

**Name : R.K.G.H.Rathnayaka**

**SLIIT ID : IT21022210**



**Sri Lanka Institute of Information Technology**

**B.Sc. Honours Degree in Information Technology**

**Specialized in Cyber Security**

**Practical Examination  
Year 4, Semester 1(2024)**

**IE4062 - Cyber Forensics and Incident Response**

**Duration: 2 Hours**

**June 2024**

**Instructions to candidate:**

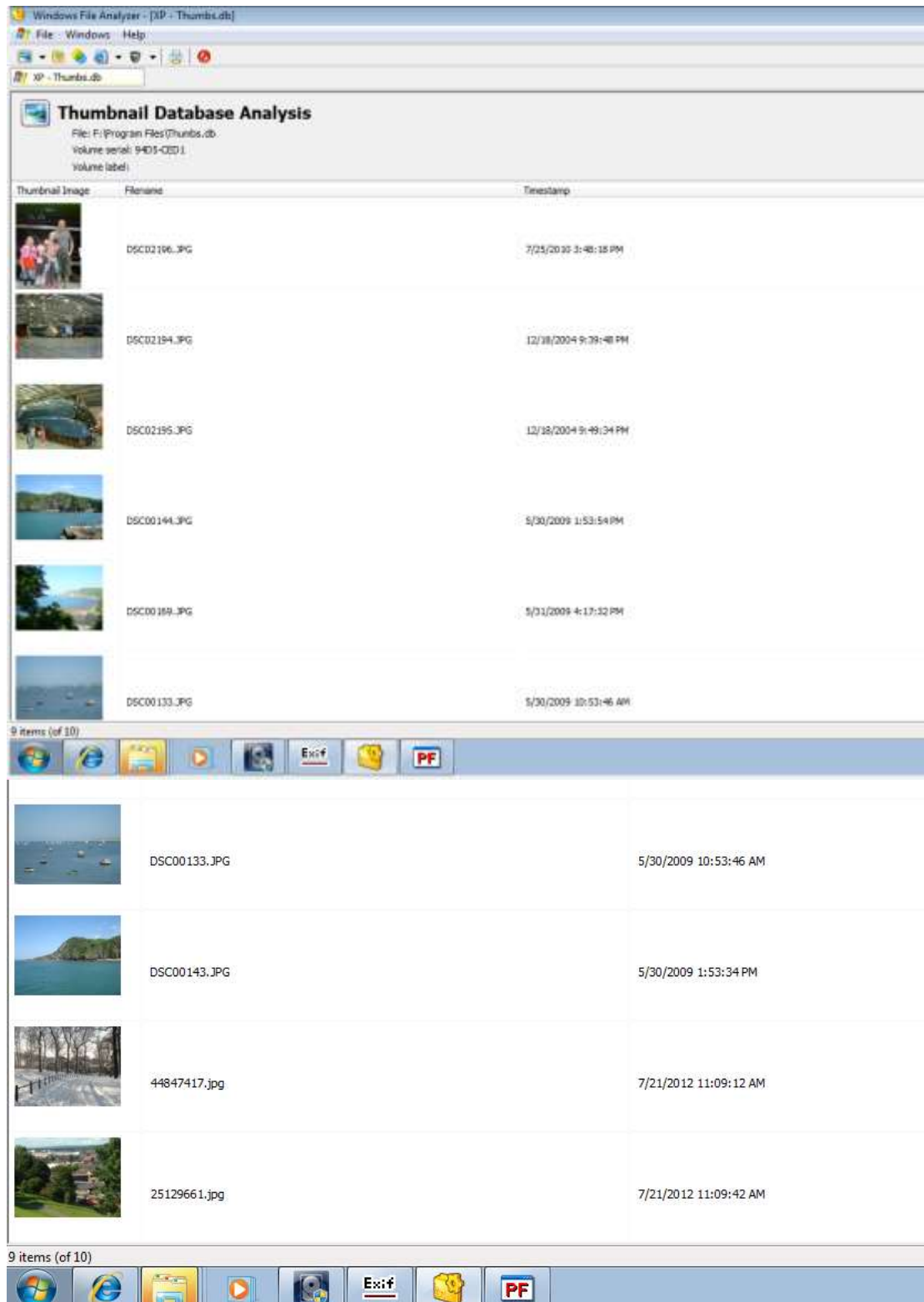
- ◆ Paper contains 4 Questions. Answer all questions.
- ◆ This paper contains 4 pages including cover page.
- ◆ Exam time is 10.00am to 12.00noon.
- ◆ You are expected to upload report with answers (pdf) to courseweb submission link before 12.10pm











## Question 1

(30 marks)

Use the raw image “Accused1\_HDD” file to answer the following Questions.

- a) Using the “Thumbs.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.



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
9 items (of 10)		
	DSC00133.JPG	5/30/2009 10:53:46 AM
	DSC00143.JPG	5/30/2009 1:53:34 PM
	44847417.jpg	7/21/2012 11:09:12 AM
	25129661.jpg	7/21/2012 11:09:42 AM
9 items (of 10)		

b) Identify the 3<sup>rd</sup> most frequently executed program on the computer included in the image?

- WUAUCLT.EXE-399A8E72.pf

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run ...	Last Run Time	Missing P...
GOOGLEUPDATE.EXE-1B12D86.pf	7/25/2012 6:56:4...	12/27/2012 12:47...	31,694	GOOGLEUPDATE.E...	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	39	12/27/2012 12:47:40 AM	No
FLASHPLAYERUPDATESERVICE.EXE-348C3027.pf	7/25/2012 6:29:3...	11/6/2012 6:25:0...	27,658	FLASHPLAYERUPD...	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	42	11/6/2012 6:25:01 PM	No
WUAUCLT.EXE-399A8E72.pf	7/25/2012 6:56:4...	12/27/2012 12:46...	35,912	WUAUCLT.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	36	12/27/2012 12:46:39 AM	No
MSEXEC.EXE-39A8CAE.pf	7/25/2012 5:01:0...	12/27/2012 12:44...	47,110	MSEXEC.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	39	12/27/2012 12:44:01 AM	No
MSMNS.EXE-3B8AB8D.pf	7/26/2012 7:02:3...	12/24/2012 4:05:...	61,362	MSMNS.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	38	12/24/2012 4:04:52 PM	No
RUNDLL32.EXE-451FC2D3.pf	7/26/2012 7:00:3...	12/27/2012 1:09:...	38,278	RUNDLL32.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	19	12/27/2012 1:09:07 AM	No
EXPLORER.EXE-271212D4.pf	7/26/2012 7:01:1...	7/26/2012 4:54:1...	195,234	EXPLORER.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	17	7/26/2012 4:54:12 PM	No
LOGONSCR-151F6A8.pf	7/25/2012 1:49:2...	12/27/2012 1:25:...	5,614	LOGONSCR	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	17	12/27/2012 1:00:58 AM	No
NTOSDDOT-BNDFAD.pf	7/25/2012 1:33:4...	12/27/2012 12:43...	431,366			38	12/27/2012 12:08:54 AM	No
LOGONUIEXE-0AF20937.pf	7/26/2012 6:50:4...	12/27/2012 1:07:...	35,258	LOGONUIEXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	11	12/27/2012 1:06:53 AM	No
EXPLORER.EXE-9B3F36A9.pf	7/26/2012 6:50:5...	12/24/2012 3:54:...	43,674	EXPLORER.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	12	12/24/2012 3:56:45 PM	No
GOOGLUPDATESERVICE.EXE-348C3027.pf	7/25/2012 5:01:1...	12/27/2012 12:47...	39,188	GOOGLUPDATE.S...	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	12	12/27/2012 12:47:34 AM	No
WSCNTFY.EXE-1B24F5E.pf	7/26/2012 6:50:5...	12/24/2012 4:02:...	7,362	WSCNTFY.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	12	12/24/2012 4:02:05 PM	No
CMD.EXE-0B784061.pf	7/25/2012 7:26:1...	12/27/2012 1:18:...	11,096	CMD.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	11	12/27/2012 1:10:25 AM	No
GOOGLTOOLBARNOTIFIER.EXE-362BC81D.pf	7/25/2012 6:25:1...	12/27/2012 12:47...	32,868	GOOGLTOOLBAR...	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	9	12/27/2012 12:47:38 AM	No
VBODRVINST.EXE-9387F4D.pf	7/26/2012 7:00:3...	7/26/2012 7:01:2...	48,806	VBODRVINST.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	9	7/26/2012 7:01:22 PM	No
NET.EXE-01A5C2F.pf	12/6/2012 6:11:3...	12/27/2012 1:18:...	10,740	NET.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	8	12/27/2012 1:10:20 AM	No

c) When was the “control.exe” was first executed on this computer included in the image?

- First executed on 9/24/2012 at 5:27:51 PM

DWWWIN.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	6	7/26/2012 4:54:23 PM
EXPLORER.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	12	12/24/2012 3:56:45 PM
FIND			10:22 AM
FLAS			6:11 PM
FLAS			5:01 PM
GOO			2:44:00 AM
GOO			8:07 PM
GOO			3:00 AM
GOO			2:44:50 AM
GOO			2:47:37 AM
GOO			6:10 PM
ISKVOLUME1\WIND...		25	
ISKVOLUME1\WIND...		27	

Properties

Filename:

CONTROL.EXE-013DBFB5.pf

Created Time:

9/27/2012 5:27:51 PM

Modified Time:

9/27/2012 5:27:51 PM

File Size:

17,826

Process EXE:

CONTROL.EXE

Process Path:

\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM3

Run Counter:

1

Last Run Time:

9/27/2012 5:27:41 PM

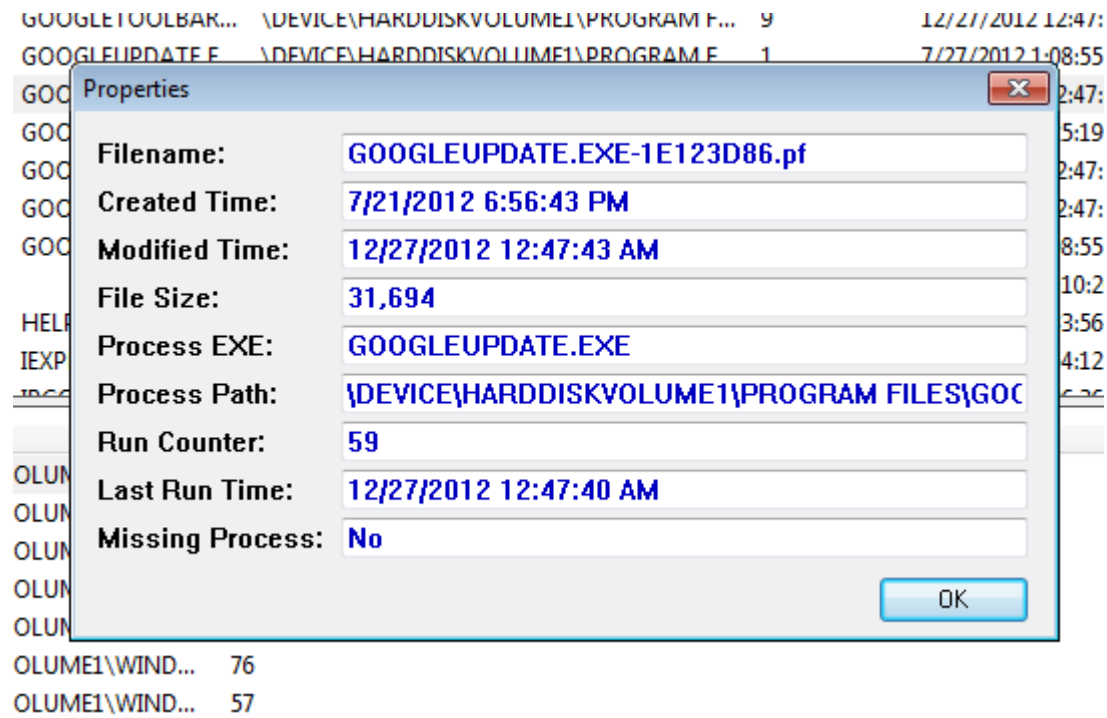
Missing Process:

No

OK

d) When was the “googleupdate.exe” was last executed on this computer included in the image?

- File last executed was 12/27/2012 at 12:47:40 AM



e) Examine the “IMG\_8192.jpg” available to and answer the following questions.

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

- Date: 2023-11-15
- Time: 10.25AM

IPTC	
Character-code definition	1B2547
Record version	0002
Taking a picture time	102526+0800
Taking a picture day	2023-11-15
Main Information	
Make	Apple
Model	iPhone 11


## Additional Data

ExifReader - IMG\_8192.jpg

File Information Help

Open \WB0XSVR\Wbox\Windows7-Shared\_Folder\CFIR LABTEST FINAL\IE4062\_CFIR Image\IMG\_8192.jpg

Thumbnail Image



GPSLongitudeRef

E

ItemName	Information
Unknown (9012)2,7	+08:00
ComponentConfiguration	YCbCr
ShutterSpeedValue	1/121Sec
ApertureValue	F1.8
BrightnessValue	EV4.3
ExposureBiasValue	EV0.0
MeteringMode	Division
Flash	Not fired(Compulsory)
FocalLength	4.25(mm)
SubjectLocation	693,1610,362,364
MakerNote	Unknown Format : 1336Bytes (Offset:818)
SubSecTime	423
SubSecTimeOriginal	423
SubSecTimeDigitized	423
FlashPixVersion	0100
ColorSpace	Uncalibrated
ExifImageWidth	4032
ExifImageHeight	3024
SensingMethod	OneChipColorArea sensor
SceneType	A directly photographed image
ExposureMode	Auto
WhiteBalance	Auto
FocalLength(35mm)	26(mm)
SceneCaptureType	Standard
Unknown (A432)5,4	807365/524263,17/4,9/5,12/5
Unknown (A433)2,6	Apple
Unknown (A434)2,45	iPhone 11 back dual wide camera 4.25mm f/1.8
Unknown (A460)3,1	2
<b>GPS Information</b>	
GPSLatitudeRef	N
GPSLatitude	3 2444.97 [DMS]
GPSLongitudeRef	E
GPSLongitude	101 4718.62 [DMS]
GPSAltitudeRef	Sea level
GPSAltitude	980153/691 meters
GPSTimeStamp	20:00:00
GPSSpeedRef	K
GPSSpeed	0/1
GPSTimeDirectionRef	True direction
GPSTimeDirection	167.201
GPSTimeBearingRef	True direction
GPSTimeBearing	167.201
GPSTimeStamp	2023:11:15
Unknown (31)	77251/14962
<b>Thumbnail Information</b>	
Compression	OLDJPEG
XResolution	72/1
YResolution	72/1
ResolutionUnit	Inch
JPEGInterchangeFormat	2630
JPEGInterchangeFormatLen...	9277

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

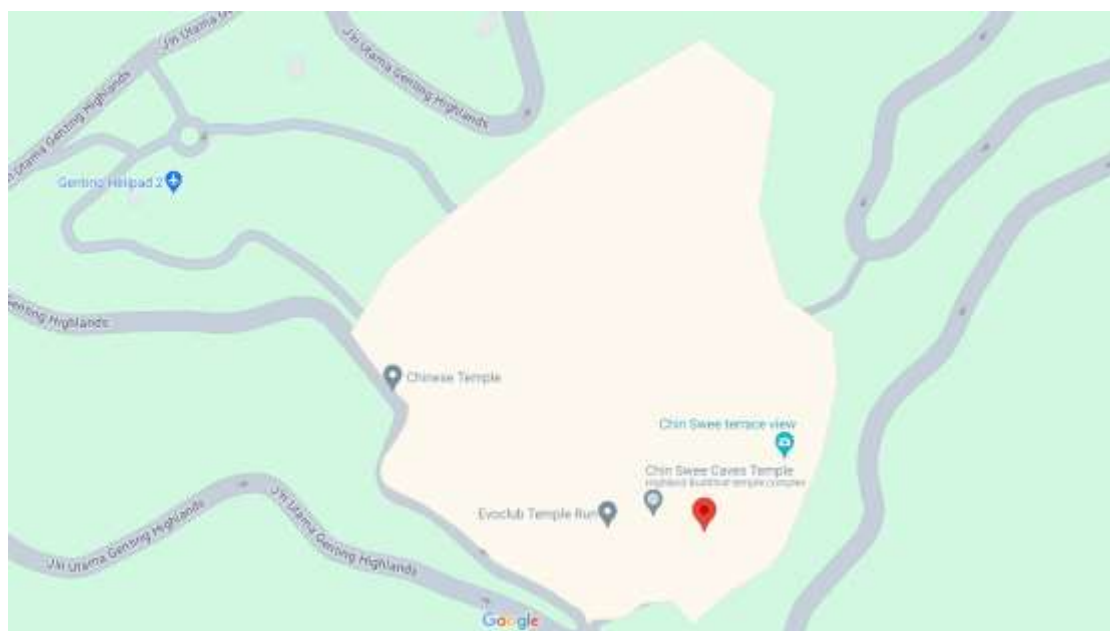
- GPS Latitude DMS: 3 2444.97
- GPS Longitude DMS: 101 4718.62
- 3 2444.97
- Degrees : 3 , Minutes: 24 , Seconds : 44.97
- 101 4718.62

- Degrees : 101 , Minutes: 24 , Seconds : 44.97

- Geolocation: 3°24'45.0"N 101°47'18.6"E

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

- The location is Chin Swee Caves Temple, 69000 Genting Highlands, Pahang, Malaysia



## Question 2

(20 marks)

Use the raw image “Accused1\_HDD” file to complete the following.

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

- Microsoft Outlook

Source Name	S	C	O	E-Mail From	E-Mail To	Subject
Outlook.pst				Outlook 2003 Team <olteam@microsoft.com>	New Outlook User	Welcome to Microsoft Office Outlook 2003

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

Yes

URL	Title	Date Created	Program Name
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	Customize Links.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h...	Free Hotmail.url	2012-07-20 1..	Internet Explorer Analyzer
http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0.	Windows Marketplace.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w...	Windows Media.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w...	Windows.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	MSN.com.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=windows..	Radio Station Guide.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	Customize Links.url	2012-07-21 2..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h...	Free Hotmail.url	2012-07-21 2..	Internet Explorer Analyzer

(5 Marks)

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)

(5 Marks)

















URL	Title	Date Created	Program Name
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	Customize Links.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h...	Free Hotmail.url	2012-07-20 1..	Internet Explorer Analyzer
http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0.	Windows Marketplace.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w...	Windows Media.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w...	Windows.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	MSN.com.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=windows..	Radio Station Guide.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	Customize Links.url	2012-07-21 2..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h...	Free Hotmail.url	2012-07-21 2..	Internet Explorer Analyzer

**d) Which web browser is used by the user?**

- Internet explorer web browser

URL	Title	Date Created	Program Name
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	Customize Links.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h...	Free Hotmail.url	2012-07-20 1..	Internet Explorer Analyzer
http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0.	Windows Marketplace.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w...	Windows Media.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w...	Windows.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	MSN.com.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=windows..	Radio Station Guide.url	2012-07-20 1..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver...	Customize Links.url	2012-07-21 2..	Internet Explorer Analyzer
http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h...	Free Hotmail.url	2012-07-21 2..	Internet Explorer Analyzer

**e) Determine the list of typed URL.**

Web History						
Table	Thumbnail	Summary				
Source Name	S	C	O	URL	Date Accessed	
 index.dat			0	bing.com/	2012-07-26 08:54:19 IST	I
 index.dat			0	c.bing.com/	2012-07-20 11:01:55 IST	I
 index.dat			0	bullzip.com/	2012-07-21 10:41:19 IST	I
 index.dat			0	bbc.co.uk/	2012-07-21 10:19:36 IST	I
 index.dat			0	accommodationforstudents.com/	2012-07-22 17:11:47 IST	I
 index.dat			0	2o7.net/	2012-07-21 10:19:45 IST	I
 index.dat			0	gigya.com/	2012-07-21 10:42:18 IST	I
 index.dat			0	adshost1.com/	2012-07-21 12:52:58 IST	I
 index.dat			0	4shared.com/	2012-07-21 12:53:05 IST	I
 index.dat			0	adnxs.com/	2012-07-26 08:54:23 IST	I
 index.dat			0	bluekai.com/	2012-07-21 10:42:15 IST	I
 index.dat			0	www.bing.com/	2012-07-26 08:54:19 IST	I
 index.dat			0	ehow.com/	2012-07-21 10:19:05 IST	I
 index.dat			0	facebook.com/	2012-07-24 09:53:27 IST	I
 index.dat			0	download.cnet.com/	2012-07-21 10:42:13 IST	I
 index.dat			0	ebay.co.uk/	2012-07-21 10:20:57 IST	I

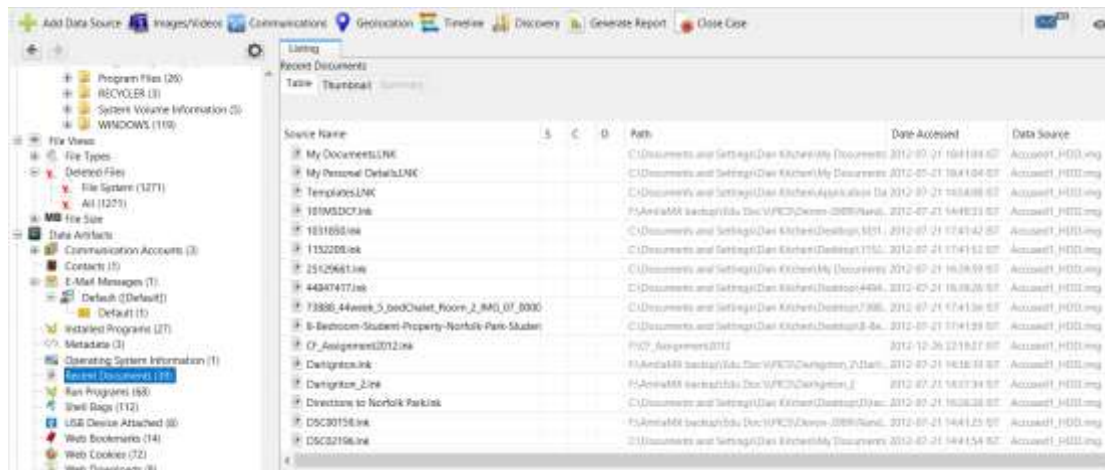


### Question 3

(20 marks)

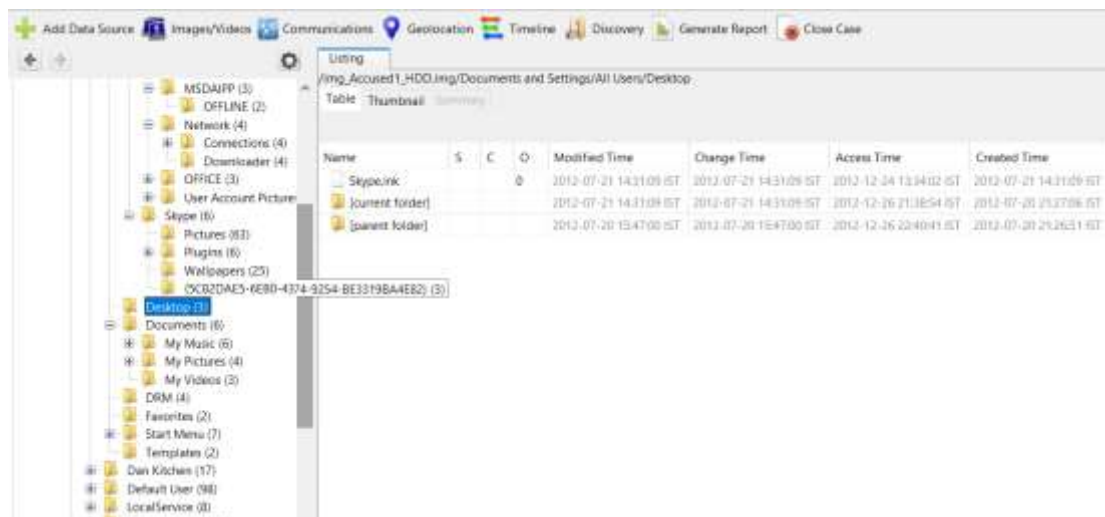
Use the raw image “Accused1\_HDD” file to complete the following.

a) Identify list of searched files.



b) Which files are on the user Desktop?

- All Users Desktop



- User: Dan Kitchen Desktop

Name	S	C	D	Modified Time	Change Time	Access Time
Windows Live Messenger Portable Edition.exe			0	2012-07-21 18:16:30 IST	2012-07-21 22:43:18 IST	2012-12-24 13:40:08 IST
Norfolk Park Directions.pdf			0	2012-07-21 17:25:25 IST	2012-07-21 17:25:25 IST	2012-07-21 17:25:25 IST
Microsoft Office Word 2003.doc			0	2012-07-24 13:25:48 IST	2012-07-24 13:25:48 IST	2012-12-24 13:34:01 IST
Microsoft Office PowerPoint 2003.ppt			0	2012-07-24 13:16:38 IST	2012-07-24 13:16:38 IST	2012-12-24 13:34:01 IST
Spider Solitaire.lnk			0	2012-07-21 17:41:42 IST	2012-07-21 17:41:42 IST	2012-12-24 13:34:02 IST
Outlook Express.lnk			0	2012-07-21 14:58:18 IST	2012-07-21 14:58:18 IST	2012-12-24 13:34:02 IST
Shortcut to Exhibit A.lnk			0	2012-07-21 13:04:30 IST	2012-07-21 13:04:30 IST	2012-12-26 22:14:06 IST
[parent folder]				2012-07-21 18:16:30 IST	2012-07-21 18:16:30 IST	2012-12-26 21:38:54 IST
[parent folder]				2012-12-24 13:32:39 IST	2012-12-24 13:32:39 IST	2012-12-26 23:39:07 IST
Norfolk Park Directions.pdf.Zone.Identifier			0	2012-07-21 17:25:25 IST	2012-07-21 17:25:25 IST	2012-07-21 17:25:25 IST
Windows Live Messenger Portable Edition.exe.Zone			0	2012-07-21 18:16:30 IST	2012-07-21 22:43:18 IST	2012-12-24 13:40:08 IST
Spider Solitaire.lnk				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

- Default User Desktop

Name	S	C	D	Modified Time	Change Time	Access Time	Created Time
[parent folder]				2012-07-20 16:20:37 IST	2012-07-20 16:20:37 IST	2012-12-24 12:45:08 IST	2012-07-20 21:12:00 IST
[current folder]				2012-07-20 21:27:06 IST	2012-07-20 21:27:06 IST	2012-07-21 18:09:29 IST	2012-07-20 21:12:00 IST

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

Name	S	C	D	Modified Time	Change Time	Access Time	Created Time	Size	Flags	Flags2
winres.dll.exe			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	418176	Hidden	Deleted
tsmon.exe			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	418176	Hidden	Deleted
BOO(TP).MACHINE_SYSTEM_PerformanceCopy			0	2012-11-26 22:00:00 IST	2012-11-26 22:00:00 IST	2012-11-26 22:00:00 IST	2012-07-20 21:26:17 IST	877676	Hidden	Deleted
exp2.exe			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	200702	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	607004	Hidden	Deleted
3dsg.exe			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	507767	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	604111	Hidden	Deleted
chnglog			0	2012-07-21 17:42:00 IST	2012-07-21 17:42:00 IST	2012-07-21 17:42:00 IST	2012-07-21 17:42:00 IST	80204	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	74946	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	74946	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	74946	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	74946	Hidden	Deleted
win32.sys			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	74946	Hidden	Deleted
GoogleUpdate.exe			0	2012-07-21 16:00:00 IST	2012-07-21 16:00:00 IST	2012-07-21 16:00:00 IST	2012-07-21 16:00:00 IST	143776	Hidden	Deleted
Recycle Bin			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	20344	Hidden	Deleted
Recycle Bin			0	2004-09-04 10:00:00 IST	2012-07-20 15:48:51 IST	2012-07-20 15:48:51 IST	2004-09-04 10:00:00 IST	20344	Hidden	Deleted

d) List of actual locations of the deleted files.

Listing									
Table Thumbnail Summary									
Name	S	C	O	Char.	Created	Known	Location		
Y wmm2res.dll.new			0	-	2012-05-22 2012-07-14 42	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/wmm2res.dll.new		
Y lsmamrt.new			0	-	2012-05-22 2004-06-14 41	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/lsmamrt.new		
Y _REGISTRY_MACHINE_SYSTEM_Fe			0	-	2012-05-22 2012-07-14 36	unknown	/img_Accused1_HDD/img/System Volume Information/_ntfsache/FAC8951D-C04B-4E71-8B36-100C1		
Y spsp2res.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/spsp2res.dll.new		
Y wmi2copy.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/wmi2copy.new		
Y bckgusd.dll.new			0	-	2012-05-22 2012-07-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/bckgusd.dll.new		
Y wmpdmr.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/wmpdmr.dll.new		
Y change.log			0	-	2012-05-22 2012-07-14 38	unknown	/img_Accused1_HDD/img/System Volume Information/_ntfsache/FAC8951D-C04B-4E71-8B36-100C1		
Y wmm2res.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/wmm2res.dll.new		
Y spb0406.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/spb0406.dll.new		
Y spb0424.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/spb0424.dll.new		
Y wmm2res.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/wmm2res.dll.new		
Y GoogleUpdateSetup_90698EA06			0	-	2012-05-22 2012-07-14 34	unknown	/img_Accused1_HDD/img/Orphan Files/GoogleUpdateSetup_90698EA060011Kase(112)		
Y MCD1.docx.new			0	-	2012-05-22 2004-06-14 32	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/MCD1.docx.new		
Y iusd.dll.new			0	-	2012-05-22 2004-06-14 38	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/iusd.dll.new		
Y fastprox.dll.new			0	-	2012-05-22 2012-07-14 47	known	/img_Accused1_HDD/img/WINDOWS/system32/ntfsache/fastprox.dll.new		

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?

Listing									
EXIF Metadata									
Table Thumbnail Summary									
Source Name	S	C	O	Source Type	Score	Date-Created	Device Model	Device Make	File Path
DSC00133.JPG			0	File	Not Notable	2009-05-30 11:53:48 IST	DSC-W130	SONY	/img_Accused1_HDD/img/Documents and Settings/Da...
DSC00144.JPG			0	File	Not Notable	2009-05-30 14:53:55 IST	DSC-W130	SONY	/img_Accused1_HDD/img/Documents and Settings/Da...
DSC00169.JPG			0	File	Not Notable	2009-05-31 17:17:33 IST	DSC-W130	SONY	/img_Accused1_HDD/img/Documents and Settings/Da...
DSC02194.JPG			0	File	Not Notable	2004-12-10 22:39:48 IST	DSC-PT2	SONY	/img_Accused1_HDD/img/Documents and Settings/Da...
DSC02195.JPG			0	File	Not Notable	2004-12-10 22:49:54 IST	DSC-PT2	SONY	/img_Accused1_HDD/img/Documents and Settings/Da...
DSC02196.JPG			0	File	Not Notable	2004-12-10 22:50:40 IST	DSC-PT2	SONY	/img_Accused1_HDD/img/Documents and Settings/Da...
Dc2.jpg			0	File	Not Notable	2009-05-30 14:53:55 IST	DSC-W130	SONY	/img_Accused1_HDD/img/RECYCLED/5-1-5-21-1609880
Dc3.jpg			0	File	Not Notable	2009-07-22 11:34:08 IST	MAXXIM TD	WENCA MINILTA	/img_Accused1_HDD/img/RECYCLED/5-1-5-21-1609880

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

- Date/time USB is plugged
- Device Make
- Device model
- Device ID
- Data Source

Listing

USB Device Attached

8 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
system			0	2012-12-26 21:39:01 IST		ROOT_HUB	452409e06560	Accused1_HDD.img
system			0	2012-12-26 21:39:00 IST		ROOT_HUB.00	456a9b7a48a0	Accused1_HDD.img
system			0	2012-07-21 14:50:03 IST	HTC (High Tech Computer Corp.)	Desire / Desire HD / Hero / Thunderbolt (iCharge Mode)	HTCHY400370	Accused1_HDD.img
system			0	2012-07-21 14:52:50 IST	Kingston Technology Company Inc.	DataTraveler 2.0 1GB/4GB Flash Drive / Patriot Xporter 4	5876158A0343	Accused1_HDD.img
system			0	2012-07-21 14:52:15 IST	Kingston Technology Company Inc.	Product: SD33	07B4040894306ffe	Accused1_HDD.img
system			0	2012-12-26 22:14:46 IST	Microm Technology Corp. / Micron USA Technology Co.	RA20329 SATA Bridge	703e4fffff	Accused1_HDD.img
system			0	2012-07-24 15:12:47 IST	Microm Technology Corp. / Micron USA Technology Co.	IM20329 SATA Bridge	704c0fffff	Accused1_HDD.img
system			0	2012-12-26 22:57:17 IST	VirtualBox	USB Tablet	5A1BF54b76B&1	Accused1_HDD.img

## Question 4

(30 marks)

a) Use the windows memory dump file “Victim1\_Mem.raw” provided to answer the following Questions.

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

- Windows 7

```
F:\SLIIT - Recordings\4Y 15\Forensic\Labs\VboxWindows7-Shared Folder\Lab Materials\Lab 10 - Volatility\volatility_2.6_windows7
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64
AS Layer1 : WindowsAPD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (F:\SLIIT - Recordings\4Y 15\Forensic\Labs\VboxWindows7-Shared Folder\Lab Materials\Lab 10 - Volatility\volatility_2.6_windows7)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800027f90a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff800027fad00L
KUSER_SHARED_DATA : 0xfffff7b000000000L
Image date and time : 2014-07-19 02:46:55 UTC+0000
Image local date and time : 2014-07-18 19:46:55 -0700
```

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

Offset(V)	Name	PID	PPID	Thds	Privs	Session	Wow64	Start	Exit
0xfffffa0000000000	System	4	0	24	500	-----	0	2014-07-19 02:39:15 UTC+0000	
0xfffffa000151c30	lsass.exe	224	4	2	20	-----	0	2014-07-19 02:39:15 UTC+0000	
0xfffffa000150e30	csrss.exe	315	308	8	414	0	0	2014-07-19 02:39:22 UTC+0000	
0xfffffa000150e40	csrss.exe	352	344	8	248	1	0	2014-07-19 02:39:37 UTC+0000	
0xfffffa000150e60	wininit.exe	360	308	3	75	0	0	2014-07-19 02:39:38 UTC+0000	
0xfffffa000150e80	winlogon.exe	388	344	7	133	1	0	2014-07-19 02:39:38 UTC+0000	
0xfffffa0001514b30	services.exe	448	360	7	197	0	0	2014-07-19 02:39:42 UTC+0000	
0xfffffa00015a230	lsass.exe	464	360	7	555	0	0	2014-07-19 02:39:42 UTC+0000	
0xfffffa00015a2b30	lsn.exe	472	360	4	144	0	0	2014-07-19 02:39:42 UTC+0000	
0xfffffa000200b960	svchost.exe	564	448	10	361	0	0	2014-07-19 02:39:45 UTC+0000	
0xfffffa00012ed450	svchost.exe	630	448	10	258	0	0	2014-07-19 02:39:46 UTC+0000	
0xfffffa0001488260	spssvc.exe	820	448	5	160	0	0	2014-07-19 02:40:00 UTC+0000	
0xfffffa00015f5b30	svchost.exe	860	448	20	423	0	0	2014-07-19 02:40:01 UTC+0000	
0xfffffa000159d960	svchost.exe	884	448	36	999	0	0	2014-07-19 02:40:01 UTC+0000	
0xfffffa00021aeb30	svchost.exe	920	448	19	455	0	0	2014-07-19 02:40:02 UTC+0000	
0xfffffa00021f3b30	svchost.exe	260	448	13	325	0	0	2014-07-19 02:40:25 UTC+0000	
0xfffffa00021f3060	svchost.exe	252	448	17	471	0	0	2014-07-19 02:40:25 UTC+0000	
0xfffffa0002299430	TrustedInstall	840	448	5	125	0	0	2014-07-19 02:40:27 UTC+0000	
0xfffffa00022e0b30	spoolsv.exe	1128	448	12	273	0	0	2014-07-19 02:40:29 UTC+0000	
0xfffffa000220eb30	svchost.exe	1156	448	19	306	0	0	2014-07-19 02:40:29 UTC+0000	
0xfffffa0001c3cb30	svchost.exe	1804	448	15	215	0	0	2014-07-19 02:40:50 UTC+0000	
0xfffffa0001c31a0	SearchIndexer	1808	448	15	755	0	0	2014-07-19 02:41:00 UTC+0000	
0xfffffa000156910	SearchProtocol	1176	1808	10	649	0	0	2014-07-19 02:41:05 UTC+0000	
0xfffffa00014d07d0	taskhost.exe	1760	448	0	192	1	0	2014-07-19 02:41:11 UTC+0000	
0xfffffa0001c91b30	dm.exe	1708	860	3	70	1	0	2014-07-19 02:41:11 UTC+0000	
0xfffffa0001c9f060	explorer.exe	904	1804	41	1089	1	0	2014-07-19 02:41:12 UTC+0000	
0xfffffa0001c92060	regsvr32.exe	1848	904	0	-----	1	0	2014-07-19 02:41:24 UTC+0000	2014-07-19 02:41:26 UTC+0000
0xfffffa0000c2cb30	smnrtwk.exe	732	448	0	210	0	0	2014-07-19 02:42:00 UTC+0000	
0xfffffa0000c81780	mscorsvw.exe	2144	448	7	95	0	1	2014-07-19 02:42:32 UTC+0000	
0xfffffa0000c8b30	mscorsvw.exe	2368	448	7	89	0	0	2014-07-19 02:42:33 UTC+0000	
0xfffffa0000f2ab30	svchost.exe	2400	448	14	343	0	0	2014-07-19 02:42:34 UTC+0000	
0xfffffa0001a0f520	SearchProtocol	2844	1808	0	280	1	0	2014-07-19 02:44:00 UTC+0000	
0xfffffa0000f503d0	WinPrvSE.exe	2512	564	7	125	0	0	2014-07-19 02:44:32 UTC+0000	
0xfffffa0002005b30	WinSCP.exe	2668	2580	6	165	1	1	2014-07-19 02:46:02 UTC+0000	
0xfffffa0000f2d560	SearchFilterW	540	1808	0	181	0	0	2014-07-19 02:46:09 UTC+0000	
0xfffffa0000f506d0	DumpIT.exe	708	904	2	45	1	1	2014-07-19 02:46:52 UTC+0000	
0xfffffa0000cd1060	conhost.exe	808	352	2	51	1	0	2014-07-19 02:46:52 UTC+0000	

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





Reference: "<https://www.processlibrary.com/en/directory/files/csrss/25806/>"

```

.....
System pid: 4
Unable to read PEB for task.
.....
smss.exe pid: 368
Command line : \SystemRoot\System32\smss.exe

Base          Size  LoadCount Path
-----
0x484d0000  0x13000  0xffff \SystemRoot\System32\smss.exe
0x76dc0000  0x13c000  0xffff C:\Windows\SYSINF32\ntdll.dll
.....
csrss.exe pid: 376
Command line : %SystemRoot%\System32\csrss.exe ObjectDirectory=Windows SharedSection=1824,12288,512 Windows-0n SubSystemType=Windows ServerDll=baseSrv,I
WinSrvConServerDllInitialization,2 ServerDll=sscsrv,4 ProfileControl=Off MaxRequestThreads=16
Service Pack 1

Base          Size  LoadCount Path
-----
0x4d2d0000  0xc5000  0xffff C:\Windows\system32\csrss.exe
0x76dc0000  0x13c000  0xffff C:\Windows\SYSINF32\ntdll.dll
0x74ec0000  0xb0000  0xffff C:\Windows\system32\CSRSSV.dll
0x74c50000  0xb0000  0x4 C:\Windows\system32\basesrv.DLL
0x74c20000  0x2c000  0x2 C:\Windows\system32\winSrv.DLL
0x77950000  0xc9000  0xb C:\Windows\system32\USER32.dll
0x775c2000  0x6e000  0xc C:\Windows\system32\GDI32.dll
0x775c2000  0x3d000  0x63 C:\Windows\SYSINF32\kernel32.dll
0x74f60000  0x40000  0x13a C:\Windows\system32\KERNIMAGE.dll
0x775b0000  0xab000  0x3 C:\Windows\system32\LPK.dll
0x77580000  0x5d000  0x3 C:\Windows\system32\GSP10.dll
0x77580000  0xacc00  0x5 C:\Windows\system32\adv32t.dll
0x74c10000  0xb0000  0x1 C:\Windows\system32\sscsrv.DLL
0x74d50000  0xc5f000  0x1 C:\Windows\system32\Sxs.dll
0x775b0000  0x6a2000  0x3 C:\Windows\system32\RPCRT4.dll
0x74d50000  0xc0000  0x2 C:\Windows\system32\CRYPTBASE.dll
0x75410000  0xc00000  0x1 C:\Windows\system32\ADVAPI32.dll
0x77290000  0x19000  0x4 C:\Windows\SYSINF32\sechost.dll
.....
csrss.exe pid: 388
Command line : %SystemRoot%\System32\csrss.exe ObjectDirectory=Windows SharedSection=1824,12288,512 Windows-0n SubSystemType=Windows ServerDll=baseSrv,I
WinSrvConServerDllInitialization,2 ServerDll=sscsrv,4 ProfileControl=Off MaxRequestThreads=16
Service Pack 1

Base          Size  LoadCount Path
-----
0x4d2d0000  0xc5000  0xffff C:\Windows\system32\csrss.exe
0x76dc0000  0x13c000  0xffff C:\Windows\SYSINF32\ntdll.dll
0x74ec0000  0xb0000  0xffff C:\Windows\system32\CSRSSV.dll

```

## 15

```

F:\SLIIT - Recordings\4Y 15\Forensic\Labs\Box\Windows7-Shared Folder\Lab Materials\Lab 10 - Volatility\volatility_2.6_win64_stdalo
malfind
Volatility Foundation Volatility Framework 2.6
Process: svchost.exe Pid: 2644 Address: 0x2b50000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 328, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02b50000 88 00 42 00 00 00 05 8b 45 14 b9 c2 8b 45 10 ..B.....E...E
0x02b50010 8b 08 8b 40 04 89 0a 89 42 04 8b 45 14 b1 00 88 ...B...B...E...
0x02b50020 00 00 00 8d 45 08 09 c2 8b 45 14 b1 00 09 0a 8b ....E.....E.....
0x02b50030 45 14 b9 c2 8b 45 08 8b 00 89 02 c7 42 04 00 00 E....E.....B...

0x02b50000 0000      OR [EAX], AL
0x02b50002 42        INC EDI
0x02b50003 0000      ADD [EAX], AL
0x02b50005 0000      ADD [EAX], AL
0x02b50007 058b451489 ADD EAX, 0x8b451489
0x02b5000c c28b45    RET 0xc28b45
0x02b5000f 108b088b4004 ADC [EBX+0x408b004], CL
0x02b50015 b90a      MOV [EDI], ECX
0x02b50017 b94204    MOV [EDI+0x4], EAX
0x02b5001a 8b4514    MOV EAX, [EBP+0x14]
0x02b5001d 810808000000 ADD DWORD [EAX], 0x08
0x02b50023 8d4508    LEA EAX, [EBP+0x8]
0x02b50026 89c2      MOV EDI, EAX
0x02b50028 8b4514    MOV EAX, [EBP+0x14]
0x02b5002b 8b08      MOV ECX, [EAX]
0x02b5002d 890a      MOV [EDI], ECX
0x02b5002f 8b4514    MOV EAX, [EBP+0x14]
0x02b50032 89c2      MOV EDI, EAX
0x02b50034 8b4508    MOV EAX, [EBP+0x8]
0x02b50037 8b00      MOV EAX, [EAX]
0x02b50039 8902      MOV [EDI], EAX
0x02b5003b c7        DB 0xc7
0x02b5003c 42        INC EDI
0x02b5003d 0400      ADD AL, 0x0
0x02b5003f 00        DB 0x0

Process: svchost.exe Pid: 2644 Address: 0x2bd0000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 256, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02bd0000 09 00 38 00 09 00 01 05 8b 55 18 8b 4d 54 8d 54 ..B.....U..MT.T
0x02bd0010 0a fc 09 04 00 1a 00 ff 95 48 37 00 00 8b 4d 1c .....H7...P..
0x02bd0020 89 08 81 45 18 fc ff ff ff 0d 45 1c 8b 4d 18 89 ...E.....E..P..
0x02bd0030 08 81 0d 18 98 02 00 00 9f 0f 90 c8 66 89 45 38 ..H.....f..EH
0x02bd0000 0900      OR [EAX], EAX

```

c) Use “Gmail - RE Order Confirmation” to answer the following Questions.  
i) What is the attacker’s email address?

- [chirathdealwis@gmail.com](mailto:chirathdealwis@gmail.com)

ii) What is the victim’s email address?

- [perern44@gmail.com](mailto:perern44@gmail.com)

iii) What is the attack that the attacker was planning to conduct? Justify your answer with evidence.

The attacker appears to be attempting a Business Email Compromise (BEC) or phishing attack. Which means the attacker is trying to deceive the recipient into transferring a large sum of money to a fraudulent bank account.

Possible Methods Used:



Impersonation: The attacker impersonates a legitimate sender (in this case, "Chirath Dealwis") and fabricates a context around an order that requires a payment to be processed.

Social Engineering: By referencing a previous communication (real or fabricated) and using details like a specific order and personal names, the attacker tries to establish legitimacy and urgency.

Bank Details: The attacker provides bank details for the recipient to transfer money to, which is controlled by the attacker.

**-- End of the Question Paper --**