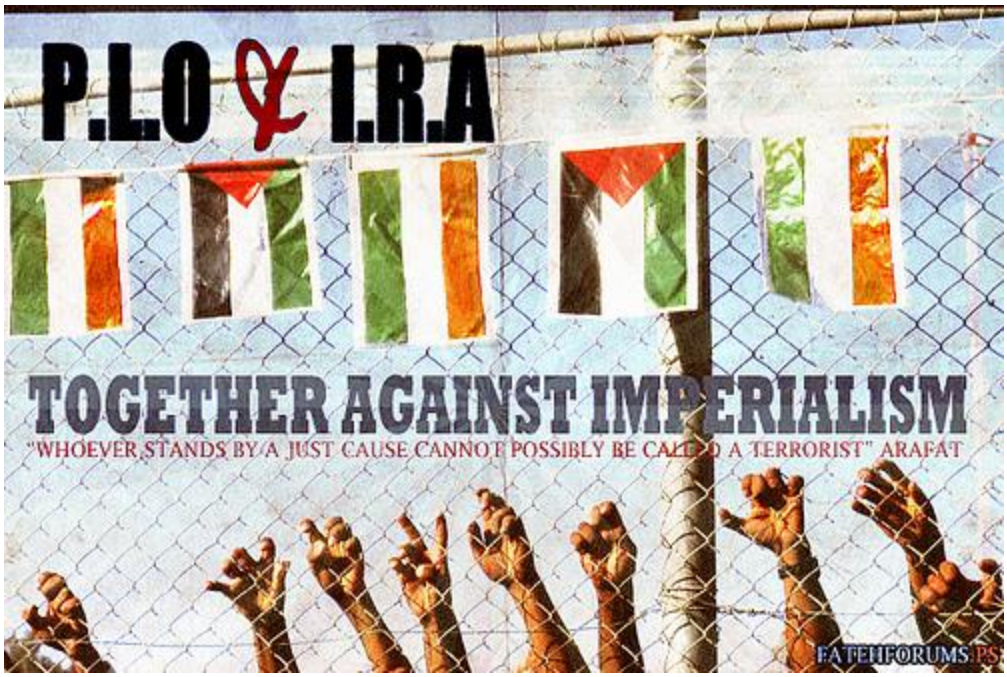


b. What attribute did you recover this information from?
Standard Information Attribute and File Name Attribute

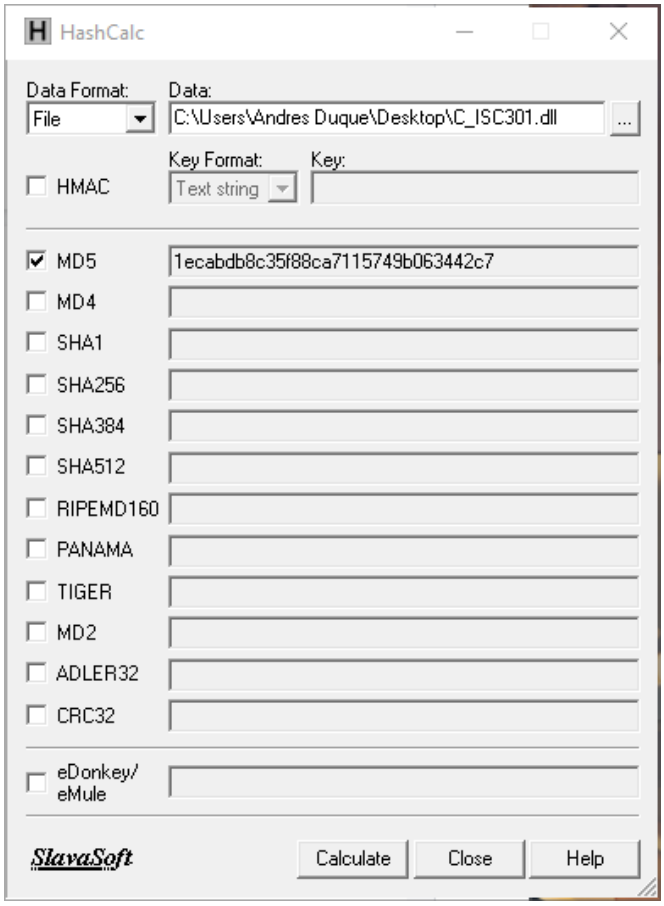
c. What is the MFT record number of this file?
Hex = 3B060000
Decimal = 1595

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**

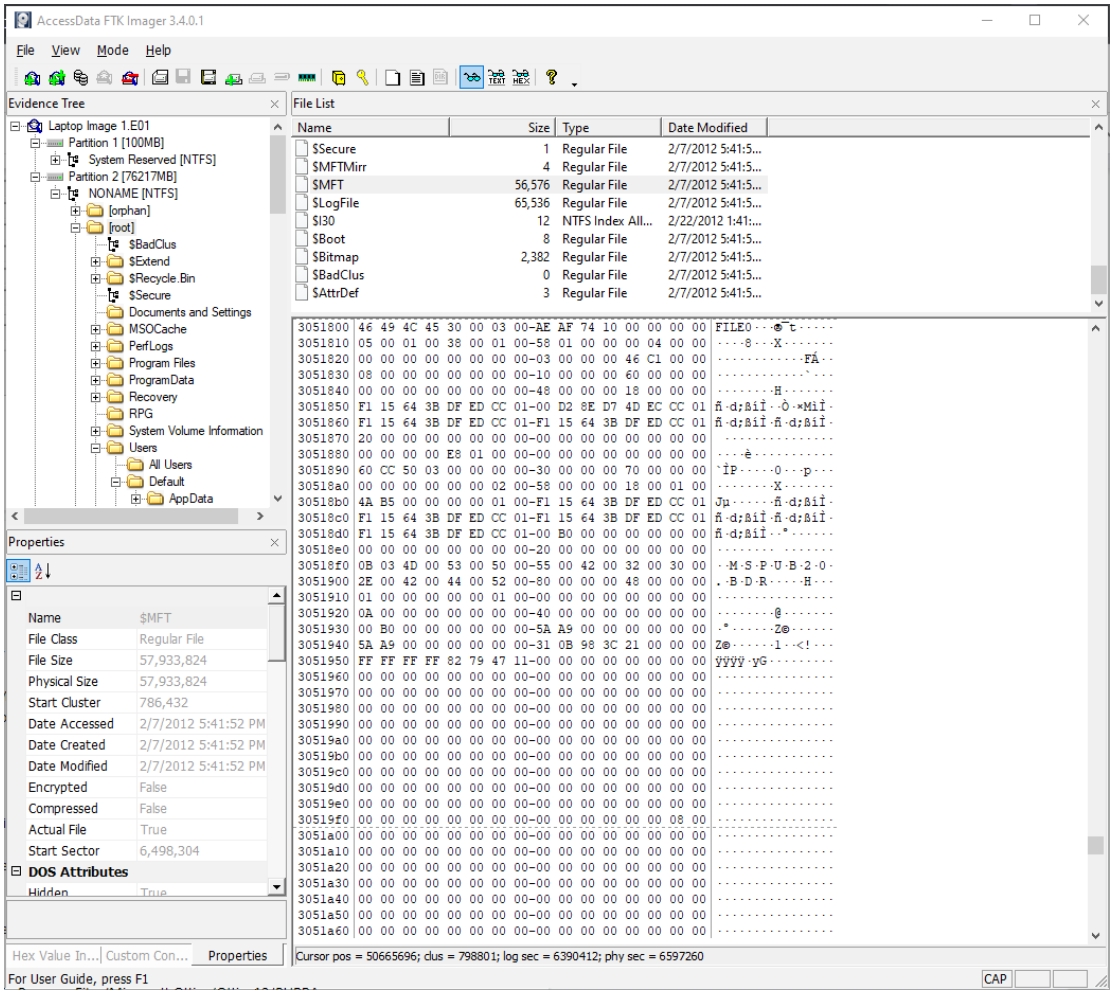
Hex = 00D28ED74DECCC01

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

- File Name Attribute

Hex = F115643BDFEDCC01

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



b. What attribute did you recover this information from?

Standard Information Attribute and File Name Attribute

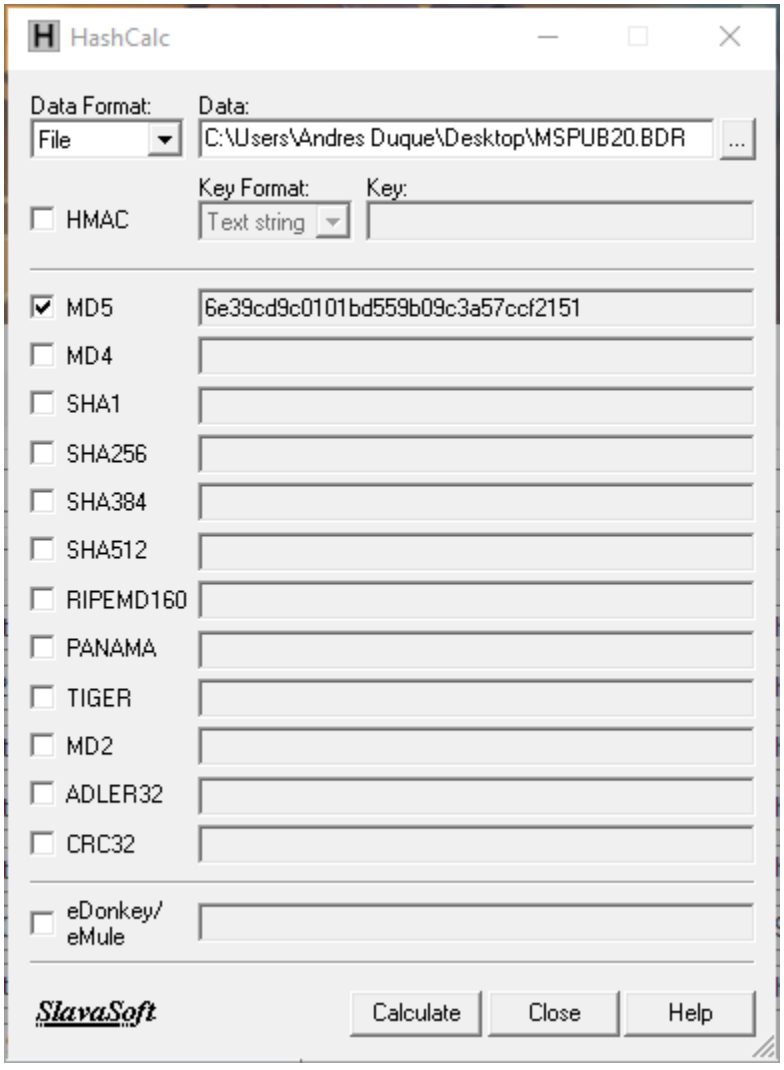
c. What is the MFT record number of this file?
Hex = 46C10000
Decimal = 49478

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**

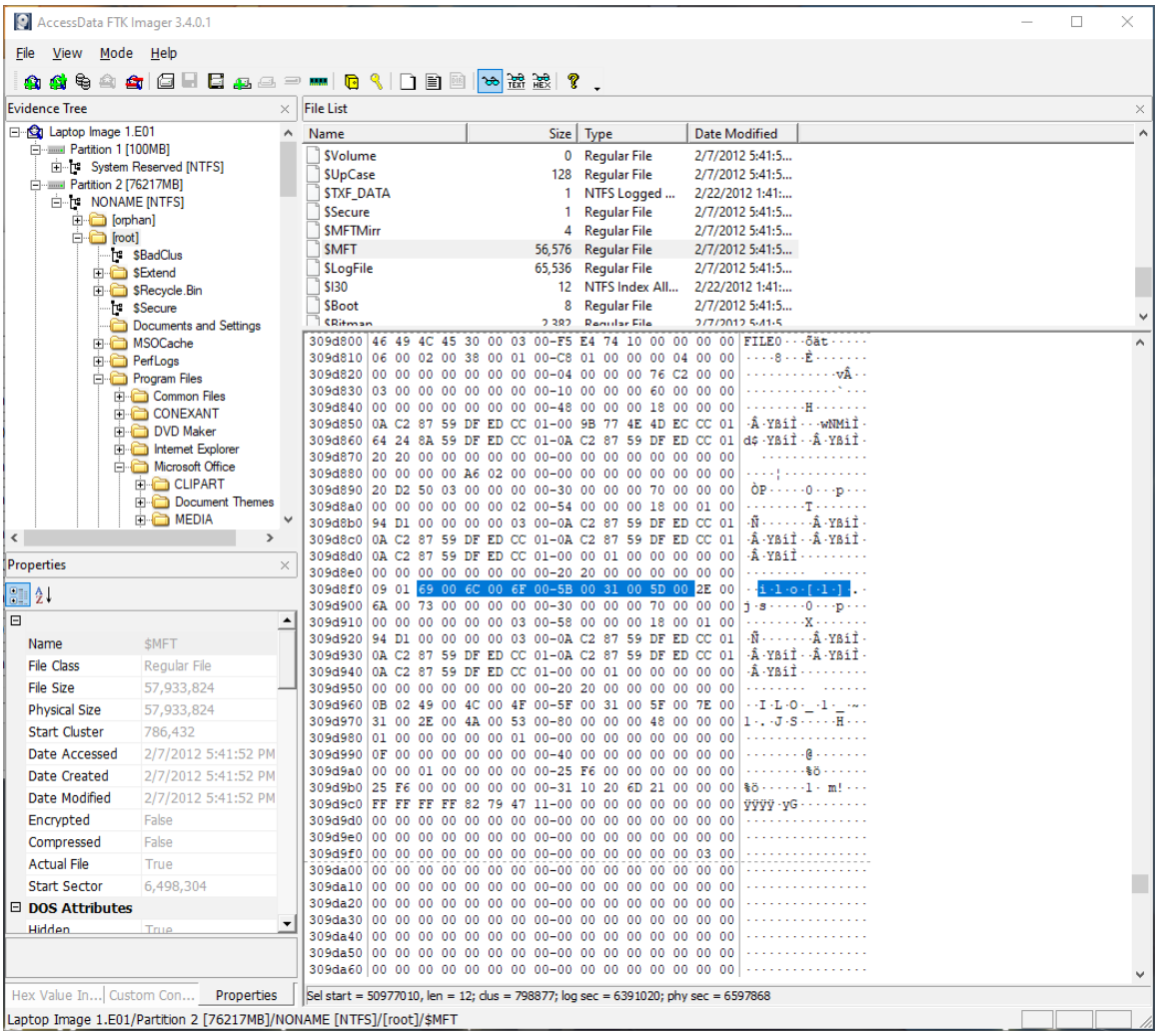
Hex = 009B774E4DECCC01

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

- File Name Attribute

Hex = 0AC28759DFEDCC01

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



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

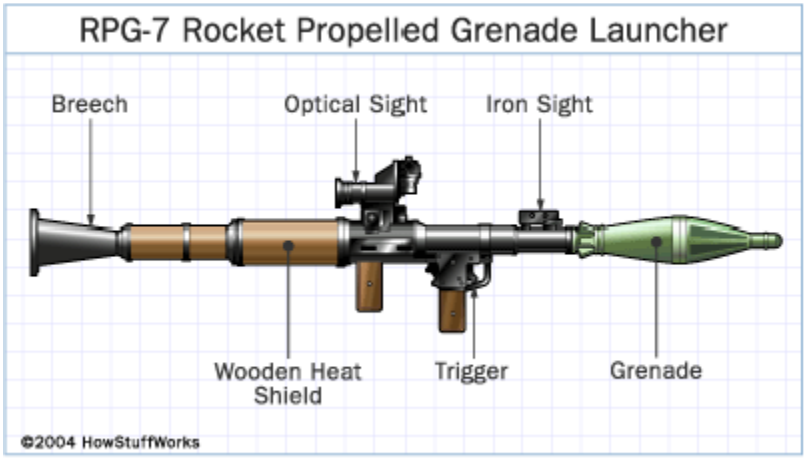
f. What is the MD5 hash value of this file?
   c08fed3c02722d5e0cf24bcf385bf369

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