VIT®

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.

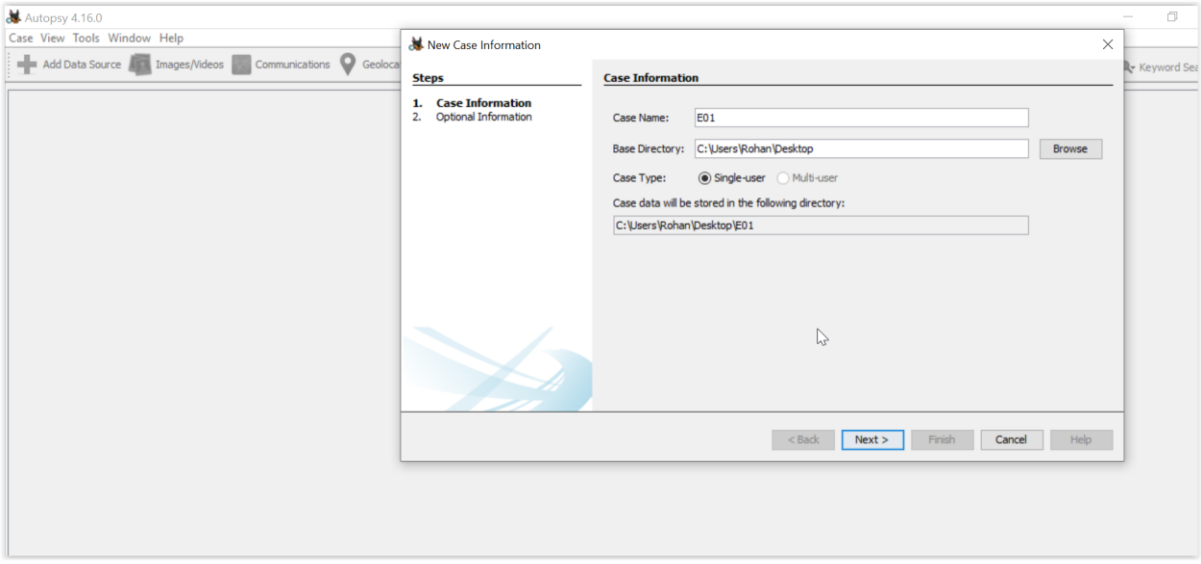
b. Utilize the dataset (Mantooth.E01 & Washer.E01) that is provided through the google drive and answer the questions accordingly.

c. Generate a report through Autopsy tool and provide your respective interpretation.

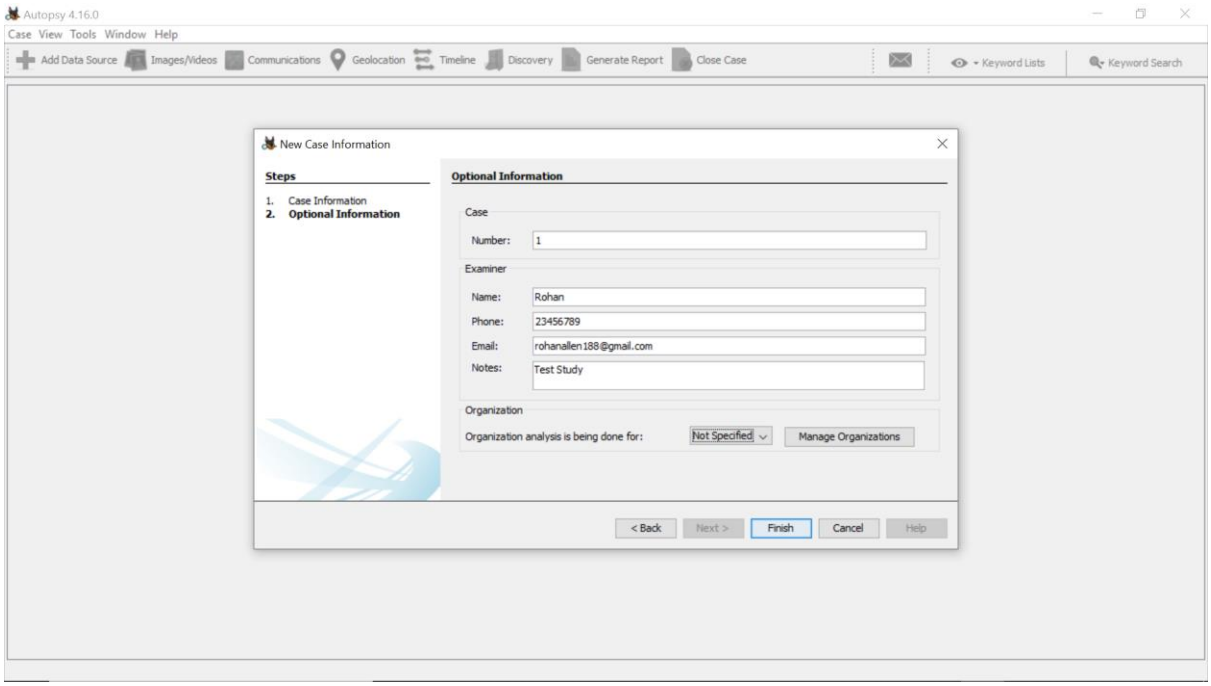
d. Combine all the files and upload as a single PDF file in VTOP.

a) Startup Page- New Case

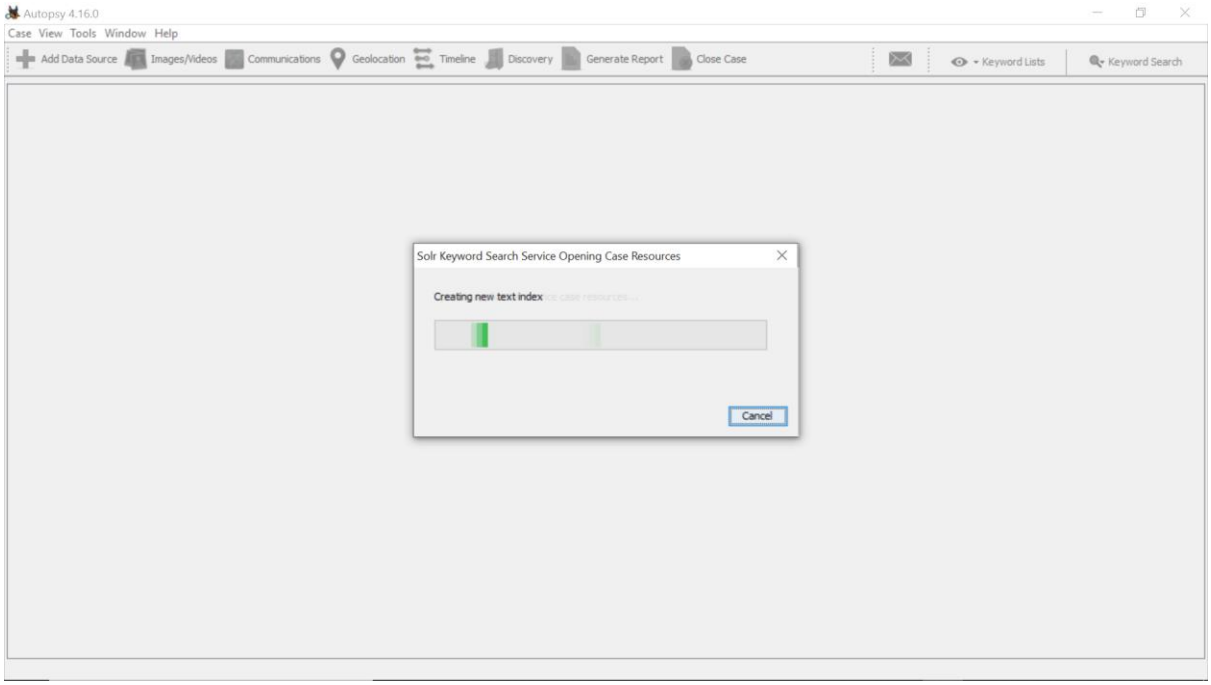
Enter Case Name and directory where it will be saved



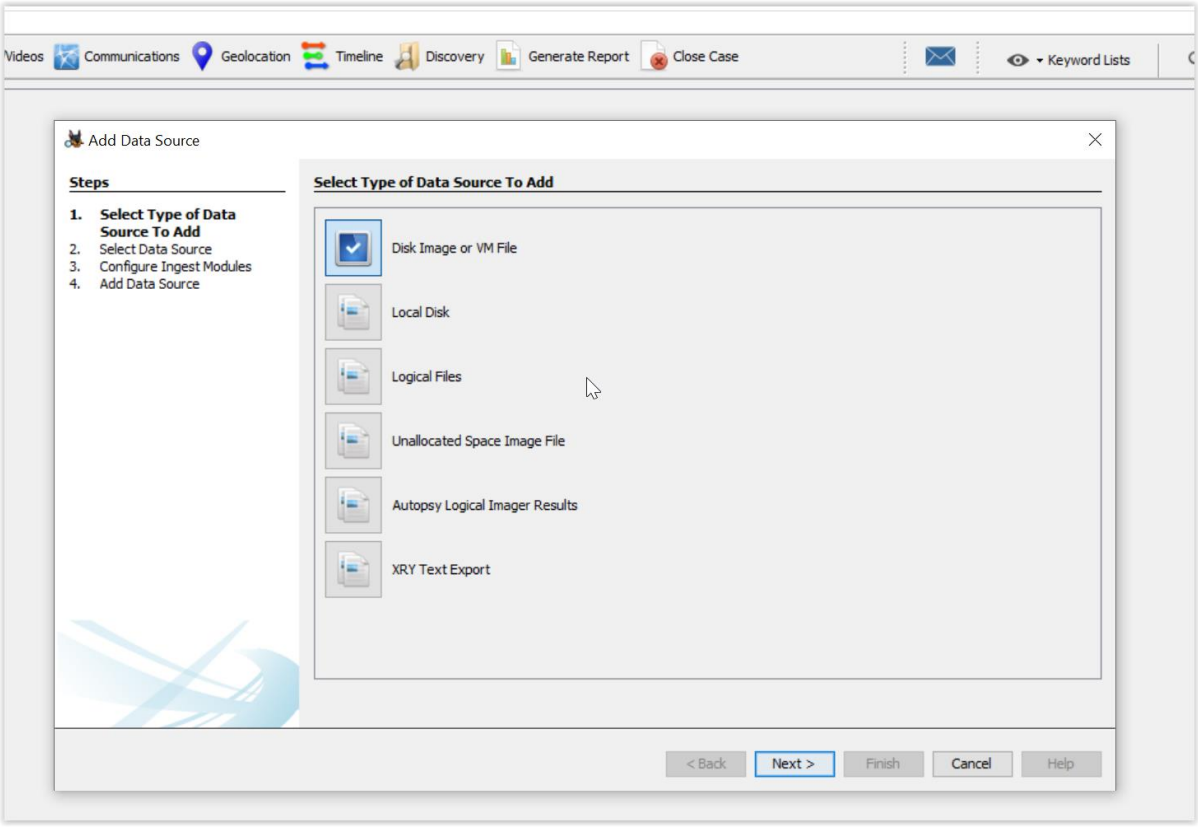
Enter Case Number, and Examiner details



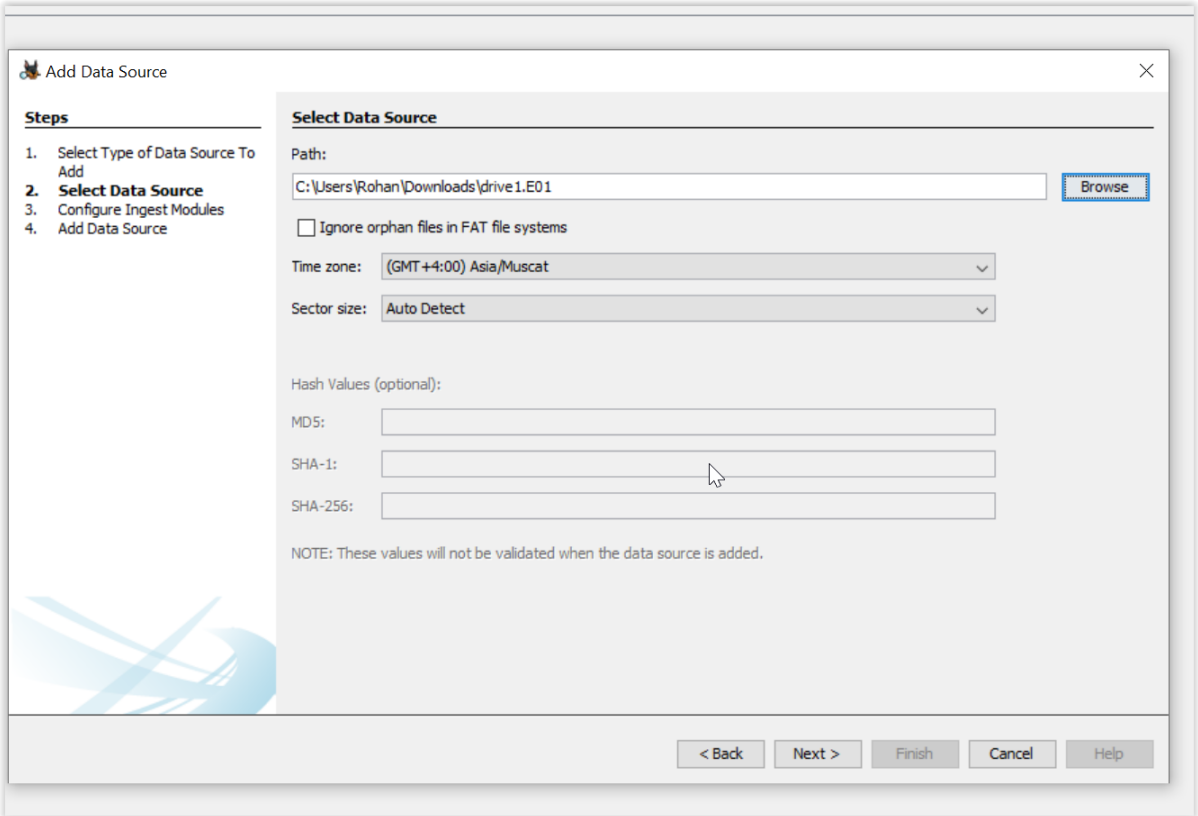
Creating Autopsy Case file



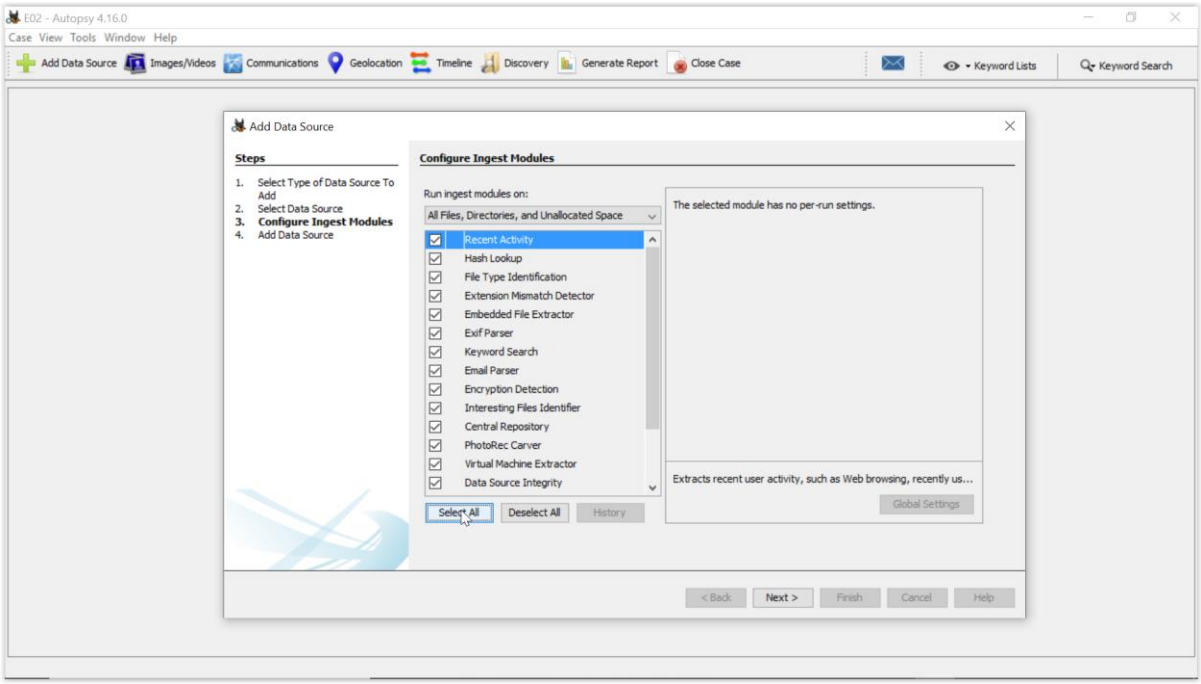
Add data source to analyse



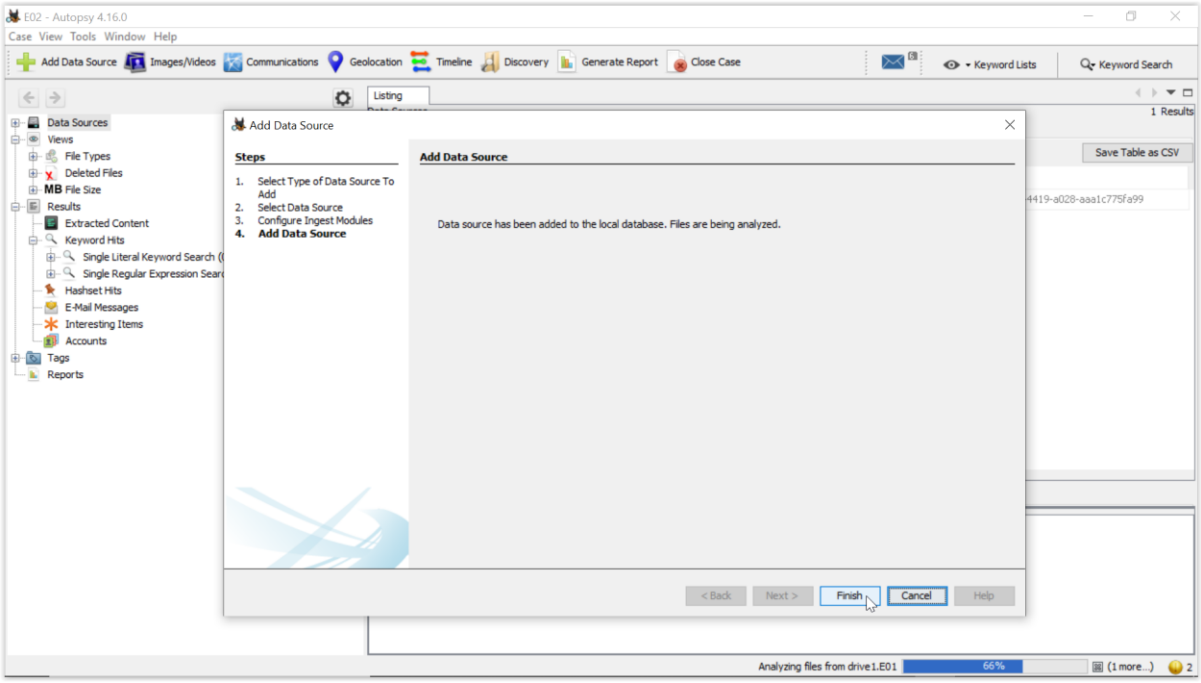
Select path to add E01 drive image to analyse. Also Select timezone



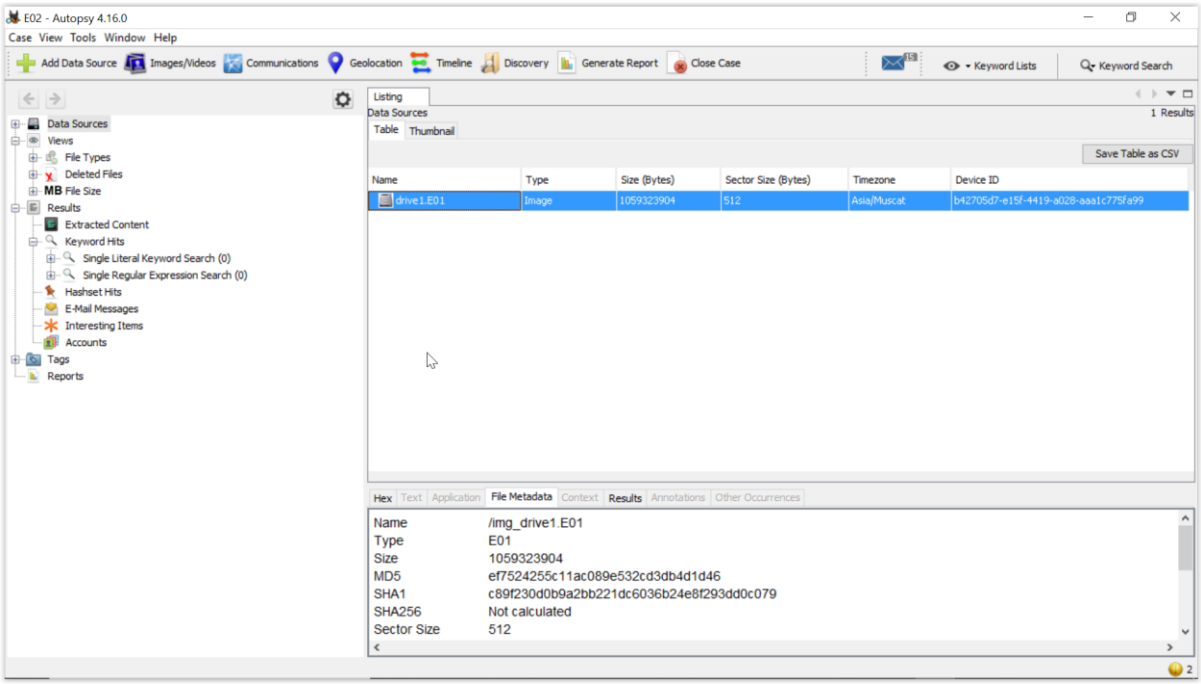
Configure ingest module to select the various types of processing you want done on your disk image. I have selected all.

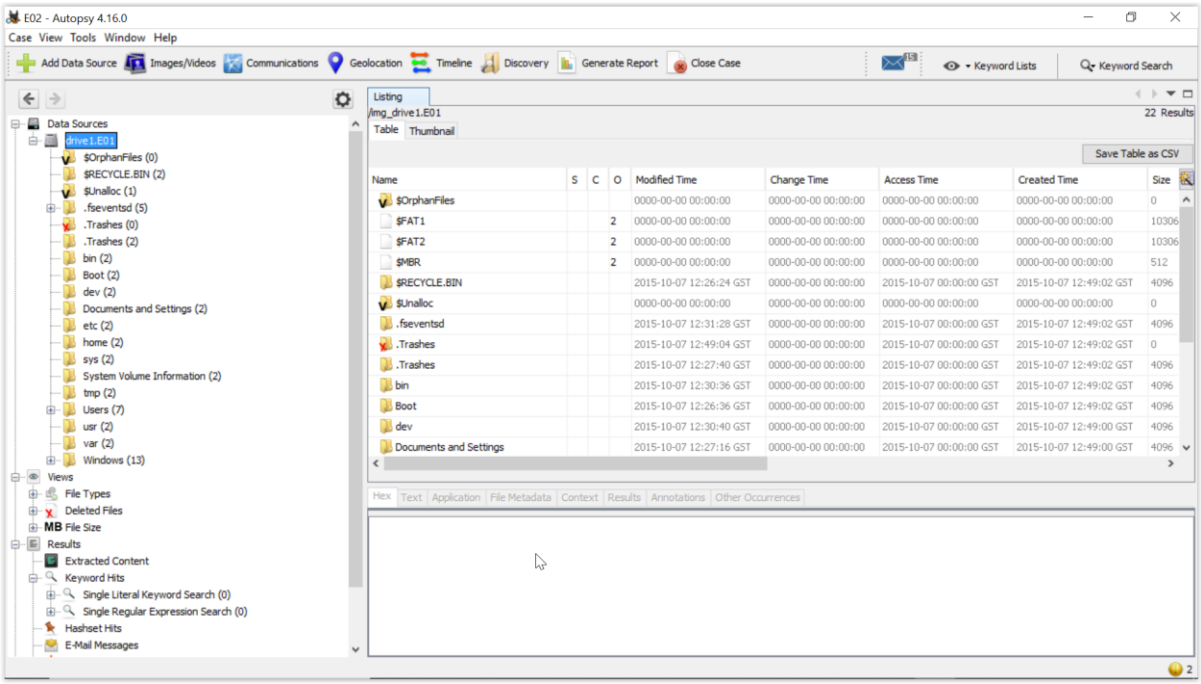


Data Source is successfully added.

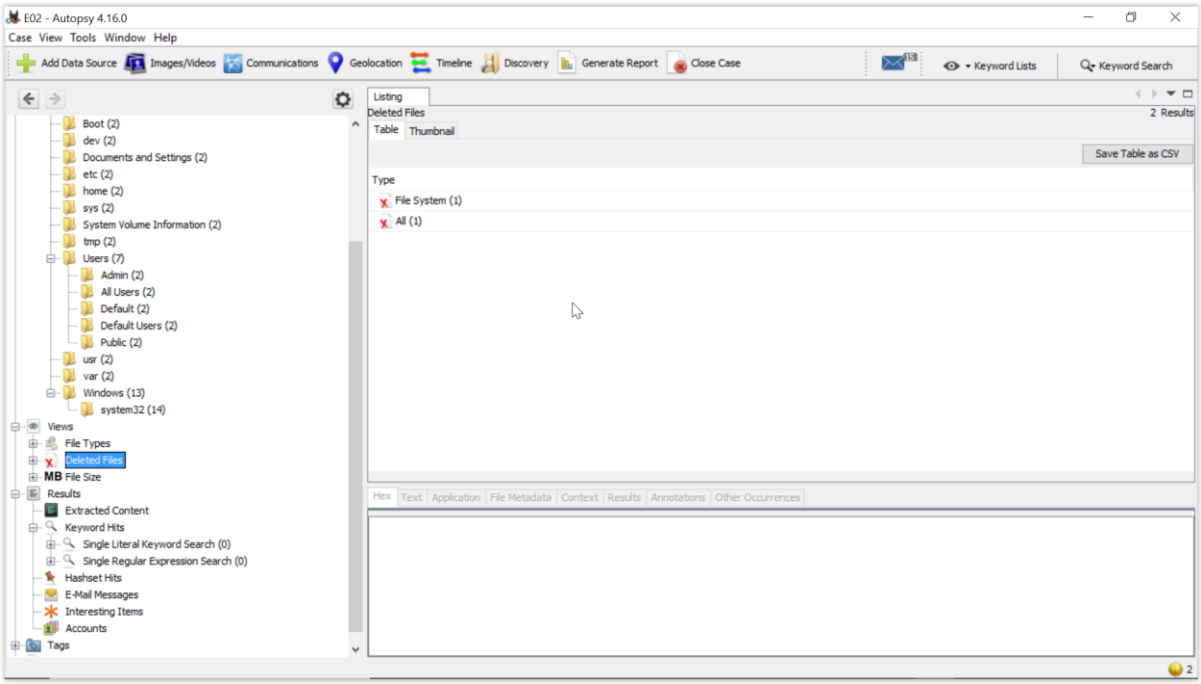


Can view information like data source, files contained, deleted files, images, videos, emails, etc and their hexadecimal and metadata information for the E01 disk image being analysed.

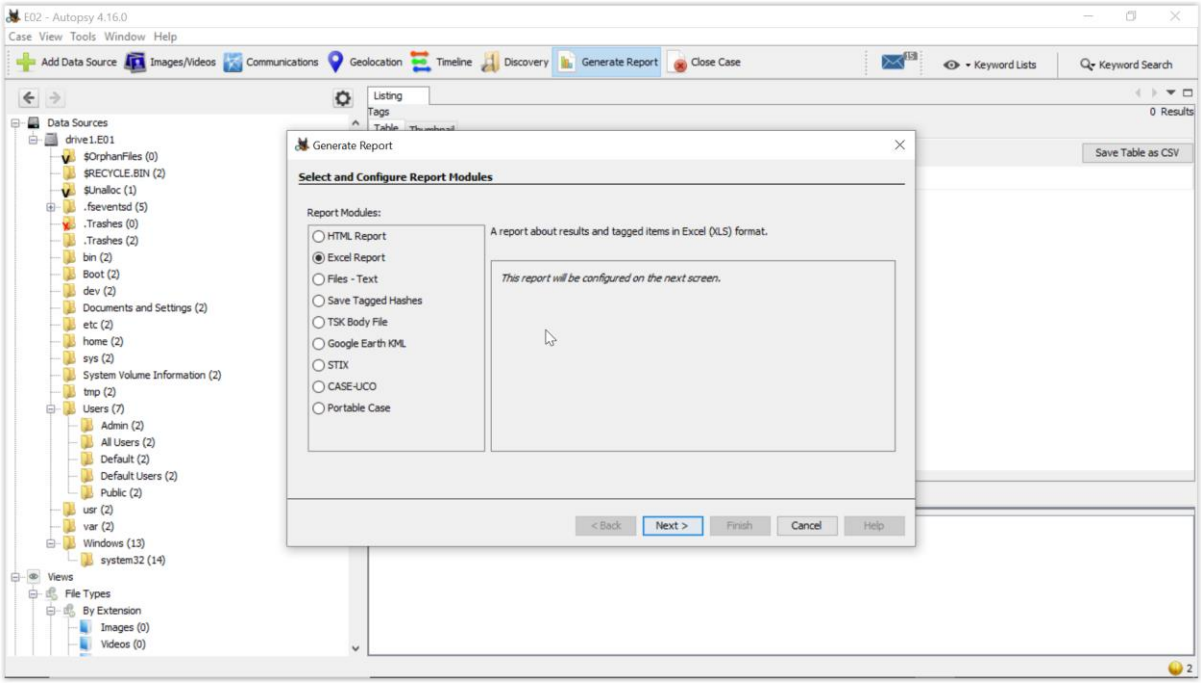




Deleted files:



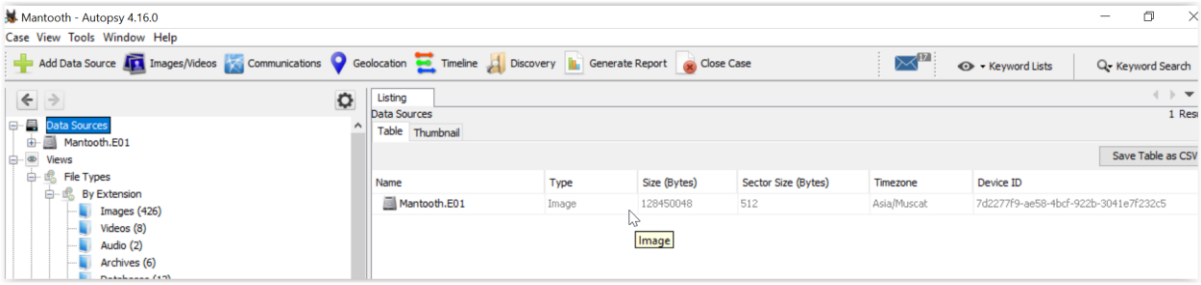
Generate excel report of case findings



b)

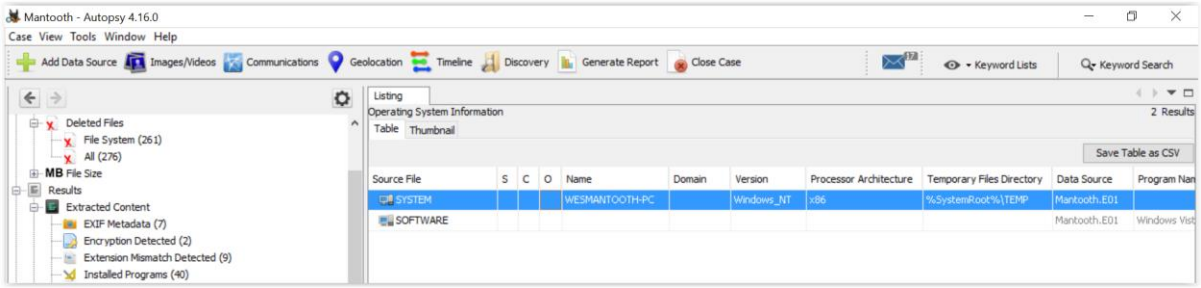
1) What type of file is Mantooth.E01

Image file

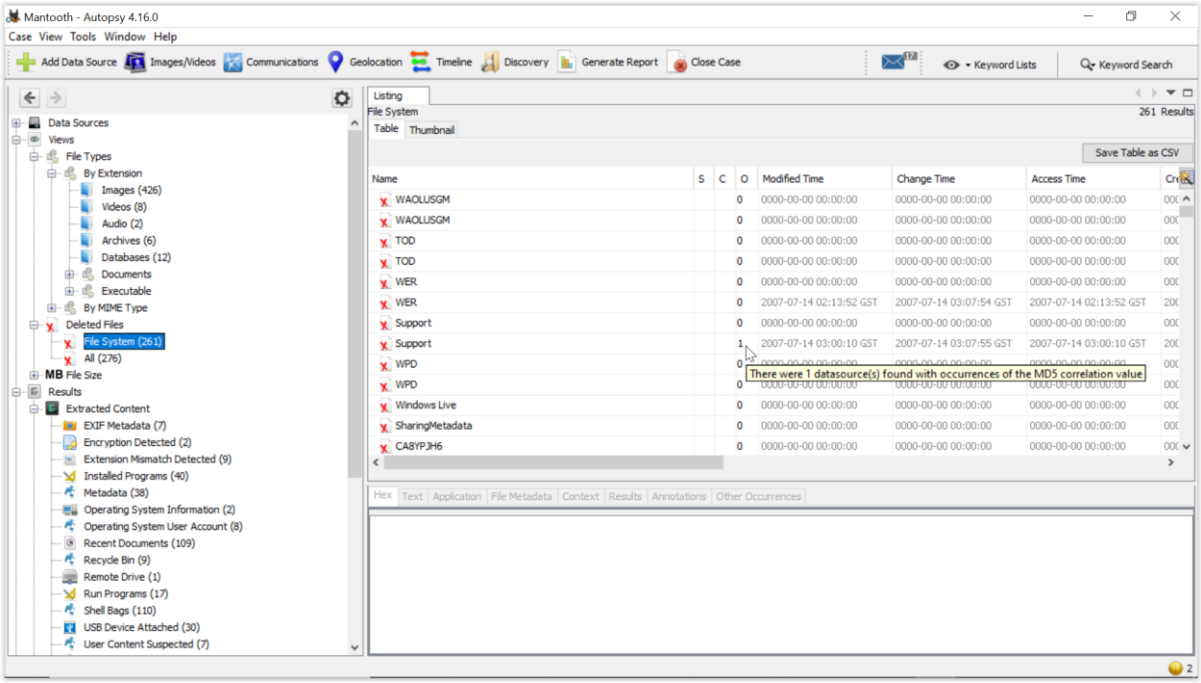


2) What is the Operating System?

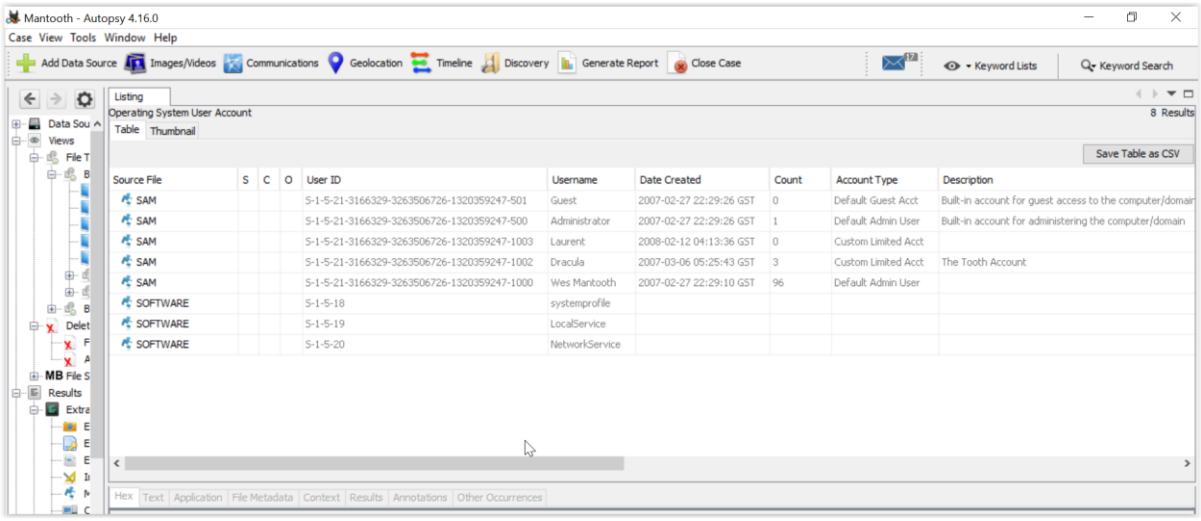
Windows_NT

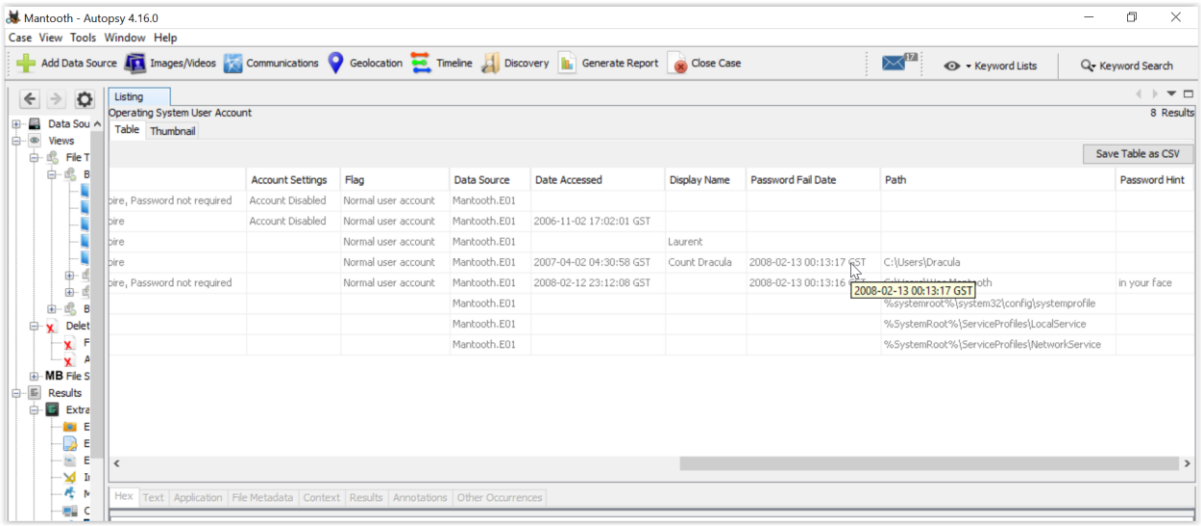


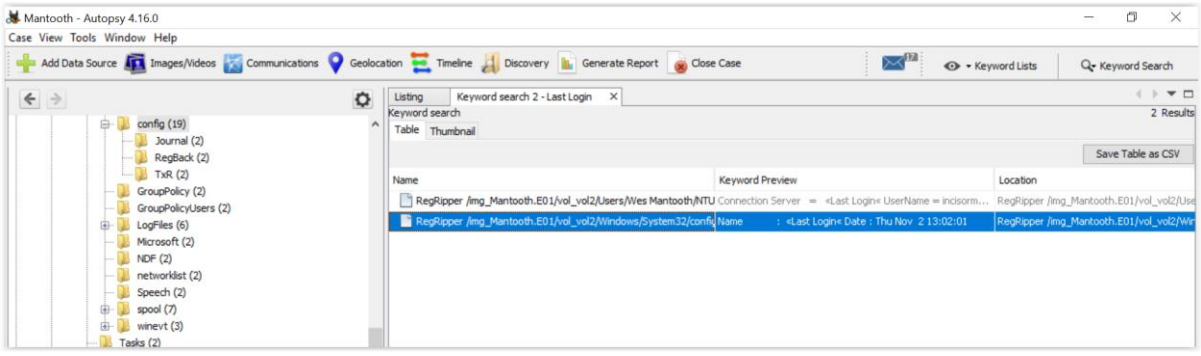
3) What is the File System?



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

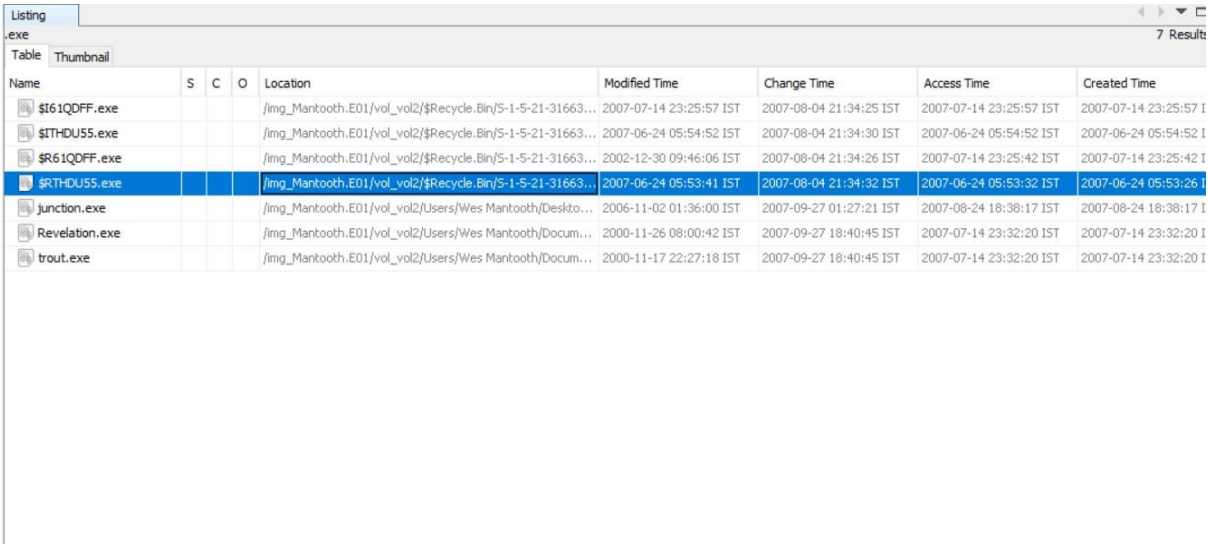




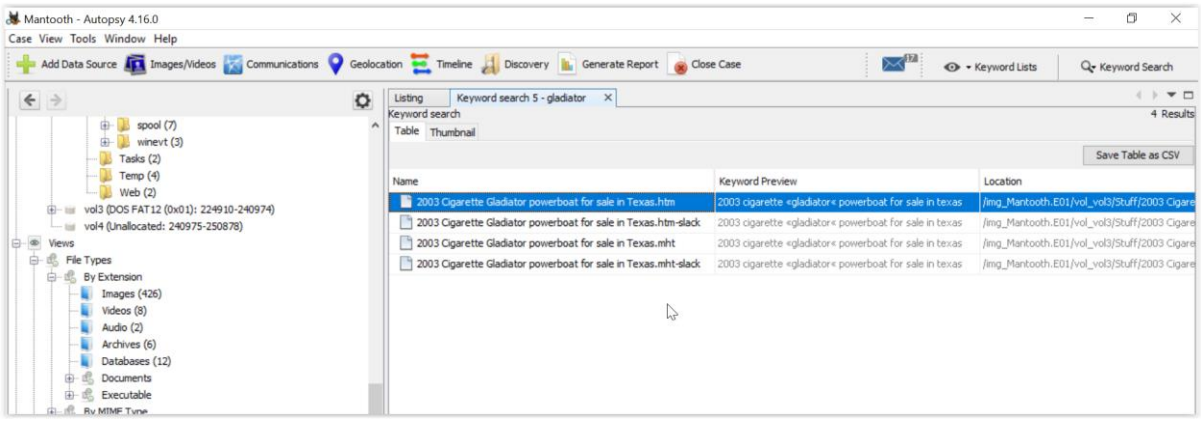


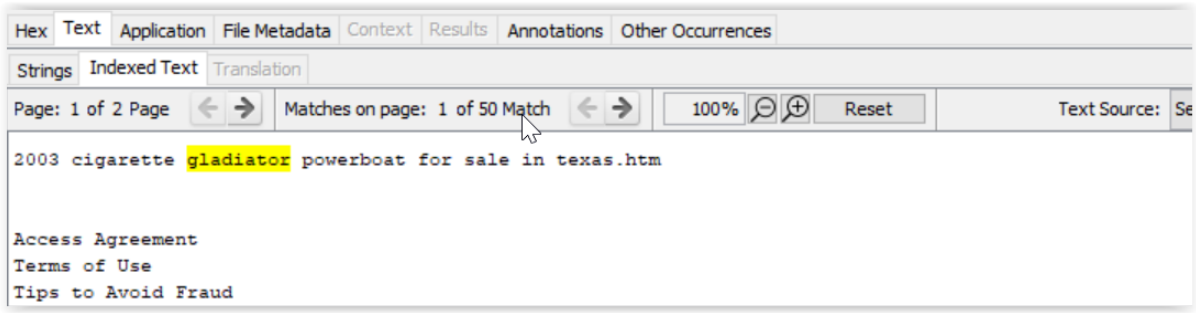
5) If there is any evidence of .exe file being deleted, describe the artifact name and document your findings.

4 .exe file are deleted



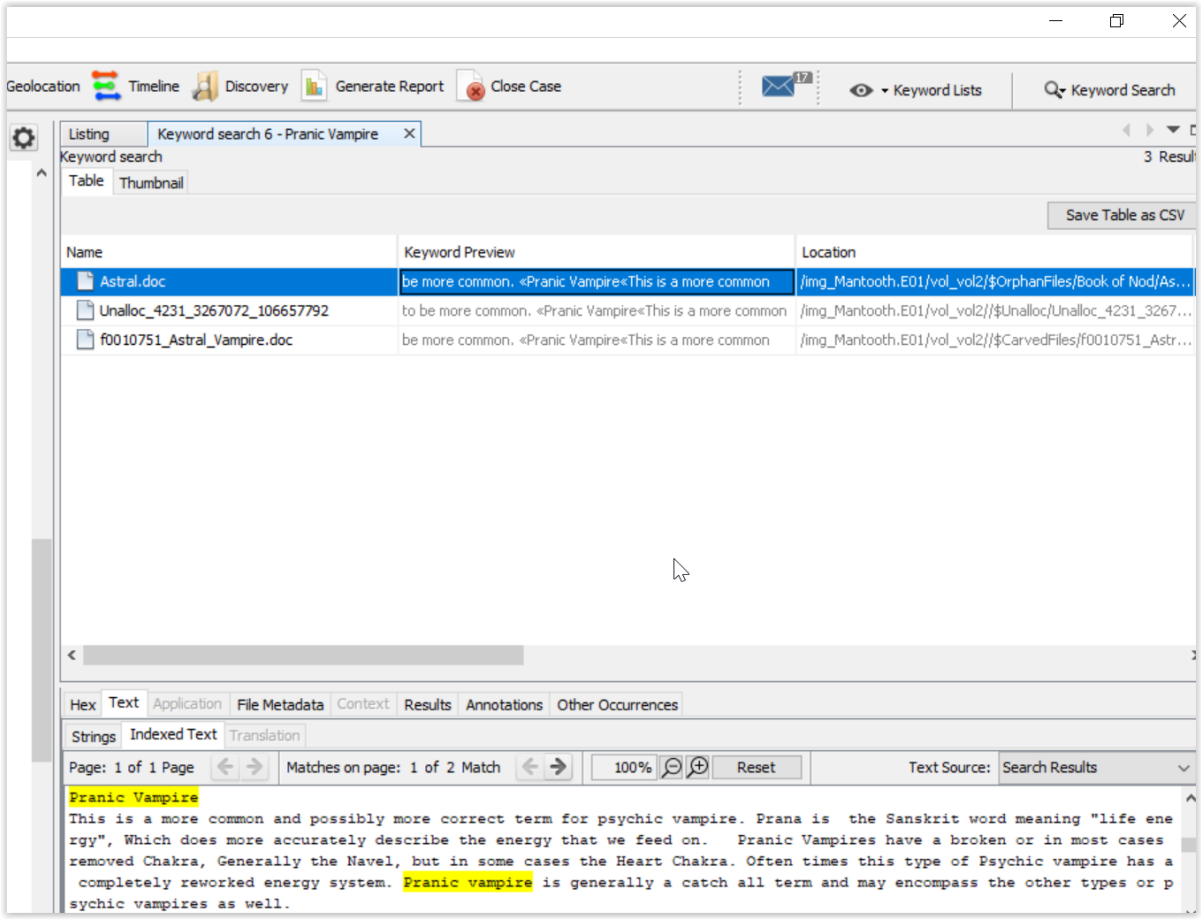
6) Find proof of communication with Gladiator

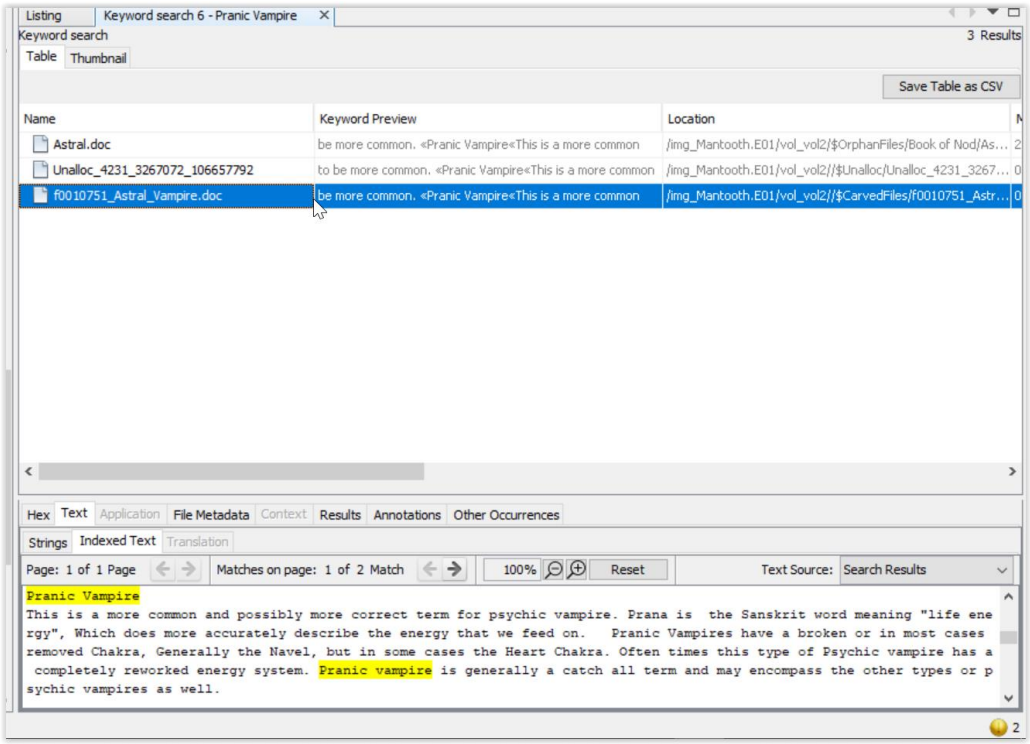




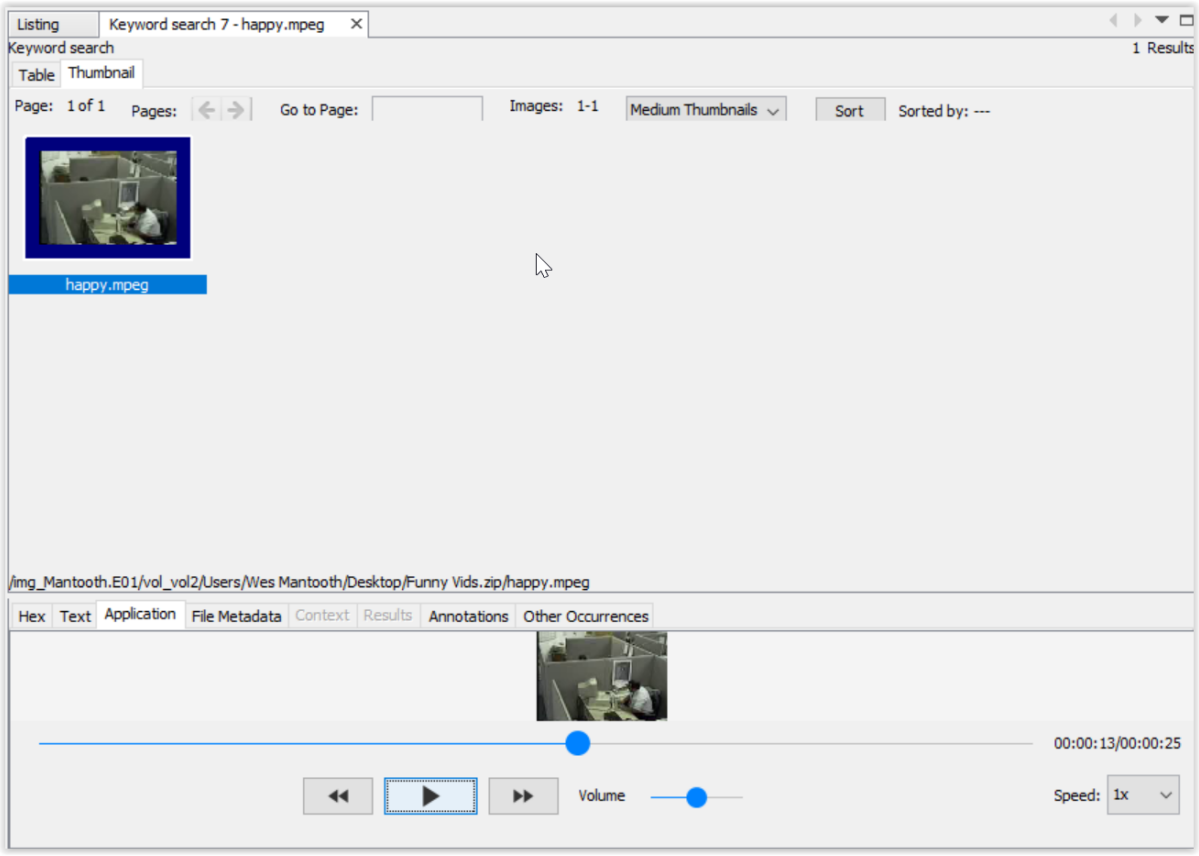
7) What is a "Pranic Vampire"? In which document is it mentioned? When was the document created?

Astral.doc and Astral_Vampire.doc

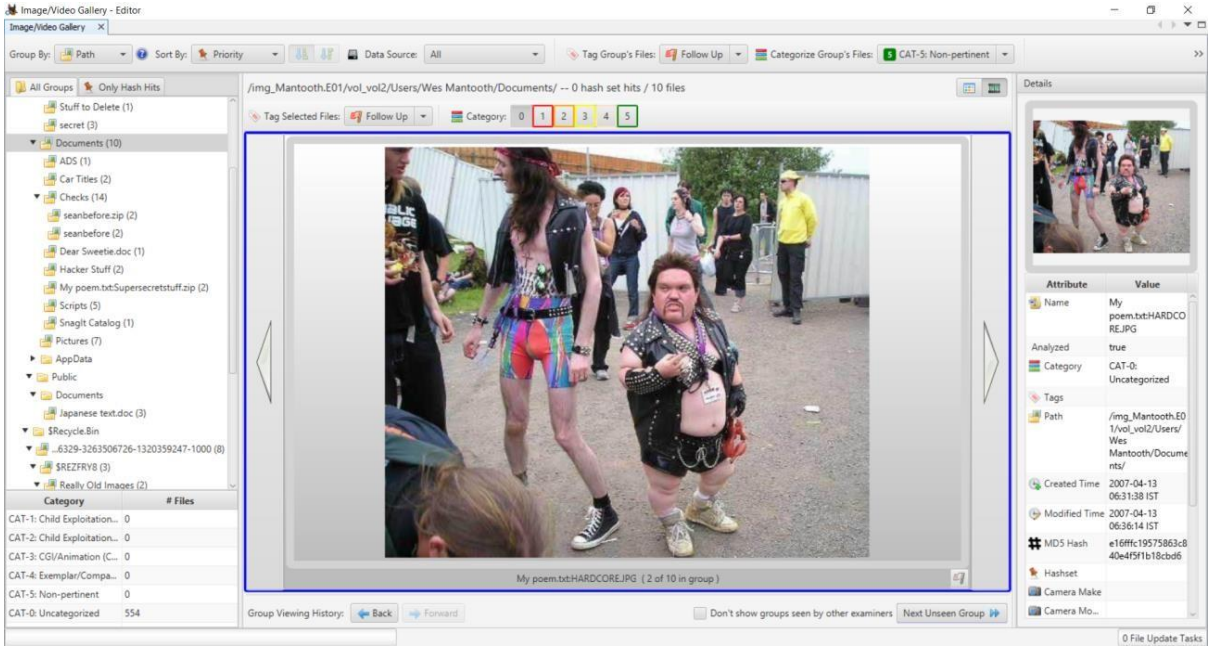

Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Keyword search 6 - Pranic Vampire
Keyword search
3 Resul
Table
Thumbnail
Save Table as CSV
Name
Keyword Preview
Location
Astral.doc
be more common. «Pranic Vampire«This is a more common
/img_Mantooth.E01/vol_vol2/$OrphanFiles/Book of Nod/As...
Unalloc_4231_3267072_106657792
to be more common. «Pranic Vampire«This is a more common
/img_Mantooth.E01/vol_vol2//$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 ene
rgy", 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 or p
sychic vampires as well.

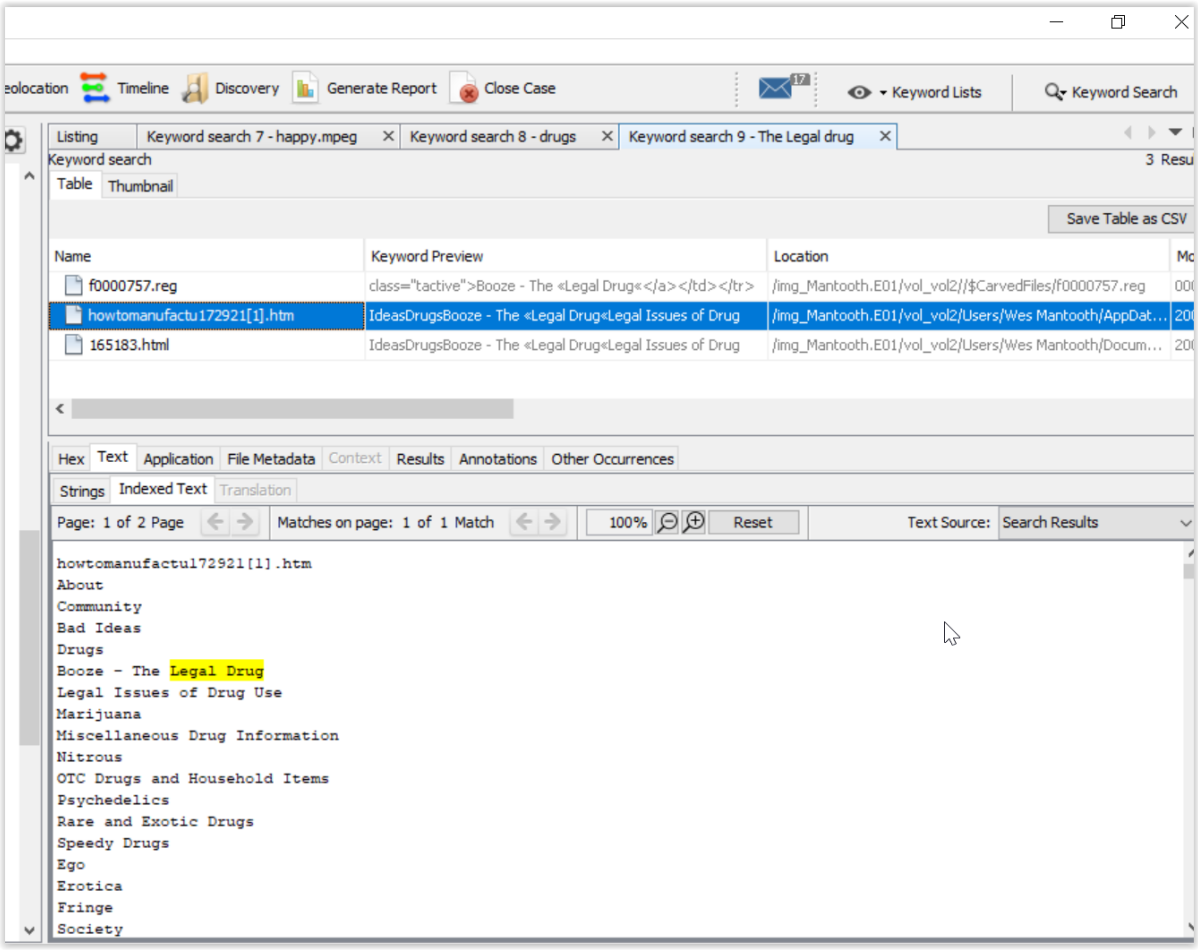

Listing
Keyword search 6 - Pranic Vampire
Keyword search
3 Results
Table
Thumbnail
Save Table as CSV
Name
Keyword Preview
Location
Astral.doc
be more common. «Pranic Vampire«This is a more common
/img_Mantooth.E01/vol_vol2/$OrphanFiles/Book of Nod/As...
Unalloc_4231_3267072_106657792
to be more common. «Pranic Vampire«This is a more common
/img_Mantooth.E01/vol_vol2//$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 ene
rgy", 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 or p
sychic vampires as well.

8) What is present in happy.mpeg?

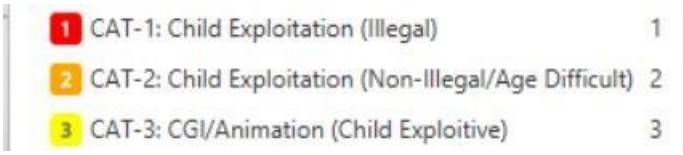


9) Check if picture of any drugs are present? If so name the drugs.





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



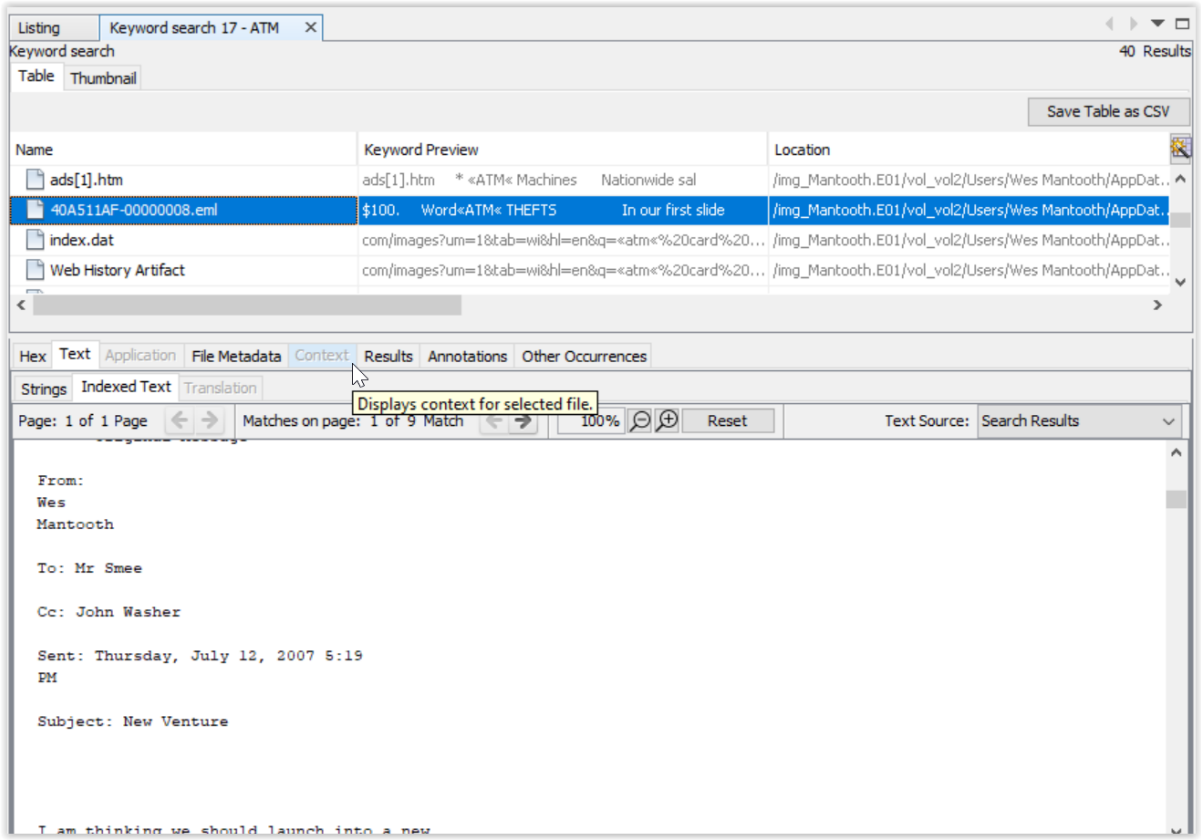
11) Summarize the finding against Mantooth

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

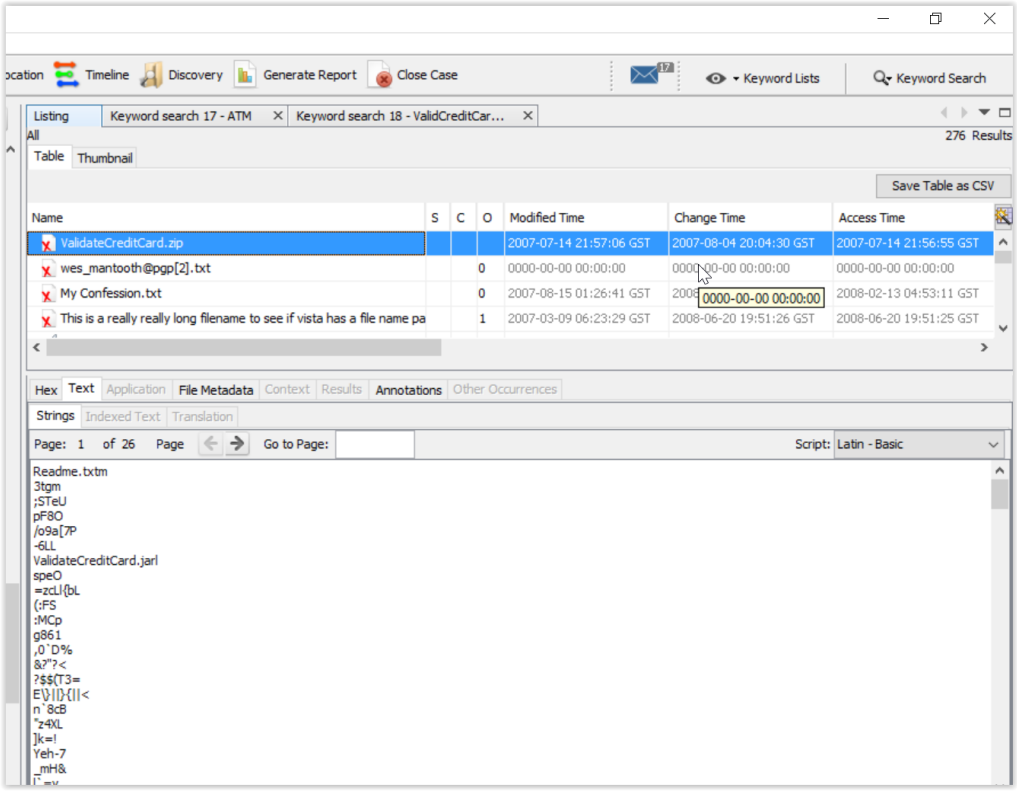
- Boose
- Marijauna
- OTC
- Speedy Drugs
- Fringe

Also Mantooth was in contact with Gladiator.

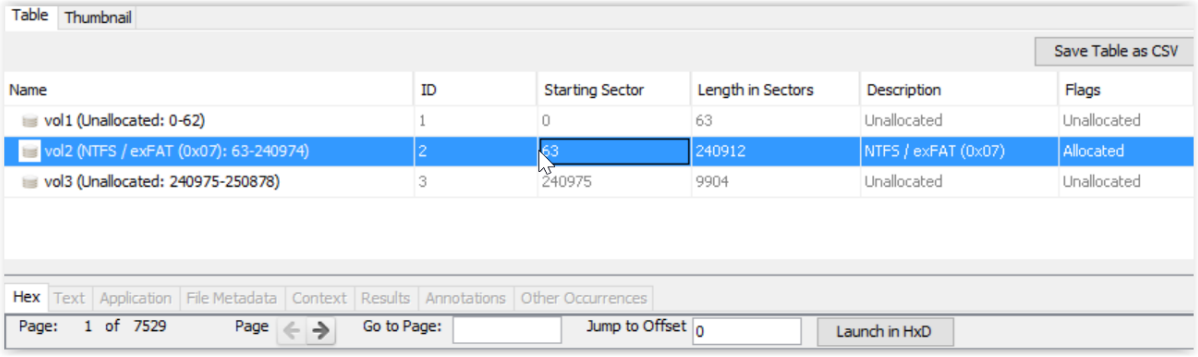
12) Mantooth received one Text Internet Email that had no subject about a stolen ATM. Who sent it to him (name and email) and when was it sent?



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

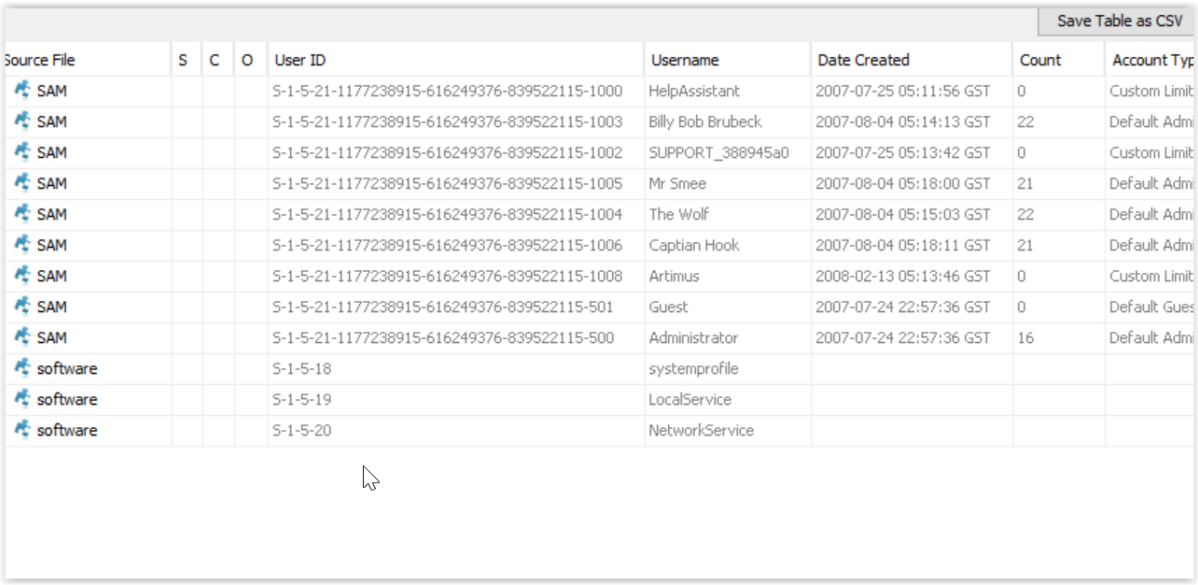

Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Keyword search 17 - ATM
Keyword search 18 - ValidCreditCar...
All
276 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
ValidateCreditCard.zip
2007-07-14 21:57:06 GST
2007-08-04 20:04:30 GST
2007-07-14 21:56:55 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
0000-00-00 00:00:00
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
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
=zcL!{bL
(:FS
:MCp
g861
,0`D%
&?"?<
?$${T3=
E\}!|}{||<
n`8cB
"z4XL
]k=!
Yeh-7
_mH&

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

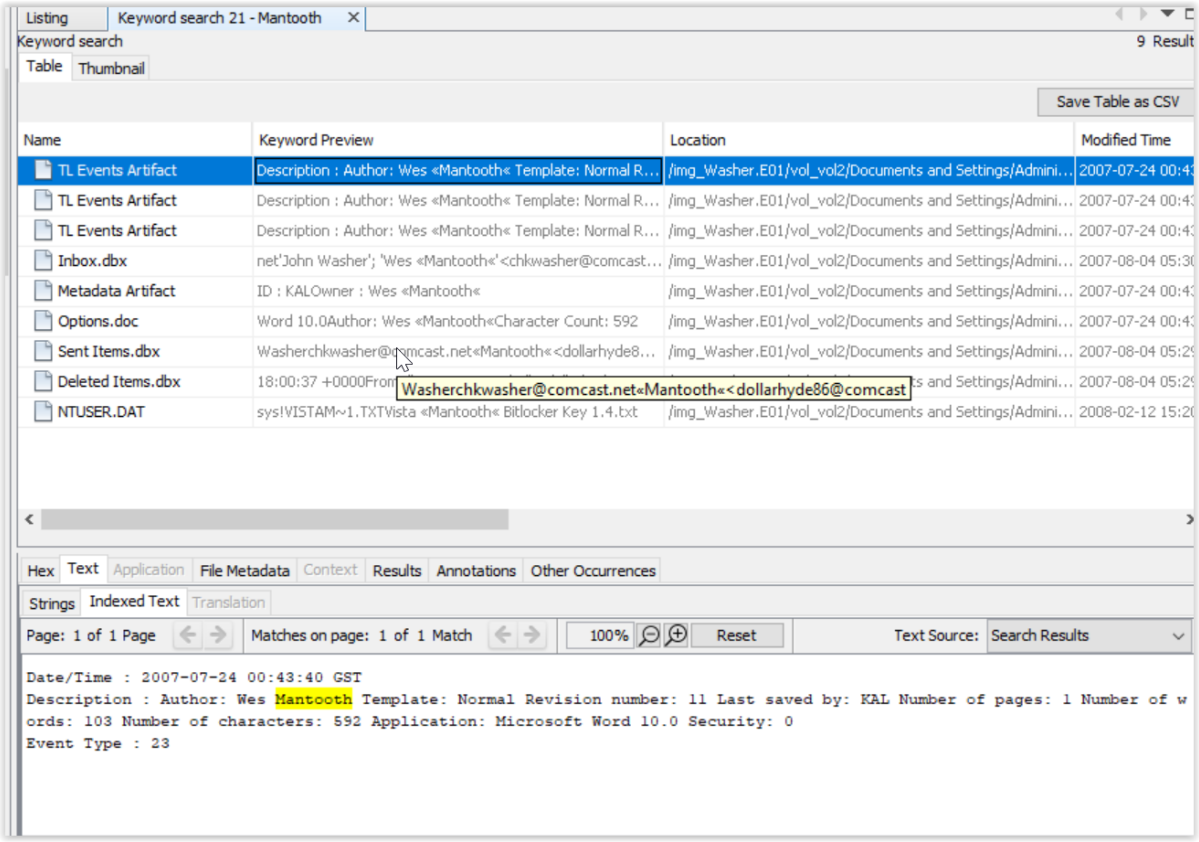


2) What is the file system of the disk image?

3) List the user names?



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


Listing
Keyword search 21 - Mantooth
Keyword search
9 Result
Table
Thumbnail
Save Table as CSV
Name
Keyword Preview
Location
Modified Time
TL Events Artifact
Description : Author: Wes «Mantooth« Template: Normal R...
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-07-24 00:43
TL Events Artifact
Description : Author: Wes «Mantooth« Template: Normal R...
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-07-24 00:43
TL Events Artifact
Description : Author: Wes «Mantooth« Template: Normal R...
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-07-24 00:43
Inbox.dbx
net'John Washer'; 'Wes «Mantooth«' <chkwasher@comcast...
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-08-04 05:30
Metadata Artifact
ID : KALOwner : Wes «Mantooth«
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-07-24 00:43
Options.doc
Word 10.0Author: Wes «Mantooth«Character Count: 592
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-07-24 00:43
Sent Items.dbx
Washerchkwasher@comcast.net«Mantooth«<dollarhyde8...
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
2007-08-04 05:29
Deleted Items.dbx
18:00:37 +0000From
Washerchkwasher@comcast.net«Mantooth«<dollarhyde86@comcast
/img_Washer.E01/vol_vol2/Documents and Settings/Admini...
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/Admini...
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 w
ords: 103 Number of characters: 592 Application: Microsoft Word 10.0 Security: 0
Event Type : 23

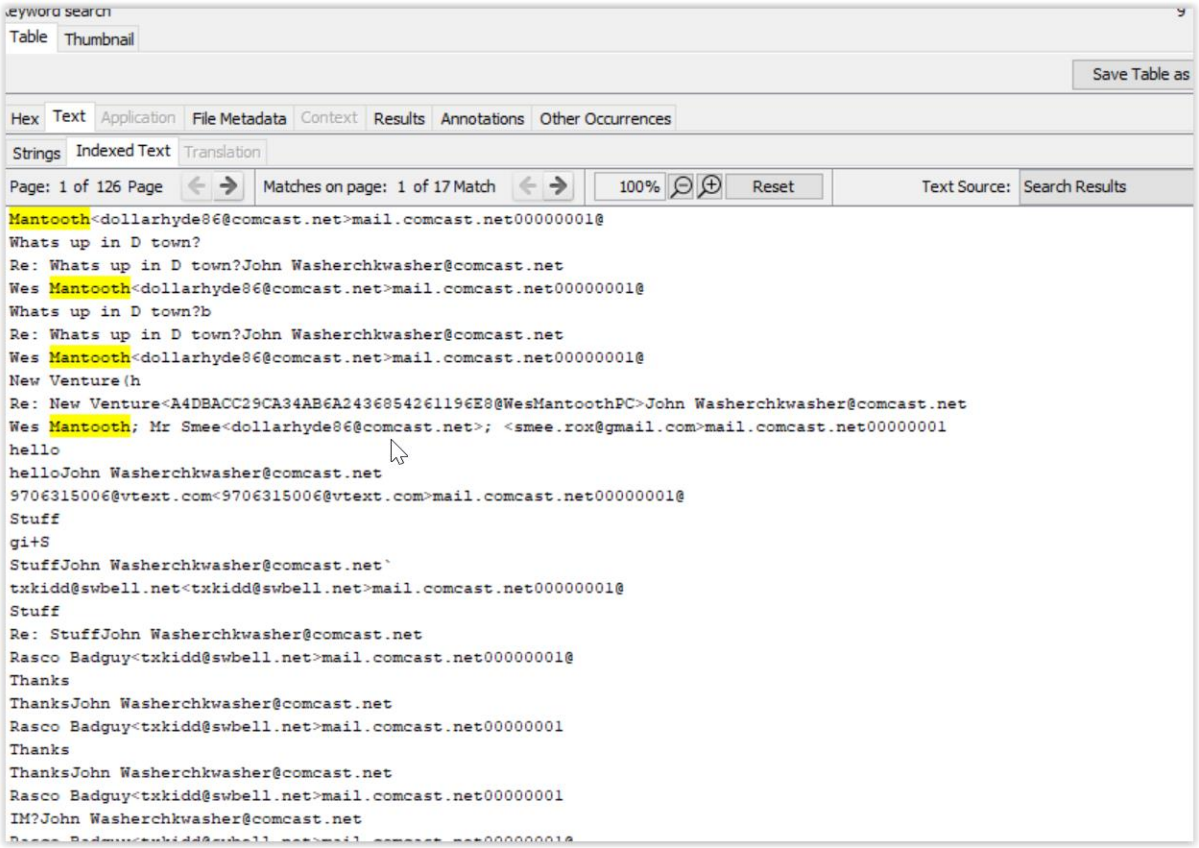


Table
Thumbnail
Save Table as
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 126 Page
Matches on page: 1 of 17 Match
100%
Reset
Text Source:
Search Results
Mantooth<dollarhyde86@comcast.net>mail.comcast.net00000001@
Whats up in D town?
Re: Whats up in D town?John Washerchkwasher@comcast.net
Wes Mantooth<dollarhyde86@comcast.net>mail.comcast.net00000001@
Whats up in D town?b
Re: Whats up in D town?John Washerchkwasher@comcast.net
Wes Mantooth<dollarhyde86@comcast.net>mail.comcast.net00000001@
New Venture(h
Re: New Venture<A4DBACC29CA34AB6A2436854261196E8@WesMantoothPC>John Washerchkwasher@comcast.net
Wes Mantooth; Mr Smee<dollarhyde86@comcast.net>; <smee.rox@gmail.com>mail.comcast.net00000001
hello
helloJohn Washerchkwasher@comcast.net
9706315006@vtext.com<9706315006@vtext.com>mail.comcast.net00000001@
Stuff
gi+S
StuffJohn Washerchkwasher@comcast.net`
txkidd@swbell.net<txkidd@swbell.net>mail.comcast.net00000001@
Stuff
Re: StuffJohn Washerchkwasher@comcast.net
Rasco Badguy<txkidd@swbell.net>mail.comcast.net00000001@
Thanks
ThanksJohn Washerchkwasher@comcast.net
Rasco Badguy<txkidd@swbell.net>mail.comcast.net00000001
Thanks
ThanksJohn Washerchkwasher@comcast.net
Rasco Badguy<txkidd@swbell.net>mail.comcast.net00000001
IM?John Washerchkwasher@comcast.net

5)

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 [redacted] 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

[redacted]

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

Lift

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

Plain

The following word should result when using the **fuzzy logic** option "1" with the word "marijuana"

Marihuana

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/Admini...	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/Admini...	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/Admini...	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/Admini...	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/Admini...	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/Admini...	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/Admini...	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: File Text

· Buy peanut butter

· Call mom

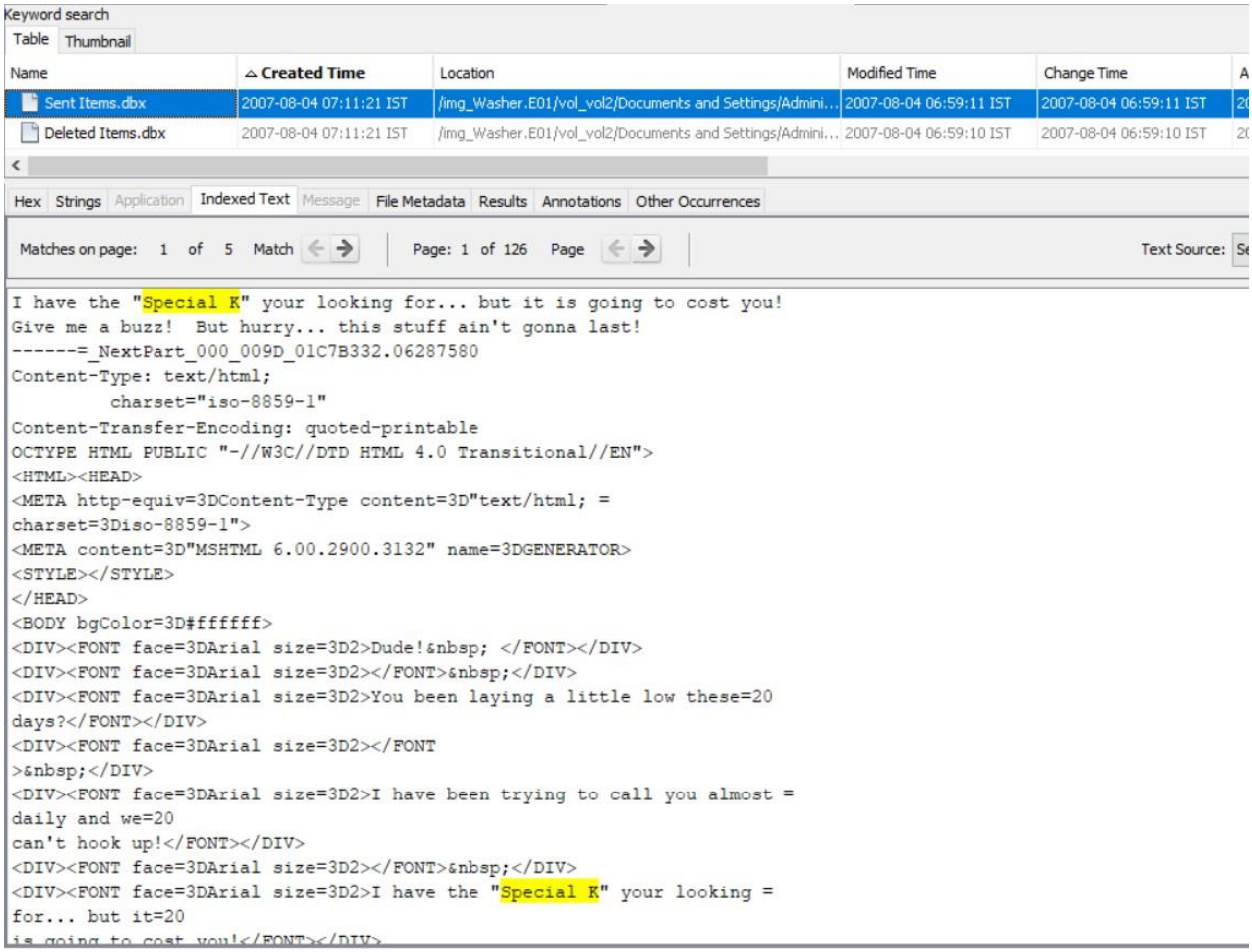
· Kill Familiars

· Burry Wes's enemies

· Confess to the police

Click here for something funny!

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



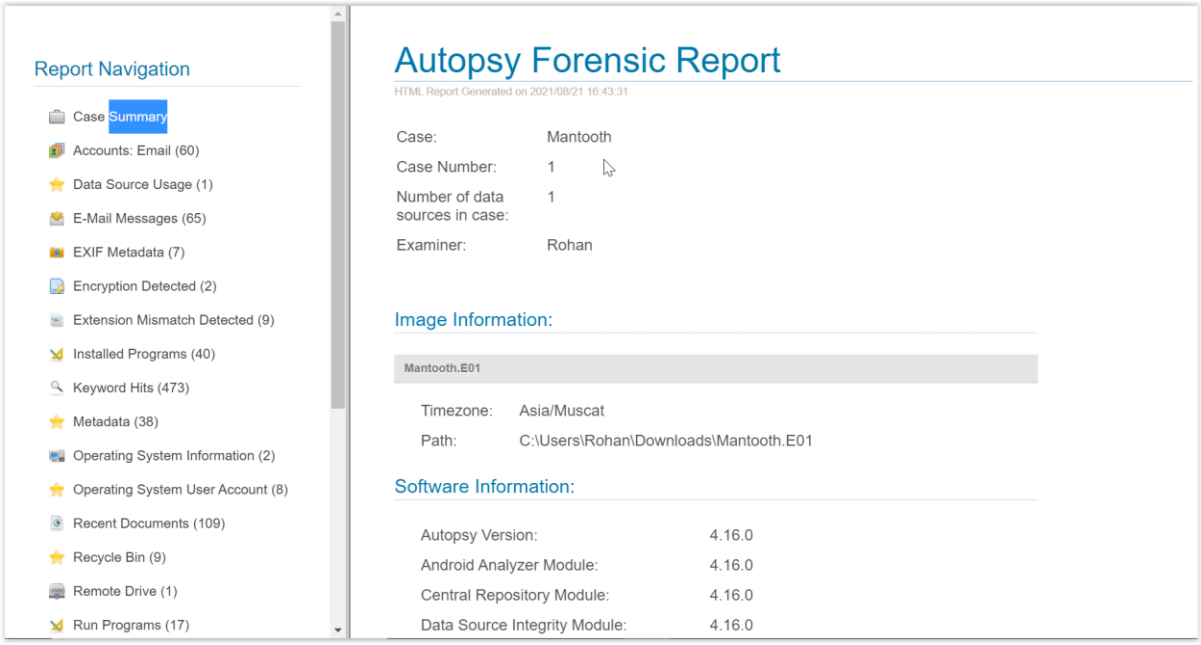
7)Find the URL that is given for making drugs quickly

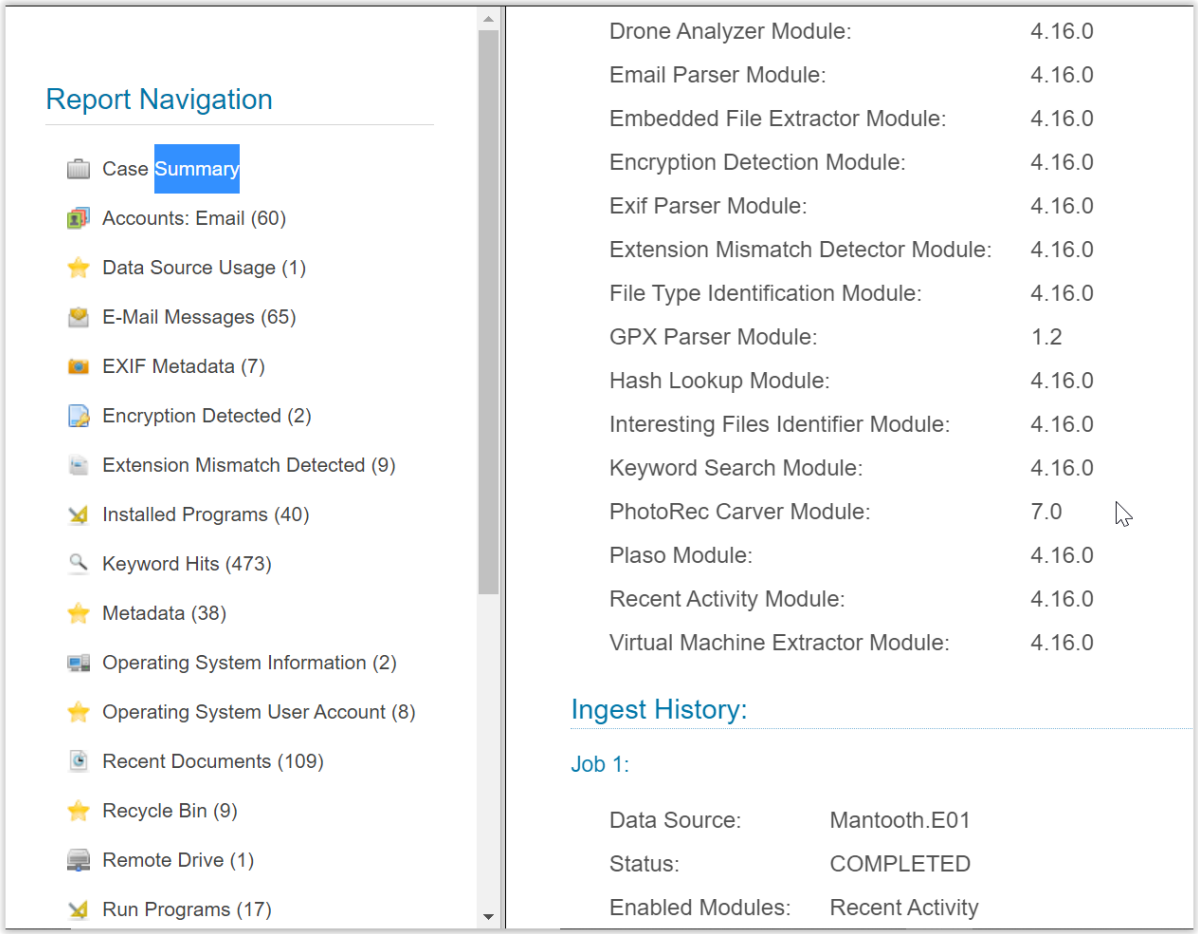
http://www.totse.com/en/drugs/speedy_drugs/howtomanufactul72921.html

8) What is the AOL IM name of Washer?

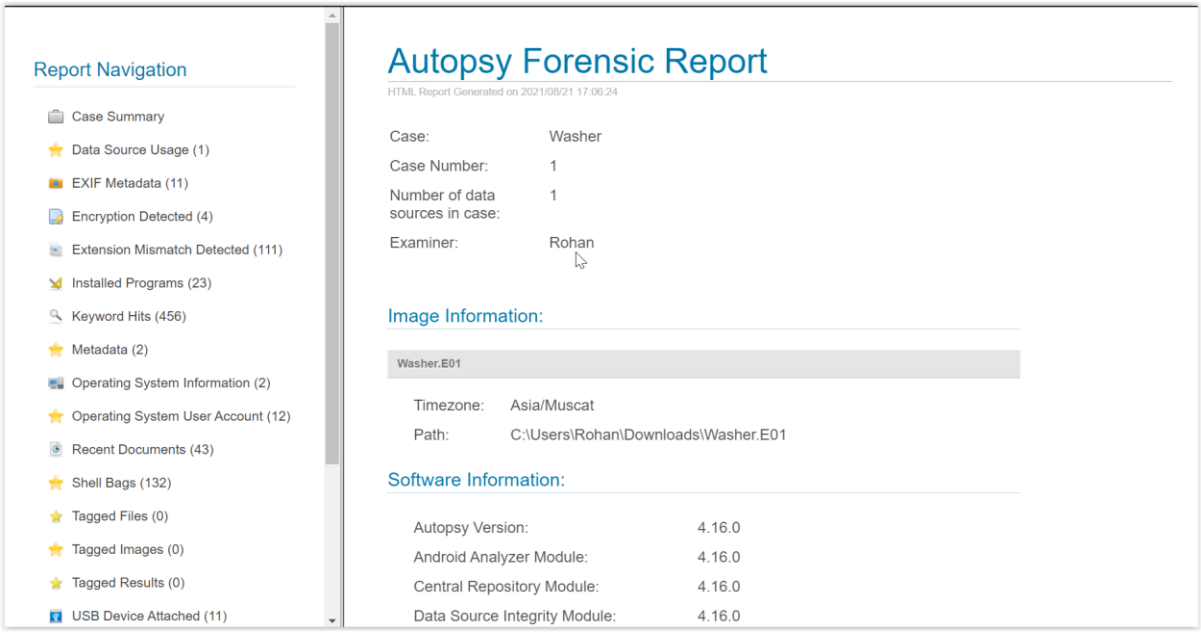
```
userinfo.bag AOL Feedbag 1.1
1024
AIM Bots
        MovieFone
Prof Gilzot
Less than 3 months to go!!!
Sharethisdotcom
Spleak
        IM Street
Buddies
rbadguy2424
Family
Co-Workers
Recent Buddies
```

c) Mantooth.E01 Report





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

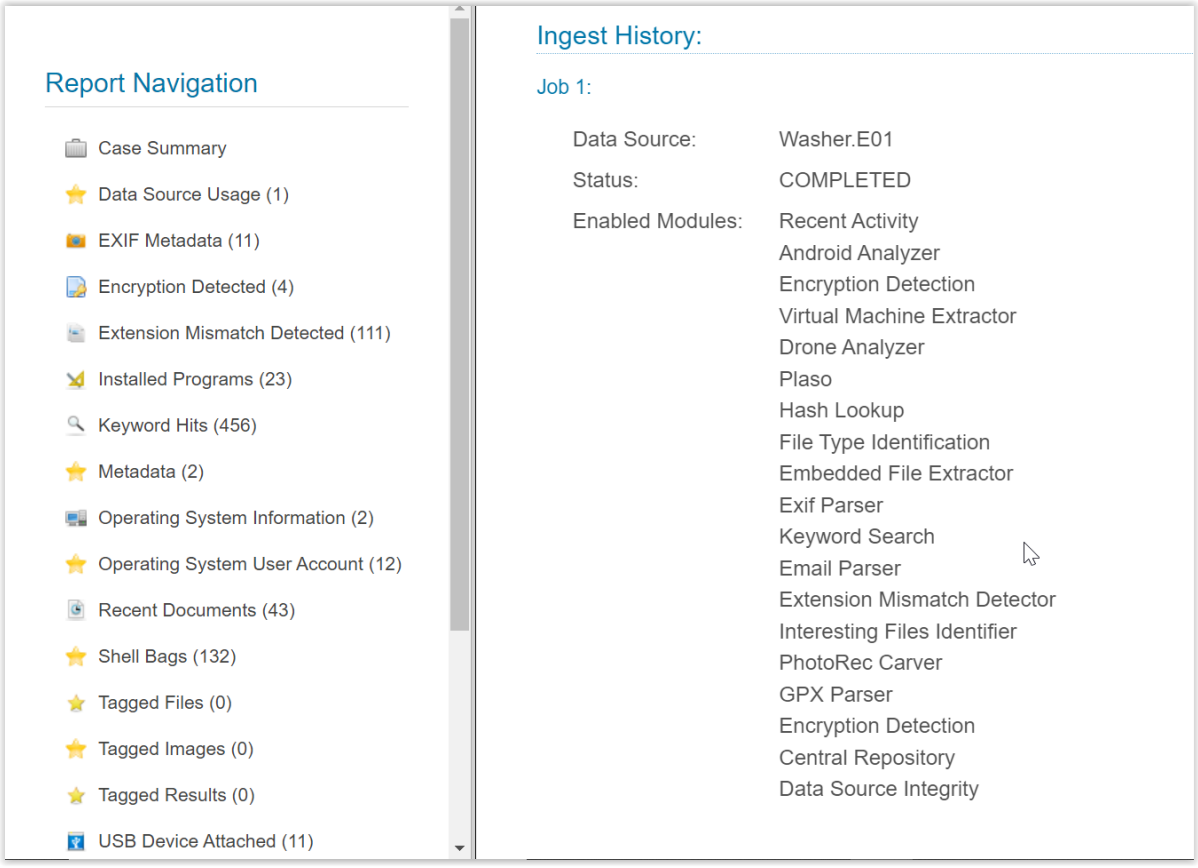
Image Information:

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