



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management

CSE3502

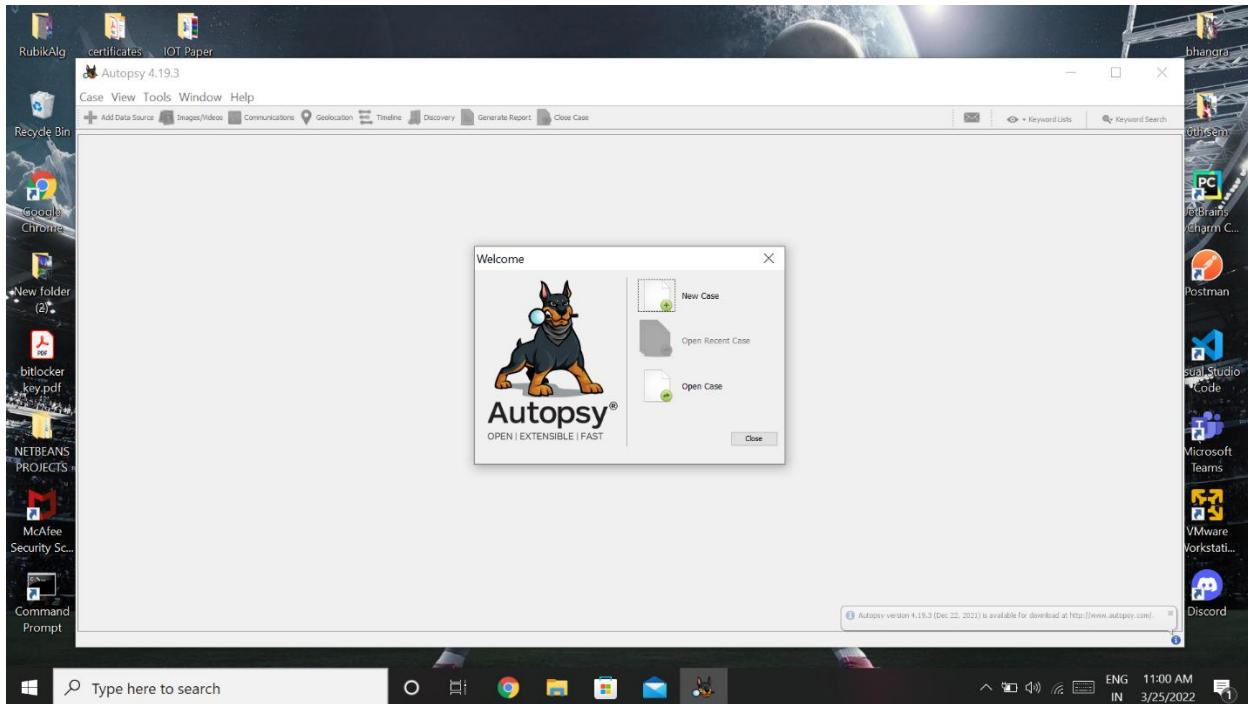
Lab Assignment 4

Autopsy

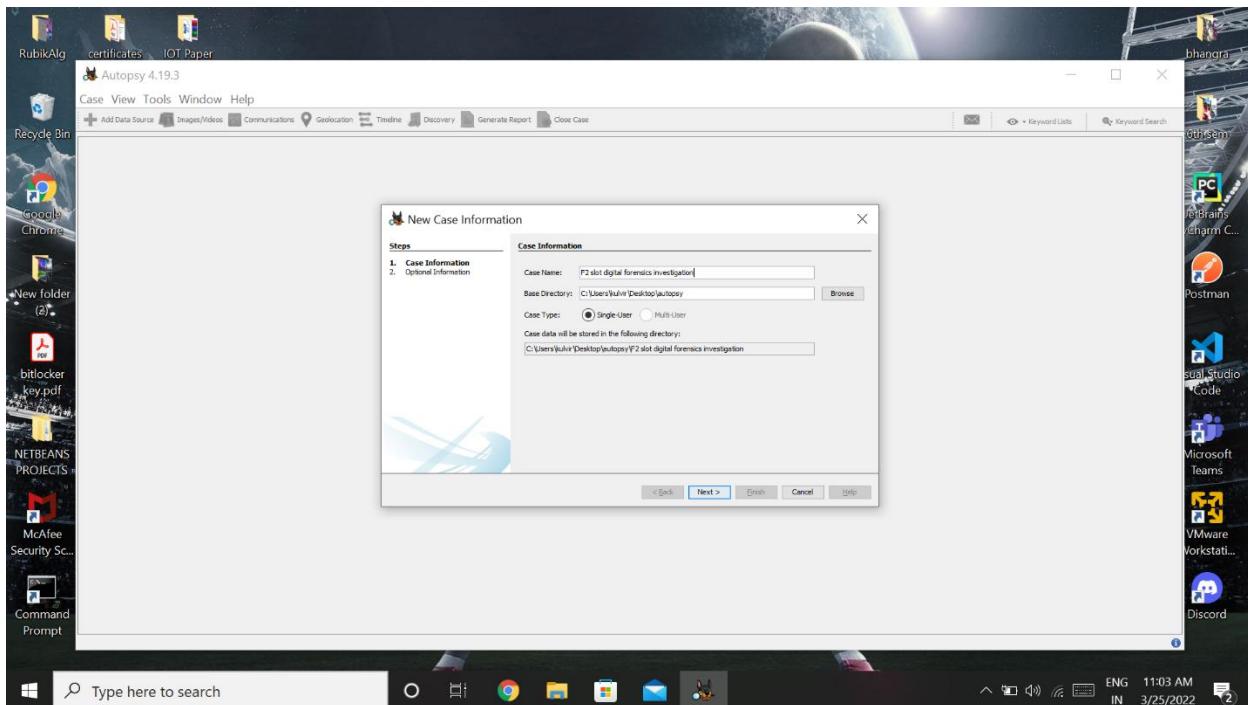
Slot : L25+L26

Name : Kulvir Singh

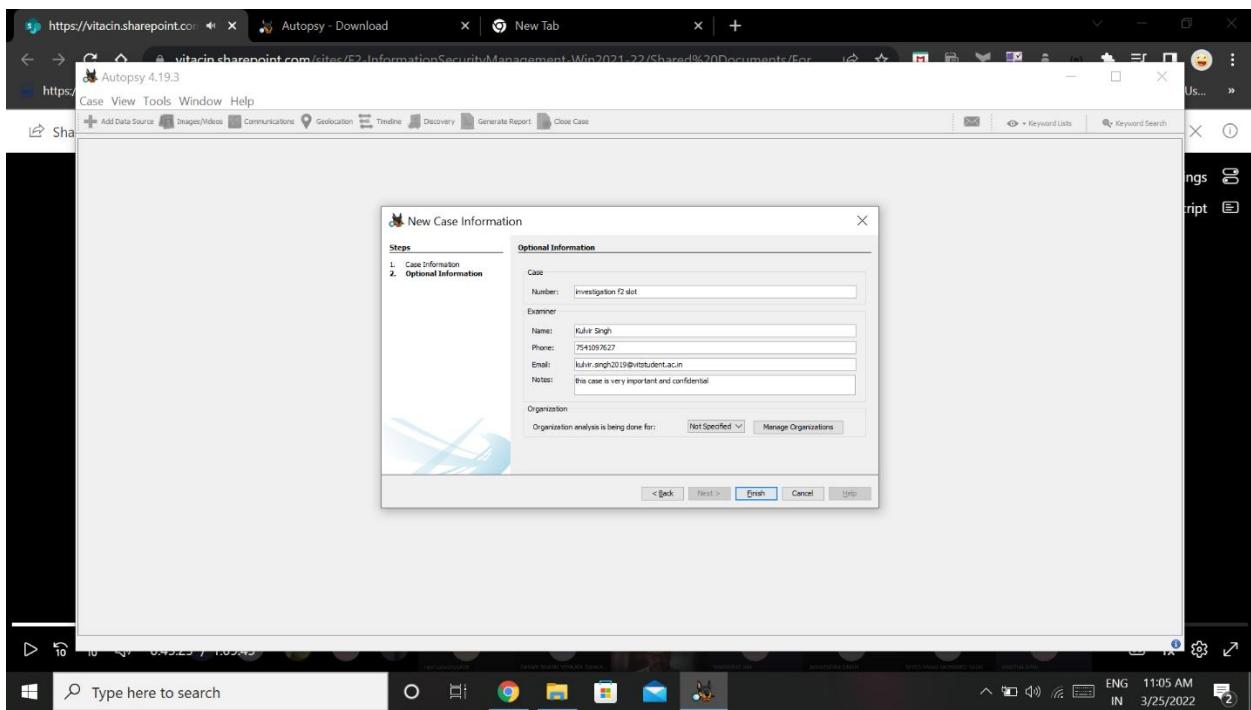
Register Number : 19BCE2074



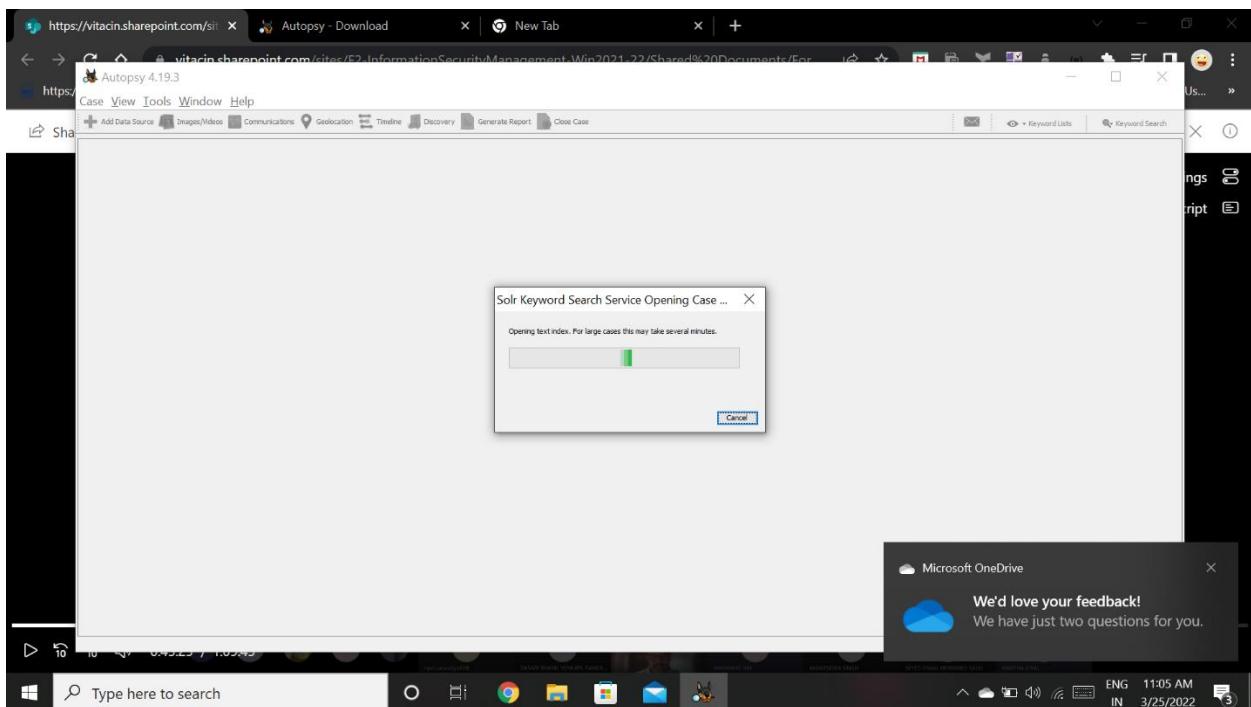
Open new case in autopsy



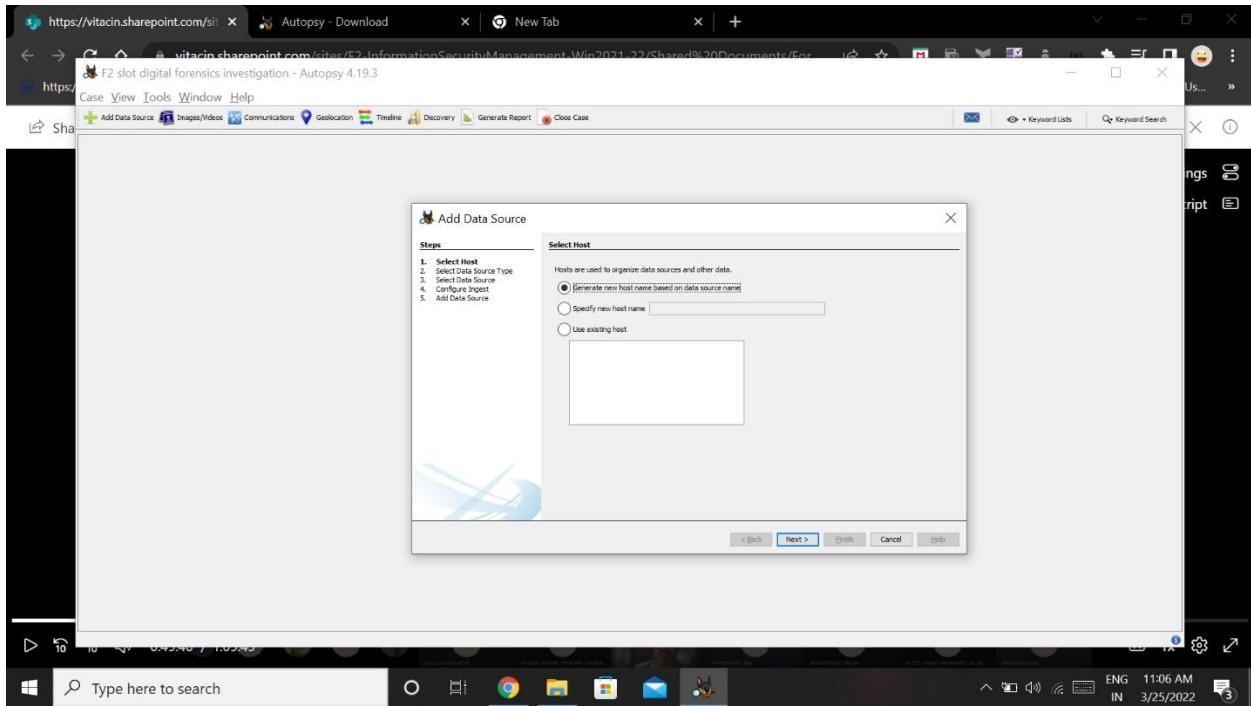
Give details about the case name and case type



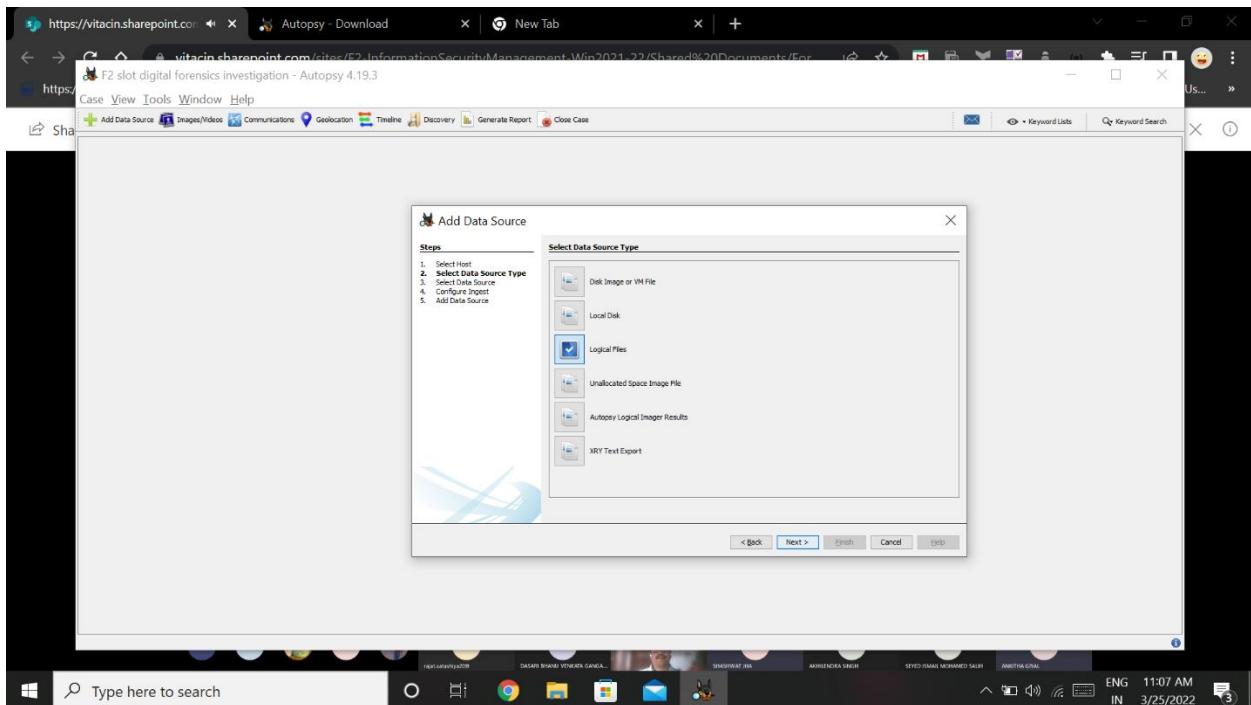
Give additional information for the new case created



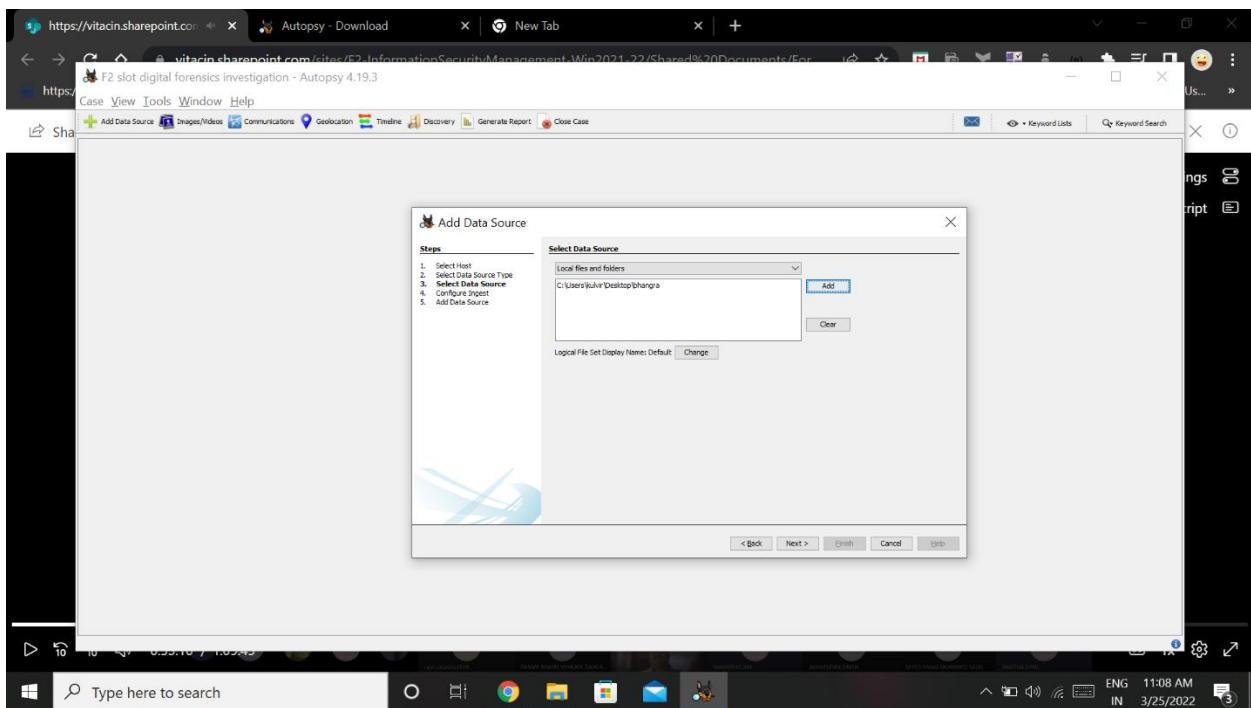
New case created



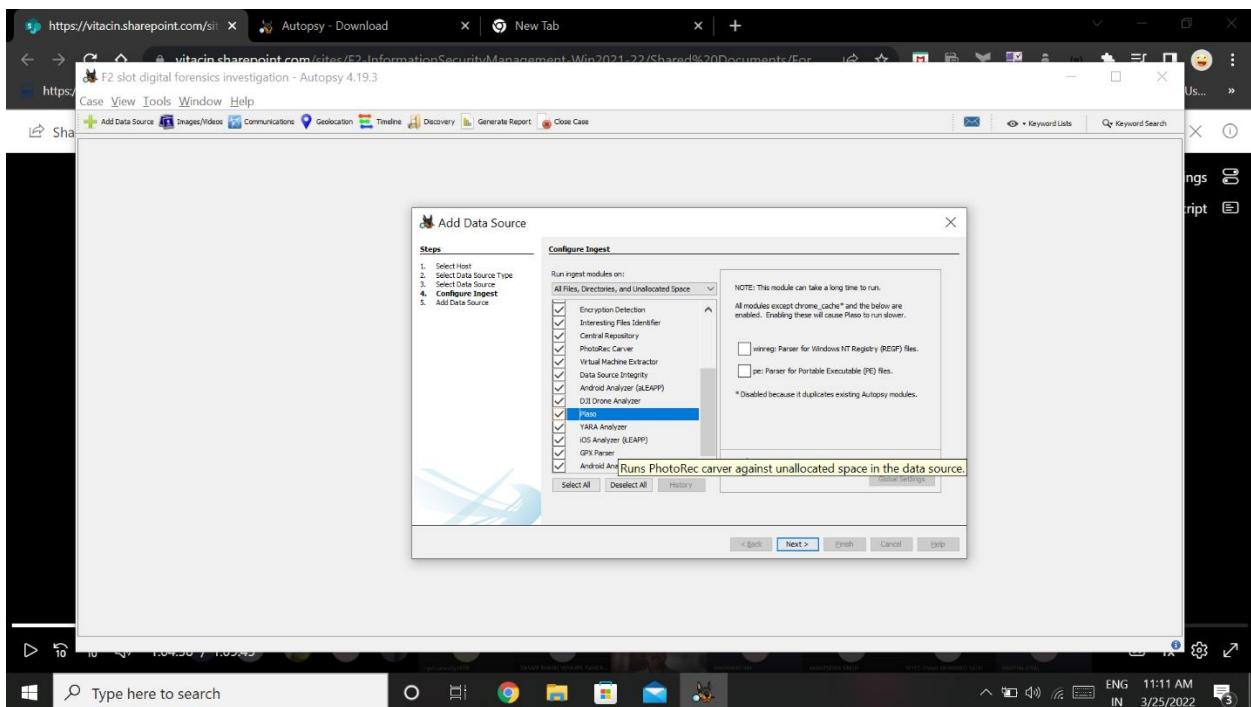
Adding a data source



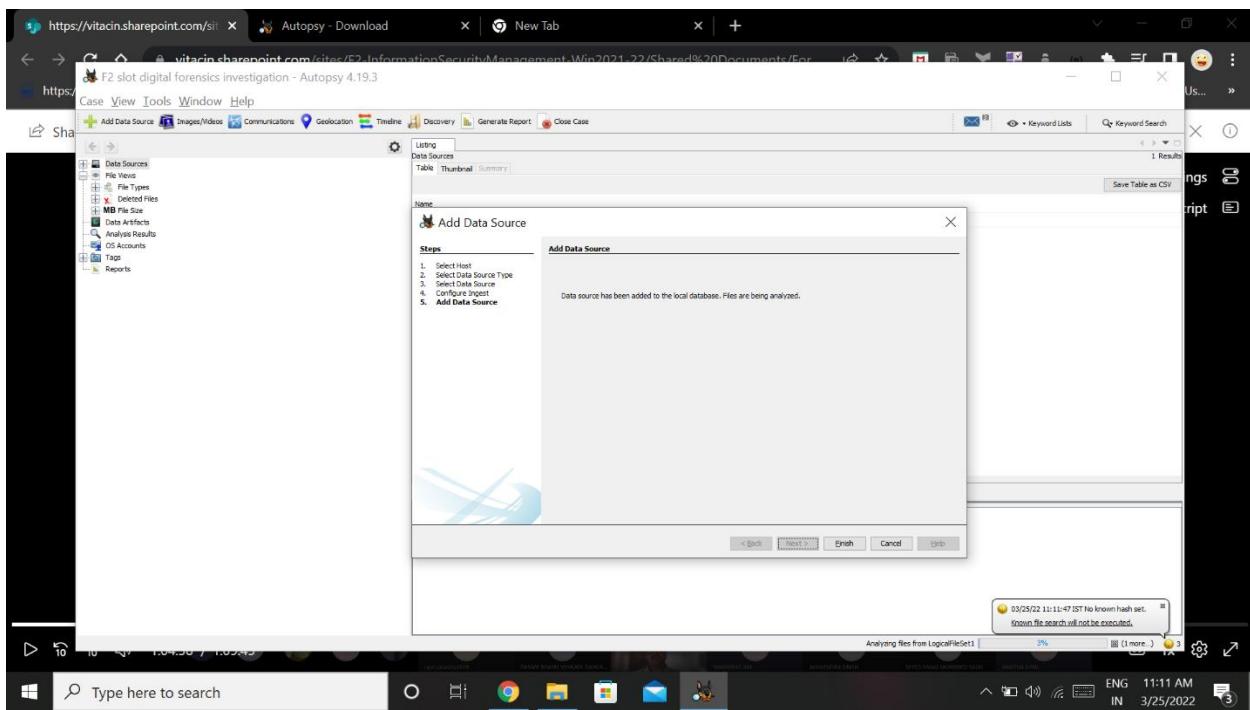
Selecting a data file for scan



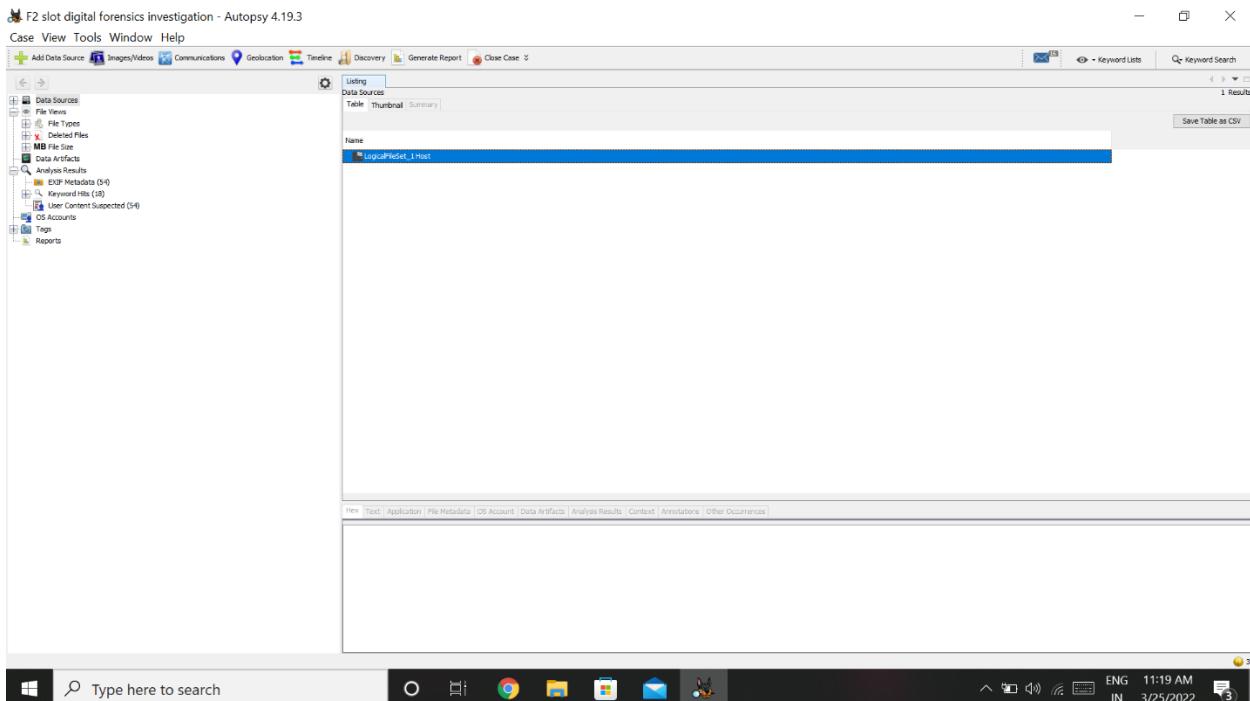
Selecting a local data source



Configuring ingest with global settings



Adding a data source



New case is setup with data source

F2 slot digital forensics investigation - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Video Communications Geolocation Timeline Discovery Generate Report Close Case

Using LogFileSet1\bhanga

Table | Thumbnail | Summary

Name S C O Modified Time Change Time Access Time Created Time Size Flag(Dr) Flag(Meta) Known Location

2cc compressed (3) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\2cc compressed (3)

3rd year video (20) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\3rd year video (20)
1st choreo (6) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\1st choreo (6)
2nd choreo (4) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\2nd choreo (4)
New folder (23) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\New folder (23)
DC Video (14) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\DC Video (14)
DC Video 2 (with saha) (12) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\DC Video 2 (with saha) (12)
JOC 2CC (10) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\JOC 2CC (10)
meet (1) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\meet (1)
PR MEET (2) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\PR MEET (2)
wd2021 (15) 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\wd2021 (15)
20201005_160213.jpg 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\20201005_160213.jpg
20201010_211811.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\20201010_211811.mp4
20201010_212651.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\20201010_212651.mp4
20201010_213502.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\20201010_213502.mp4
20201010_173045.jpg 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\20201010_173045.jpg
2cc.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\2cc.mp4
ah lai garden.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\ah lai garden.mp4
ah lai room.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\ah lai room.mp4
final garden trim.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\final garden trim.mp4
final garden.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\final garden.mp4
final room complete.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\final room complete.mp4
luvru_yt.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\luvru_yt.mp4
nel app.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\nel app.mp4
read sync untrmed.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\read sync untrmed.mp4
read sync Trim.mp4 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Allocated Allocated Unknown ,LogFileSet1\bhanga\read sync Trim.mp4

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: \LogFileSet1\bhanga\3rd year video
Type: Local Directory
MIME Type: null
Size: 0
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 0000-00-00 00:00:00
Accessed: 0000-00-00 00:00:00
Created: 0000-00-00 00:00:00
Changed: 0000-00-00 00:00:00

Type here to search

ENG 11:24 AM IN 3/25/2022

Viewing all the files inside the folder

F2 slot digital forensics investigation - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Video Communications Geolocation Timeline Discovery Generate Report Close Case

Using LogFileSet1\PR MEET

Table | Thumbnail | Summary

Name S C O Modified Time Change Time Access Time Created Time Size Flag(Dr) Flag(Meta) Known Location

PR Meet(5.4.21).txt 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 565 Allocated Allocated Unknown ,LogFileSet1\bhanga\PR MEET\PR Meet(5.4.21).txt [0C354804-4F94]

Deleted Files

File System (0)
All (0)

MB File Size

MB 50 - 200MB (6)
MB 200+ - 1GB (4)
MB 1GB+ (0)

Data Artifacts

Analysis Results

EXP Metadata (54)

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page: 1 of 1 Matches on page: - of - Match: ⌂ 100% ⌂ Reset Text Source: File Text

1) Enable Remix Feature for Insta Reels
DC page will talk a story about enabling remix feature of reels. After that teams can share their stories that they(team) have enabled remix feature.

2) member to create a reel using remix feature from each team.
Name of the member creating the reel to be given on or before 10th April

3) Search and upload aesthetic and good pics of team(individual or group). Pics should be of offline events, practices etc.
Deadline is 10th April

Reminder: Submission of video by each team on or before 10th April for approval

Type here to search

ENG 11:40 AM IN 3/25/2022

Selecting the txt file and analyzing it

F2 slot digital forensics investigation - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Video Communications Geolocation Timeline Discovery Generate Report Close Case

LogicalFileSet\lhangra\PR MEET

Listing Table: Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag(Dr)	Flag(Meta)	Known	Location	MD5 Hash
PR MEET(6.4.21).txt	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	565	Allocated	Allocated	Unknown	\LogicalFileSet\lhangra\PR MEET\PR Meet(6.4.21).txt	0236e88d64f9af...

File Types

- By Extension: Images (54), Videos (39), Audio (89), Archives (0), Databases (0), Documents (0), Executable (0), Java (0), JavaScript (0), Shell (0), XML (0), ZIP (0), MP3 (0), MP4 (89)
- By MIME Type: image (56), text (plan (1), video (1), mp4 (89))

Deleted Files

- File System (0)
- All (0)

MB File Size

- MB 50 - 200MB (63)
- MB 200+ - 1GB+ (4)
- MB 1GB+ (0)

Data Artifacts

- Analysis Results
- EXP Metadata (54)

Type here to search

ENG 11:40 AM IN 3/25/2022

Viewing the file metadata

F2 slot digital forensics investigation - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Video Communications Geolocation Timeline Discovery Generate Report Close Case

LogicalFileSet\lhangra

Listing Table: Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Phone Numbers	Email Addresses	URLs	Credit Card Numbers
2cc compressed	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
3rd year video	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
DC Video	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
DC Video 2 (with saha)	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
JOC 2CC	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
mod1	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
PR MEET	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
wdd2021	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
2020_0005_190219.jpg	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
2020_01_02_1181.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
2020_01_02_1216.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
2020_01_02_213902.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
2020_04_4_173045.jpg	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
2cc.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
ah lai garden.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
ah lai room.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
final garden trim.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
final garden.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
final room complete.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
suvar_yt.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
nel app.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
read sync untrn.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
read sync trim.mp4	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				

Restrict search to the selected data sources:

LogicalFileSet1

Search Manage Lists File Indexed: 271

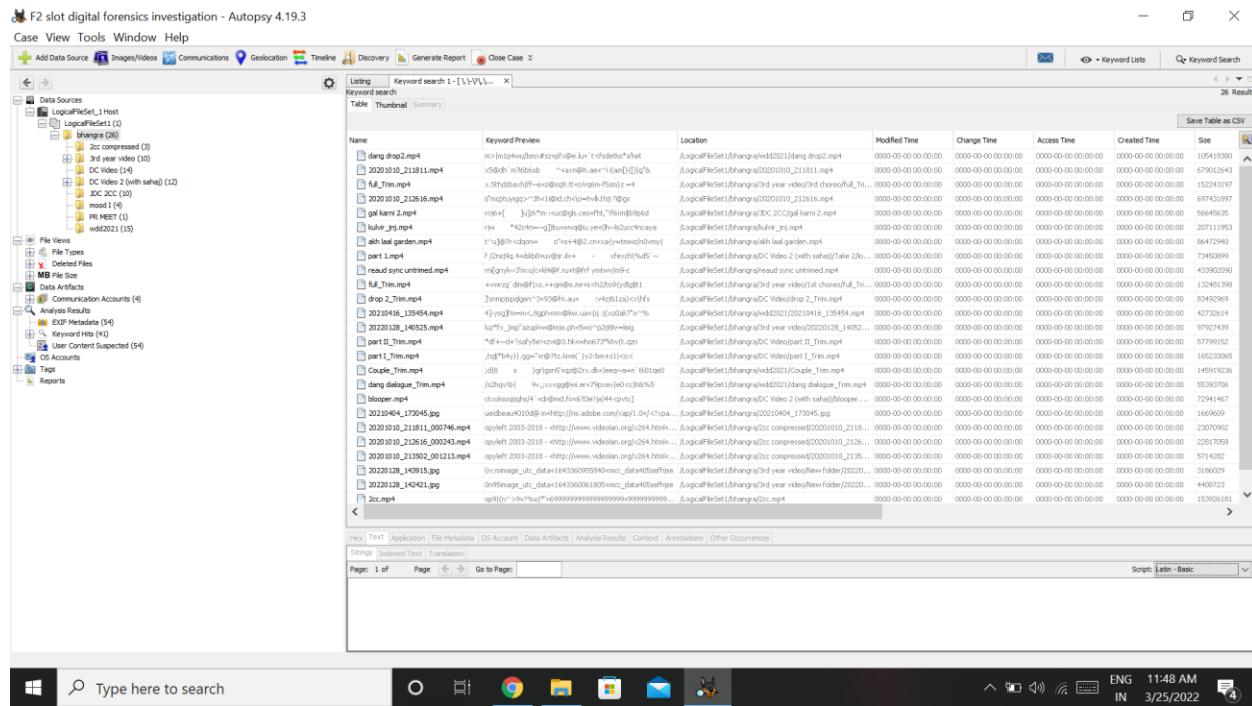
Phone Numbers
Email Addresses
URLs
Credit Card Numbers

String [Indexed Text] Translation

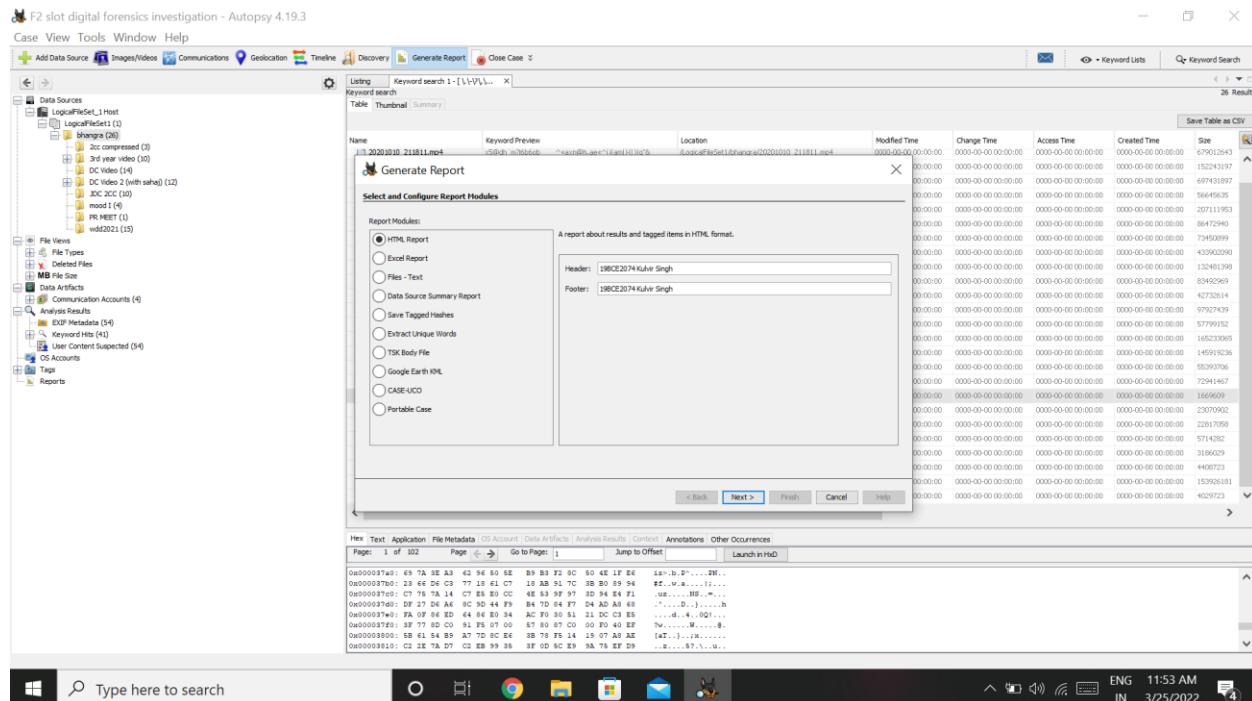
Page: 1 of Page: Go to Page: Script: Latin - Basic

ENG 11:47 AM IN 3/25/2022

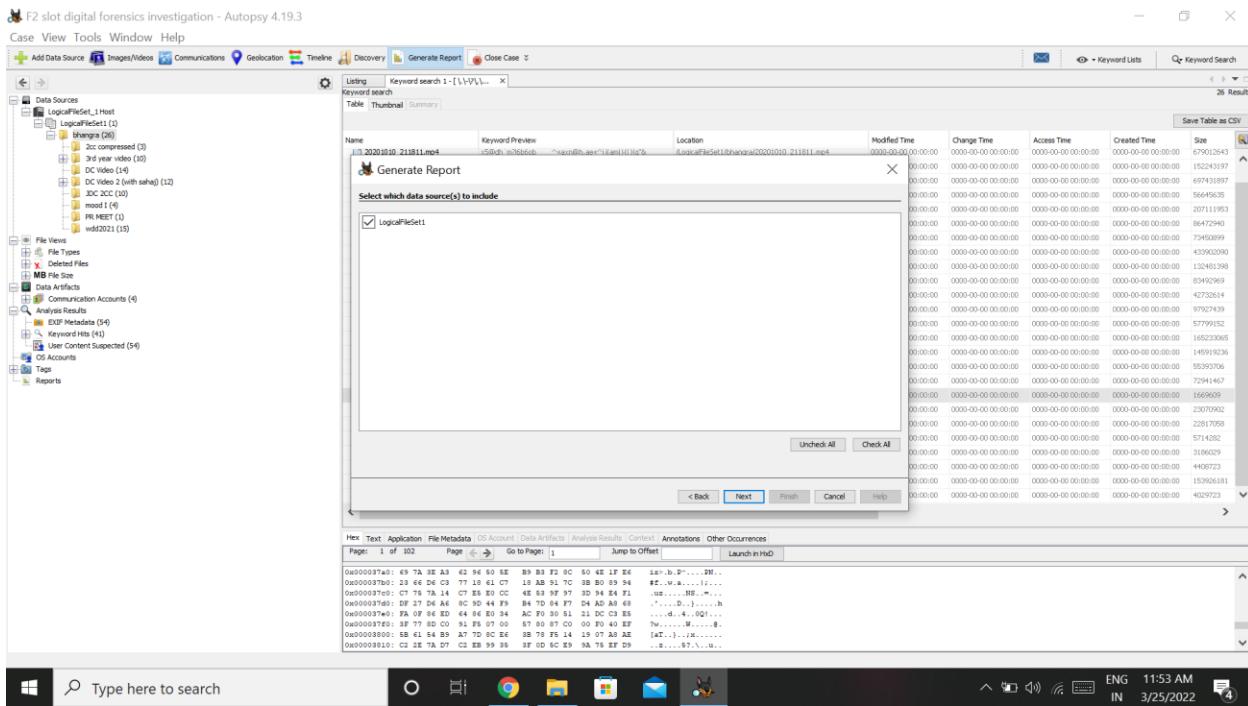
using a keyword type search



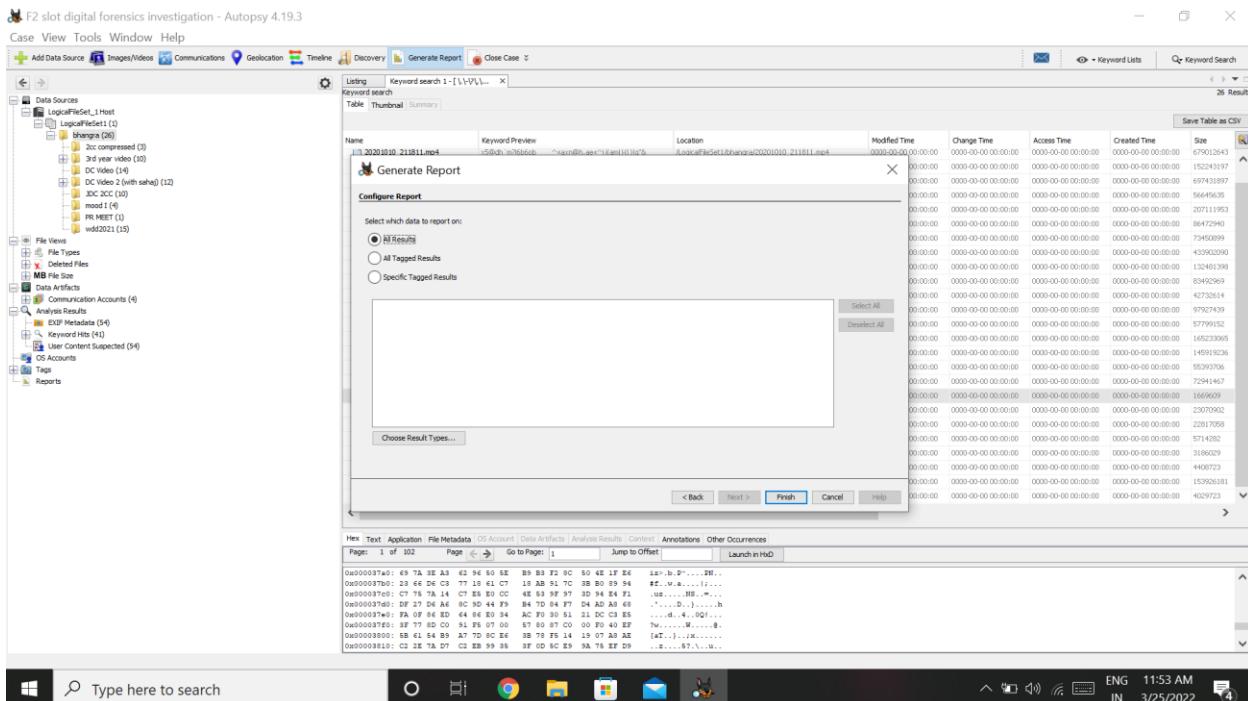
Results of keyword search



Generating report of keyword search



Production of report



Publishing the report

The screenshot shows the Autopsy 4.19.3 digital forensics investigation interface. The top navigation bar includes 'File', 'Add Data Source', 'Images/Videos', 'Communications', 'Geolocation', 'Timeline', 'Discovery', 'Generate Report', 'Close Case', and 'Help'. A search bar at the top right contains 'Keyword search 1-1111...' and a 'Keyword Lists' button. The main window displays a file tree on the left with categories like 'Data Sources', 'LogonFileGet_1 Host', 'LogonFileSet1 (1)', 'bhanga (26)', 'JOC 2022 (12)', 'mod1 (4)', 'PR MEET (1)', 'wdf2021 (15)', 'File Types', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'EXP Metadata (54)', 'User Content Suspected (54)', 'OS Accounts', 'Tags', and 'Reports'. The central area shows a list of files with columns for 'Name', 'Keyword Preview', 'Location', 'Modified Time', 'Change Time', 'Access Time', 'Created Time', and 'Size'. A file named '202010_211811.mp4' is selected. A modal dialog titled 'Report Generation Progress...' indicates the process is 'Complete' and provides the path 'HTML Report : C:\Users\luv_\report.html'. At the bottom, there are 'Cancel' and 'Close' buttons. The status bar at the bottom right shows 'ENG 11:54 AM IN 3/25/2022 4'.

Finalized report

Report Navigation

- Case Summary
- Accounts: Credit Card (4)
- EXIF Metadata (54)
- Keyword Hits (41)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (54)

19BCE2074 Kulvir Singh

Autopsy Forensic Report

HTML Report Generated on 2022/02/25 11:53:36

Case:	F2 slot digital forensics investigation
Case Number:	investigation f2 slot
Number of data sources in case:	1
Notes:	this case is very important and confidential
Examiner:	Kulvir Singh

Image Information:

[Report.html](#)

Autopsy Forensic Report for case

File | C:/Users/kulvir/Desktop/autopsy/F2%20slot%20digital%20forensics%20investigation/Reports/F2%20...

https://vttop.vit.ac.in... WhatsApp Buttons - Pure babel cli install Firebase-node - Cl... javascript - await is... Sequelize CRUD 101 Node.js | MySQL-Cr... (41) Passport JS Us...

19BCE2074 Kulvir Singh

Report Navigation

- Case Summary
- Accounts: Credit Card (4)**
- EXIF Metadata (54)
- Keyword Hits (41)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (54)

Accounts: Credit Card

Review Status	Card Number	ID	Keyword	Keyword Preview
Undecided	617537645005	617537645005	617537645005	nrz? image_utc_data«1617537645005« mcc_data405self
Undecided	643360061805	643360061805	643360061805	0n95 image_utc_data«1643360061805« mcc_data405self
Undecided	643360955840	643360955840	643360955840	(iv:m image_utc_data«1643360955840« mcc_data405self
Undecided	69999999999999999999	69999999999999999999	69999999999999999999	op 9 (n^>9v? %o)*«69999999999999999999«999999999

19BCE2074 Kulvir Singh

Credit card keyword search result

Autopsy Forensic Report for case

File | C:/Users/kulvir/Desktop/autopsy/F2%20slot%20digital%20forensics%20investigation/Reports/F2%20...

https://vttop.vit.ac.in... WhatsApp Buttons - Pure babel cli install Firebase-node - Cl... javascript - await is... Sequelize CRUD 101 Node.js | MySQL-Cr... (41) Passport JS Us...

Email Addresses

Report Navigation

- Case Summary
- Accounts: Credit Card (4)
- EXIF Metadata (54)
- Keyword Hits (41)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (54)

+qm@s.mr	Preview	Source File	Tags
+ vwrzg `dim@ fjs .«+qm@s.mr« s<h2/ to9{y dlg\$ t1 /LogicalFileSet1/bhangra/3rd year video/1st choreo/full_Trim.mp4			
+ vwrzg `dim@ fjs .«+qm@s.mr« s<h2/ to9{y dlg\$ t1 /LogicalFileSet1/bhangra/3rd year video/1st choreo/full_Trim.mp4			

1i@id.ch	Preview	Source File	Tags
ij"m cput yiqg >^3h «1i@id.ch« lo=h vlk1 hij ?@gs /LogicalFileSet1/bhangra/20201010_212616.mp4			
ij"m cput yiqg >^3h «1i@id.ch« lo=h vlk1 hij ?@gs /LogicalFileSet1/bhangra/20201010_212616.mp4			

93@fn.au	Preview	Source File	Tags
�snmp jspql gen^3 «93@fn.au« : v4zj& 1za<x \hfs /LogicalFileSet1/bhangra/DC Video/drop 2_Trim.mp4			
�snmp jspql gen^3 «93@fn.au« : v4zj& 1za<x \hfs /LogicalFileSet1/bhangra/DC Video/drop 2_Trim.mp4			

axn@h.ae	Preview	Source File	Tags
x5 @dh` m?l6 b6ob ^«axn@h.ae« ^i i (am[)() lg& /LogicalFileSet1/bhangra/20201010_211811.mp4			
x5 @dh` m?l6 b6ob ^«axn@h.ae« ^i i (am[)() lg& /LogicalFileSet1/bhangra/20201010_211811.mp4			

dr@md.fo	Preview	Source File	Tags
ctx oksoq ijqh s/4* «dr@md.fo«6?1 3e?ja 44<pv tc] /LogicalFileSet1/bhangra/DC Video 2 (with sahaj)/blooper.mp4			

Email address keyword search result

Report Navigation

- Case Summary
- Accounts: Credit Card (4)
- EXIF Metadata (54)
- Keyword Hits (41)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (54)

19BCE2074 Kulvir Singh

User Content Suspected

Comment	Source File	Tags
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/20201005_190219.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/20210404_173045.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_140819.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_140828.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_140925.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_141022.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_142421.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_142433.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_142519.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_142525.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143910.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143915.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143933.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143936.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143949.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143950 - Copy.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_143950.jpg		
EXIF metadata data exists for this file. ./LogicalFileSet1/bhangra/3rd year video/New folder/20220128_144016.jpg		

User content suspected result