



**VIT<sup>®</sup>**

**Vellore Institute of Technology**

(Deemed to be University under section 3 of UGC Act, 1956)

## Cyber Forensics and Investigation

Course Code: BCI4001

Slot: L55+L56

Faculty: Dr. AJU D

Assessment: 1

18BCI0247

Rohan Allen

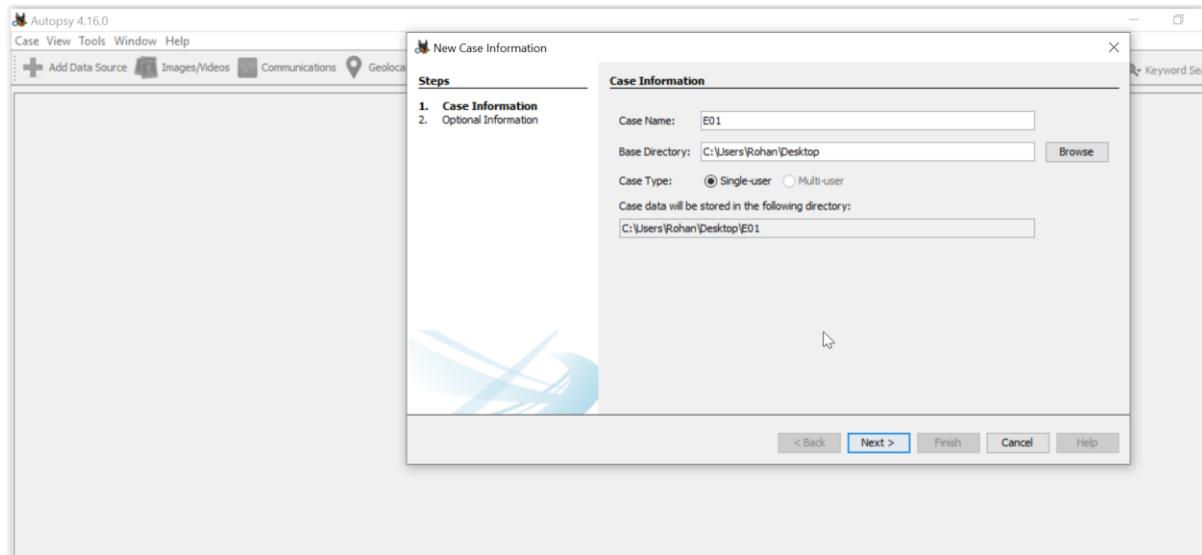
### **Exercise 1:**

1. Autopsy
  - a. A study on Autopsy tool and brief about the functions and features of the tool.
  - b. Utilize the dataset (Mantooth.E01 & Washer.E01) that is provided through the google drive and answer the questions accordingly.
  - c. Generate a report through Autopsy tool and provide your respective interpretation.
  - d. Combine all the files and upload as a single PDF file in VTOP.

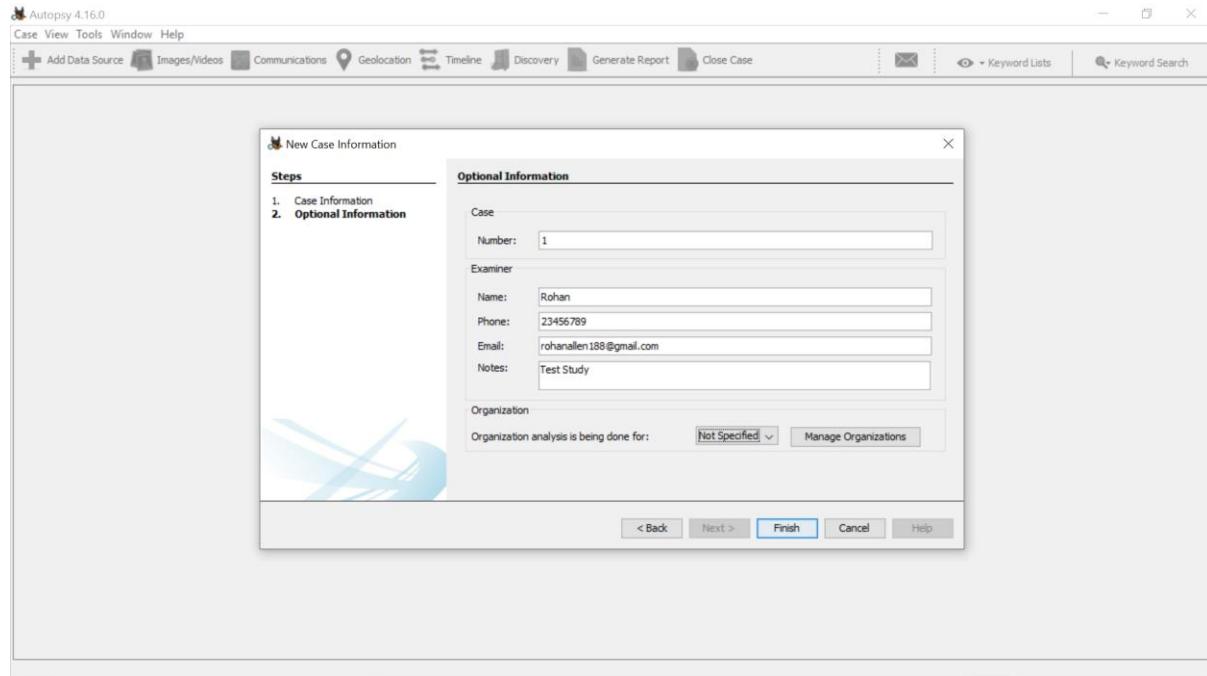
a) Startup Page- New Case



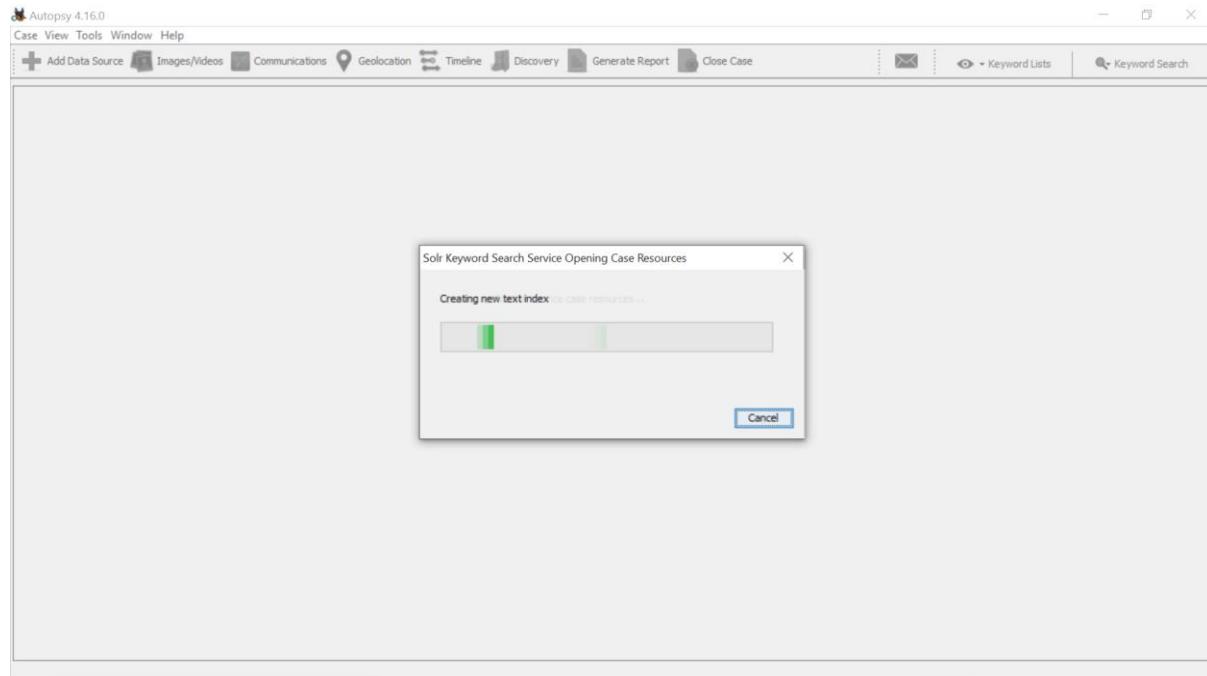
Enter Case Name and directory where it will be saved



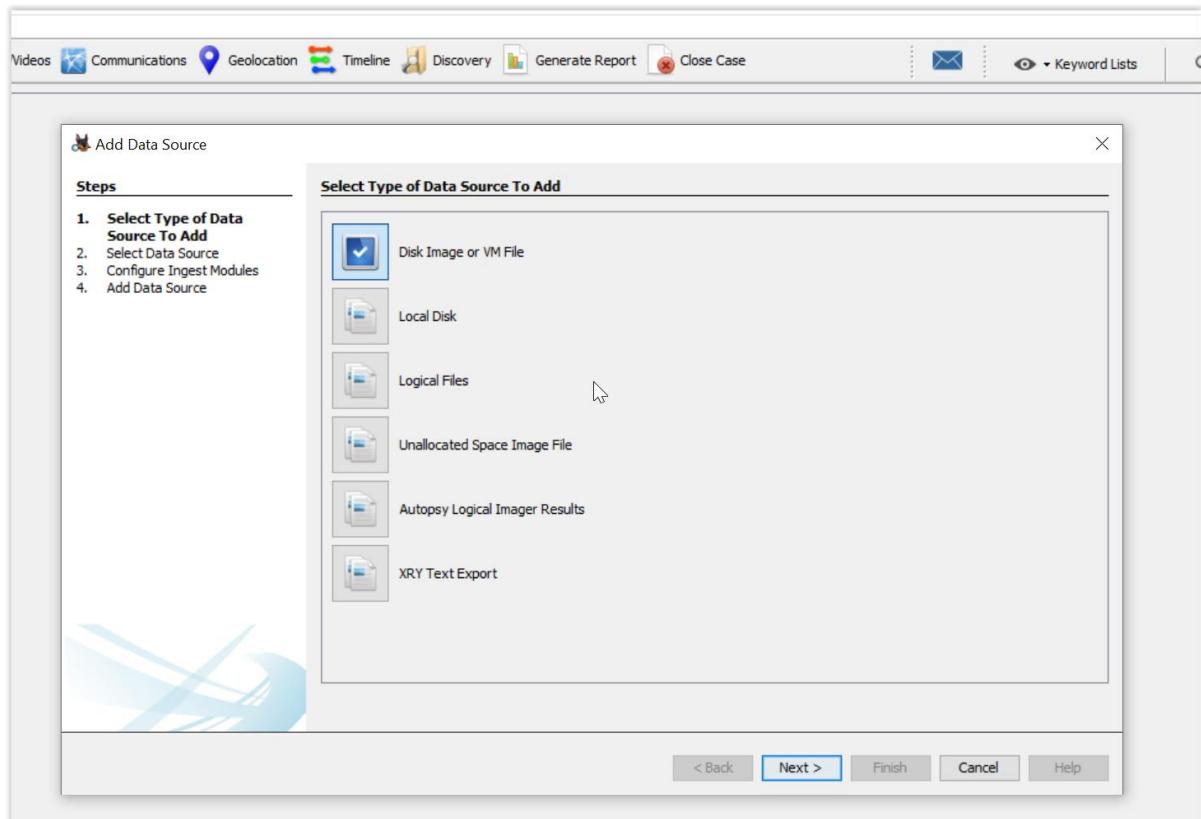
## Enter Case Number, and Examiner details



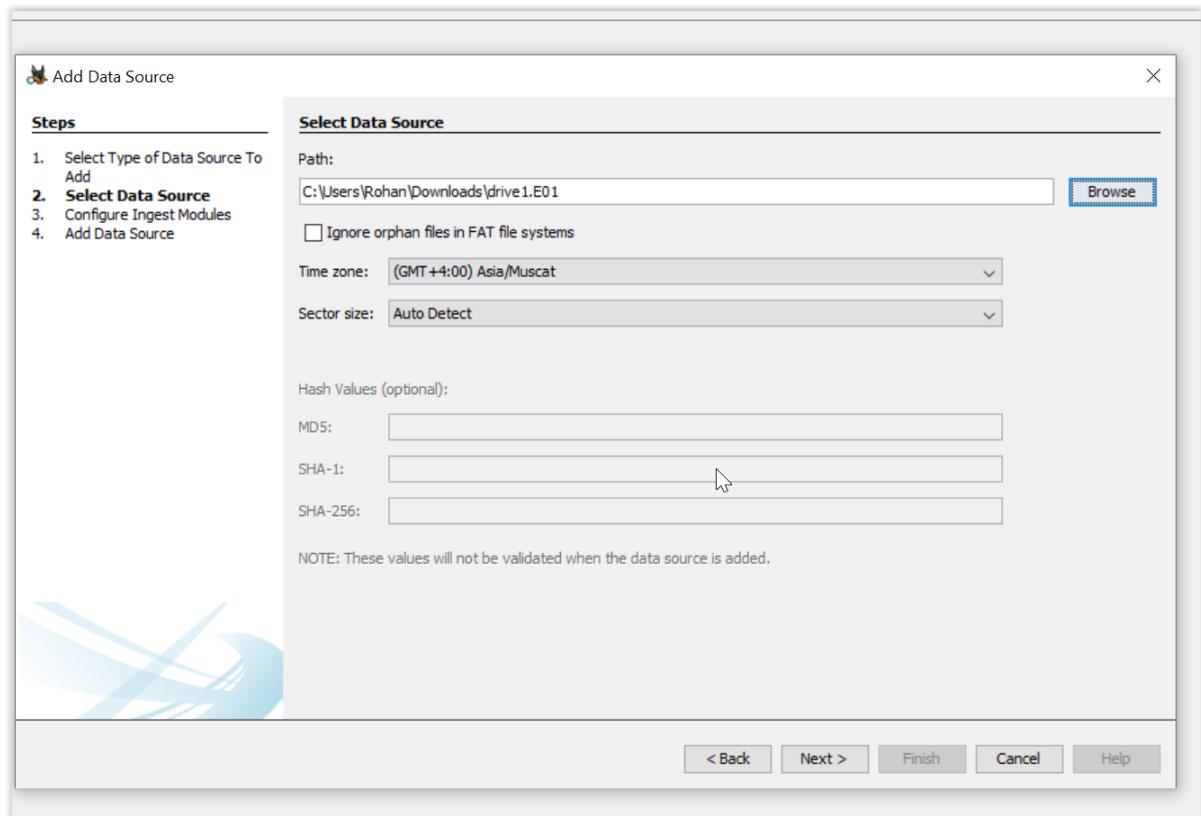
## Creating Autopsy Case file



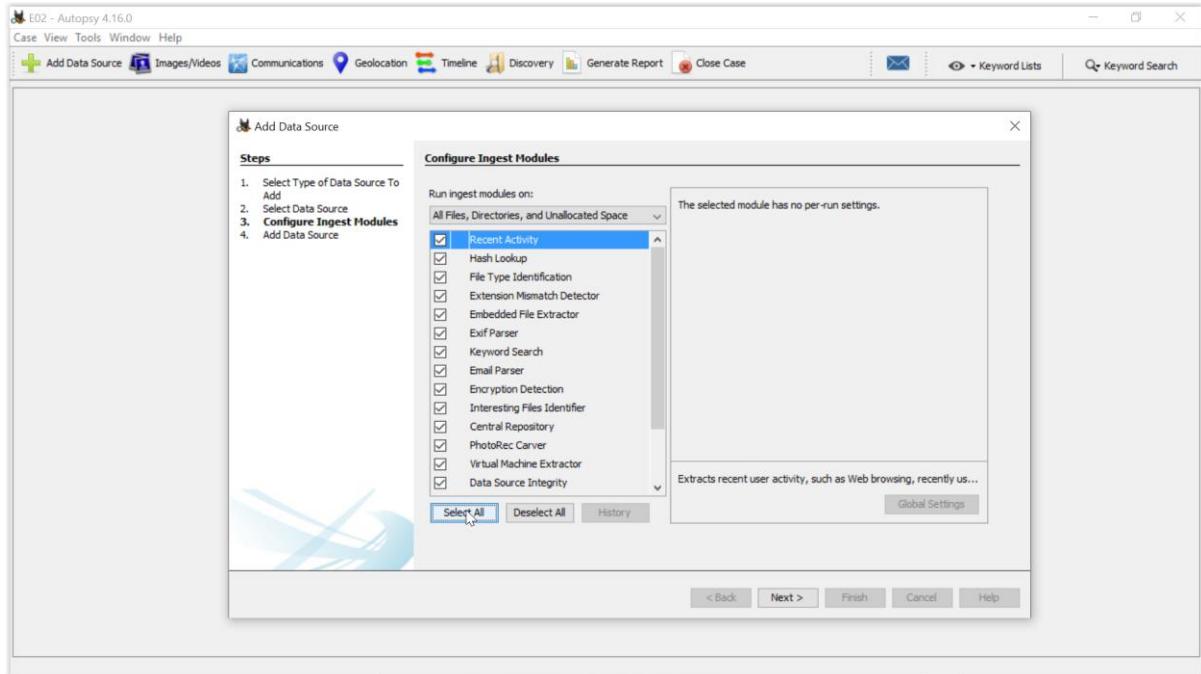
## Add data source to analyse



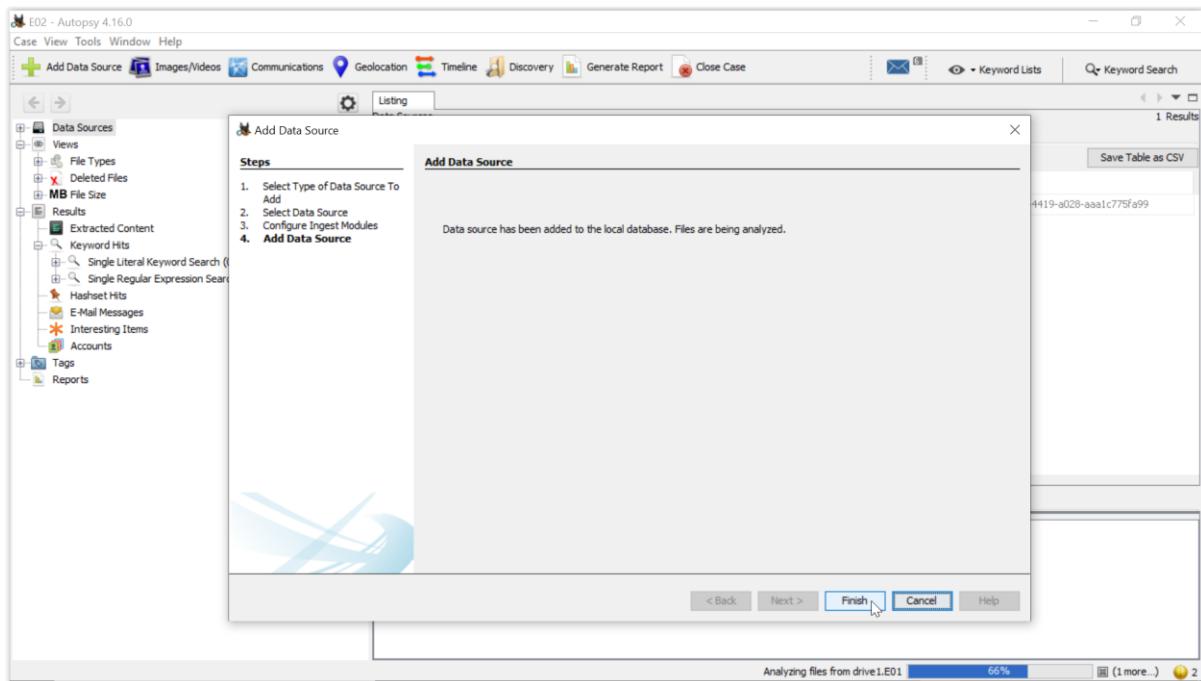
Select path to add E01 drive image to analyse. Also Select timezone



Configure ingest module to select the various types of processing you want done on your disk image. I have selected all.



Data Source is successfully added.



Can view information like data source, files contained, deleted files, images, videos, emails, etc and their hexadecimal and metadata information for the E01 disk image being analysed.

The screenshot shows the Autopsy 4.16.0 interface. The left sidebar displays a tree view of data sources, views, and results. A single data source entry for 'drive1.E01' is selected. The main pane shows a table listing the data source details:

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
drive1.E01	Image	1059323904	512	Asia/Muscat	b42705d7-e15f-4419-a028-aaac775fa99

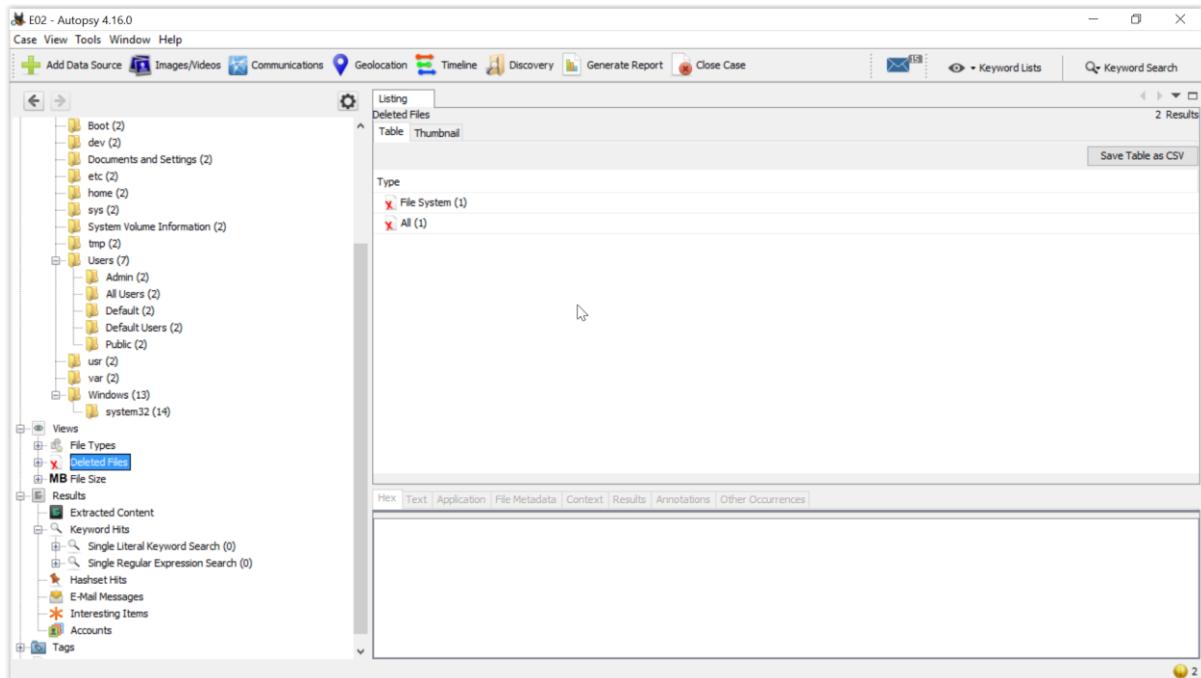
Below the table, a detailed file metadata panel is open, showing the following information for the selected data source:

Name	Type	Size	MD5	SHA1	SHA256	Sector Size
/img_drive1.E01	E01	1059323904	ef7524255c11ac089e532cd3db4d1d46	c89f230db9a2bb21dc6036b24e8f293dd0c079	Not calculated	512

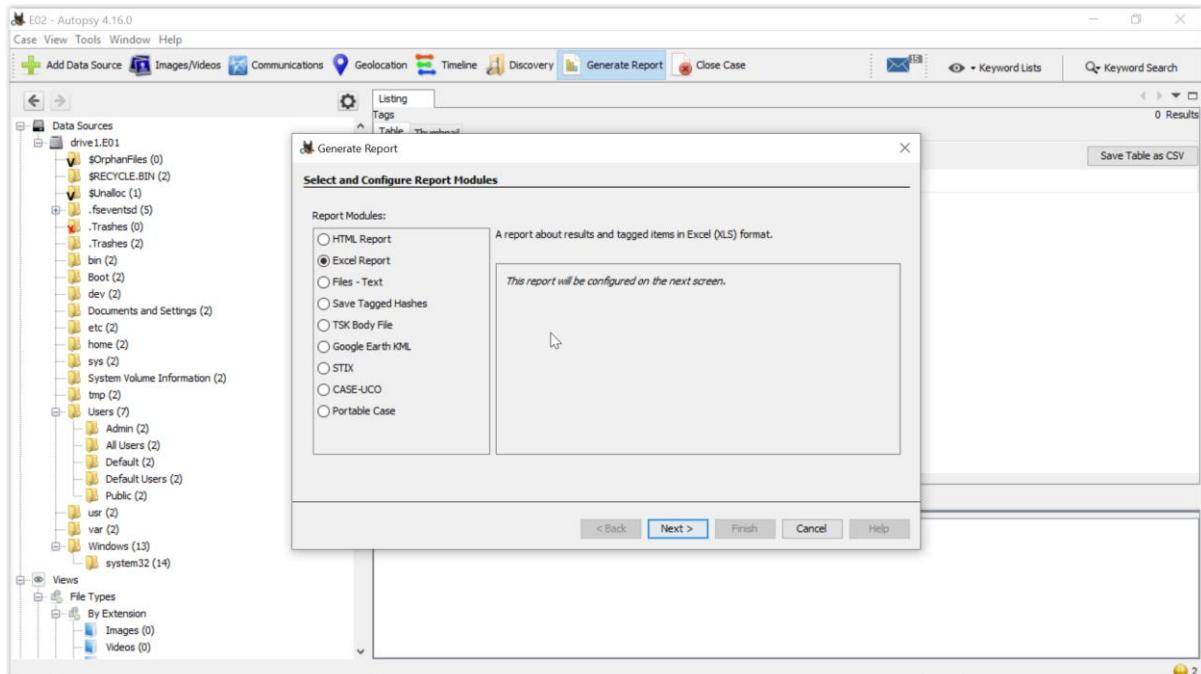
The screenshot shows the Autopsy 4.16.0 interface with the 'drive1.E01' data source selected. The left sidebar shows a detailed listing of files and folders within the drive. The main pane displays a table of file metadata for all entries:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
\$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
.\$FAT1	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10306
.\$FAT2	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10306
.\$MBR	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512
.\$RECYCLE.BIN				2015-10-07 12:26:24 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:02 GST	4096
.\$Inalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
.fseventsds				2015-10-07 12:31:28 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:02 GST	4096
.Trashes				2015-10-07 12:49:04 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:02 GST	0
.Trashes				2015-10-07 12:27:40 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:02 GST	4096
bin				2015-10-07 12:30:36 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:02 GST	4096
Boot				2015-10-07 12:26:36 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:02 GST	4096
dev				2015-10-07 12:30:40 GST	2000-00-00 00:00:00	2015-10-07 00:00:00	2015-10-07 12:49:00 GST	4096
etc								
home								
sys								
System Volume Information								
tmp								
Users	(7)							
usr	(2)							
var	(2)							
Windows	(13)							

## Deleted files:



## Generate excel report of case findings



b)

## 1) What type of file is Mantooth.E01

Image file

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Mantooth.E01	Image	128450048	512	Asia/Muscat	7d2277f9-ae58-4bcf-922b-3041e7f232c5

## 2) What is the Operating System?

Windows\_NT

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name
SYSTEM	0	0	0	WESMANTOOTH-PC	Windows_NT	x86	%SystemRoot%\TEMP	Mantooth.E01	Mantooth.E01	Windows Vista
SOFTWARE										

## 3) What is the File System?

Name	S	C	O	Modified Time	Change Time	Access Time
WAOLUSGM	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
WAOLUSGM	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
TOD	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
TOD	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
WER	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
WER	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Support	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Support	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
WPD	1	0	0	2007-07-14 02:13:52 GST	2007-07-14 02:13:52 GST	2007-07-14 02:13:52 GST
WPD	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Windows Live	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
SharingMetadata	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
CABYPJH6	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

4) Provide the account name and last login information for each account present in Mantooth

Source File	S	C	O	User ID	Username	Date Created	Count	Account Type	Description
				S-1-5-21-3166329-3263506726-1320359247-501	Guest	2007-02-27 22:29:26 GST	0	Default Guest Acct	Built-in account for guest access to the computer/domain
				S-1-5-21-3166329-3263506726-1320359247-500	Administrator	2007-02-27 22:29:26 GST	1	Default Admin User	Built-in account for administering the computer/domain
				S-1-5-21-3166329-3263506726-1320359247-1003	Laurent	2008-02-12 04:13:36 GST	0	Custom Limited Acct	
				S-1-5-21-3166329-3263506726-1320359247-1002	Dracula	2007-03-06 05:25:43 GST	3	Custom Limited Acct	The Tooth Account
				S-1-5-21-3166329-3263506726-1320359247-1000	Wes Mantooth	2007-02-27 22:29:10 GST	96	Default Admin User	
				SOFTWARE					
				S-1-5-18	systemprofile				
				S-1-5-19	LocalService				
				S-1-5-20	NetworkService				

Source File	Account Settings	Flag	Data Source	Date Accessed	Display Name	Password Fail Date	Path	Password Hint
core; Password not required	Account Disabled	Normal user account	Mantooth.E01					
core	Account Disabled	Normal user account	Mantooth.E01	2006-11-02 17:02:01 GST				
core		Normal user account	Mantooth.E01		Laurent			
core		Normal user account	Mantooth.E01	2007-04-02 04:30:58 GST	Count Dracula	2008-02-13 00:13:17 GST	C:\Users\Dracula	
core; Password not required		Normal user account	Mantooth.E01	2008-02-12 23:12:08 GST		2008-02-13 00:13:16	ntuser.dat	in your face
			Mantooth.E01			2008-02-13 00:13:17 GST	%SystemRoot%\system32\config\systemprofile	
			Mantooth.E01				%SystemRoot%\ServiceProfiles\LocalService	
			Mantooth.E01				%SystemRoot%\ServiceProfiles\NetworkService	

Name	Keyword Preview	Location
RegRipper /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/NTU Connection Server	= <Last Login> UserName = incisorm...	RegRipper /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/NTU Connection Server
RegRipper /img_Mantooth.E01/vol_vol2/Windows/System32/config	Name : <Last Login Date : Thu Nov 2 13:02:01	RegRipper /img_Mantooth.E01/vol_vol2/Windows/System32/config

5) If there is any evidence of .exe file being deleted, describe the artifact name and document your findings.

## 4 .exe file are deleted

Listing								
.exe	S	C	O	Location	Modified Time	Change Time	Access Time	Created Time
\$!61QDFF.exe				/img_Mantooth.E01/vol_vol2/\$Recycle.Bin/S-1-5-21-31663...	2007-07-14 23:25:57 IST	2007-08-04 21:34:25 IST	2007-07-14 23:25:57 IST	2007-07-14 23:25:57 I
\$!THDU55.exe				/img_Mantooth.E01/vol_vol2/\$Recycle.Bin/S-1-5-21-31663...	2007-06-24 05:54:52 IST	2007-08-04 21:34:30 IST	2007-06-24 05:54:52 IST	2007-06-24 05:54:52 I
\$R61QDFF.exe				/img_Mantooth.E01/vol_vol2/\$Recycle.Bin/S-1-5-21-31663...	2002-12-30 09:46:06 IST	2007-08-04 21:34:26 IST	2007-07-14 23:25:42 IST	2007-07-14 23:25:42 I
\$RTHDU55.exe				/img_Mantooth.E01/vol_vol2/\$Recycle.Bin/S-1-5-21-31663...	2007-06-24 05:53:41 IST	2007-08-04 21:34:32 IST	2007-06-24 05:53:32 IST	2007-06-24 05:53:26 I
junction.exe				/img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Desktop/junction.exe	2006-11-02 01:36:00 IST	2007-09-27 01:27:21 IST	2007-08-24 18:38:17 IST	2007-08-24 18:38:17 I
Revelation.exe				/img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/Revelation.exe	2000-11-26 08:00:42 IST	2007-09-27 18:40:45 IST	2007-07-14 23:32:20 IST	2007-07-14 23:32:20 I
trout.exe				/img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/trout.exe	2000-11-17 22:27:18 IST	2007-09-27 18:40:45 IST	2007-07-14 23:32:20 IST	2007-07-14 23:32:20 I

## 6) Find proof of communication with Gladiator

The screenshot shows the Autopsy 4.16.0 interface. On the left, the file tree displays volumes (vol0, vol3, vol4) and file types (Images, Videos, Audio, Archives, Databases, Documents, Executable). In the center, a 'Keyword search' panel is open with the query 'gladiator'. It shows a table with four results:

Name	Keyword Preview	Location
2003 Cigarette Gladiator powerboat for sale in Texas.htm	2003 cigarette «gladiator» powerboat for sale in texas	/img_Mantooth.E01/vol_vol3/Stuff/2003 Cigare...
2003 Cigarette Gladiator powerboat for sale in Texas.htm-slack	2003 cigarette «gladiator» powerboat for sale in texas	/img_Mantooth.E01/vol_vol3/Stuff/2003 Cigare...
2003 Cigarette Gladiator powerboat for sale in Texas.mht	2003 cigarette «gladiator» powerboat for sale in texas	/img_Mantooth.E01/vol_vol3/Stuff/2003 Cigare...
2003 Cigarette Gladiator powerboat for sale in Texas.mht-slack	2003 cigarette «gladiator» powerboat for sale in texas	/img_Mantooth.E01/vol_vol3/Stuff/2003 Cigare...

At the bottom, a text viewer pane shows the content of the first result: "2003 cigarette gladiator powerboat for sale in texas.htm". The pane includes navigation buttons, a search bar, and a zoom slider.

## 7) What is a "Pranic Vampire"? In which document is it mentioned? When was the document created?

Astral.doc and Astral\_Vampire.doc

Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Listing Keyword search 6 - Pranic Vampire X

Keyword search

Table Thumbnail Save Table as CSV

Name	Keyword Preview	Location
Astral.doc	be more common. «Pranic Vampire«This is a more common	/Img_Mantooth.E01/vol_vol2/\$OrphanFiles/Book of Nod/As...
Unalloc_4231_3267072_106657792	to be more common. «Pranic Vampire«This is a more common	/Img_Mantooth.E01/vol_vol2//\$Unalloc/Unalloc_4231_3267...
f0010751_Astral_Vampire.doc	be more common. «Pranic Vampire«This is a more common	/Img_Mantooth.E01/vol_vol2//\$CarvedFiles/f0010751_Astr...

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: 1 of 2 Match 100% Reset Text Source: Search Results

**Pranic Vampire**

This is a more common and possibly more correct term for psychic vampire. Prana is the Sanskrit word meaning "life energy", which does more accurately describe the energy that we feed on. Pranic Vampires have a broken or in most cases removed Chakra, generally the Navel, but in some cases the Heart Chakra. Often times this type of Psychic vampire has a completely reworked energy system. **Pranic vampire** is generally a catch all term and may encompass the other types of psychic vampires as well.

Listing Keyword search 6 - Pranic Vampire X

Keyword search

Table Thumbnail Save Table as CSV

Name	Keyword Preview	Location
Astral.doc	be more common. «Pranic Vampire«This is a more common	/Img_Mantooth.E01/vol_vol2/\$OrphanFiles/Book of Nod/As...
Unalloc_4231_3267072_106657792	to be more common. «Pranic Vampire«This is a more common	/Img_Mantooth.E01/vol_vol2//\$Unalloc/Unalloc_4231_3267...
f0010751_Astral_Vampire.doc	be more common. «Pranic Vampire«This is a more common	/Img_Mantooth.E01/vol_vol2//\$CarvedFiles/f0010751_Astr...

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: 1 of 2 Match 100% Reset Text Source: Search Results

**Pranic Vampire**

This is a more common and possibly more correct term for psychic vampire. Prana is the Sanskrit word meaning "life energy", which does more accurately describe the energy that we feed on. Pranic Vampires have a broken or in most cases removed Chakra, generally the Navel, but in some cases the Heart Chakra. Often times this type of Psychic vampire has a completely reworked energy system. **Pranic vampire** is generally a catch all term and may encompass the other types of psychic vampires as well.

## 8) What is present in happy.mpeg?

Listing Keyword search 7 - happy.mpeg

Keyword search

Table Thumbnail

Page: 1 of 1 Pages: < > Go to Page: Images: 1-1 Medium Thumbnails Sort Sorted by: ---

happy.mpeg

/img\_Mantooth.E01/vol\_vo2/Users/Wes Mantooth/Desktop/Funny Vids.zip/happy.mpeg

Hex Text Application File Metadata Context Results Annotations Other Occurrences

00:00:13/00:00:25

Speed: 1x

## 9) Check if picture of any drugs are present? If so name the drugs.

Image/Video Gallery - Editor

Image/Video Gallery

Group By Path Sort By Priority Data Source All Tag Group's Files Follow Up Categorize Group's Files CAT-5: Non-pertinent

All Groups Only Hash Hits

secret (3)

Documents (10)

ADS (1)

Car Titles (2)

Checks (14)

seanbefore.zip (2)

seanbefore (2)

Dear Sweetie.doc (1)

Hacker Stuff (2)

My poem.txtSupersecretstuff.zip (2)

Scripts (5)

Snapt Catalog

Pictures (7)

AppData

Public

Documents

Japanese text.doc (3)

\$Recycle.Bin

.8329-3263506726-1320359247-1000 (8)

\$REZFRY8 (3)

Really Old Images (2)

CAT-1: Child Exploitation... 0

CAT-2: Child Exploitation... 0

CAT-3: CGI/Animation... 0

CAT-4: Exemplar/Compa... 0

CAT-5: Non-pertinent 0

CAT-0: Uncategorized 554

Category # Files

Details

Attribute Value

Name My poem.txtHARDCO RE.JPG

Analyzed true

Category CAT-0: Uncategorized

Tags /img\_Mantooth.E0 1/vol\_vo2/Users/ Wes Mantooth/Docume nts/

Created Time 2007-04-13 06:31:38 IST

Modified Time 2007-04-13 06:36:14 IST

MDS Hash e16fffc19575863c8

Hashset 40e4f5f1b18cbd6

Camera Make

Camera Mo...

My poem.txtHARDCORE.JPG ( 2 of 10 in group )

Group Viewing History Back Forward Don't show groups seen by other examiners Next Unseen Group 0 File Update Tasks

The screenshot shows a digital forensic analysis interface with multiple tabs at the top: 'Listing', 'Keyword search 7 - happy.mpeg', 'Keyword search 8 - drugs', and 'Keyword search 9 - The Legal drug'. The 'Keyword search 9 - The Legal drug' tab is active. Below the tabs is a table view with columns 'Name', 'Keyword Preview', and 'Location'. Three files are listed: 'f0000757.reg', 'howtomanufactu172921[1].htm' (which is selected), and '165183.html'. The 'Keyword Preview' column shows snippets from the selected file related to 'Booze - The Legal Drug'. Below the table is a preview pane displaying the contents of 'howtomanufactu172921[1].htm', which includes a list of various substances and topics like 'Booze - The Legal Drug', 'Marijuana', and 'OTC Drugs and Household Items'. At the bottom of the preview pane, there are search controls for page navigation and text matching.

10) Find the list of criminal activities Mantooth was involved in and the associated artifacts.

- |   |   |   |
|---|---|---|
| 1 | CAT-1: Child Exploitation (Illegal)                   | 1 |
| 2 | CAT-2: Child Exploitation (Non-Illegal/Age Difficult) | 2 |
| 3 | CAT-3: CGI/Animation (Child Exploitive)               | 3 |

11) Summarize the finding against Mantooth

Mantooth was involved in Child Exploitation and drug trafficking of the following drugs:

- Booze
- Marijauna
- OTC
- Speedy Drugs
- Fringe

Also Mantooth was in contact with Gladiator.

12) Mantooth received one Text Internet Email that had no subject about a stolen ATM. Who sent it to him (name and email) and when was it sent?

The screenshot shows a digital forensic analysis interface. At the top, a title bar reads "Listing Keyword search 17 - ATM" and "40 Results". Below the title bar is a toolbar with "Table" and "Thumbnail" buttons, and a "Save Table as CSV" button. The main area is a table with three columns: "Name", "Keyword Preview", and "Location". The "Name" column lists file names like "ads[1].htm", "40A511AF-00000008.eml", "index.dat", and "Web History Artifact". The "Keyword Preview" column shows snippets of the files, such as "ads[1].htm \* <ATM< Machines Nationwide sal" and "\$100. Word<ATM< THEFTS In our first slide". The "Location" column shows paths like "/img\_Mantooth.E01/vol\_vol2/Users/Wes Mantooth/AppDat..". Below the table is a navigation bar with tabs: Hex, Text, Application, File Metadata, Context, Results, Annotations, Other Occurrences. The "Text" tab is selected. Underneath the tabs is a sub-navigation bar with "Strings", "Indexed Text", and "Translation", with "Translation" being the active tab. A tooltip for "Translation" says "Displays context for selected file.". Below the sub-navigation are search controls: "Page: 1 of 1 Page", "Matches on page: 1 of 9 Match", "100%", and "Reset". To the right of these controls are "Text Source: Search Results" and a dropdown menu. The main content area displays the email message content:

```
From:  
Wes  
Mantooth  
  
To: Mr Smee  
  
Cc: John Washer  
  
Sent: Thursday, July 12, 2007 5:19  
PM  
  
Subject: New Venture  
  
  
T am thinking we should launch into a new
```

13) Find when and who deleted the file ValidCreditCard.jar

Screenshot of a digital forensic tool interface showing search results and file details.

**Search Results:**

Name	S	C	O	Modified Time	Change Time	Access Time
ValidateCreditCard.zip				2007-07-14 21:57:06 GST	2007-08-04 20:04:30 GST	2007-07-14 21:56:59 GST
wes_mantooth@pgp[2].txt		0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
My Confession.txt		0		2007-08-15 01:26:41 GST	2008-02-13 04:53:11 GST	2008-02-13 04:53:11 GST
This is a really really long filename to see if vista has a file name pa		1		2007-03-09 06:23:29 GST	2008-06-20 19:51:26 GST	2008-06-20 19:51:25 GST

**File Details:**

ValidateCreditCard.zip

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 26 Page Go to Page: Script: Latin - Basic

```
Readme.txtm
3tgm
;StEU
pF8O
/o9a[7P
-6LL
ValidateCreditCard.jarl
speO
=zclj/bl
(HFS
:McP
o861
,0'D%
&?"?<
?$$T3=
EV\|}|||<
n 8CB
z4XL
jk=!
Yeh-7
_mH&
^_mV
```

- 1) What is the starting sector of Partition 2 and what is the size of it?

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-62)	1	0	63	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 63-240974)	2	63	240912	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 240975-250878)	3	240975	9904	Unallocated	Unallocated

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Page: 1 of 7529 Page ← → Go to Page: Jump to Offset 0 Launch in HxD

- 2) What is the file system of the disk image?

vol2 (NTFS / exFAT (0x07): 63-240974) | 2 | 63 | 240912 | NTFS / exFAT (0x07) | Allocated

- 3) List the user names?

Source File	S	C	O	User ID	Username	Date Created	Count	Account Type
SAM				S-1-5-21-1177238915-616249376-839522115-1000	HelpAssistant	2007-07-25 05:11:56 GST	0	Custom Limit
SAM				S-1-5-21-1177238915-616249376-839522115-1003	Billy Bob Brubeck	2007-08-04 05:14:13 GST	22	Default Admin
SAM				S-1-5-21-1177238915-616249376-839522115-1002	SUPPORT_388945a0	2007-07-25 05:13:42 GST	0	Custom Limit
SAM				S-1-5-21-1177238915-616249376-839522115-1005	Mr Smee	2007-08-04 05:18:00 GST	21	Default Admin
SAM				S-1-5-21-1177238915-616249376-839522115-1004	The Wolf	2007-08-04 05:15:03 GST	22	Default Admin
SAM				S-1-5-21-1177238915-616249376-839522115-1006	Captian Hook	2007-08-04 05:18:11 GST	21	Default Admin
SAM				S-1-5-21-1177238915-616249376-839522115-1008	Artimus	2008-02-13 05:13:46 GST	0	Custom Limit
SAM				S-1-5-21-1177238915-616249376-839522115-501	Guest	2007-07-24 22:57:36 GST	0	Default Guest
SAM				S-1-5-21-1177238915-616249376-839522115-500	Administrator	2007-07-24 22:57:36 GST	16	Default Admin
software				S-1-5-18	systemprofile			
software				S-1-5-19	LocalService			
software				S-1-5-20	NetworkService			

- 4) Does Washer know Mantooth? Yes, proof of communication:

Listing Keyword search 21 - Mantooth

Name	Keyword Preview	Location	Modified Time
TL Events Artifact	Description : Author: Wes <Mantooth> Template: Normal R...	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-07-24 00:43
TL Events Artifact	Description : Author: Wes <Mantooth> Template: Normal R...	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-07-24 00:43
TL Events Artifact	Description : Author: Wes <Mantooth> Template: Normal R...	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-07-24 00:43
Inbox.dbx	net'John Washer'; 'Wes <Mantooth><chkwisher@comcast...	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-08-04 05:30
Metadata Artifact	ID : KALOwner : Wes <Mantooth>	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-07-24 00:43
Options.doc	Word 10.0Author: Wes <Mantooth>Character Count: 592	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-07-24 00:43
Sent Items.dbx	Washerchkwisher@comcast.net<Mantooth><dollarhyde86@comcast...	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-08-04 05:29
Deleted Items.dbx	18:00:37 +0000From: Washerchkwisher@comcast.net<Mantooth><dollarhyde86@comcast...	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-08-04 05:29
NTUSER.DAT	sys!VISTAM~1.TXTVista <Mantooth> Bitlocker Key 1.4.txt	/img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2008-02-12 15:20

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page    Matches on page: 1 of 1 Match    100%      Reset    Text Source: Search Results

```
Date/Time : 2007-07-24 00:43:40 GST
Description : Author: Wes Mantooth Template: Normal Revision number: 11 Last saved by: KAL Number of pages: 1 Number of words: 103 Number of characters: 592 Application: Microsoft Word 10.0 Security: 0
Event Type : 23
```

Keyword search

Name	Keyword Preview	Location	Modified Time
Table			
Thumbnail			

Save Table as

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 126 Page    Matches on page: 1 of 17 Match    100%      Reset    Text Source: Search Results

```
Mantooth<dollarhyde86@comcast.net>mail.comcast.net00000001@
Whats up in D town?
Re: Whats up in D town?John Washerchkwisher@comcast.net
Wes Mantooth<dollarhyde86@comcast.net>mail.comcast.net00000001@
Whats up in D town?b
Re: Whats up in D town?John Washerchkwisher@comcast.net
Wes Mantooth<dollarhyde86@comcast.net>mail.comcast.net00000001@
New Venture(h
Re: New Venture<A4DBACC29CA34AB6A2436854261196E8@WesMantoothPC>John Washerchkwisher@comcast.net
Wes Mantooth; Mr Smee<dollarhyde86@comcast.net>; <smee.rox@gmail.com>mail.comcast.net00000001
hello
helloJohn Washerchkwisher@comcast.net
9706315006@vttext.com<9706315006@vttext.com>mail.comcast.net00000001@
Stuff
gi+S
StuffJohn Washerchkwisher@comcast.net
txkidd@swbell.net<txkidd@swbell.net>mail.comcast.net00000001@
Stuff
Re: StuffJohn Washerchkwisher@comcast.net
Rasco Badguy<txkidd@swbell.net>mail.comcast.net00000001@
Thanks
ThanksJohn Washerchkwisher@comcast.net
Rasco Badguy<txkidd@swbell.net>mail.comcast.net00000001
Thanks
ThanksJohn Washerchkwisher@comcast.net
Rasco Badguy<txkidd@swbell.net>mail.comcast.net00000001
IM?John Washerchkwisher@comcast.net
D...Badguy<txkidd@swbell.net>mail.comcast.net00000001@
```

- 6) How many .doc files are there? Extract all, document what is their content and their md5 values.



This is a test document to demonstrate the abilities of **Dijang** and its optional search parameters ...

The following words should result in hits when the **stemming** option is applied to the word "kill". Kill

Killed

Killer

Killing

**Kill**

The following word should result in hits when the **synonym** option is applied to the word "raise"

Raise

Lift

The following word should result in hits when the **phonetic** option is applied to the word "plane"

Plane

Marijuana

Plain

Name	S	C	O	Location	Modified Time	Change Time	Access Time
Washers To Do List.doc.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2008-02-12 06:25:06 IST	2008-02-12 06:49:43 IST	2008-02-13 10:54:49 IST	
X marks the spot.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2007-07-26 01:56:37 IST	2008-02-14 01:06:08 IST	2007-07-26 01:56:37 IST	
How To Steal Credit Numbers.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2007-07-26 01:37:55 IST	2007-07-26 01:38:36 IST	2007-07-26 02:01:43 IST	
Options.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2007-07-24 02:13:40 IST	2007-07-24 02:13:40 IST	2007-07-26 01:22:17 IST	
SLIST.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2007-07-26 01:37:47 IST	2007-07-26 01:38:32 IST	2007-07-26 02:01:43 IST	
The Dealz.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2007-07-26 01:56:24 IST	2007-07-26 01:56:24 IST	2007-07-26 02:01:43 IST	
X marks the spot.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Administr... 2007-07-26 01:56:50 IST	2007-07-26 01:56:50 IST	2007-07-26 02:01:43 IST	
winword.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Billy B... 2001-08-23 17:30:00 IST	2007-08-04 06:52:45 IST	2007-08-04 06:48:23 IST	
winword.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Captia... 2001-08-23 17:30:00 IST	2007-08-04 06:52:57 IST	2007-08-04 06:49:14 IST	
winword.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Mr Sm... 2001-08-23 17:30:00 IST	2007-08-04 06:53:34 IST	2007-08-04 06:49:30 IST	
winword.doc				/img_Washer.E01/vol_vol2/Documents and Settings/The W... 2001-08-23 17:30:00 IST	2007-08-04 06:53:13 IST	2007-08-04 06:49:44 IST	
winword2.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Billy B... 2001-08-23 17:30:00 IST	2007-08-04 06:52:45 IST	2007-08-04 06:48:23 IST	
winword2.doc				/img_Washer.E01/vol_vol2/Documents and Settings/Captia... 2001-08-23 17:30:00 IST	2007-08-04 06:52:57 IST	2007-08-04 06:49:14 IST	

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Matches on page: - of - Match   | Page: 1 of 1 Page   | Text Source:

- Buy peanut butter
- Call mom
- Kill Familiars
- Burry Wes's enemies
- Confess to the police

Click here for something funny!

- 6) Who are all involved in the discussion about "Special K".

Keyword search

Name	Created Time	Location	Modified Time	Change Time	A
Sent Items.dbx	2007-08-04 07:11:21 IST	/Img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-08-04 06:59:11 IST	2007-08-04 06:59:11 IST	20
Deleted Items.dbx	2007-08-04 07:11:21 IST	/Img_Washer.E01/vol_vol2/Documents and Settings/Administr...	2007-08-04 06:59:10 IST	2007-08-04 06:59:10 IST	20

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Matches on page: 1 of 5 Match | Page: 1 of 126 Page | Text Source:

```
I have the "Special K" your looking for... but it is going to cost you!
Give me a buzz! But hurry... this stuff ain't gonna last!
-----_NextPart_000_009D_01C7B332.06287580
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
OCTET-TYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html";
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.3132" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>Dude!&nbsp; </FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT>&nbsp;</DIV>
<DIV><FONT face=3DArial size=3D2>You been laying a little low these=20
days?</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT
>&nbsp;</DIV>
<DIV><FONT face=3DArial size=3D2>I have been trying to call you almost =
daily and we=20
can't hook up!</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT>&nbsp;</DIV>
<DIV><FONT face=3DArial size=3D2>I have the "Special K" your looking =
for... but it=20
is going to cost you!</FONT></DIV>
```

7) Find the URL that is given for making drugs quickly

[http://www.totse.com/en/drugs/speedy\\_drugs/howtomanufactul72921.html](http://www.totse.com/en/drugs/speedy_drugs/howtomanufactul72921.html)

8) What is the AOL IM name of Washer?

```
userinfo.bag AOL Feedbag 1.1
1024
AIM Bots
    MovieFone
Prof Gilzot
Less than 3 months to go!!!
Sharethisdotcom
Spleak
    IM Street
Buddies
rbadguy2424
Family
Co-Workers
Recent Buddies
```

### c) Mantooth.E01 Report

#### Report Navigation

- Case Summary
- Accounts: Email (60)
- Data Source Usage (1)
- E-Mail Messages (65)
- EXIF Metadata (7)
- Encryption Detected (2)
- Extension Mismatch Detected (9)
- Installed Programs (40)
- Keyword Hits (473)
- Metadata (38)
- Operating System Information (2)
- Operating System User Account (8)
- Recent Documents (109)
- Recycle Bin (9)
- Remote Drive (1)
- Run Programs (17)

#### Autopsy Forensic Report

HTML Report Generated on 2021/08/21 16:43:31

Case: Mantooth  
Case Number: 1  
Number of data sources in case: 1  
Examiner: Rohan

#### Image Information:

Mantooth.E01

Timezone: Asia/Muscat  
Path: C:\Users\Rohan\Downloads\Mantooth.E01

#### Software Information:

Autopsy Version:	4.16.0
Android Analyzer Module:	4.16.0
Central Repository Module:	4.16.0
Data Source Integrity Module:	4.16.0

#### Report Navigation

- Case Summary
- Accounts: Email (60)
- Data Source Usage (1)
- E-Mail Messages (65)
- EXIF Metadata (7)
- Encryption Detected (2)
- Extension Mismatch Detected (9)
- Installed Programs (40)
- Keyword Hits (473)
- Metadata (38)
- Operating System Information (2)
- Operating System User Account (8)
- Recent Documents (109)
- Recycle Bin (9)
- Remote Drive (1)
- Run Programs (17)

Drone Analyzer Module:	4.16.0
Email Parser Module:	4.16.0
Embedded File Extractor Module:	4.16.0
Encryption Detection Module:	4.16.0
Exif Parser Module:	4.16.0
Extension Mismatch Detector Module:	4.16.0
File Type Identification Module:	4.16.0
GPX Parser Module:	1.2
Hash Lookup Module:	4.16.0
Interesting Files Identifier Module:	4.16.0
Keyword Search Module:	4.16.0
PhotoRec Carver Module:	7.0
Plaso Module:	4.16.0
Recent Activity Module:	4.16.0
Virtual Machine Extractor Module:	4.16.0

#### Ingest History:

Job 1:

Data Source:	Mantooth.E01
Status:	COMPLETED
Enabled Modules:	Recent Activity

# Washer.E01 Report

## Report Navigation

- Case Summary
- ★ Data Source Usage (1)
- EXIF Metadata (11)
- Encryption Detected (4)
- Extension Mismatch Detected (111)
- Installed Programs (23)
- Keyword Hits (456)
- Metadata (2)
- Operating System Information (2)
- Operating System User Account (12)
- Recent Documents (43)
- Shell Bags (132)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- USB Device Attached (11)

## Autopsy Forensic Report

HTML Report Generated on 2021/08/21 17:06:24

Case: Washer  
Case Number: 1  
Number of data sources in case: 1  
Examiner: Rohan

**Image Information:**

Washer.E01

Timezone: Asia/Muscat  
Path: C:\Users\Rohan\Downloads\Washer.E01

**Software Information:**

Autopsy Version:	4.16.0
Android Analyzer Module:	4.16.0
Central Repository Module:	4.16.0
Data Source Integrity Module:	4.16.0

## Report Navigation

- Case Summary
- ★ Data Source Usage (1)
- EXIF Metadata (11)
- Encryption Detected (4)
- Extension Mismatch Detected (111)
- Installed Programs (23)
- Keyword Hits (456)
- Metadata (2)
- Operating System Information (2)
- Operating System User Account (12)
- Recent Documents (43)
- Shell Bags (132)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- USB Device Attached (11)

## Ingest History:

Job 1:

Data Source:	Washer.E01
Status:	COMPLETED
Enabled Modules:	Recent Activity Android Analyzer Encryption Detection Virtual Machine Extractor Drone Analyzer Plaso Hash Lookup File Type Identification Embedded File Extractor Exif Parser Keyword Search Email Parser Extension Mismatch Detector Interesting Files Identifier PhotoRec Carver GPX Parser Encryption Detection Central Repository Data Source Integrity

