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: 2

18BCI0247

Rohan Allen

Exercise 2: FTK Imager 27/8/21

1. Create a disk image using FTK imager for different storages.

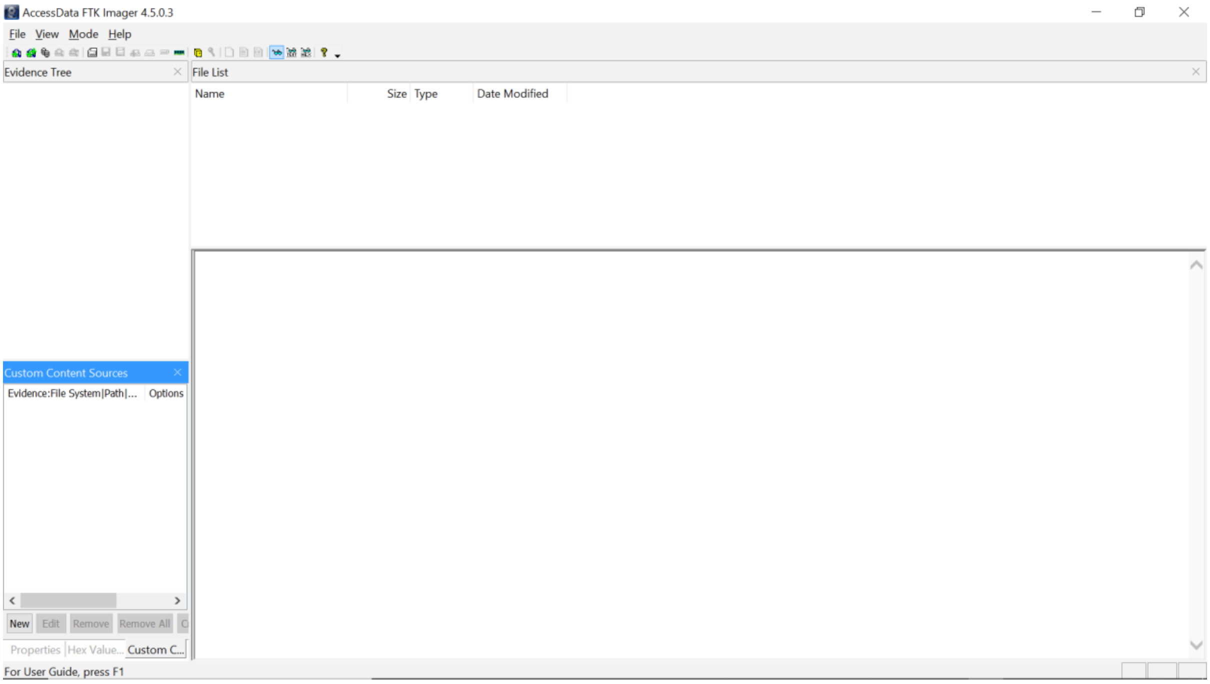
2. Analyze the disk image (.E01 /.dd) and generate a forensic report using Autopsy.

AIM:

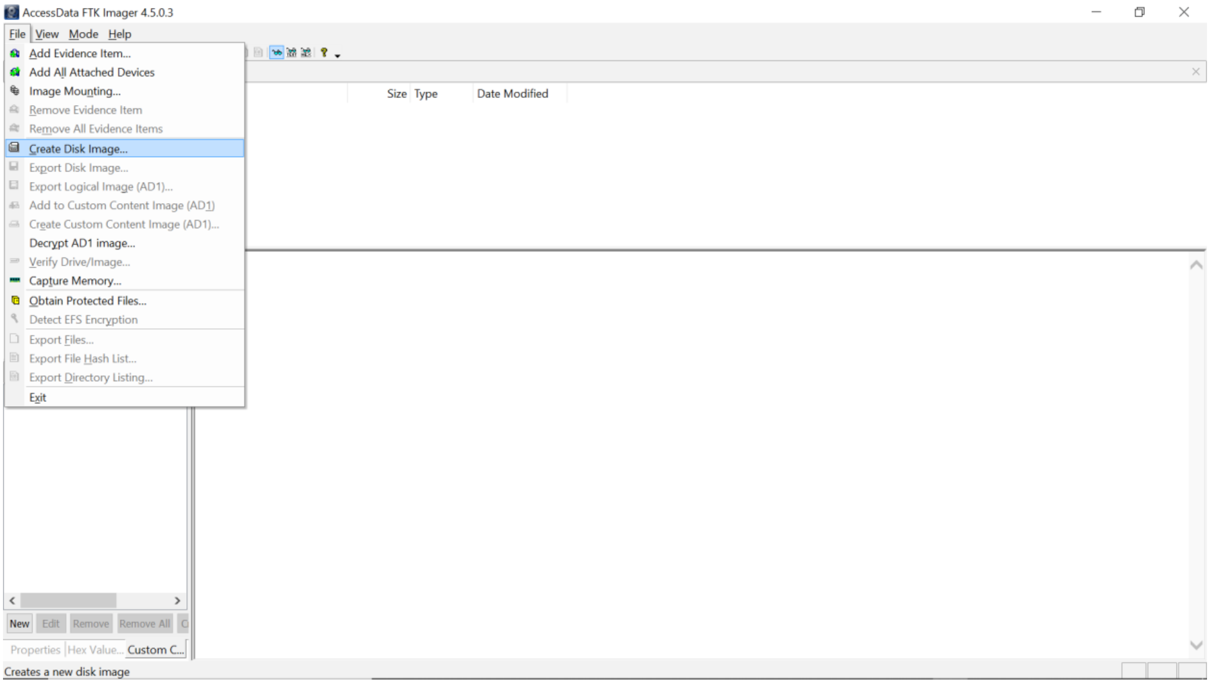
To create a disk image of my USB using FTK Imager and to analyse that disk using Autopsy.

Procedure

a) Open FTK-Imager

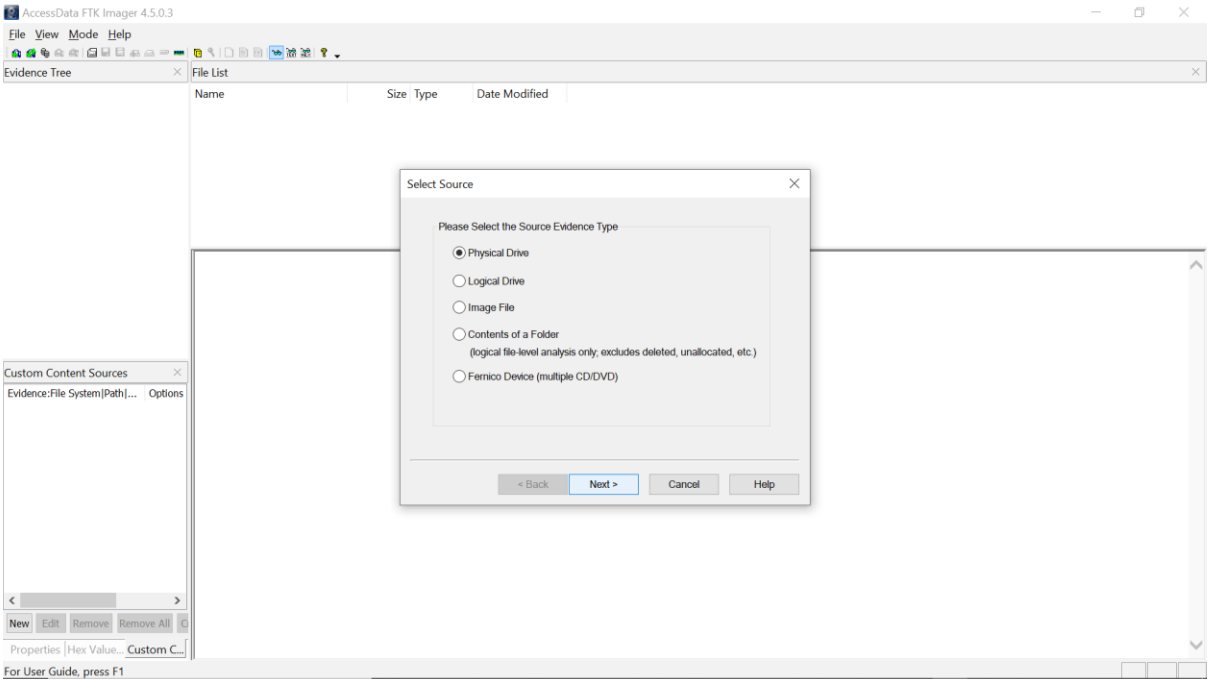


Create Disk file



Creates a new disk image

Choose physical drive



Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

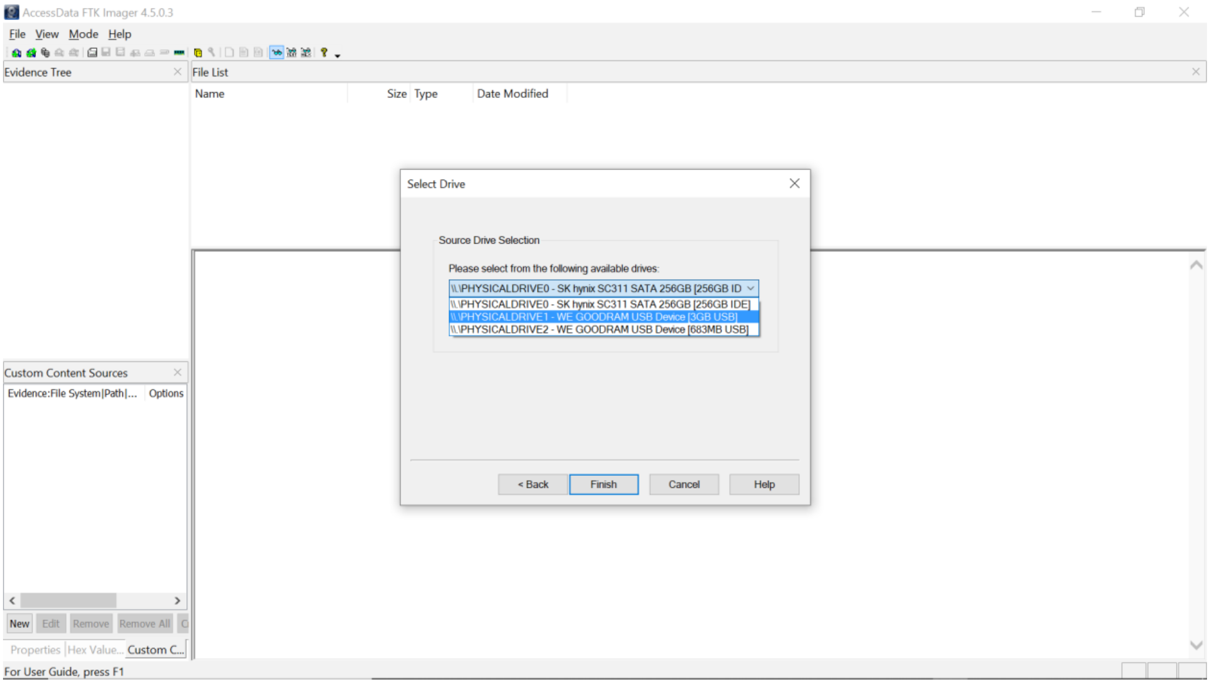
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

For User Guide, press F1

Chose the usb-3gb(Trend Micro USB)



Select Drive

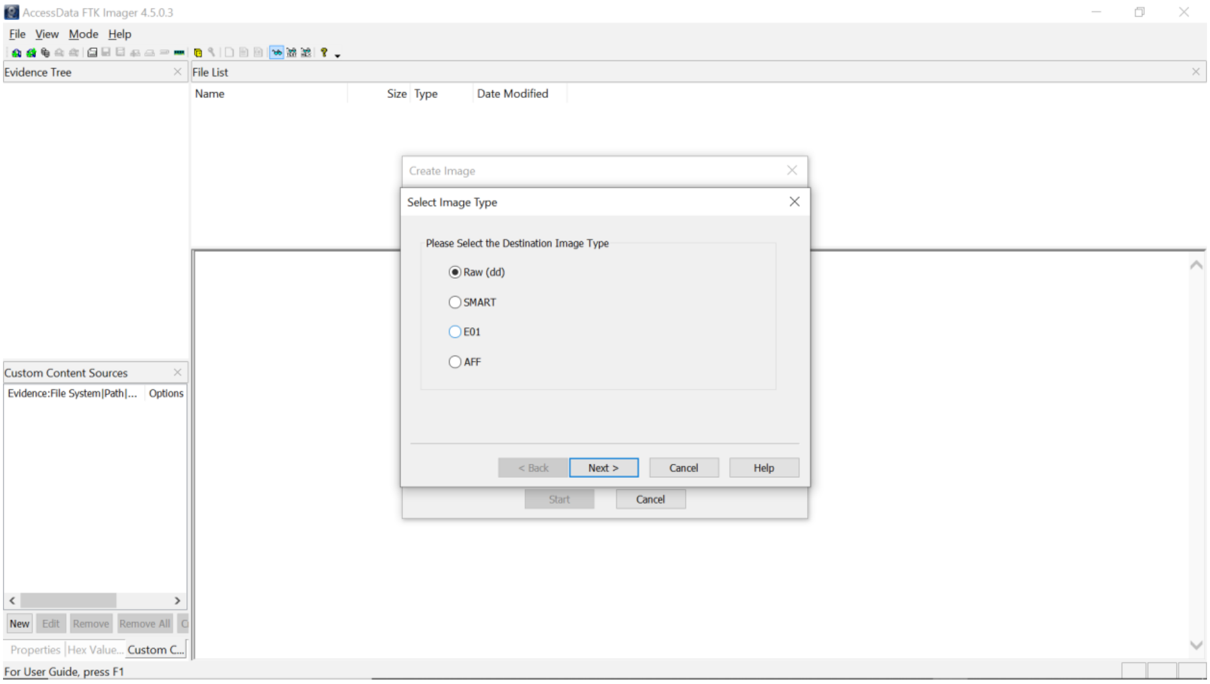
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - SK hynix SC311 SATA 256GB [256GB ID

\\.\PHYSICALDRIVE0 - SK hynix SC311 SATA 256GB [256GB IDE]
\\.\PHYSICALDRIVE1 - WE GOODRAM USB Device [3GB USB]
\\.\PHYSICALDRIVE2 - WE GOODRAM USB Device [683MB USB]

Select image type as raw



Select Image Type

Please Select the Destination Image Type

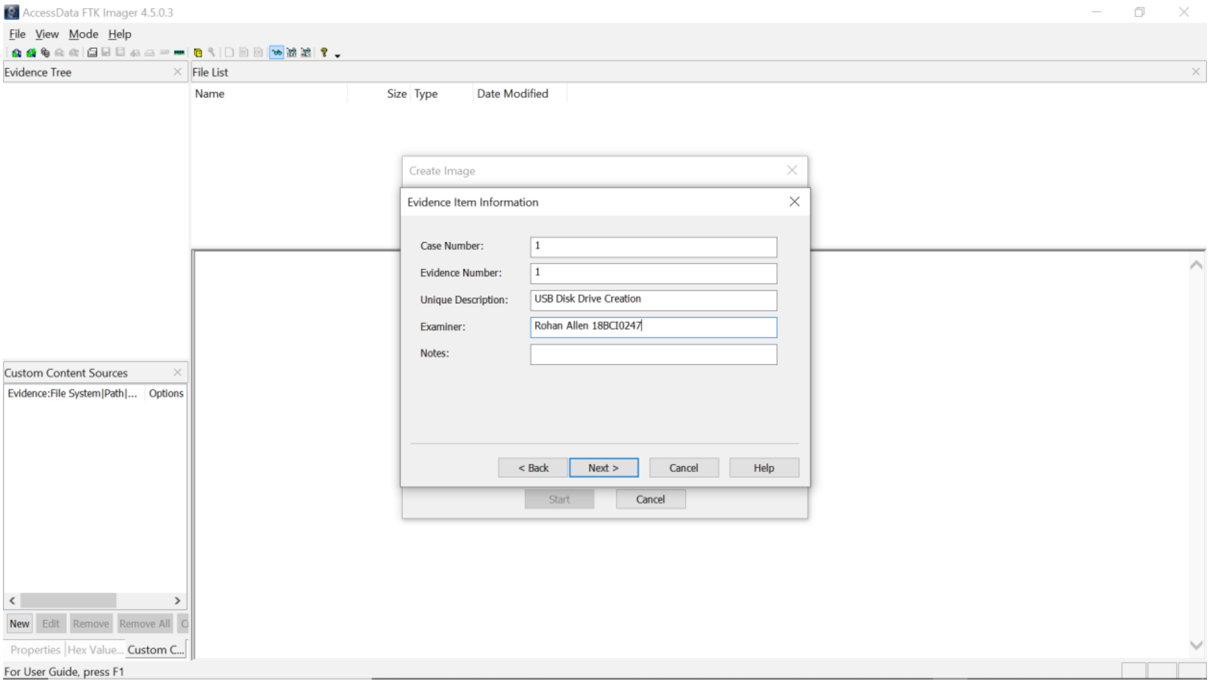
● Raw (dd)

○ SMART

○ E01

○ AFF

Enter disk image information



Case Number: 1

Evidence Number: 1

Unique Description: USB Disk Drive Creation

Examiner: Rohan Allen 18BCI0247

Notes:

Select disk image name and destination address

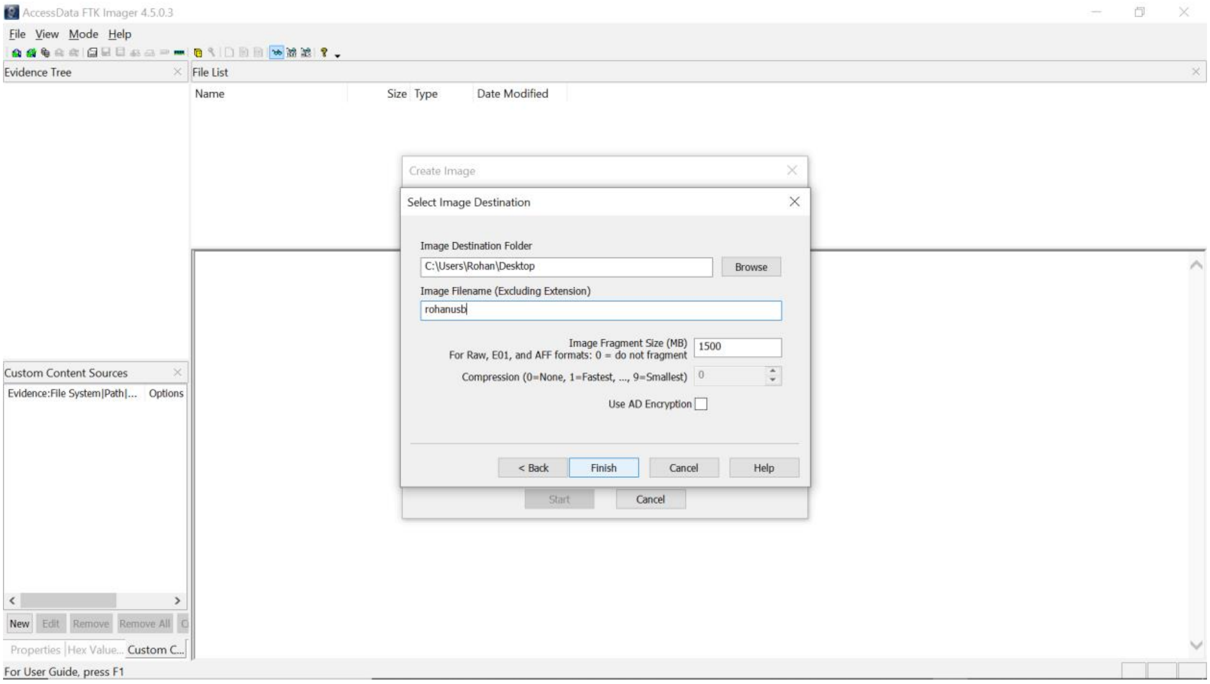


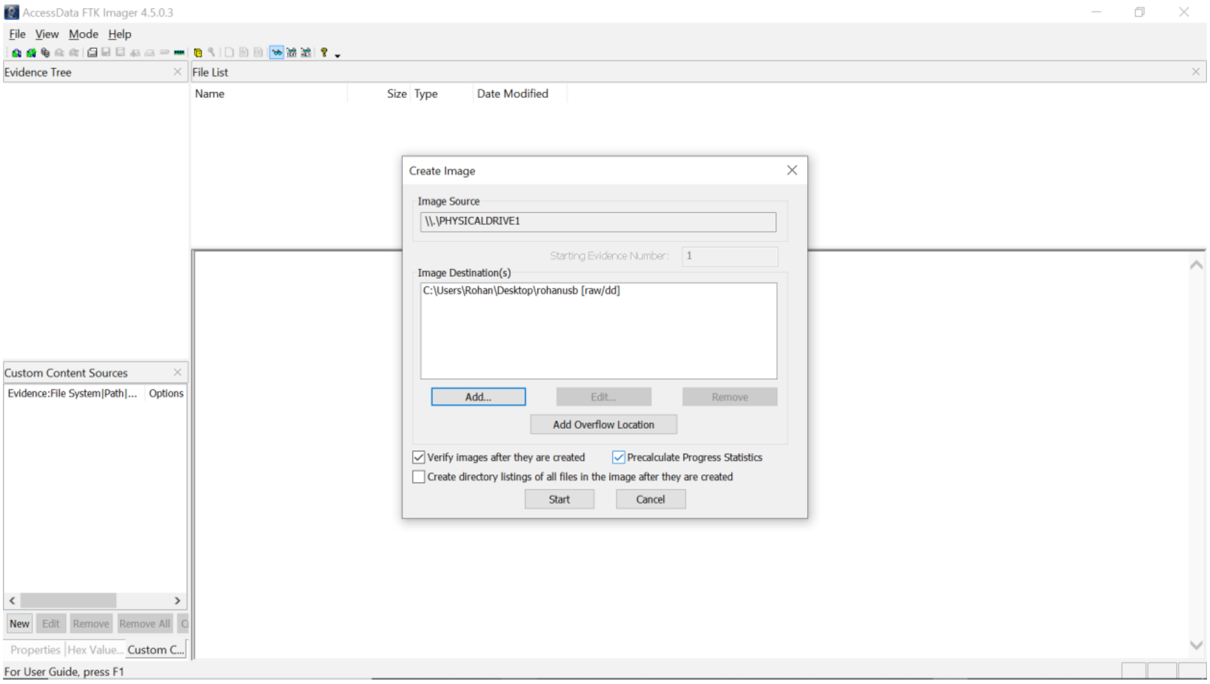
Image Destination Folder: C:\Users\Rohan\Desktop

Image Filename (Excluding Extension): rohanusb

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Custom Content Sources
Evidence:File System|Path|... Options
New Edit Remove Remove All C
Properties Hex Value... Custom C...
For User Guide, press F1

Create Image

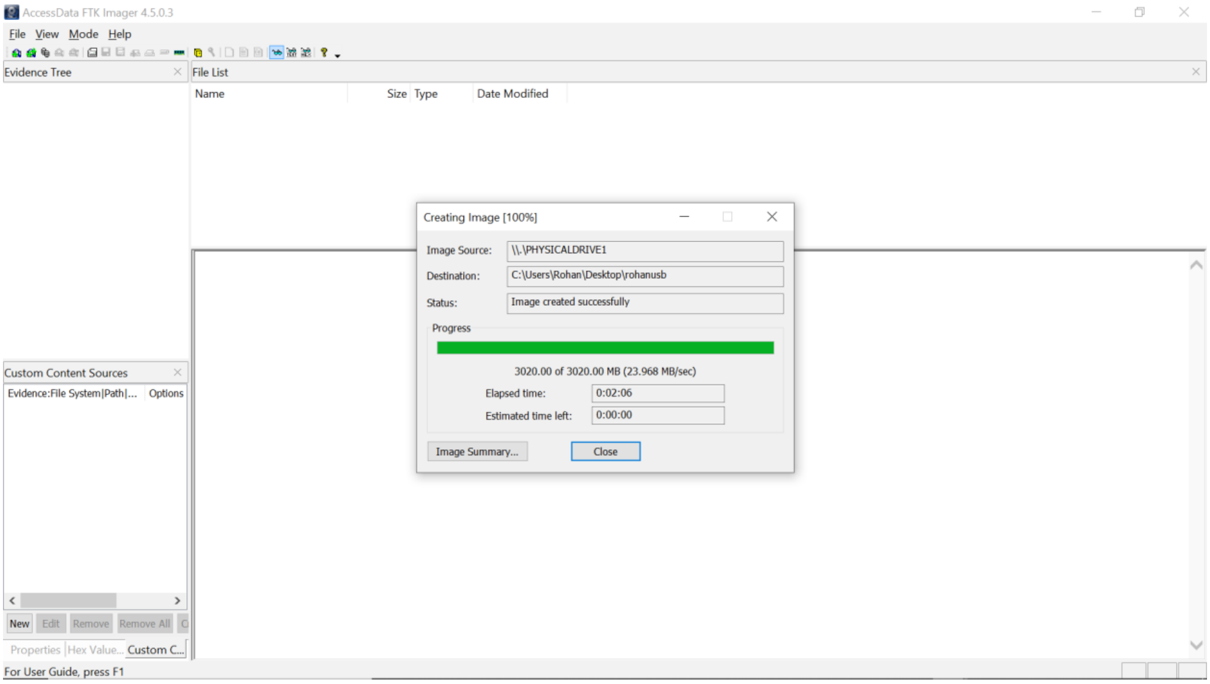
Image Source
\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)
C:\Users\Rohan\Desktop\rohanusb [raw/dd]

☑ Verify images after they are created ☑ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created

Success

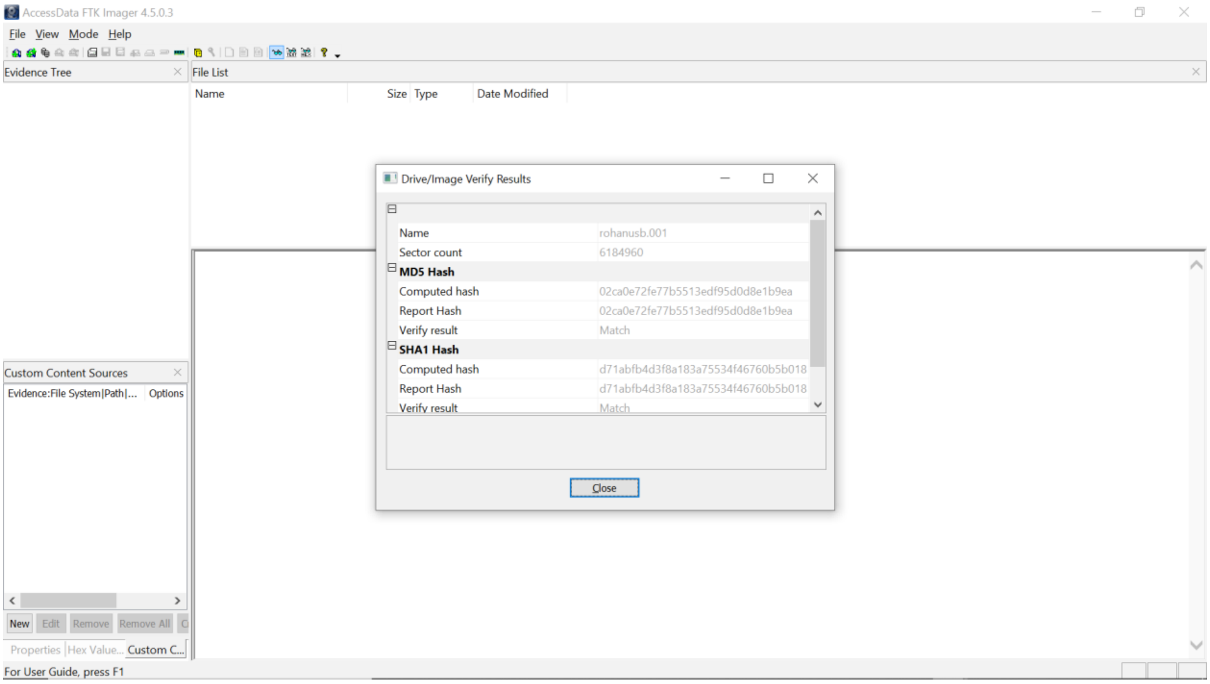

AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Custom Content Sources
Evidence:File System|Path|... Options
New Edit Remove Remove All C
Properties Hex Value... Custom C...
For User Guide, press F1

Creating Image [100%]

Image Source: \\.\PHYSICALDRIVE1
Destination: C:\Users\Rohan\Desktop\rohanusb
Status: Image created successfully

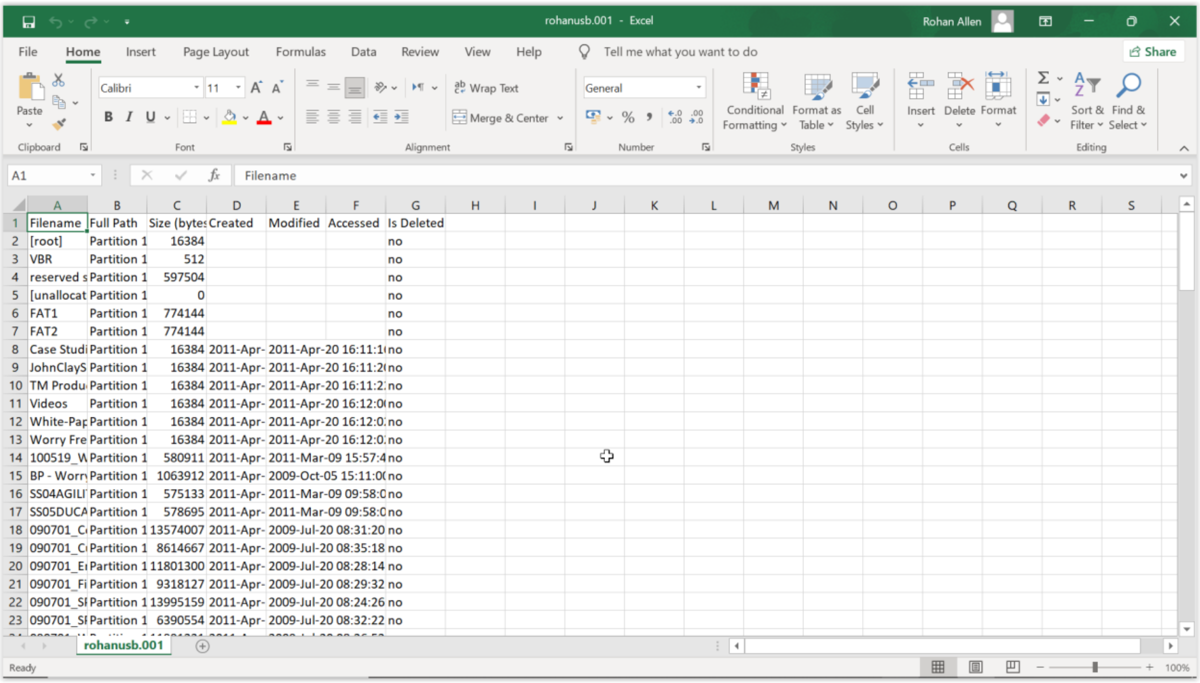
Progress
3020.00 of 3020.00 MB (23.968 MB/sec)
Elapsed time: 0:02:06
Estimated time left: 0:00:00

Disk Image verify results:



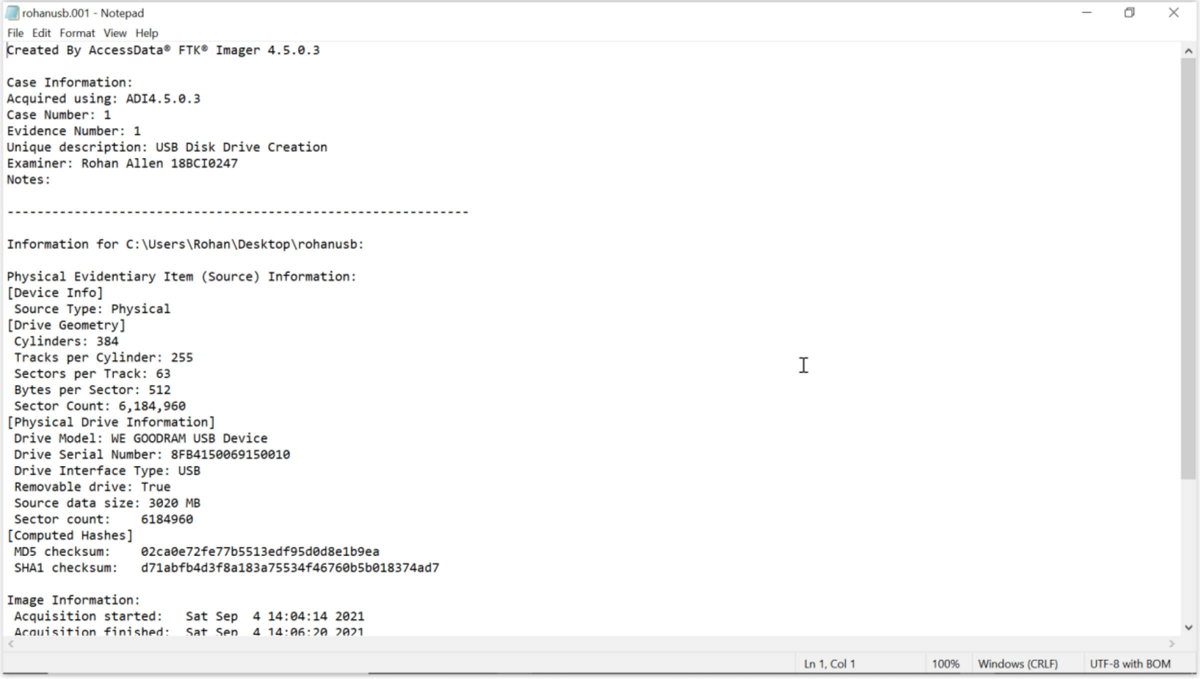
Name	rohanusb.001
Sector count	6184960
MD5 Hash	
Computed hash	02ca0e72fe77b5513edf95d0d8e1b9ea
Report Hash	02ca0e72fe77b5513edf95d0d8e1b9ea
Verify result	Match
SHA1 Hash	
Computed hash	d71abfb4d3f8a183a75534f46760b5b018
Report Hash	d71abfb4d3f8a183a75534f46760b5b018
Verify result	Match

Excel Sheet with data of usb file image



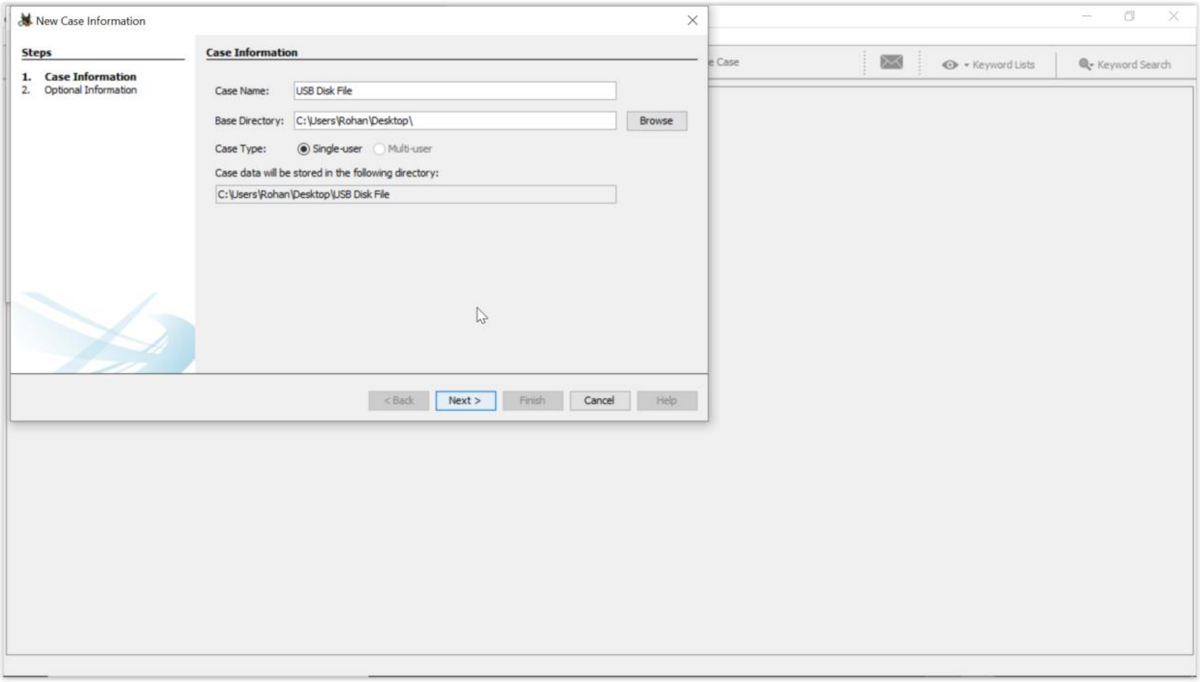
	A	B	C	D	E	F	G
1	Filename	Full Path	Size (bytes	Created	Modified	Accessed	Is Deleted
2	[root]	Partition 1	16384				no
3	VBR	Partition 1	512				no
4	reserved s	Partition 1	597504				no
5	[unallocat	Partition 1	0				no
6	FAT1	Partition 1	774144				no
7	FAT2	Partition 1	774144				no
8	Case Studi	Partition 1	16384	2011-Apr-	2011-Apr-20 16:11:1		no
9	JohnClayS	Partition 1	16384	2011-Apr-	2011-Apr-20 16:11:2		no
10	TM Produ	Partition 1	16384	2011-Apr-	2011-Apr-20 16:11:2		no
11	Videos	Partition 1	16384	2011-Apr-	2011-Apr-20 16:12:0		no
12	White-Pap	Partition 1	16384	2011-Apr-	2011-Apr-20 16:12:0		no
13	Worry Fre	Partition 1	16384	2011-Apr-	2011-Apr-20 16:12:0		no
14	100519_W	Partition 1	580911	2011-Apr-	2011-Mar-09 15:57:4		no
15	BP - Worry	Partition 1	1063912	2011-Apr-	2009-Oct-05 15:11:0		no
16	SS04AGILI	Partition 1	575133	2011-Apr-	2011-Mar-09 09:58:0		no
17	SS05DUCA	Partition 1	578695	2011-Apr-	2011-Mar-09 09:58:0		no
18	090701_C	Partition 1	13574007	2011-Apr-	2009-Jul-20 08:31:20		no
19	090701_C	Partition 1	8614667	2011-Apr-	2009-Jul-20 08:35:18		no
20	090701_E	Partition 1	11801300	2011-Apr-	2009-Jul-20 08:28:14		no
21	090701_Fi	Partition 1	9318127	2011-Apr-	2009-Jul-20 08:29:32		no
22	090701_S	Partition 1	13995159	2011-Apr-	2009-Jul-20 08:24:26		no
23	090701_S	Partition 1	6390554	2011-Apr-	2009-Jul-20 08:32:22		no

Text Doc with Image Summary:



```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 1
Evidence Number: 1
Unique description: USB Disk Drive Creation
Examiner: Rohan Allen 18BCI0247
Notes:

--------------------------------------------------------------

Information for C:\Users\Rohan\Desktop\rohanusb:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 384
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 6,184,960
[Physical Drive Information]
 Drive Model: WE GOODRAM USB Device
 Drive Serial Number: 8FB4150069150010
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 3020 MB
 Sector count:    6184960
[Computed Hashes]
 MD5 checksum:    02ca0e72fe77b5513edf95d0d8e1b9ea
 SHA1 checksum:   d71abfb4d3f8a183a75534f46760b5b018374ad7

Image Information:
 Acquisition started:   Sat Sep  4 14:04:14 2021
 Acquisition finished:  Sat Sep  4 14:06:20 2021
```

Analyse disk image in autopsy



Case Information

Case Name: USB Disk File

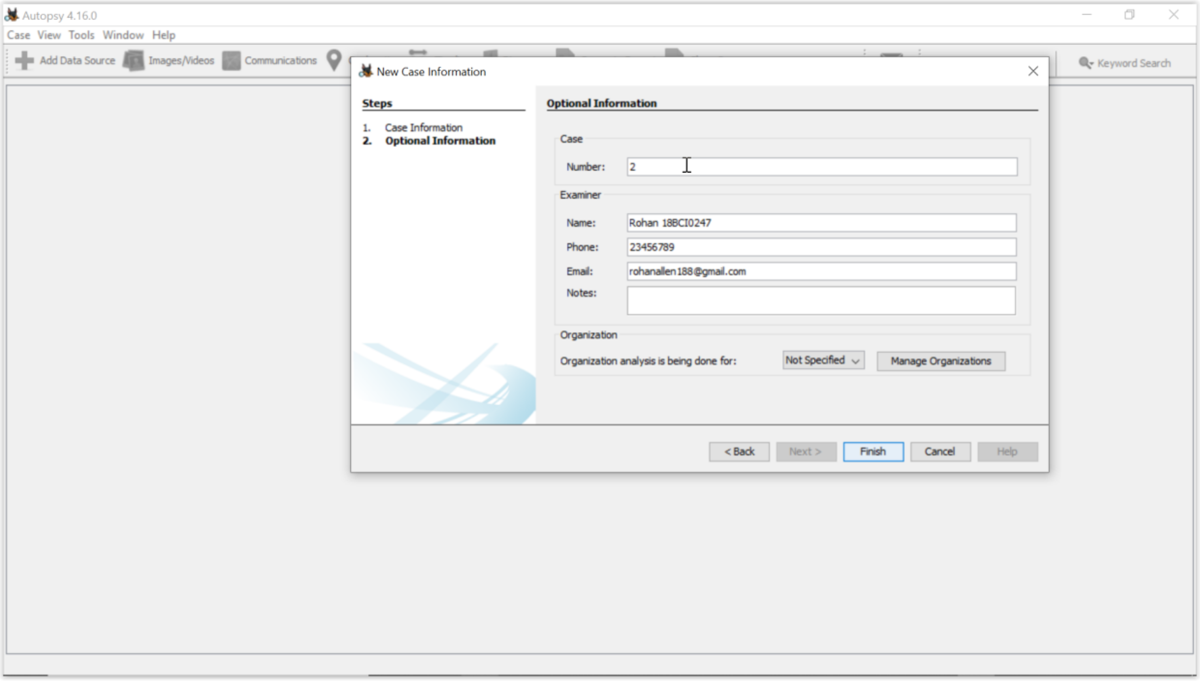
Base Directory: C:\Users\Rohan\Desktop\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\Rohan\Desktop\USB Disk File

Enter Case Number, and Examiner details



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 2

Examiner

Name: Rohan 18BCI0247

Phone: 23456789

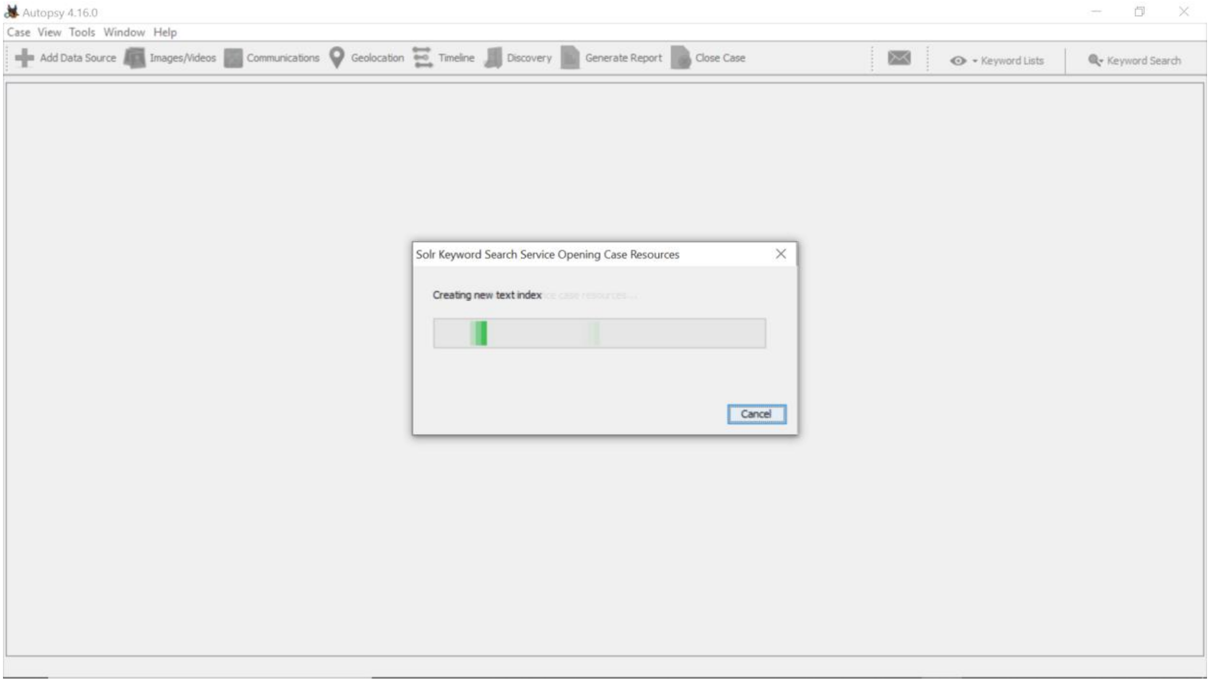
Email: rohanallen188@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

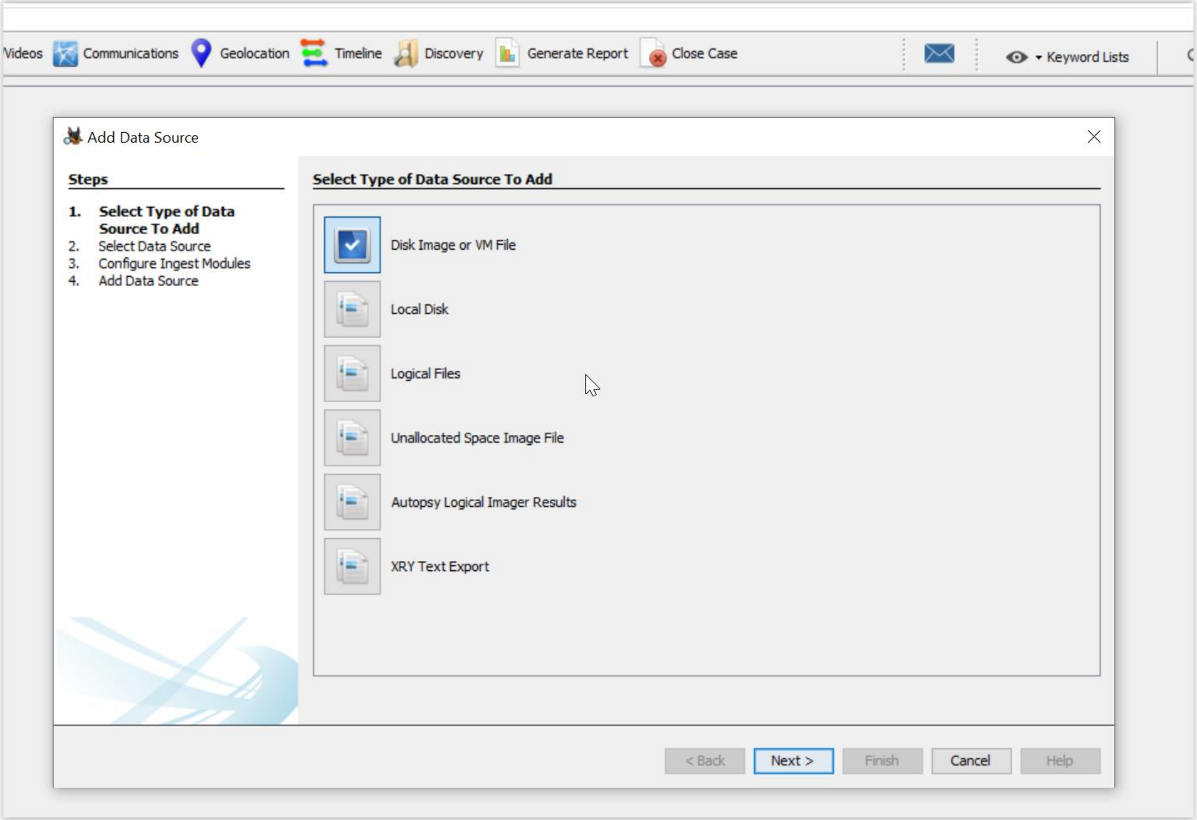
Creating Autopsy Case file



Solr Keyword Search Service Opening Case Resources

Creating new text index

Add data source to analyse



Add Data Source

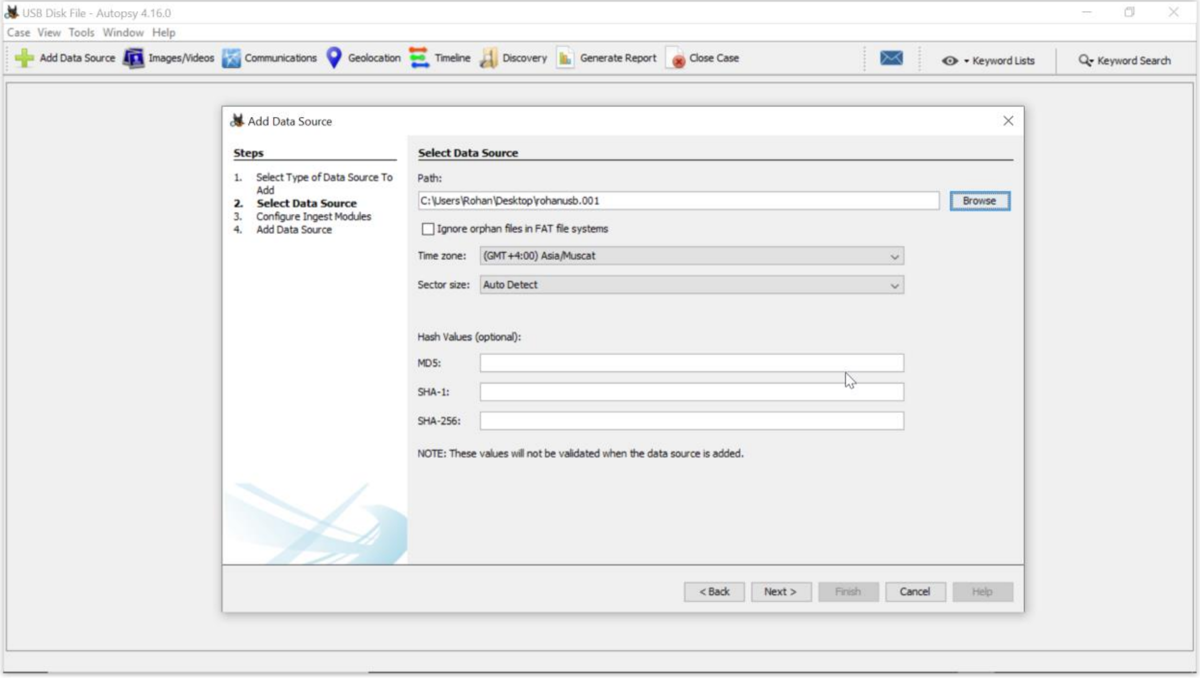
Steps

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

- ☑ Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

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



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: C:\Users\Rohan\Desktop\rohanusb.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT+4:00) Asia/Muscat

Sector size: Auto Detect

Hash Values (optional):

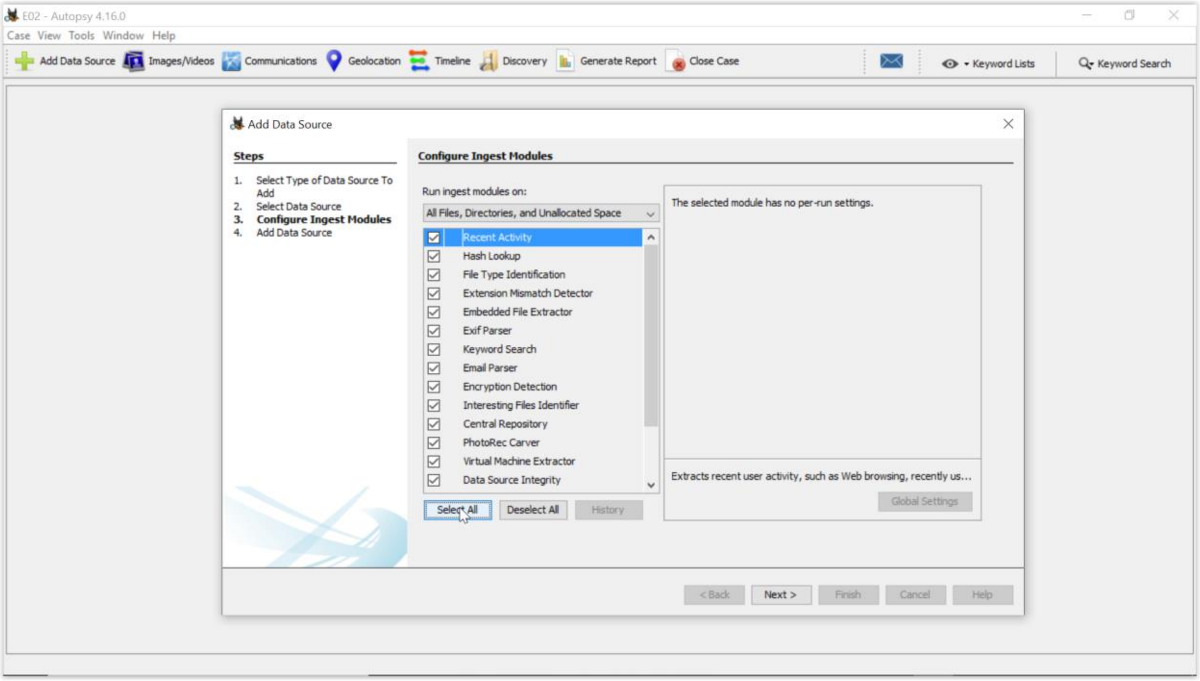
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

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



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on:

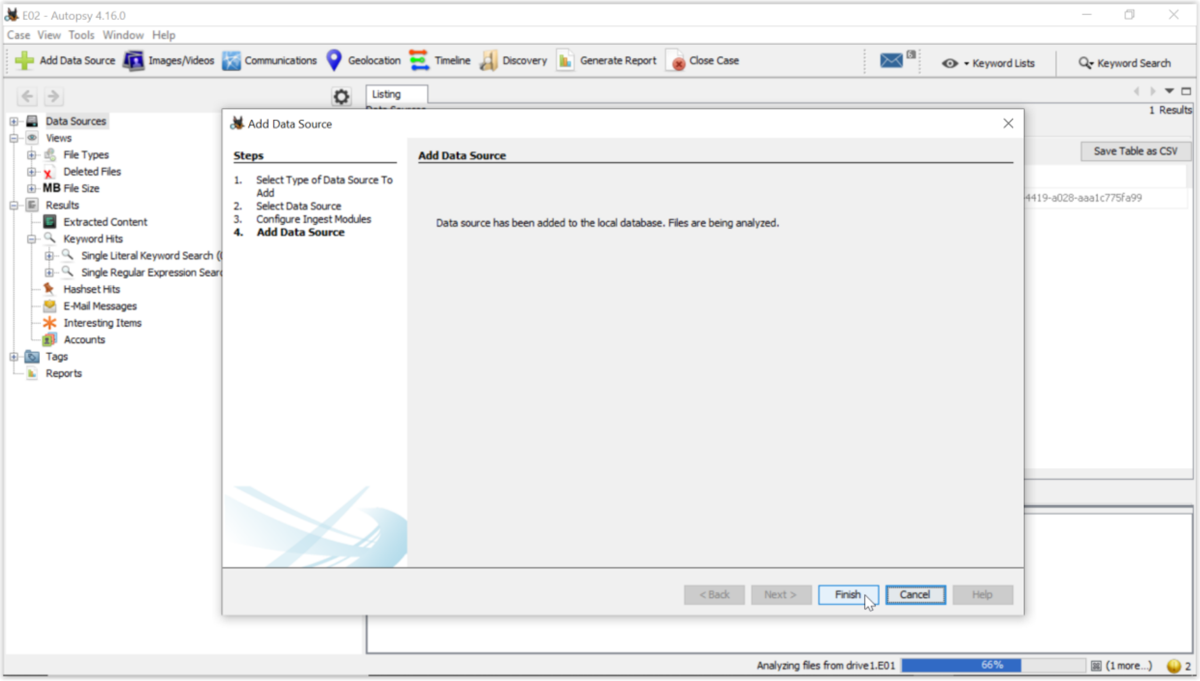
All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Data Source is successfully added.



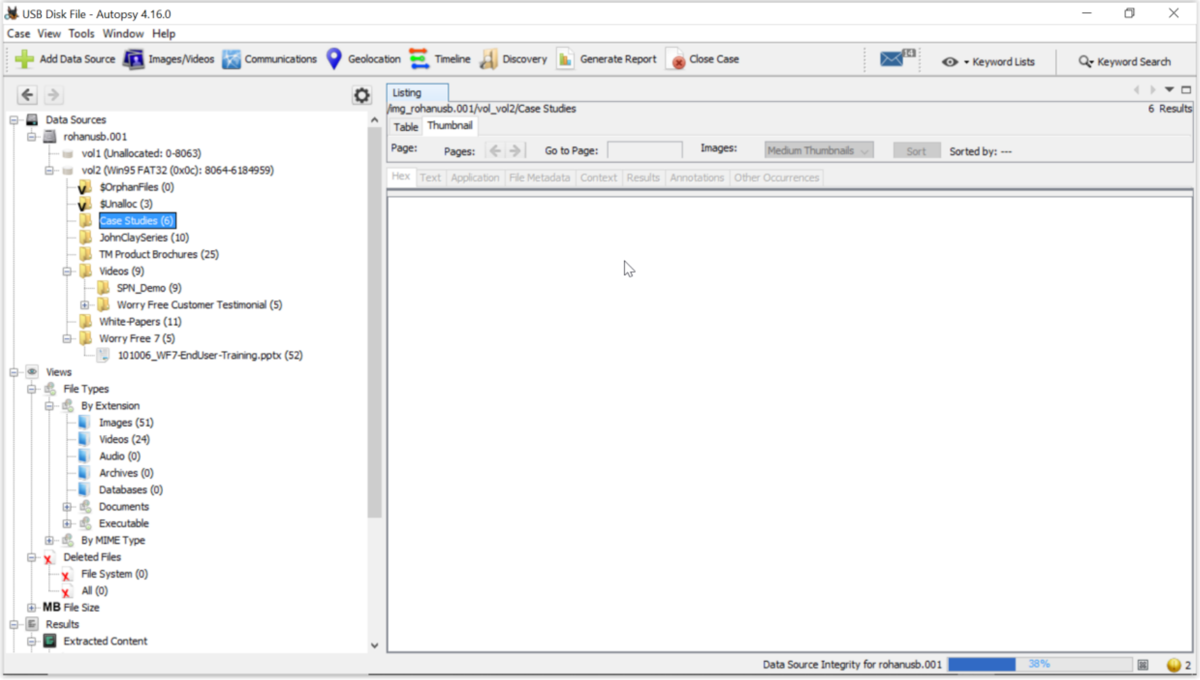
Steps

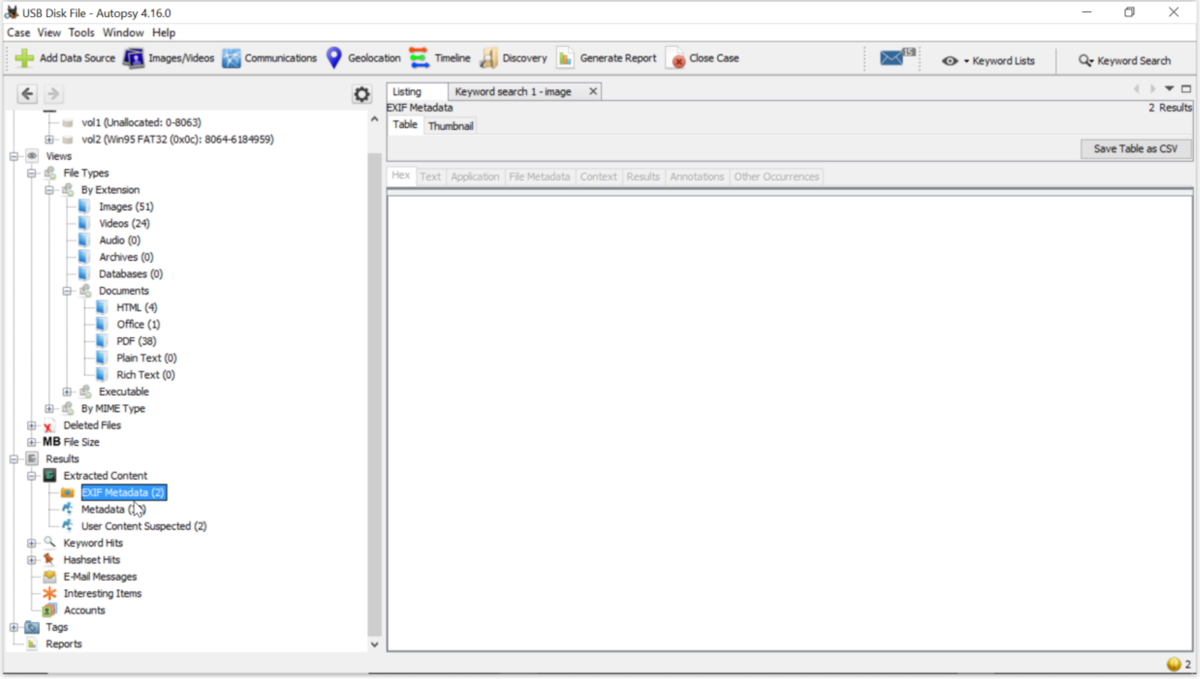
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

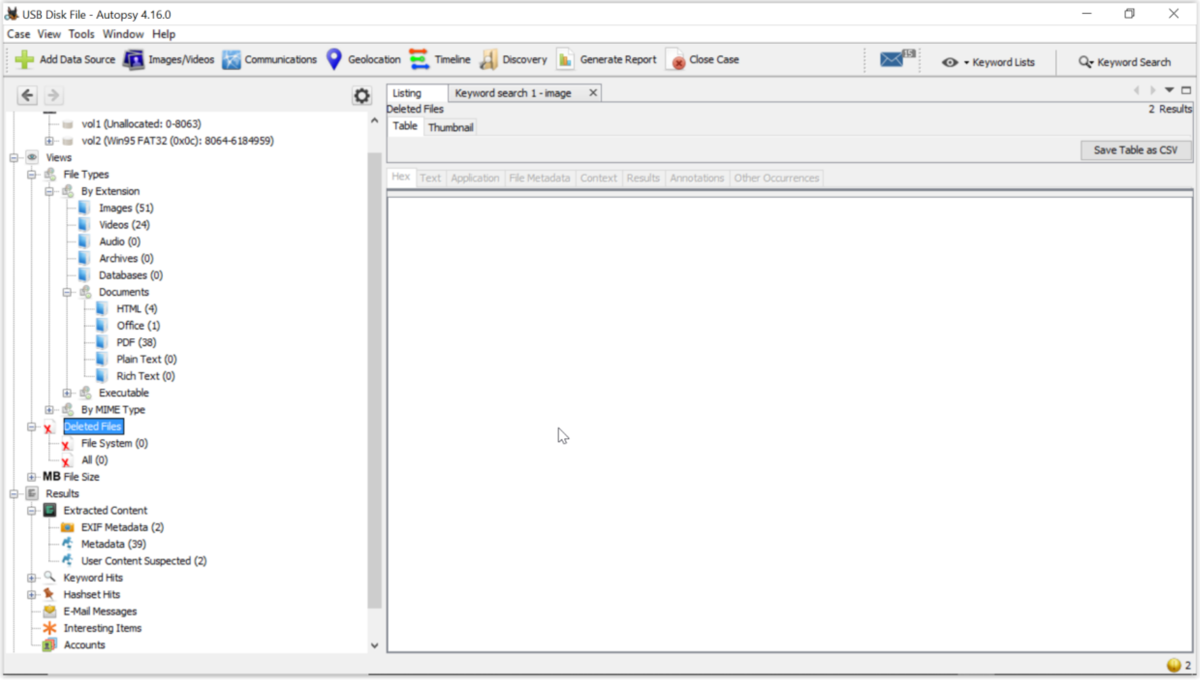
Data source has been added to the local database. Files are being analyzed.

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

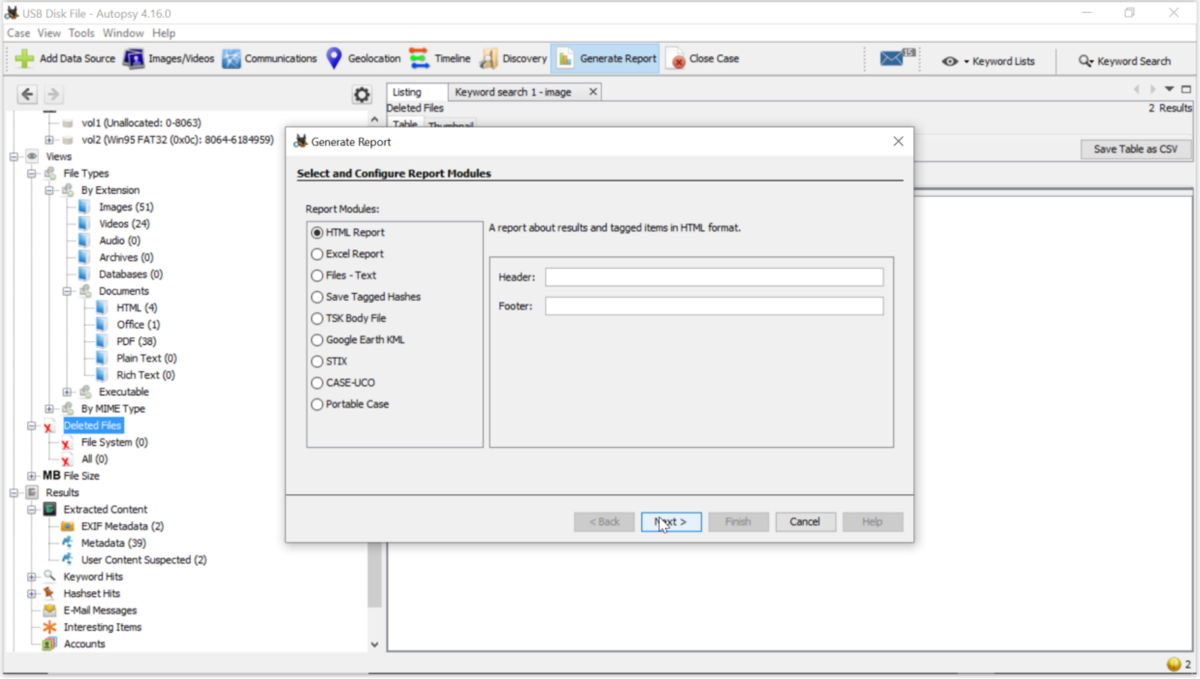




Deleted files:



Generate html report of case findings

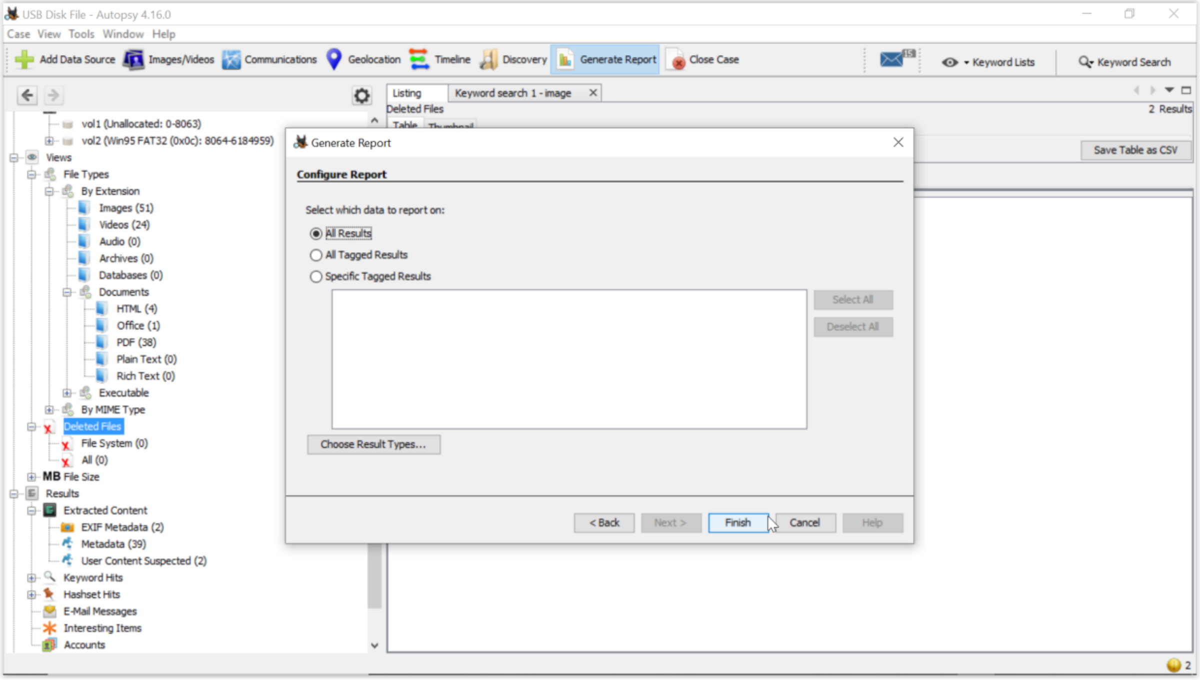


● HTML Report
○ Excel Report
○ Files - Text
○ Save Tagged Hashes
○ TSK Body File
○ Google Earth KML
○ STIX
○ CASE-UCO
○ Portable Case

A report about results and tagged items in HTML format.

Header:

Footer:



Generate Report

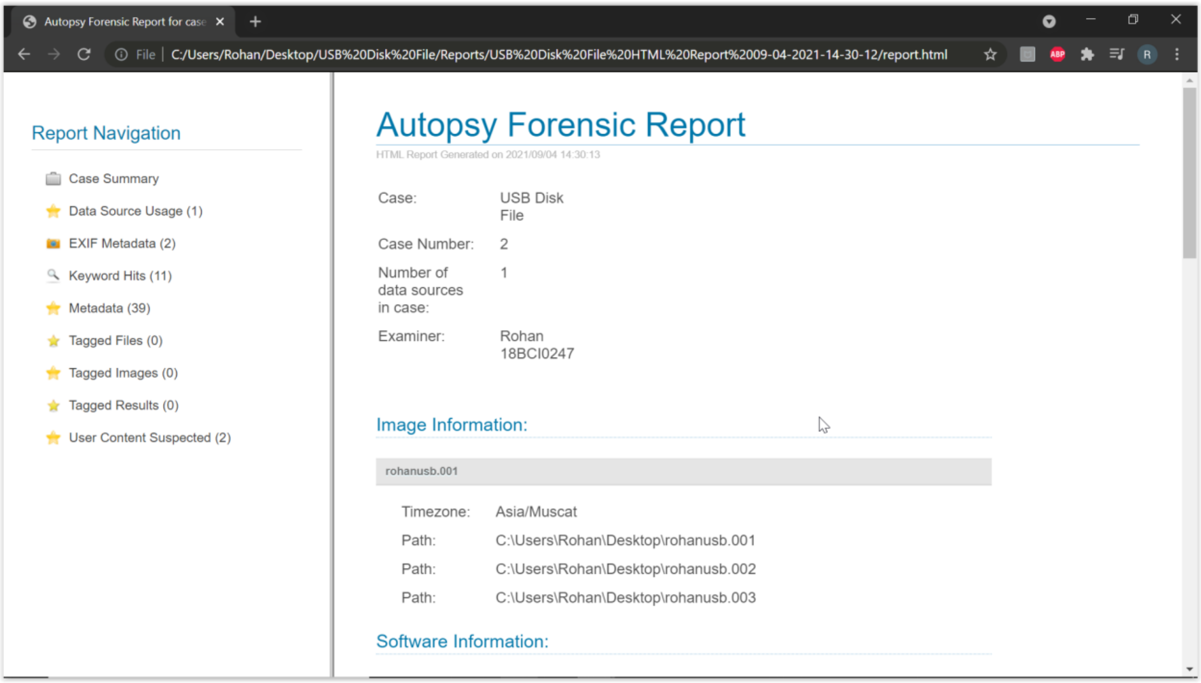
Configure Report

Select which data to report on:

● All Results

○ All Tagged Results

○ Specific Tagged Results


Autopsy Forensic Report for case
C:/Users/Rohan/Desktop/USB%20Disk%20File/Reports/USB%20Disk%20File%20HTML%20Report%2009-04-2021-14-30-12/report.html

Report Navigation

- Case Summary
- Data Source Usage (1)
- EXIF Metadata (2)
- Keyword Hits (11)
- Metadata (39)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (2)

Autopsy Forensic Report

HTML Report Generated on 2021/09/04 14:30:13

Case:	USB Disk File
Case Number:	2
Number of data sources in case:	1
Examiner:	Rohan 18BCI0247

Image Information:

rohanusb.001

Timezone:	Asia/Muscat
Path:	C:\Users\Rohan\Desktop\rohanusb.001
Path:	C:\Users\Rohan\Desktop\rohanusb.002
Path:	C:\Users\Rohan\Desktop\rohanusb.003

Software Information: