Name :Gunathilaka S.B.M.B.S.A

SLIIT ID : IT20028046

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Practical Examination
Year 4, Semester 1/2 (2023)

IE4062 - Cyber Forensics and Incident Response

Duration: 2 Hours

June 2023

Instructions to candidate:

- Paper contains 4 questions. Answer all questions.
- This paper contains 3 pages including cover page.
- Exam time is 05.00pm to 07.00pm
- You are expected to upload report with answers (pdf) to courseweb submission link before 07.05pm

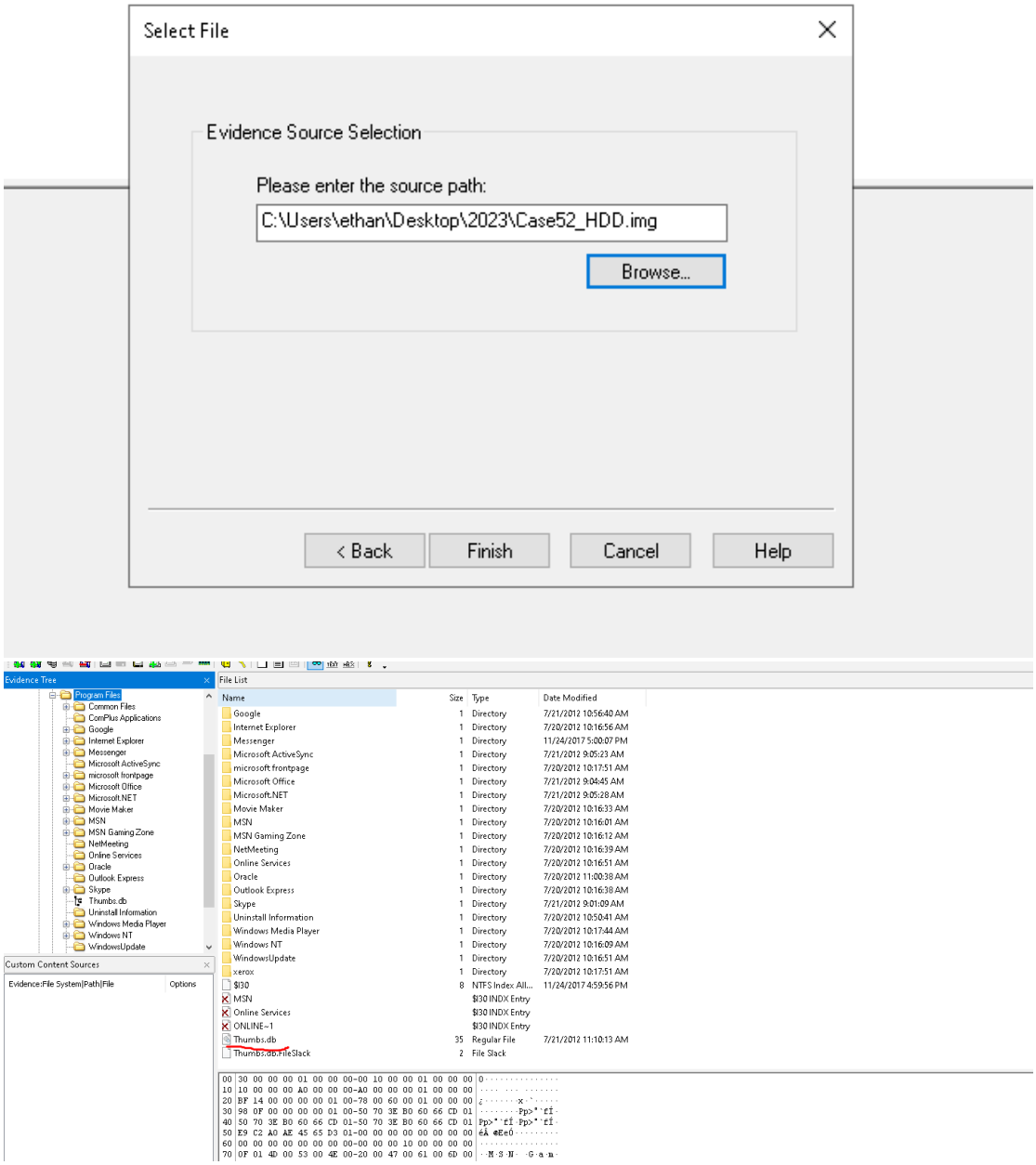
Question 1 (30 marks)

Use the raw image “Case52_HDD” file to answer the following Questions.

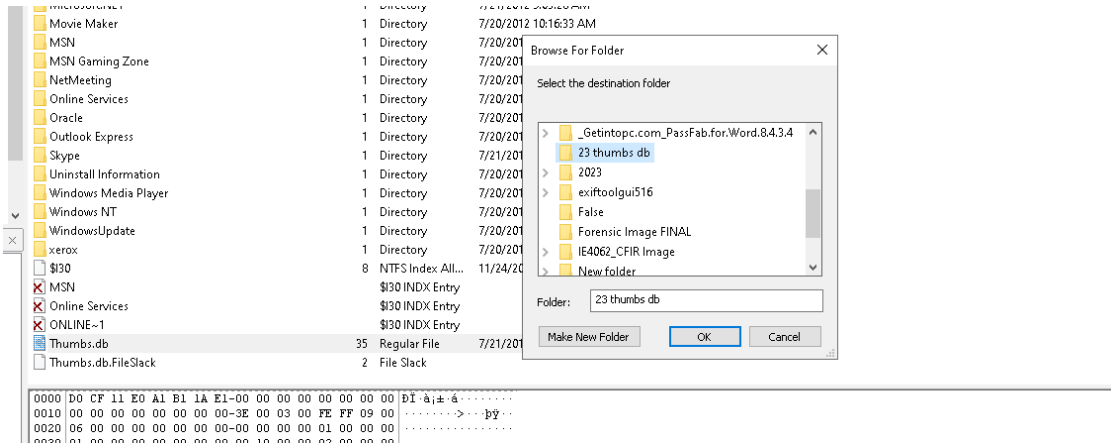
a) Using the “Thmbs.db” file in Programme files folder of the raw image find the file names and file create date time stamp of images, from image folder this thumbnail database acquired.

Answer

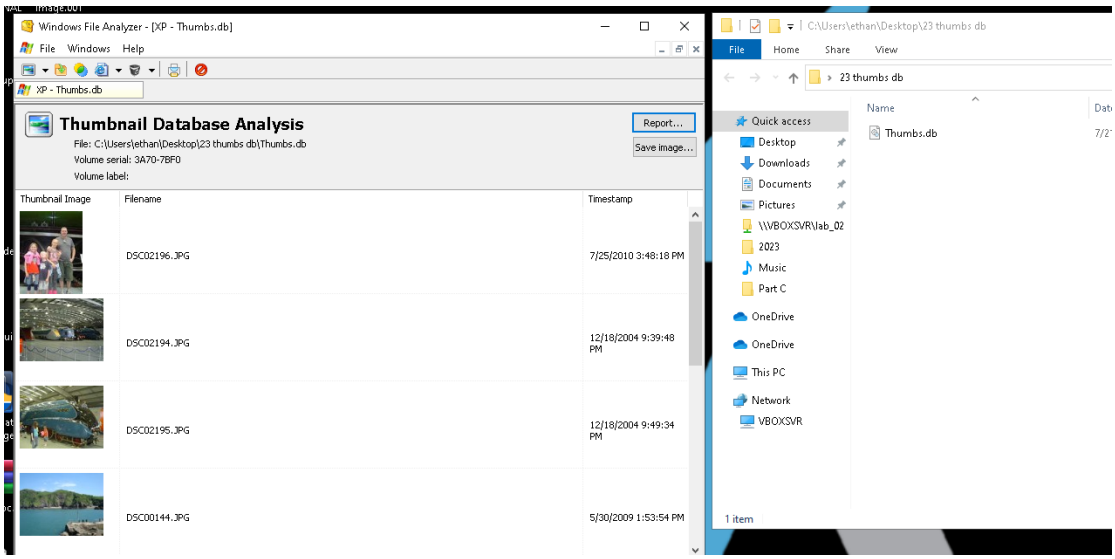
- First using FTK imager add Case52_HDD.img as a evidence.then locate the file under the program files directory.



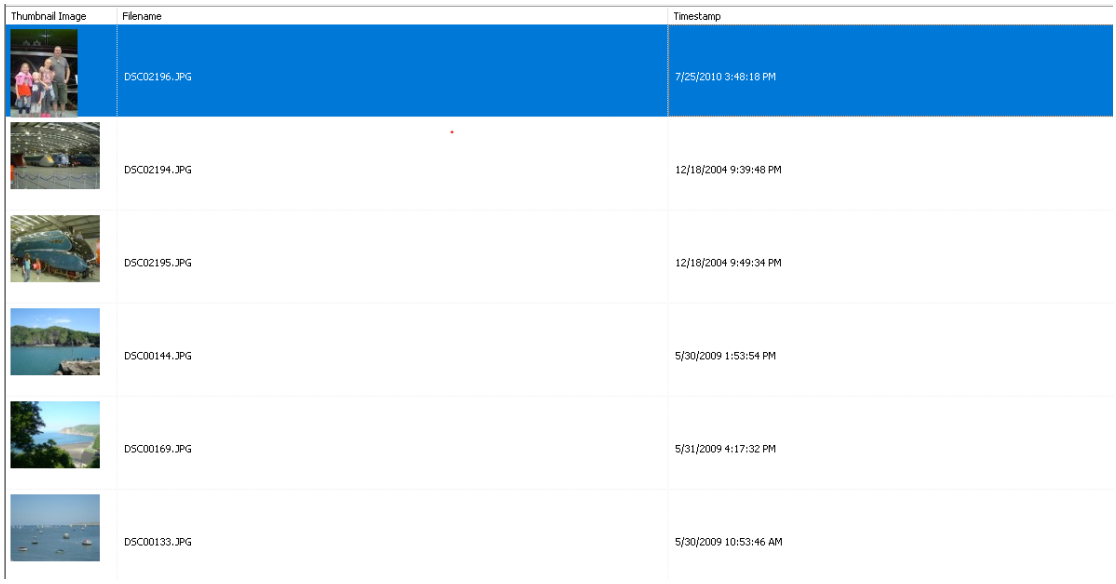
- Then export the located thumbs.db file to a folder called “23 thumbs db” on desktop of the machine.



- Then we need the windows file analyzer tool. After opening that tool go to file > analyze thumbnail database > Windows XP. then select the file that we found earlier using FTK imager.



- Then we can see a thumbnail views and their time stamps clearly.

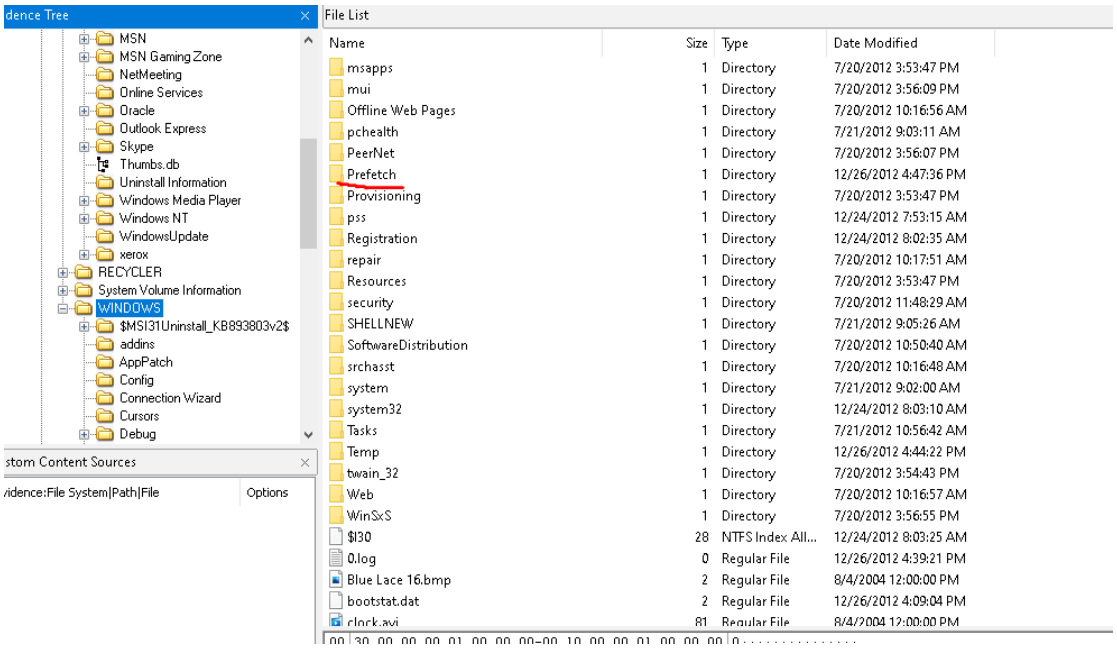


Thumbnail Image	Filename	Timestamp
	DSC02196.JPG	7/25/2010 3:48:18 PM
	DSC02194.JPG	12/18/2004 9:39:48 PM
	DSC02195.JPG	12/18/2004 9:49:34 PM
	DSC00144.JPG	5/30/2009 1:53:54 PM
	DSC00169.JPG	5/31/2009 4:17:32 PM
	DSC00133.JPG	5/30/2009 10:53:46 AM

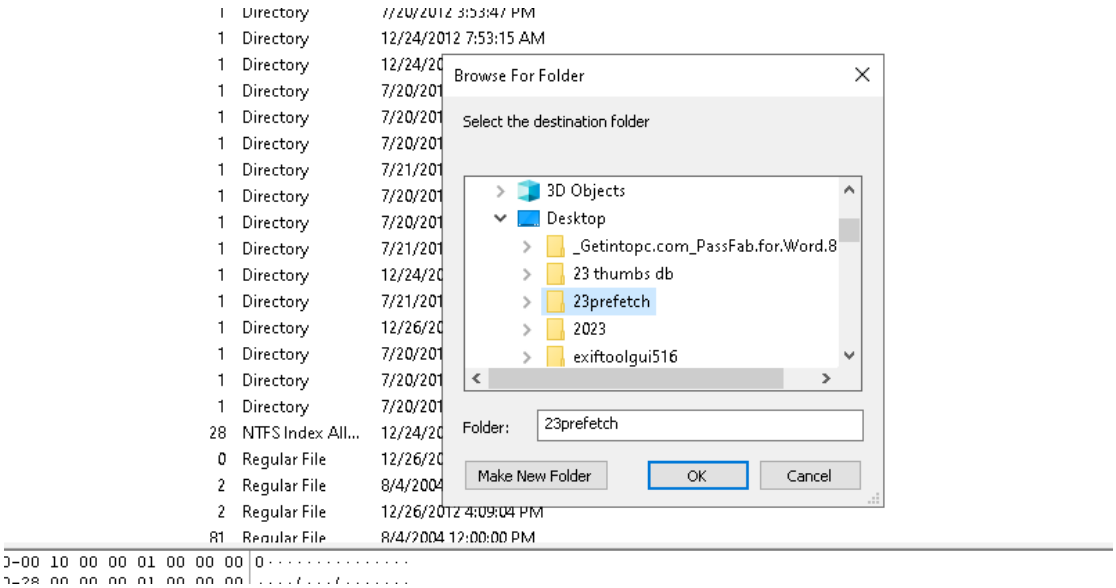
b) Identify the 2nd most frequently executed program on the computer included in the image?

Answer

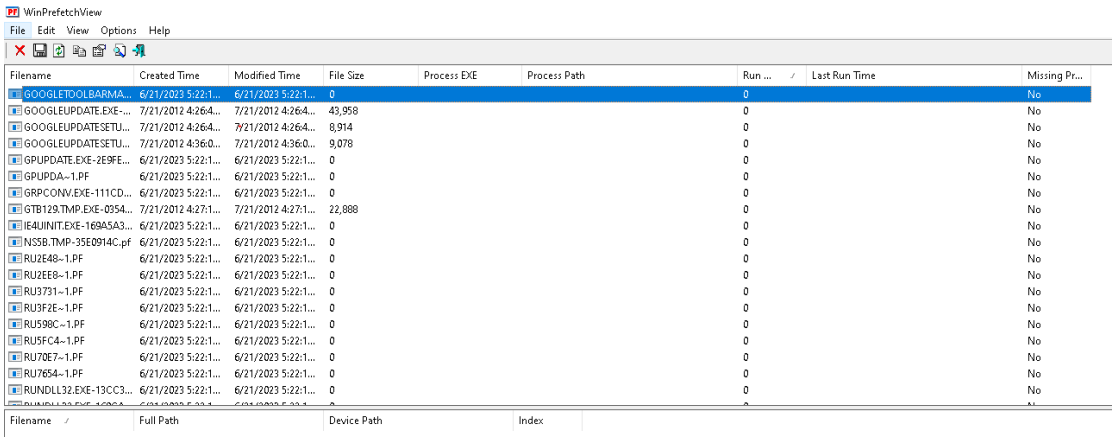
- First I located the file using FTK imager



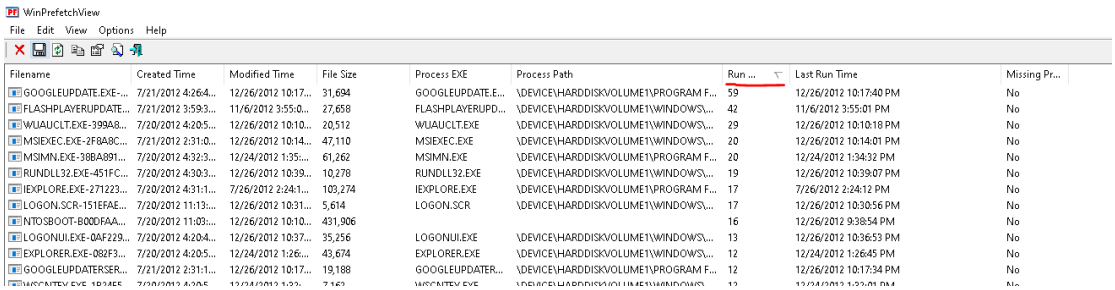
- Then we need to export to another location of our forensic lab machine.i named that destination folder as “ 23prefetch”.



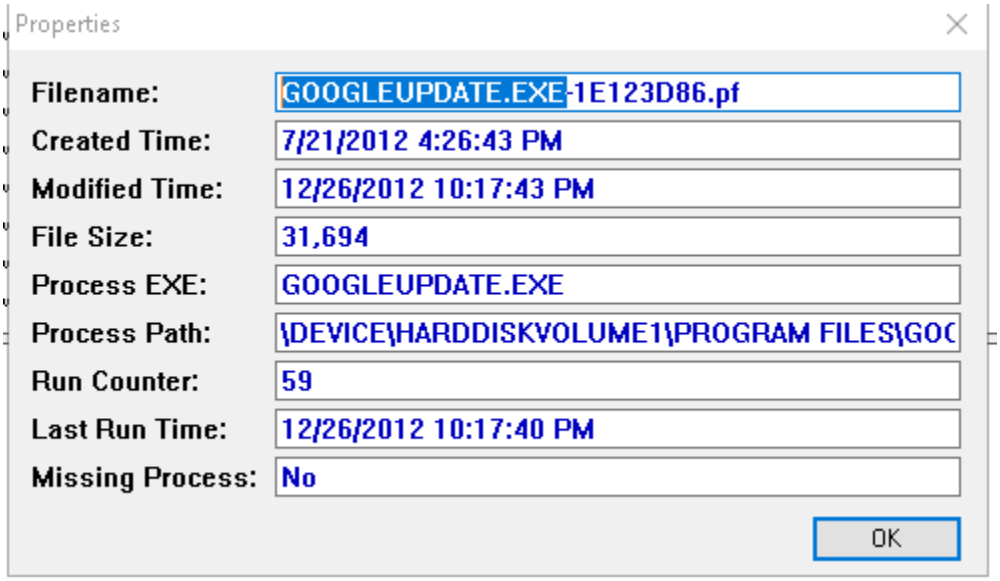
- Then I need winprefetchview tool to analyse this.but when I open it it shows the lab machine's prefetch files.i don't need those files.so go to options>advance options and give the exported prefetch file's location.
- Now I can see the prefetch files that I want to analyse.



- Then we need to click on the "Run" tab to sort the prefetch files.



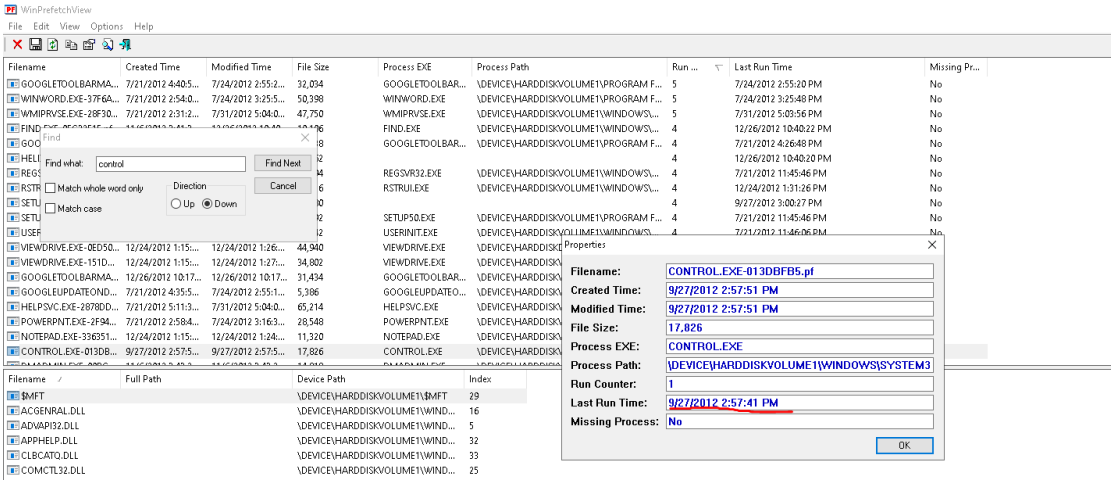
- Accoding to this analyse the most frequently executed program is "GOOGLEUPDATE.EXE"



c) When was the "control.exe" was last executed on this computer included in the image?

Answer

- to locate the control.exe we can use the search option.then click on the located entry to see its details.

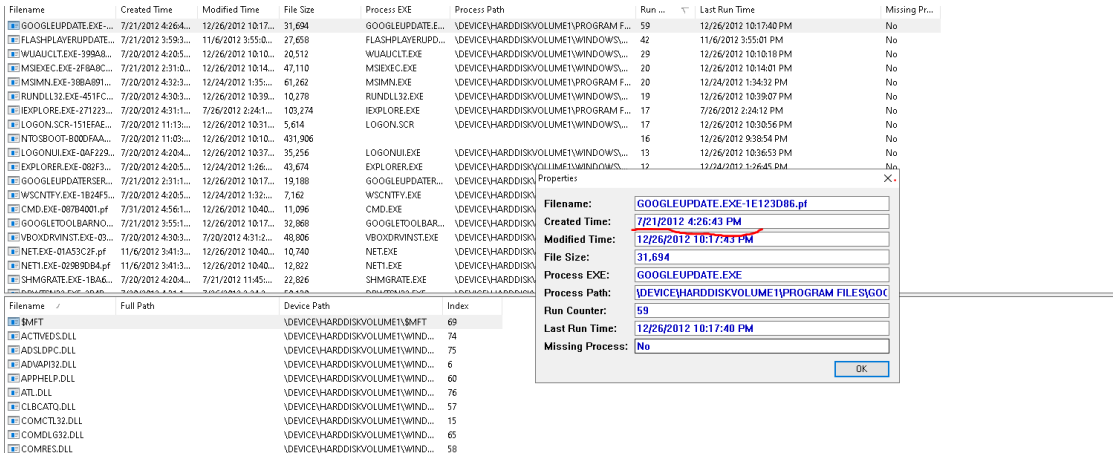


- As it shows the last run time is at 2:57:41 PM on 9/27/2012 .

d) When was the "googleupdate.exe" was first executed on this computer included in the image?

Answer

As same as the previous one I located the entry using search option and click on it to see it's details.



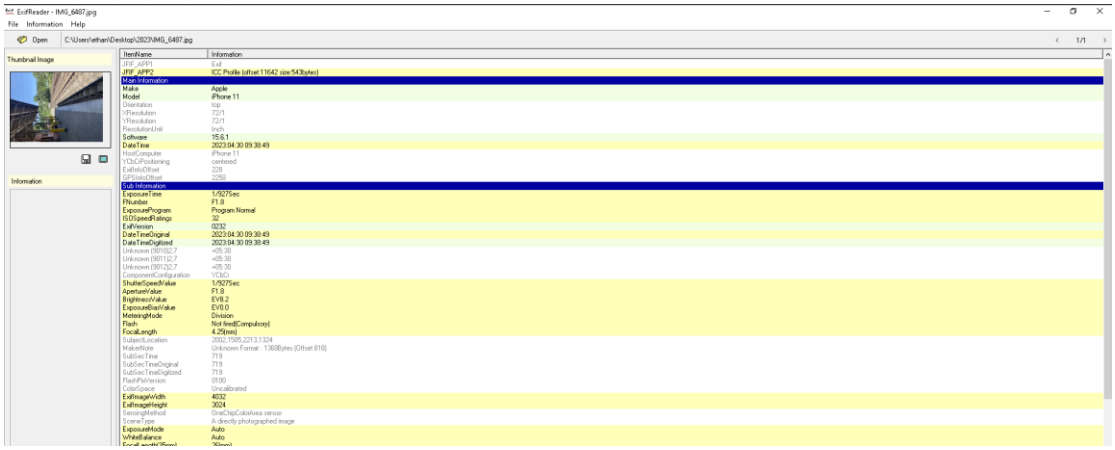
- The entry was created when the program executed for the first time .so according to this was executed for the first time on 7/21/2012 at 4:26:43 PM.

e) Examine the "IMG_6487.jpg" available to and answer the following questions.

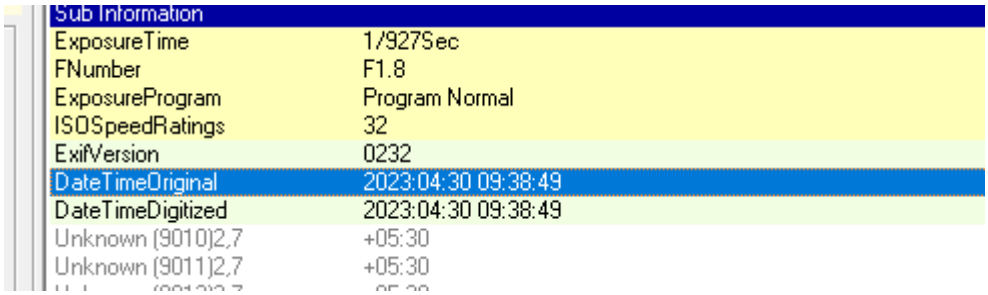
i) What is the date and time that the picture was taken?

Answer

- To do this we need exifread tool to read the image's exif data.so I open the file using the exifread tool.



- After doing some analysis on this data we can find the date and time the picture was taken.



- The date is 2023:04:30 and the time is 09:38:49.

ii) What is the Degrees, Minutes & Seconds and Reference Points (N,S,W,E) of the picture?

- To find this we need to go through the exifdata using exifread.

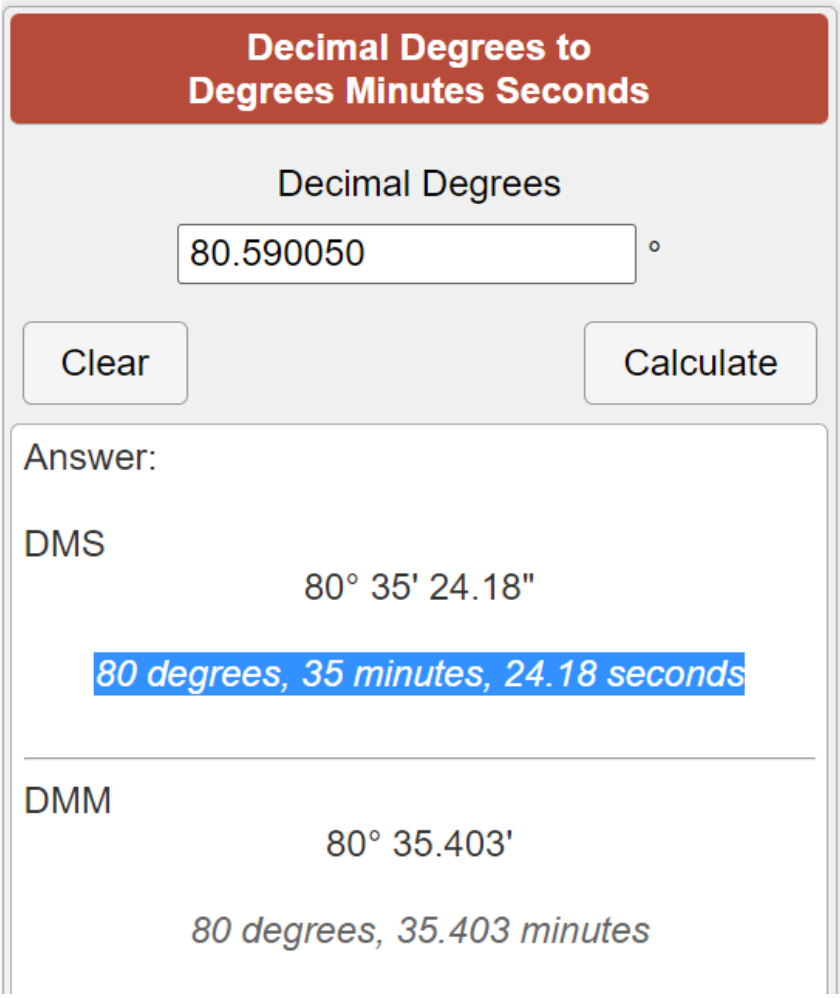
GPS Informtion	
GPSLatitudeRef	N
GPSLatitude	7 1526.6 [DMS]
GPSLongitudeRef	E
GPSLongitude	80 3524.18 [DMS]
GPSAltitudeRef	Sea level
GPSAltitude	846297/1766 meters
GPSSpeedRef	K
GPSSpeed	30209/70205
GPSImgDirectionRef	True direction
GPSImgDirection	248.16
GPSDestBearingRef	True direction
GPSDestBearing	248.16
Unknown (31)	120541/24622
Thumbnail Information	
Compression	OLDJPEG

- Then

Latitude north *7 degrees, 15 minutes, 26.6004 seconds*

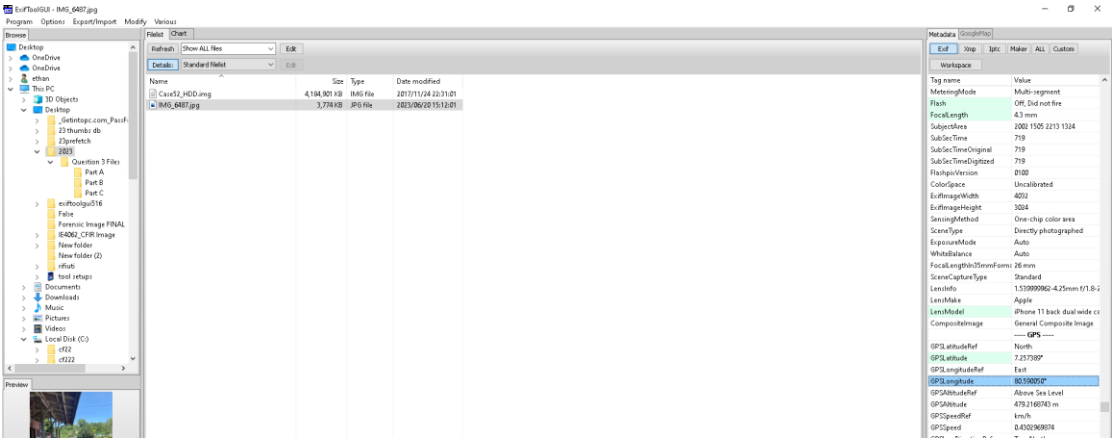
Longitude east *80 degrees, 35 minutes, 24.18 seconds*

- For calculate this we need a calculater



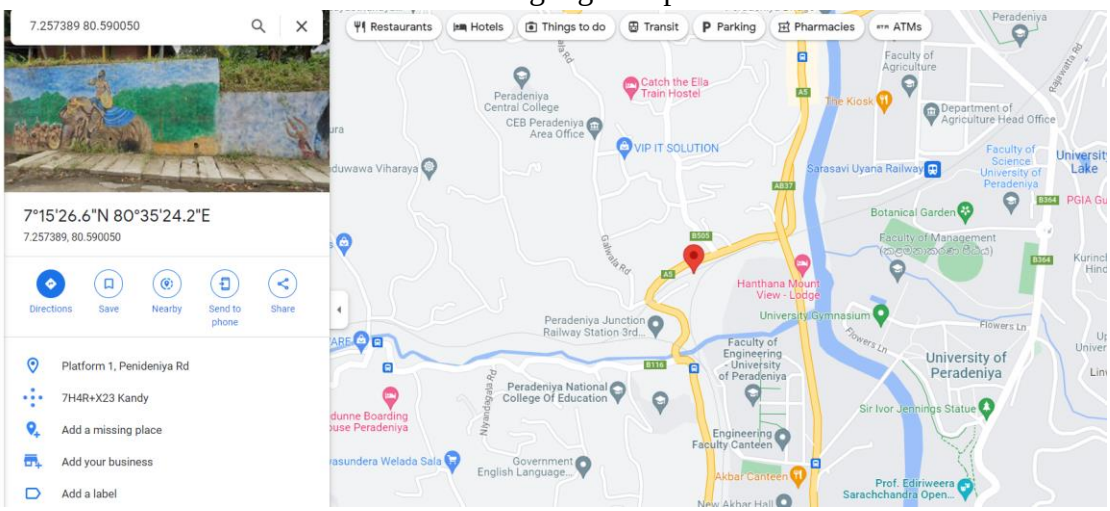
iii) Where, exactly the location of the photo? (Location Name).

- To get the correct latitiude and the longitude I used a another exifdata reader called “exiftoolgui”.



GPSLatitudeRef	North
GPSLatitude	7.257389°
GPSLongitudeRef	East
GPSLongitude	80.590050°
GPSAltitudeRef	Above Sea Level
GPSAltitude	479.2168743 m

- Now we can enter these values to the google map to find the exact location.

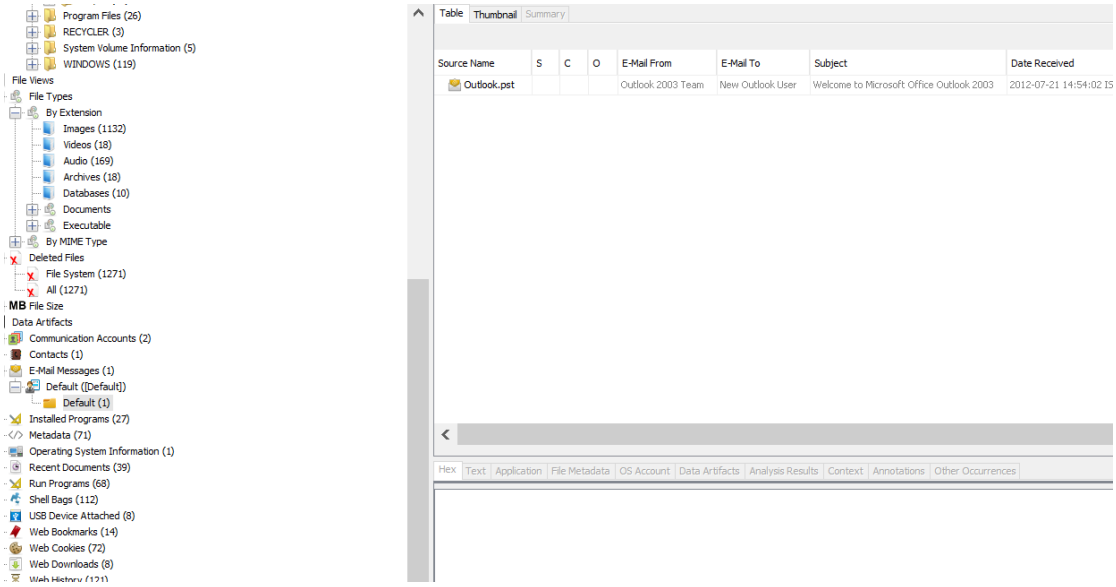


Question 2 (20 marks)

Use the raw image "Case52_HDD" file to complete the following.

a) What is the email client application used by the user? (Name the exact client)

- It is outlook using autopsy we can easily find it under the email messages.



b) Determine whether any sensitive information stored in the user email and justify your answer with the relevant evidence (i.e. user email account details and message artefacts)

c) Can you identify any document(s) which may contain evidence about the (personal details) user? List the evidence name(s) and the location(s)

d) Which web browser is used by the user?

e) Determine the list of typed URLs.

Question 3 (30 marks)

a) Use the windows memory dump file "Windows_Mem_Dump.raw" provided to answer the following Questions.

i) From which operating system this memory dump is taken? (Name the most probable OS)?

ii) Determine the list of all the processor(s) that were running when the memory was captured.

iii) Determine the TCP connection(s) that were active at the time of the memory acquisition.

b) Use the windows memory dump file "Memory_Img.raw" to answer the following Questions. You are required to provide a screenshot of your result and command you have executed.

i) Determine the list of all the processor(s) that were running when the memory was captured.
ii) List the suspicious process and explain why it is suspicious.
iii) List DLLs from this memory image.
iv) What type of malware is identified? Justify your answer.

c) Use "Reply Email" to answer the following Questions.
i) What is the attacker's email address?
ii) What is the victim's email address?
iii) What is the attack that the attacker was planning to conduct? Justify your answer with evidence.

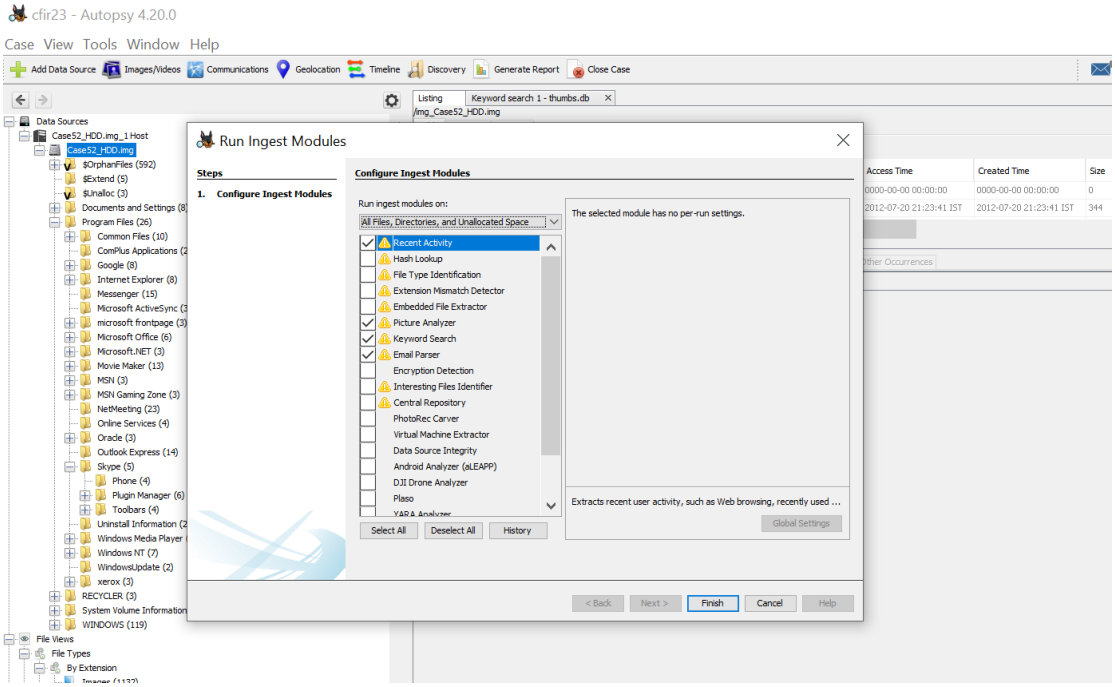
Question 4 (20 marks)

Use the raw image "Case52_HDD" file to complete the following.

a) Identify list of searched files.

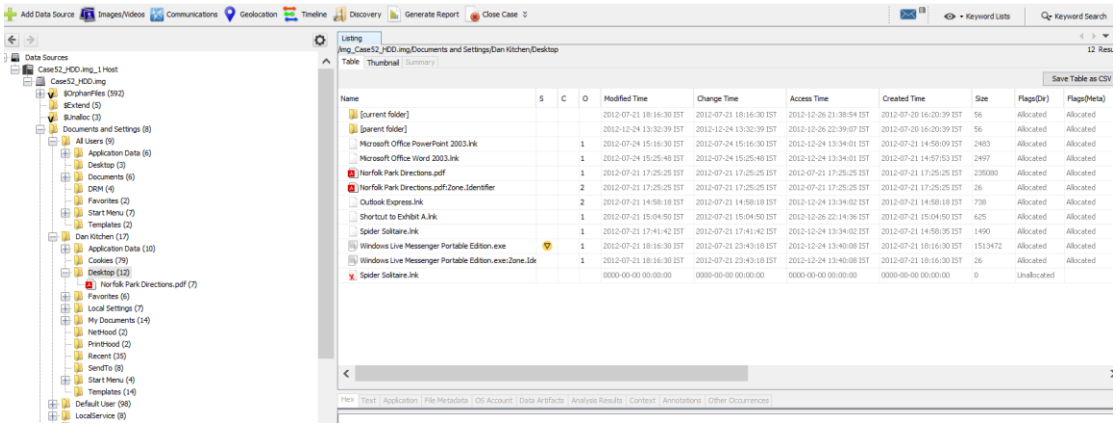
Answer

- To do this I'm using autopsy tool. For that I added the image to the tool and enable the needed modules under "run ingest modules'.



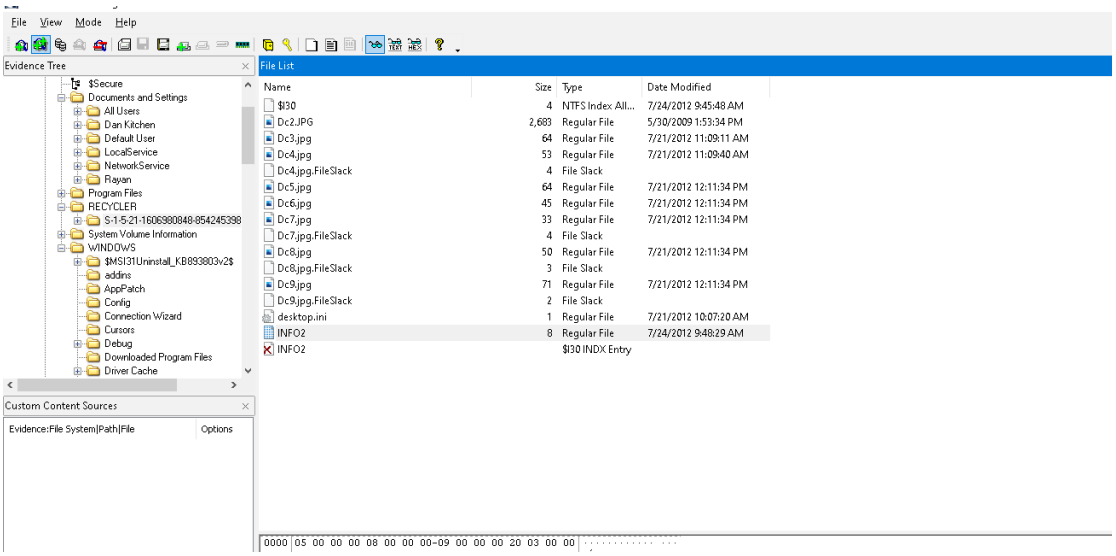
b) Which files are on the user Desktop?

- To do this we can easily go the the users location using autopsy.for that we can go to the image file>documents and settngs>Dan kitchen>desktop.

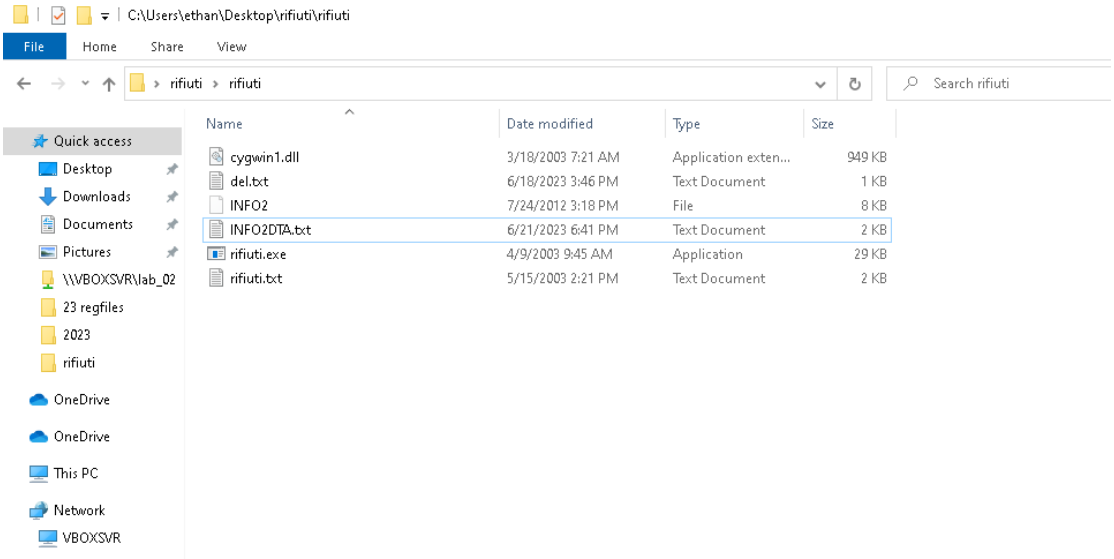


c) Identify which files were deleted and are still in the Recycle bin.

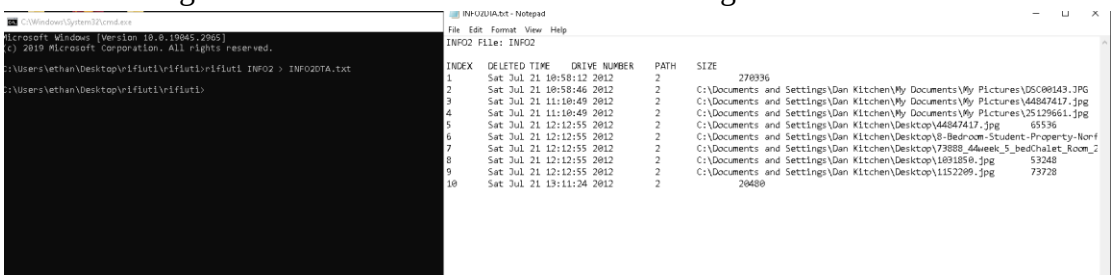
- To identify deleted files we have to find the INFO2 file . for that we can use FTK imager and export that file to another prefered location.



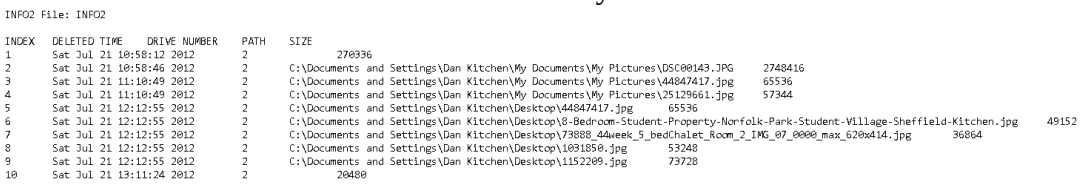
- Then we can use rifiuti .to do that I moved the info2 file to the same directory that rifiuti program exists.



- Then using cmd we can run the refiuti tool.in here I got the results to a txt file.



- Now we have the files which are in the recycle bin.

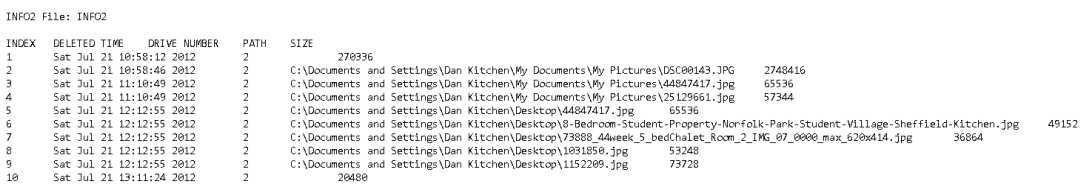


```
INFO2 File: INFO2

INDEX   DELETED TIME    DRIVE NUMBER    PATH    SIZE
1       Sat Jul 21 10:58:12 2012        2               270336
2       Sat Jul 21 10:58:46 2012        2       C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\DSC00143.JPG     2748416
3       Sat Jul 21 11:10:49 2012        2       C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\44847417.jpg     65536
4       Sat Jul 21 11:10:49 2012        2       C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\25129661.jpg     57344
5       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\44847417.jpg      65536
6       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\8-Bedroom-Student-Property-Norfolk-Park-Student-Village-Sheffield-Kitchen.jpg     49152
7       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\73888_44week_5_bedChalet_Room_2_IMG_07_0000_max_620x414.jpg       36864
8       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\1031850.jpg       53248
9       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\1152209.jpg       73728
10      Sat Jul 21 13:11:24 2012        2               20480
```

d) List of actual locations of the deleted files.

- In the previous step we got the file locations as well.



```
INFO2 File: INFO2

INDEX   DELETED TIME    DRIVE NUMBER    PATH    SIZE
1       Sat Jul 21 10:58:12 2012        2               270336
2       Sat Jul 21 10:58:46 2012        2       C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\DSC00143.JPG     2748416
3       Sat Jul 21 11:10:49 2012        2       C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\44847417.jpg     65536
4       Sat Jul 21 11:10:49 2012        2       C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\25129661.jpg     57344
5       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\44847417.jpg      65536
6       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\8-Bedroom-Student-Property-Norfolk-Park-Student-Village-Sheffield-Kitchen.jpg     49152
7       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\73888_44week_5_bedChalet_Room_2_IMG_07_0000_max_620x414.jpg       36864
8       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\1031850.jpg       53248
9       Sat Jul 21 12:12:55 2012        2       C:\Documents and Settings\Dan Kitchen\Desktop\1152209.jpg       73728
10      Sat Jul 21 13:11:24 2012        2               20480
```

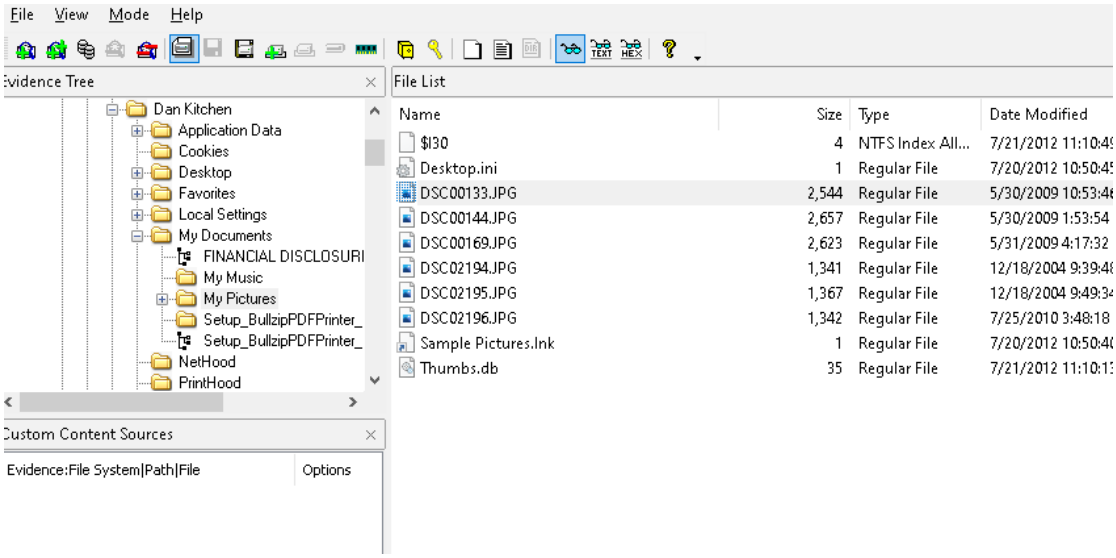
e) Assuming that the images stored on the disk image were taken with the machine's owner digital camera, what make, and model was the digital camera used?

to do this we can go to the file location

INFO2 File: INFO2

INDEX	DELETED TIME	DRIVE NUMBER	PATH	SIZE
1	Sat Jul 21 10:58:12 2012	2		270336
2	Sat Jul 21 10:58:46 2012	2	C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\DSC00143.JPG	2748416
3	Sat Jul 21 11:10:49 2012	2	C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\44847417.jpg	65536
4	Sat Jul 21 11:10:49 2012	2	C:\Documents and Settings\Dan Kitchen\My Documents\My Pictures\25129661.jpg	57344
5	Sat Jul 21 12:12:55 2012	2	C:\Documents and Settings\Dan Kitchen\Desktop\44847417.jpg	65536
6	Sat Jul 21 12:12:55 2012	2	C:\Documents and Settings\Dan Kitchen\Desktop\8-Bedroom-Student-Property-Norfolk-Park-Student-Village-Sheffield-Kitchen.jpg	49152
7	Sat Jul 21 12:12:55 2012	2	C:\Documents and Settings\Dan Kitchen\Desktop\73888_44week_5_bedChalet_Room_2_IMG_07_0000_max_620x414.jpg	36864
8	Sat Jul 21 12:12:55 2012	2	C:\Documents and Settings\Dan Kitchen\Desktop\1031850.jpg	53248
9	Sat Jul 21 12:12:55 2012	2	C:\Documents and Settings\Dan Kitchen\Desktop\1152209.jpg	73728
10	Sat Jul 21 13:11:24 2012	2		20480

I choose the first location.and using ftk imager I went to that location and get one image exported

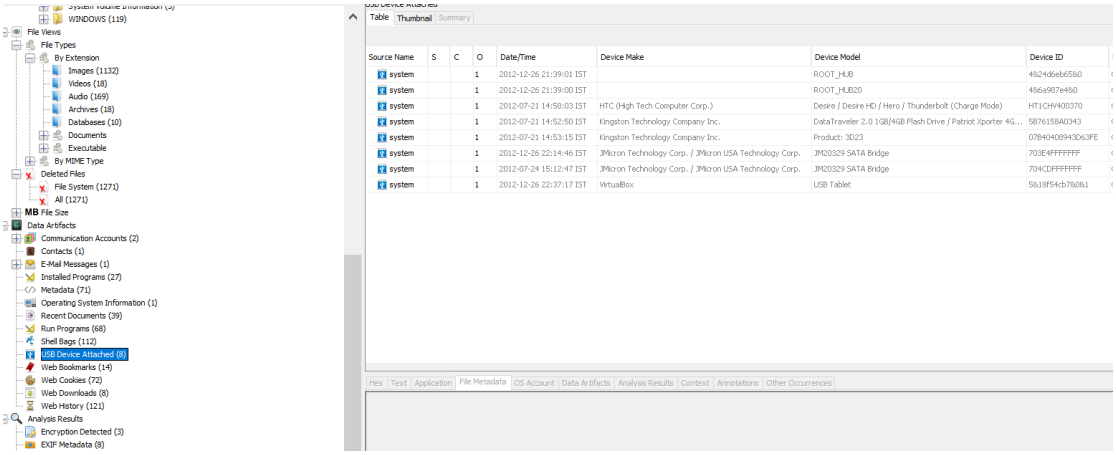


Then using exifread we can red the exifdate.

In here we can see the camera model.

f) What information can you gather about that USB mass storage devices plug into this machine?

To do this we can use autopsy .by following the file tree we can find the "usb device attach"and expand it.



-- End of the Question Paper --