CSE3501-Information Security Analysis and Audit

Lab 9+10

Lab Assignment-8(Autopsy)

Submitted by: Alokam Nikhitha

Reg No:19BCE2555

Autopsy:

Autopsy is computer software that makes it simpler to deploy many of the open source programs and plugins used in The Sleuth Kit.[1] The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data. The tool is largely maintained by Basis Technology Corp. with the assistance of programmers from the community. The company sells support services and training for using the product.

The tool is designed with these principles in mind:

Extensible — the user should be able to add new functionality by creating plugins that can analyze all or part of the underlying data source.

Centralised — the tool must offer a standard and consistent mechanism for accessing all features and modules.

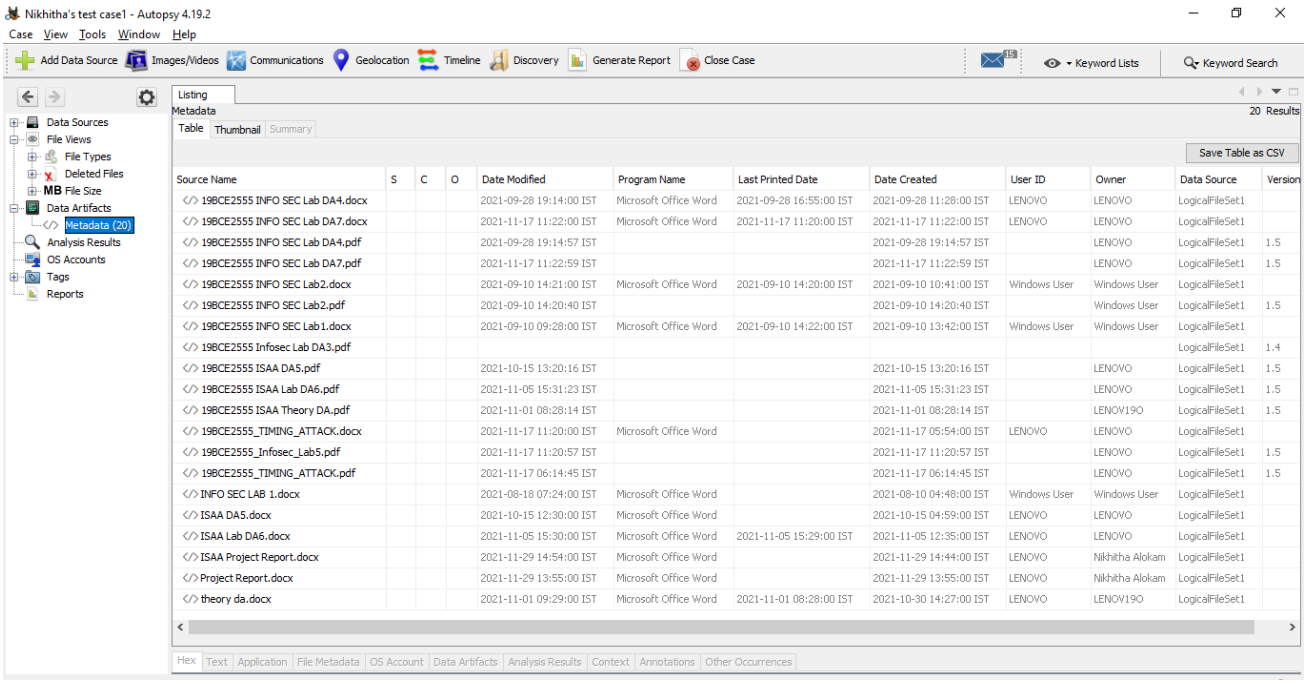
Ease of Use — the Autopsy Browser must offer the wizards and historical tools to make it easier for users to repeat their steps without excessive reconfiguration.

Multiple Users — the tool should be usable by one investigator or coordinate the work of a team.

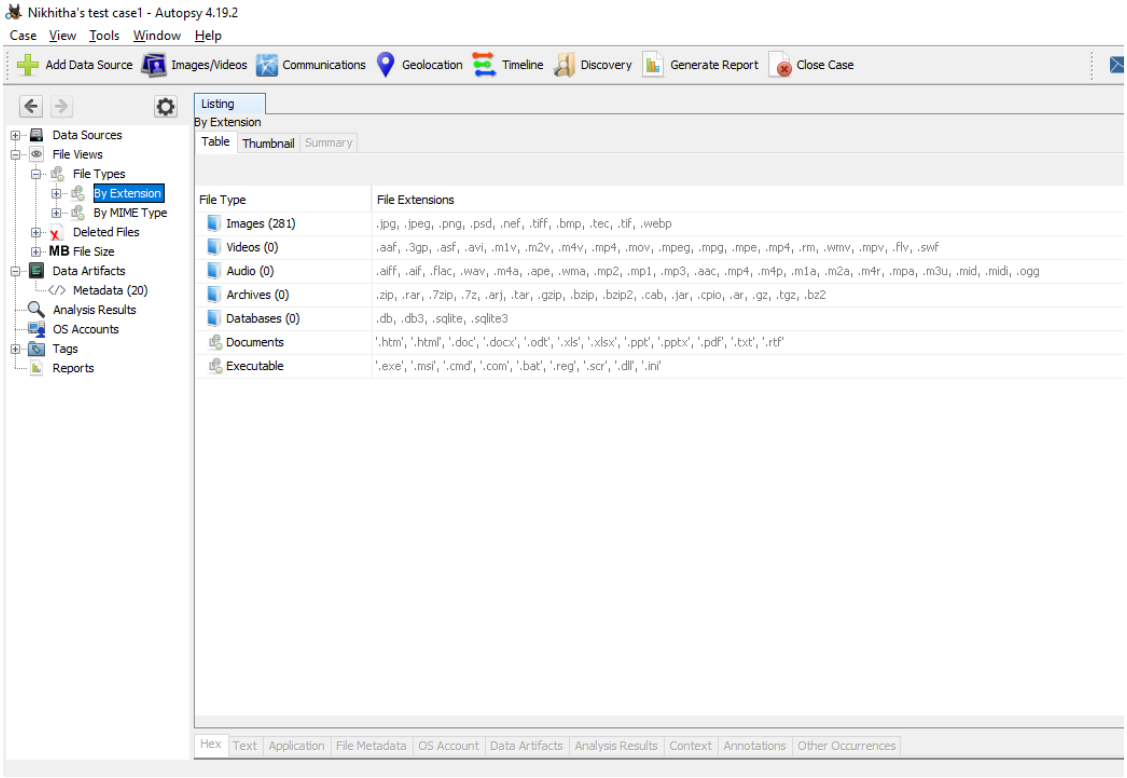
The core browser can be extended by adding modules that help scan the files (called "ingesting"), browse the results (called "viewing") or summarize results (called "reporting"). A collection of open-source modules allow customization.

In this lab we are using Single User and We are doing Autopsy on ISAA Folder in Desktop

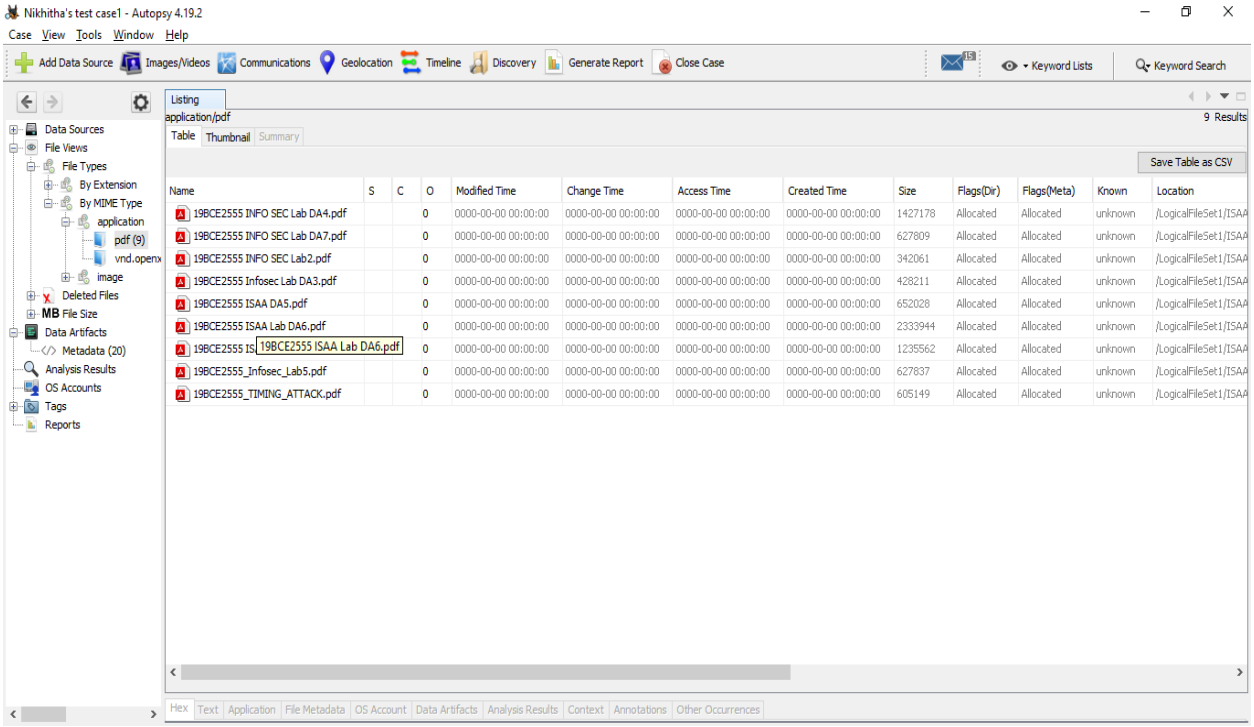
List of Files present in the folder



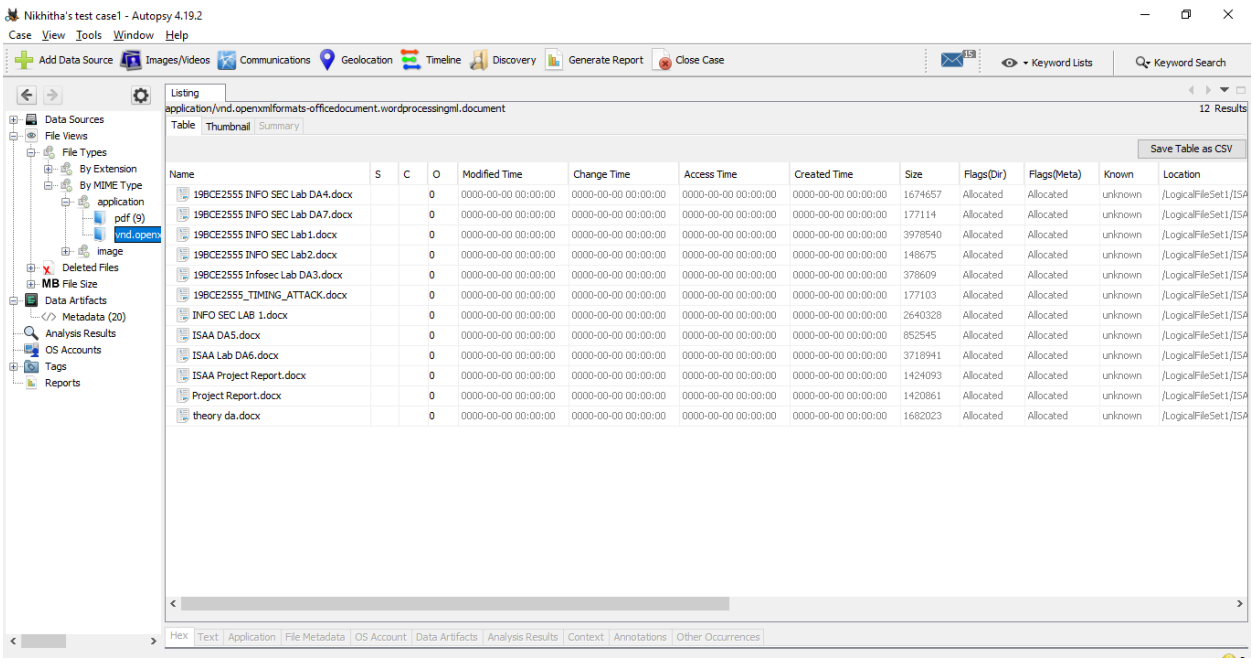
List of various types of files in that folder



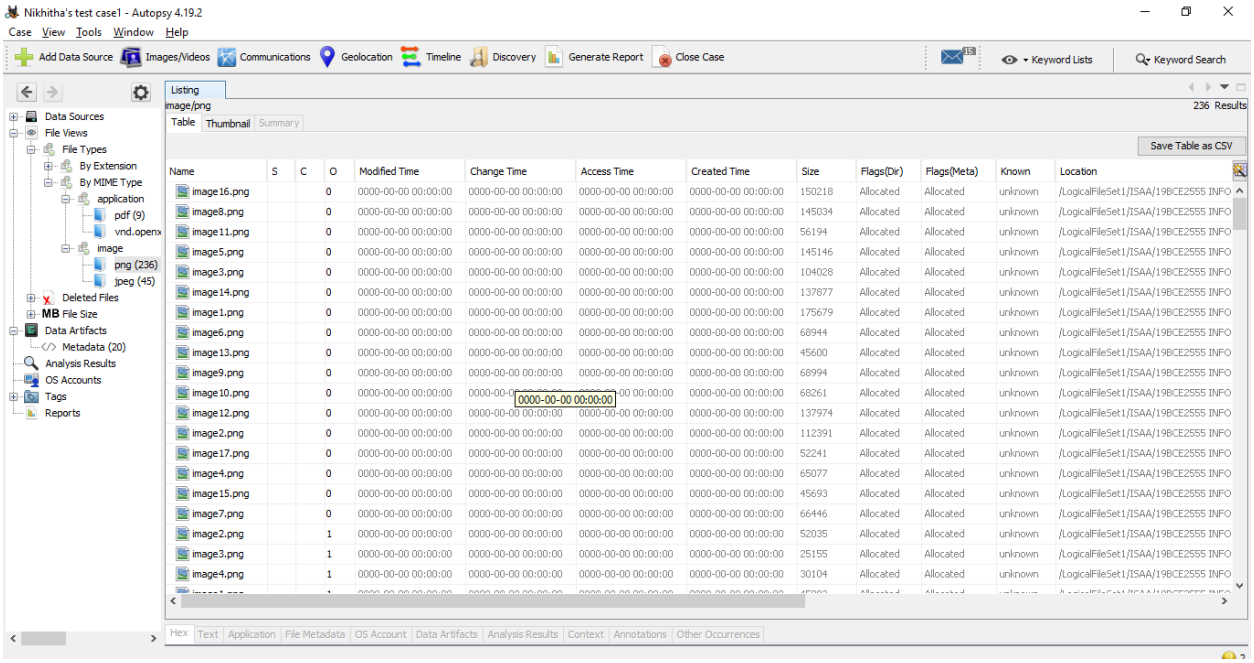
List of PDF Files in the ISAA Folder



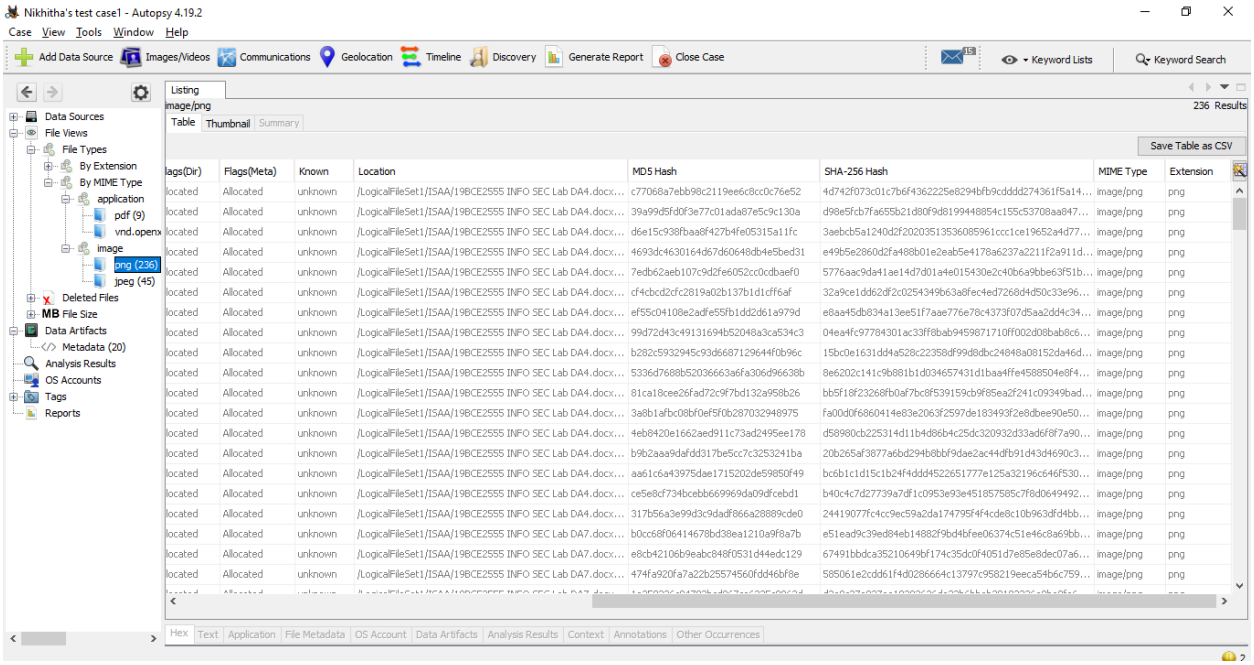
List of all Word Documents inside the Folder



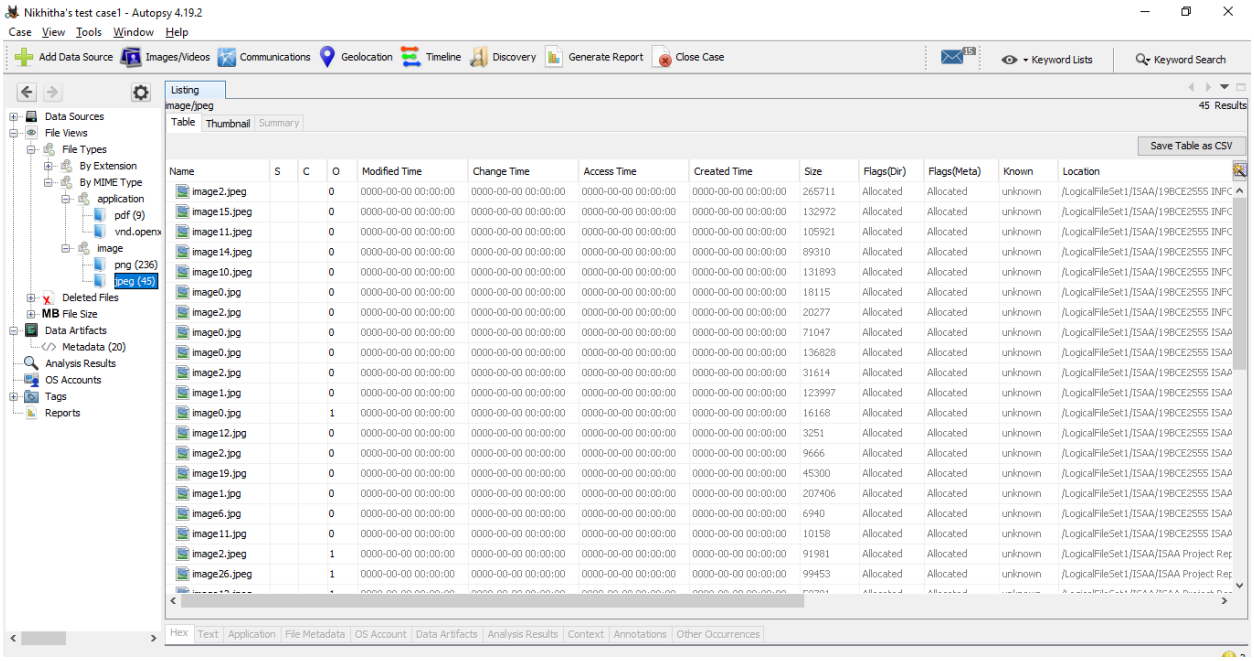
List of all images in .png form in files that are present inside the folder “ISAA”



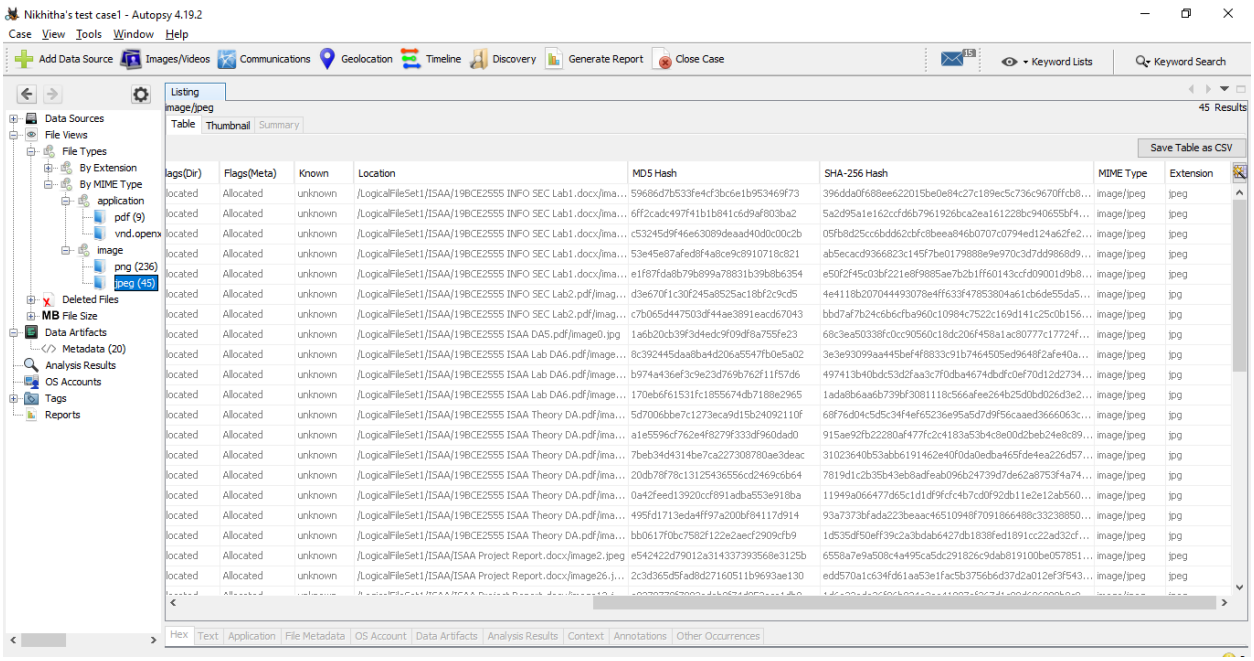
The HD5 Hash and SHA -256 Hash of those images



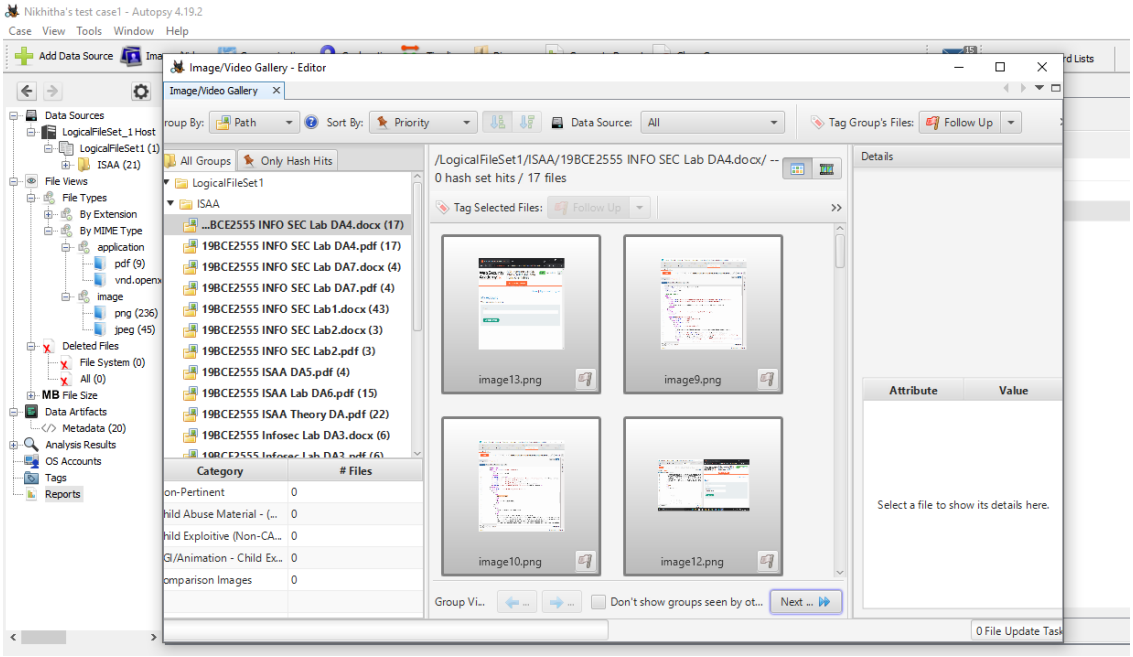
List of all images in .jpg form inside the files that are present inside the folder “ISAA”



The HD5 Hash and SHA -256 Hash of those images

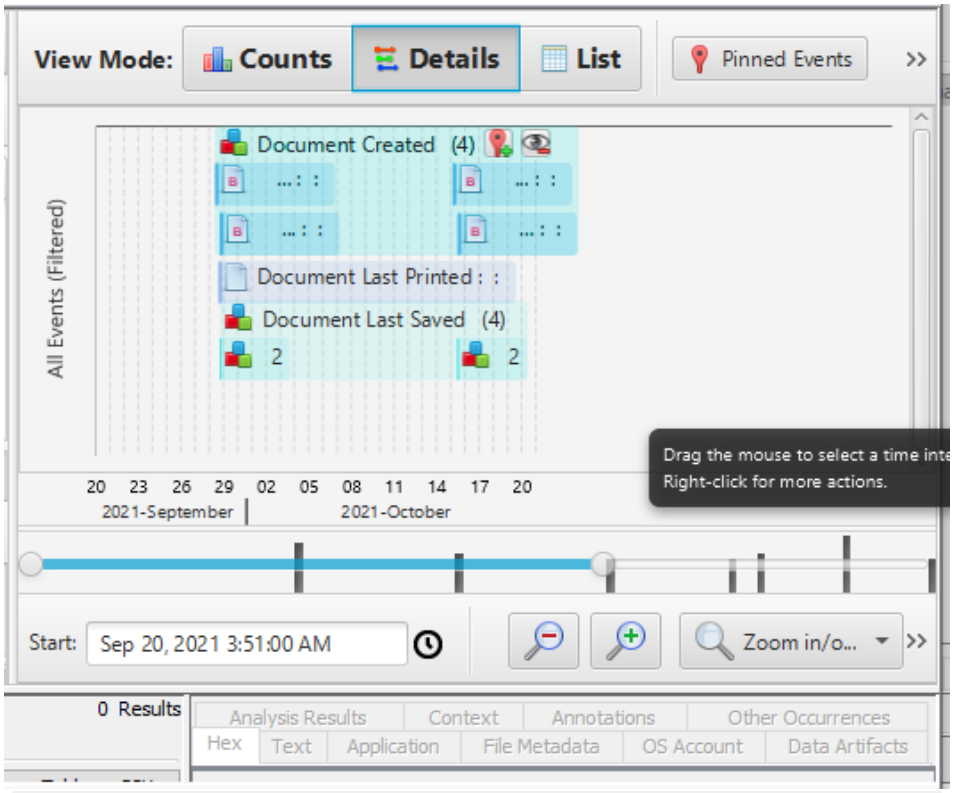


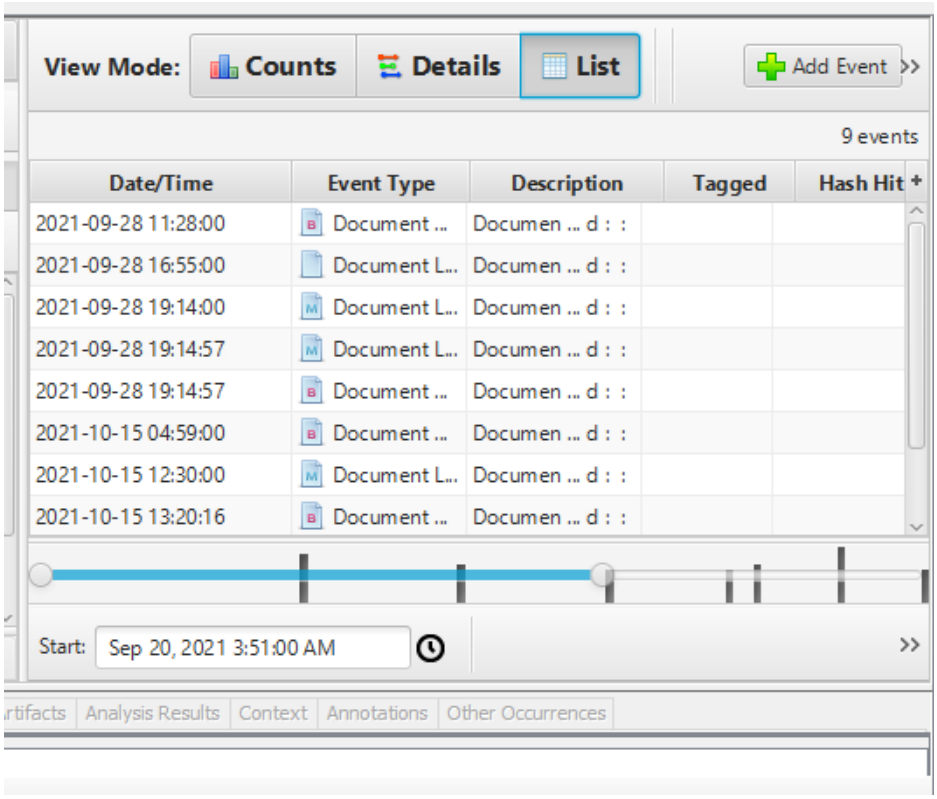
List of Images from each File in the Folder

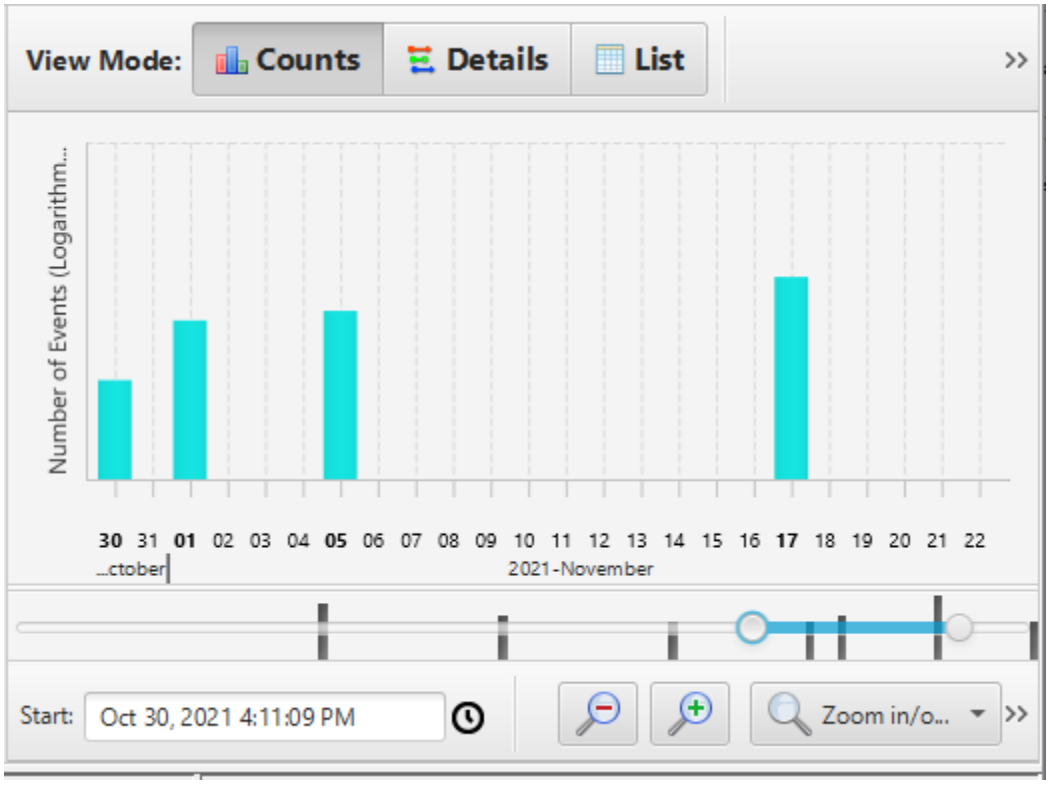


This is showing the geolocation of the data. It helps us in getting the location of the attackers because attackers can be anywhere.

Time line of the Docs in the Folder






View Mode:
Counts
Details
List
Number of Events (Logarithm...
30 31 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22
...ctober
2021-November
Start:
Oct 30, 2021 4:11:09 PM
Zoom in/o...

Autopsy Forensic Report of folder “ISAA” from desktop in HTML format

Report Navigation

- Case Summary
- Metadata (20)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2021/12/03 21:20:40

Case:	Nikhitha's test_case 1
Case Number:	1
Number of data sources in case:	1
Examiner:	Alokam Nikhitha

Image Information:

LogicalFileSet1

Software Information:

Autopsy Version:	4.19.2
Android Analyzer Module:	4.19.2
Android Analyzer (aLEAPP) Module:	4.19.2
Central Repository Module:	4.19.2

Report Navigation

- Case Summary
- Metadata (20)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)

Ingest History:

Job 1:

Data Source:	LogicalFileSet1
Status:	COMPLETED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification Extension Mismatch Detector Embedded File Extractor Picture Analyzer Keyword Search Email Parser Encryption Detection Interesting Files Identifier Central Repository PhotoRec Carver Virtual Machine Extractor Data Source Integrity Android Analyzer (aLEAPP) DJI Drone Analyzer YARA Analyzer iOS Analyzer (iLEAPP) Android Analyzer GPX Parser

Meta Data(Date of File created and Modified in the folder)

Report Navigation

- Case Summary
- Metadata (20)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)

Metadata

Date Created	Date Modified	Last Printed Date	Owner	Program Name	User ID	Version
						1.4
2021-08-10 04:48:00 IST	2021-08-18 07:24:00 IST		Windows User	Microsoft Office Word	Windows User	
2021-09-10 10:41:00 IST	2021-09-10 14:21:00 IST	2021-09-10 14:20:00 IST	Windows User	Microsoft Office Word	Windows User	
2021-09-10 13:42:00 IST	2021-09-10 09:28:00 IST	2021-09-10 14:22:00 IST	Windows User	Microsoft Office Word	Windows User	
2021-09-10 14:20:40 IST	2021-09-10 14:20:40 IST		Windows User			1.5
2021-09-28 11:28:00 IST	2021-09-28 19:14:00 IST	2021-09-28 16:55:00 IST	LENOVO	Microsoft Office Word	LENOVO	
2021-09-28 19:14:57 IST	2021-09-28 19:14:57 IST		LENOVO			1.5
2021-10-15 04:59:00 IST	2021-10-15 12:30:00 IST		LENOVO	Microsoft Office Word	LENOVO	
2021-10-15 13:20:16 IST	2021-10-15 13:20:16 IST		LENOVO			1.5
2021-10-30 14:27:00 IST	2021-11-01 09:29:00 IST	2021-11-01 08:28:00 IST	LENOV19O	Microsoft Office Word	LENOVO	
2021-11-01 08:28:14 IST	2021-11-01 08:28:14 IST		LENOV19O			1.5
2021-11-05 12:35:00 IST	2021-11-05 15:30:00 IST	2021-11-05 15:29:00 IST	LENOVO	Microsoft Office Word	LENOVO	
2021-11-05 15:31:23 IST	2021-11-05 15:31:23 IST		LENOVO			1.5
2021-11-17 05:54:00 IST	2021-11-17 11:20:00 IST		LENOVO	Microsoft Office Word	LENOVO	
2021-11-17 06:14:45 IST	2021-11-17 06:14:45 IST		LENOVO			1.5
2021-11-17 11:20:57 IST	2021-11-17 11:20:57 IST		LENOVO			1.5
2021-11-17 11:22:00 IST	2021-11-17 11:22:00 IST	2021-11-17 11:20:00 IST	LENOVO	Microsoft Office Word	LENOVO	
2021-11-17 11:22:59 IST	2021-11-17 11:22:59 IST		LENOVO			1.5
2021-11-29 13:55:00 IST	2021-11-29 13:55:00 IST		Nikhitha Alokam	Microsoft Office Word	LENOVO	
2021-11-29 14:44:00 IST	2021-11-29 14:54:00 IST		Nikhitha Alokam	Microsoft Office Word	LENOVO	