

Software and Cybersecurity Lab

CS445 Lab4

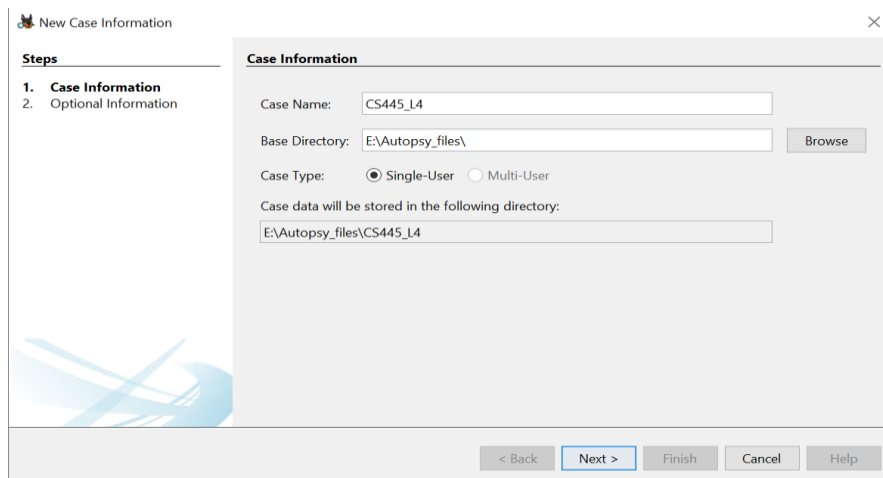
Name: Dipean Dasgupta

ID: 202151188

Objective: To perform analysis and investigation of digital data using Autopsy software, commonly referred to as "Autopsy"; an open-source digital forensics platform.

Task1: Data Acquisition

Step1: Creating case in Autopsy software

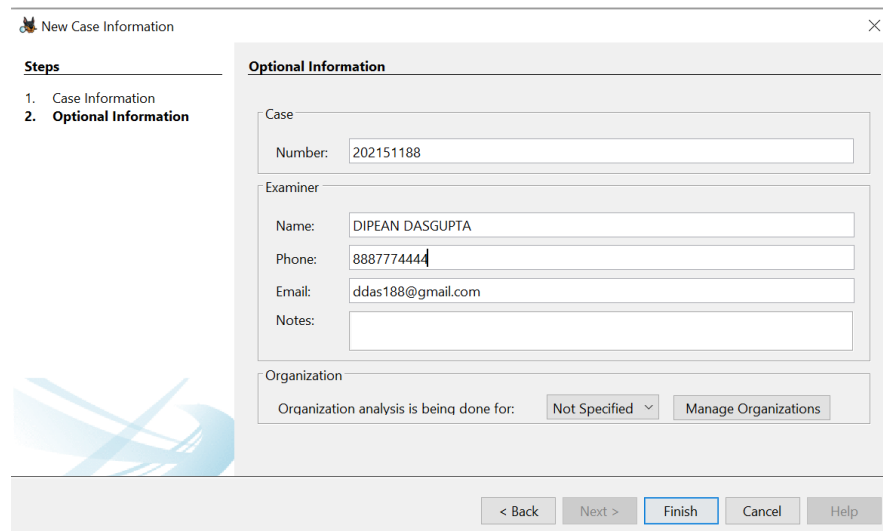


The screenshot shows the 'New Case Information' dialog box in Autopsy software. The 'Steps' panel on the left indicates '1. Case Information' is the current step. The 'Case Information' section contains the following fields:

- Case Name: CS445_L4
- Base Directory: E:\Autopsy_files\ (with a 'Browse' button)
- Case Type: ☒ Single-User ☐ Multi-User
- Case data will be stored in the following directory: E:\Autopsy_files\CS445_L4

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

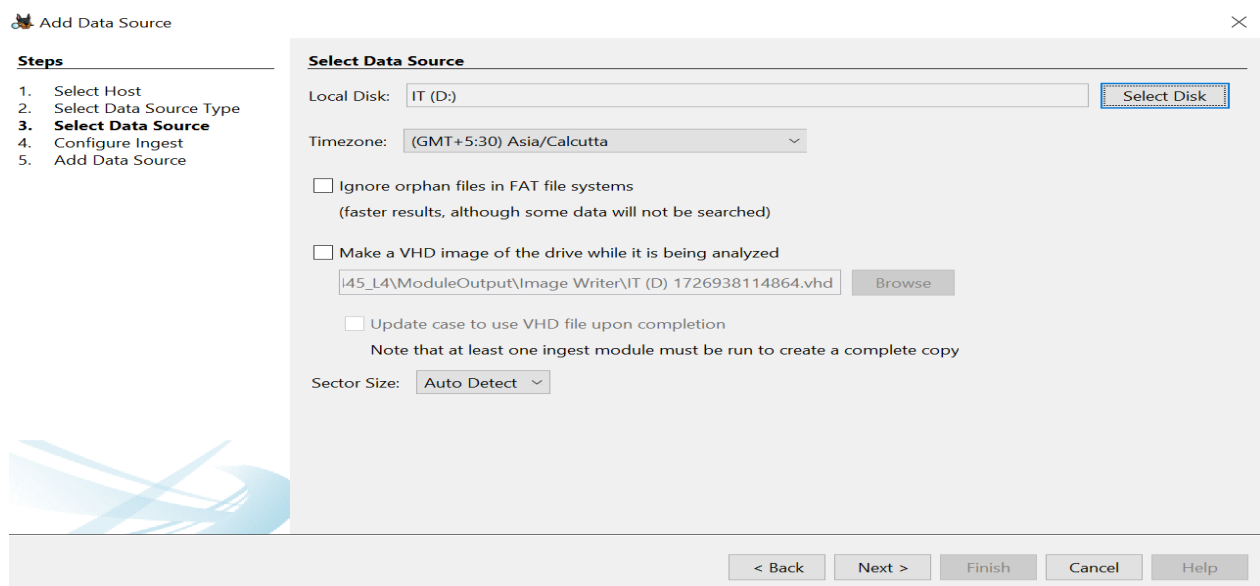
Step2: Filling in the details of Case and Examiner



The screenshot shows the 'New Case Information' dialog box in Autopsy software, now on 'Step 2: Optional Information'. The 'Optional Information' section contains the following fields:

- Case Number: 202151188
- Examiner Name: DIPEAN DASGUPTA
- Examiner Phone: 8887774444
- Examiner Email: ddas188@gmail.com
- Examiner Notes: (empty text area)
- Organization analysis is being done for: Not Specified (with a dropdown arrow) and a 'Manage Organizations' button

At the bottom, the navigation buttons are: '< Back', 'Next >', 'Finish' (highlighted in blue), 'Cancel', and 'Help'.



Disk Drive D has been selected for Autopsy. The drive has around 6 GB of files.

Using FTK imager, a forensic imaging tool, forensic image of the drive have been created

```

Information for E:\imager\image:

Physical Evidentiary Item (Source) Information:
[Device Info]
  Source Type: Logical
[Drive Geometry]
  Bytes per Sector: 512
  Sector Count: 12,036,096
[Physical Drive Information]
  Removable drive: False
  Source data size: 5877 MB
  Sector count: 12036096
[Computed Hashes]
  MD5 checksum: 2a347ac781852524472f18be64c39ce2
  SHA1 checksum: 16cf40e1f9bcd019c1515283889a37c94dccba53

Image Information:
  Acquisition started: Sat Sep 21 18:46:48 2024
  Acquisition finished: Sat Sep 21 18:47:37 2024
  Segment list:
    E:\imager\image.s01
    E:\imager\image.s02

Image Verification Results:
  Verification started: Sat Sep 21 18:47:37 2024
  Verification finished: Sat Sep 21 18:48:12 2024
  MD5 checksum: 2a347ac781852524472f18be64c39ce2 : verified
  SHA1 checksum: 16cf40e1f9bcd019c1515283889a37c94dccba53 : verified

```

The integrity of the acquired image using a hash algorithm (e.g., MD5, SHA-1) is verified and the hash value is documented.

Challenges: Since the contents in the drive was much; it took a significant amount of time to acquire the Image and verification of integrity.

Task2: File Analysis:

File Structure

The screenshot displays the Autopsy 4.21.0 interface. The left pane shows the 'Data Sources' tree with 'D:' expanded, listing various folders and their file counts. The right pane shows a 'Listing' table with columns 'File Type' and 'File Extensions'.

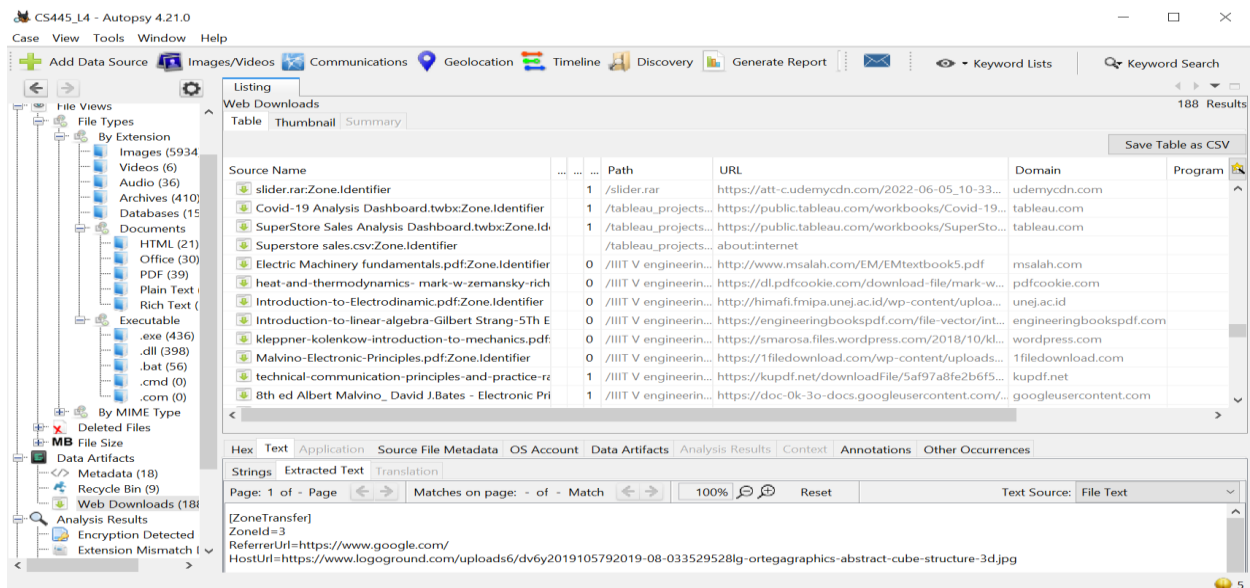
Data Sources Tree (D:):

- \$OrphanFiles (6425)
- \$Extend (7)
- \$RECYCLE.BIN (4)
- \$Unalloc (60)
- _temp_matlab_R2022a_Prerelease_win64 (3)
- BasicPyProjects (7)
- C program (15)
- C++ (9)
- CompNet (3)
- Cprogramming (108)
- Downloads (2)
- eclab (96)
- Embeddedlab (21)
- Eslab (3)
- Excel (5)
- flutter_Skiome (14)
- GitProjects (14)
- GRE (5)
- idmdocs (51)
- IIIT V engineering books (7)
- IMG (2)
- iverilog (12)
- Java (10)
- MSI35314.tmp (2)
- Music (32)
- My software (35)
- mysql-8.3.0-winx64 (10)
- Need for Speed - Most Wanted (34)
- Others (3)

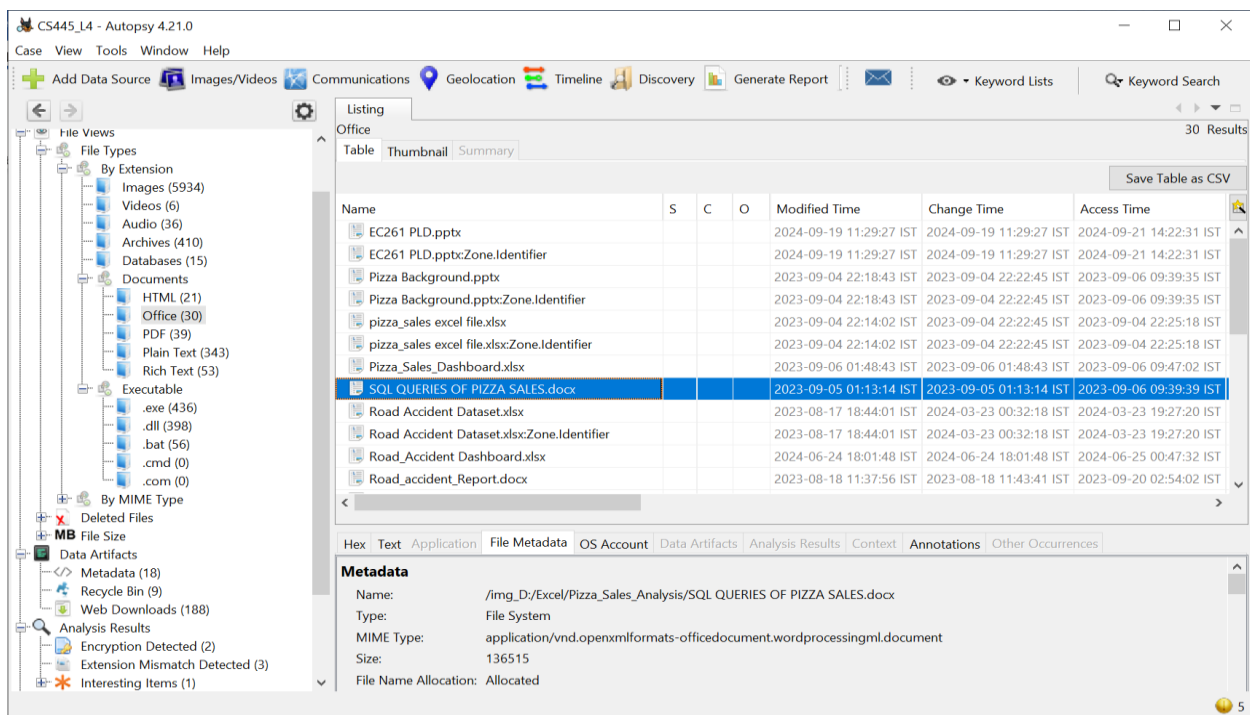
Listing Table:

File Type	File Extensions
Images (5934)	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
Videos (6)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (36)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
Archives (410)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (15)	.db, .db3, .sqlite, .sqlite3
Documents	.html, .htm, .doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx, .pdf, .txt, .rtf
Executable	.exe, .msi, .cmd, .com, .bat, .reg, .scr, .dll, .ini

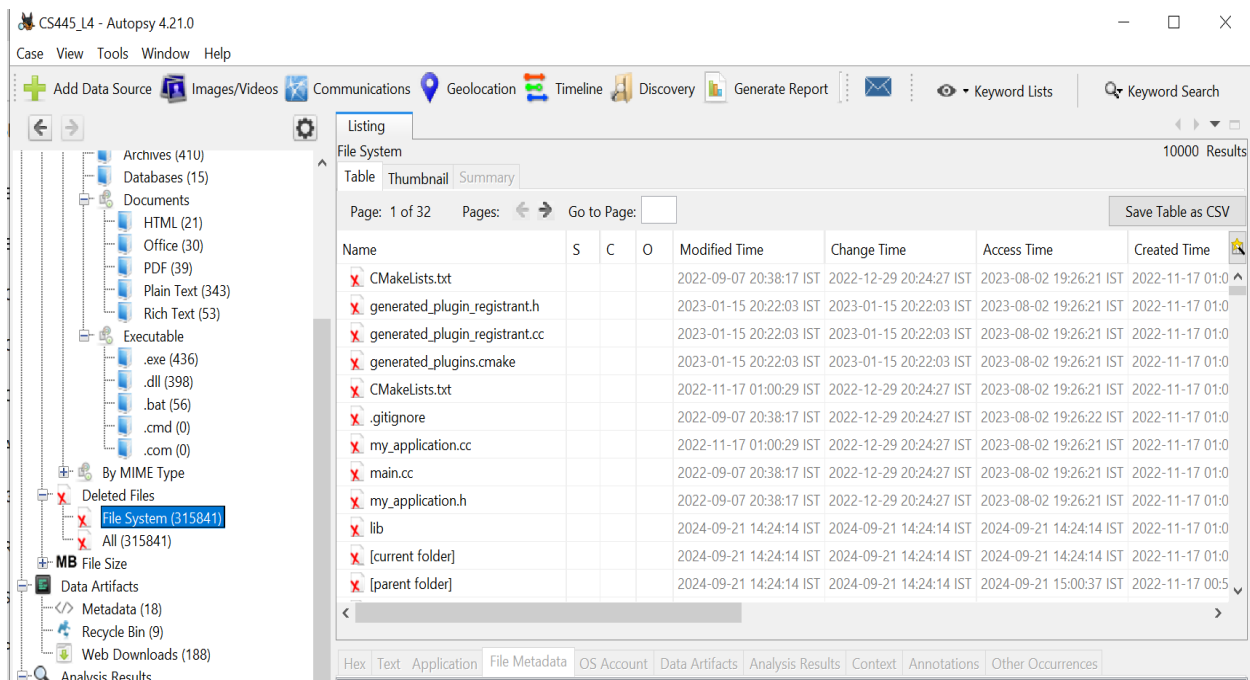
File structure of the inspected D drive is uploaded above.



Web browser history for the last month has been captured. No suspicious activity detected.



The docx files were checked but no docx file was modified last month. Selected file in the image was modified almost a year ago.



These are the list of deleted files which were deleted from the drive or moved away to another storage.

Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No notable hash set.	2024/09/21 15:36:14
Hash Lookup	1		No known hash set.	2024/09/21 15:36:14
Recent Activity	1		Started D:	2024/09/21 15:36:16
Recent Activity	1		Finished D: - No errors reported	2024/09/21 15:36:53
Recent Activity	1		D: - Browser Results	2024/09/21 15:36:53
aLeapp	1		aLeapp Processing Completed	2024/09/21 15:40:40
DJI Drone Analyzer	1		Started D:	2024/09/21 15:40:40
iLeapp	1		iLeapp Processing Completed	2024/09/21 15:42:57
Embedded File Extractor	1		Error unpacking slider.rar	2024/09/21 15:44:45
Embedded File Extractor	1		Error unpacking Skiome.rar	2024/09/21 15:44:49
Encryption Detection	1		Encryption Detected Match: 2464202208091701768584.pdf	2024/09/21 15:51:27
Embedded File Extractor	1		Encrypted file in archive detected.	2024/09/21 15:51:57
Interesting Files Identifier	1		Interesting File Match: Encryption Programs(qdbus.exe)	2024/09/21 16:07:05
GPX Parser	1		0 files found	2024/09/21 16:24:47
File Type Identification	1		File Type Id Results	2024/09/21 16:24:47
Extension Mismatch Detector	1		File Extension Mismatch Results	2024/09/21 16:24:47
PhotoRec Carver	1		PhotoRec Results	2024/09/21 16:24:47
GPX Parser	1		0 files found	2024/09/21 16:24:47

Sort by: Time Total: 18 Unique: 18

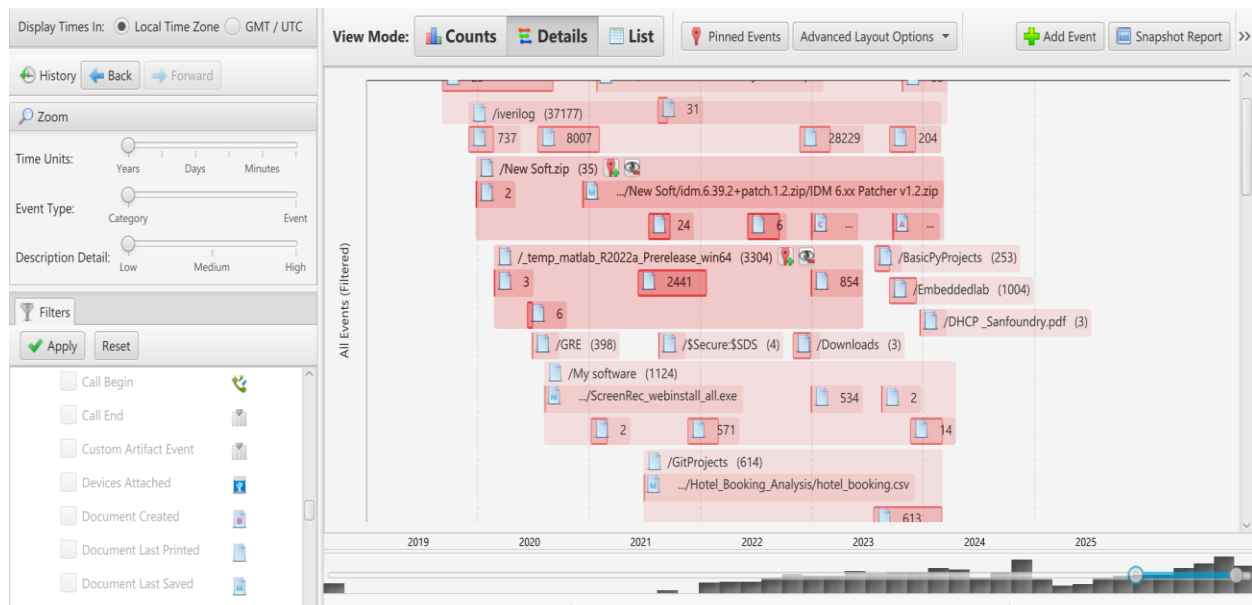
Here is the report of the other tests that has been done on the contents of the drive. The result is satisfactory.

TASK3: Timeline Analysis



The timeline analysis is done using Plaso. Timeframe was from 2020 to 2024. Most of activities that are shown in red are associated with changes in files in the file system. Blue portions depict significant web activity and downloads.

Timestamp wise is displayed below:



For more details and description including time, List wise view is shared

Timeline - Editor

Timeline x

Display Times In: Local Time Zone GMT / UTC

View Mode: Counts Details List

Add Event Snapshot Report Refresh View

History Back Forward

Filters

☒ Must include text:

enter filter string

☐ Must be tagged

☐ Must have hash hit

☐ Limit data sources to

☐ D: (ID: 1)

☐ Limit file types to

☐ Media

☐ Documents

☐ Executables

☐ Other

Hidden Descriptions

Date/Time	Event Type	Description	Tagged	Hash Hit
2023-11-19 10:37:14	_C_M	/OrphanFiles/wizards/pxact/pcorcs/axi_gpio_v1_00_a/data		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/XilinxProcessorIPLib/dri ... c_v2_00_a/doc/html/api/xdsdac_l_8h.html		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/XilinxProcessorIPLib/drivers/scugic_v1_03_a/data/scugic_v2_1_0.mdd		
2023-11-19 10:37:14	_C_	/OrphanFiles/hw/XilinxProcessorIPLib/pc ... hernet_v3_01_a/doc/html/change_log.html		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/XilinxProcessorIPLib/drivers/wdttb_v2_00_a/examples/index.html		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/ThirdParty/sw_services/lwi ... _a/src/lwip-1.4.0/src/include/lwip/netif.h		
2023-11-19 10:37:14	_C_	/OrphanFiles/hw/XilinxProcessorIPLib/pc ... blaze_v8_50_a/hdl/vhdl/data_flow_gti.vhd		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/XilinxProcessorIPLib/drivers/spi_v3_03_a/data/spi_header.h		
2023-11-19 10:37:14	_C_M	/OrphanFiles/sw/ThirdParty/bsp/linux_2_6_v1_07_a/dist/wr12.0/arch/powerpc/kernel		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/XilinxProcessorIPLib/dri ... _v1_00_a/doc/html/api/functions_vars.html		
2023-11-19 10:37:14	_C_	/OrphanFiles/hw/XilinxProcessorIPLib/pc ... _timer_v1_03_a/data/axi_timer_v2_1_0.pao		
2023-11-19 10:37:14	_C_	/OrphanFiles/hw/XilinxProcessorIPLib/pc ... stats_v5_00_a/hdl/vhdl/MemXLib_utils.vhd		
2023-11-19 10:37:14	_C_M	/OrphanFiles/hw/XilinxProcessorIPLib/pcorcs/axi_ethernet_v3_01_a/doc/html		
2023-11-19 10:37:14	_C_	/OrphanFiles/doc/usenglish/SDK_doc/images/boot_image_authentication.png		
2023-11-19 10:37:14	_C_	/OrphanFiles/sw/XilinxProcessorIPLib/dri ... sb_v4_02_a/doc/html/api/struct_x_usb.html		
2023-11-19 10:37:14	_C_	/OrphanFiles/hw/XilinxProcessorIPLib/ih/nc ... rilon/axi_ncie_mm_s_v1_04_a_romnator.v		

Start: Nov 28, 2019, 7:37:51 AM

Jump By: year

End: Sep 21, 2024, 3:27:09 PM

ANALYSIS RESULTS:

Analysis Results

3 Results

Table

Thumbnail

Summary

Page: 1

Pages: 1

Go to Page: 1

Save Table as CSV

Artifact Type	Child Count	Name
Encryption Detected (2)	2	
Extension Mismatch Detected (3)	3	
Interesting Items (1)		Interesting Items

In analysis results, 2 files were detected having encryption; 3 files had extension mismatch and 1 item were interesting.

Encryption Programs

1 Results

Table

Thumbnail

Summary

Page: 1 of 1

Pages: 1

Go to Page: 1

Save Table as CSV

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Category	File Path
gdbus.exe				File	Likely Notable		Encryption Programs		Gpg4win	/img_D:/iverilog/gtkw

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Metadata

Name: /img_D:/iverilog/gtkwave/bin/gdbus.exe

Type: File System

MIME Type: application/x-msdownload

Size: 47104

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2021-02-04 15:40:50 IST

Accessed: 2024-09-21 14:51:08 IST

Created: 2022-11-22 15:48:17 IST

Changed: 2022-12-29 20:24:27 IST

MD5: 9dadeb242c7893f917ac196f641b66be

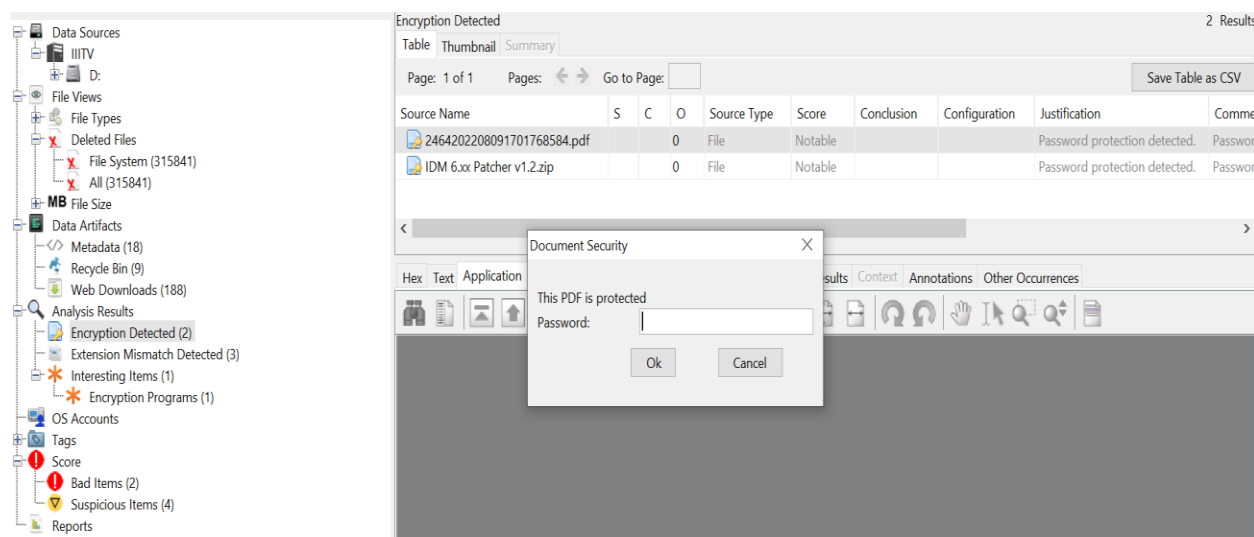
SHA-256: 027d4793b9a1b38714bfde746b3c103aaa414e8e11bad3a9088f9eaa0c5d8fb9

Hash Lookup Results: UNKNOWN

Internal ID: 52114

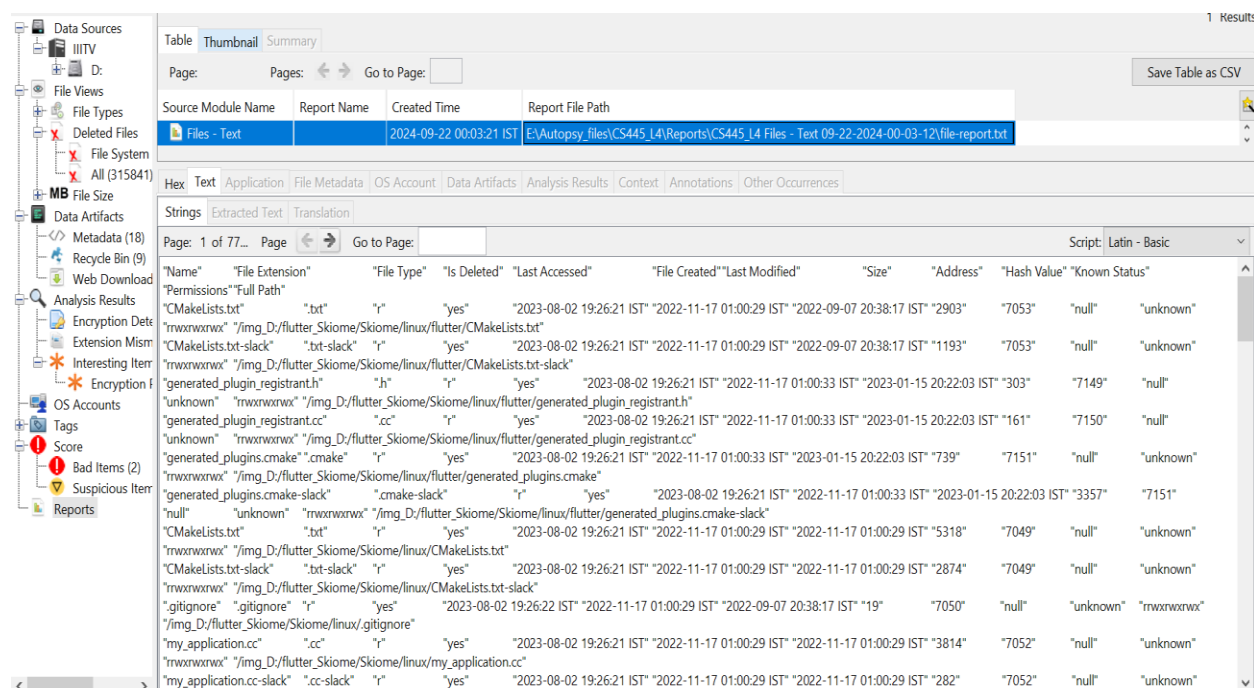
Details of the interesting Item. It's an application.

INTERESTING OBSERVATION:



In the scan analysis, a pdf was listed as encrypted file; autopsy being a digital forensic software is not able to check the pdf bypassing the password.

REPORT GENERATION:



A full fledged analysis report is prepared. A snapshot of the report text file is shared in next page:

file-report.txt - Notepad

Name	File Extension	File Type	Is Deleted	Last Accessed	File Created	Last Modified	Size	Address	Hash Value	Ki
"CMakeLists.txt"	".txt"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"2903"	"71"		
"CMakeLists.txt-slack"	".txt-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"1"			
"generated_plugin_registrant.h"	".h"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:33 IST"	"2023-01-15 20:22:03 IST"	"31"			
"generated_plugins.cc"	".cc"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:33 IST"	"2023-01-15 20:22:03 IST"	"31"			
"generated_plugins.cmake"	".cmake"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:33 IST"	"2023-01-15 20:22:03 IST"	"31"			
"generated_plugins.cmake-slack"	".cmake-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:33 IST"	"2023-01-15 20:22:03 IST"	"31"			
"CMakeLists.txt"	".txt"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-11-17 01:00:29 IST"	"5318"	"71"		
"CMakeLists.txt-slack"	".txt-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-11-17 01:00:29 IST"	"21"			
".gitignore"	".gitignore"	"r"	"yes"	"2023-08-02 19:26:22 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"19"	"71"		
"my_application.cc"	".cc"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-11-17 01:00:29 IST"	"3814"	"71"		
"my_application.cc-slack"	".cc-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-11-17 01:00:29 IST"	"21"			
"main.cc"	".cc"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"186"	"7054"	"ni"	
"my_application.h"	".h"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"406"	"71"		
".gitignore"	".gitignore"	"r"	"yes"	"2023-08-02 19:26:22 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"96"	"71"		
"Flutter-Generated.xcconfig"	".xcconfig"	"r"	"yes"	"2022-12-10 15:55:41 IST"	"2022-12-10 15:55:41 IST"	"2022-12-10 15:55:41 IST"	"41"			
"Flutter_export_environment.sh"	".sh"	"r"	"yes"	"2022-12-10 15:55:41 IST"	"2022-12-10 15:55:41 IST"	"2022-12-10 15:55:41 IST"	"41"			
"Flutter-Debug.xcconfig"	".xcconfig"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"17"			
"Flutter-Release.xcconfig"	".xcconfig"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"17"			
"GeneratedPluginRegistrant.swift"	".swift"	"r"	"yes"	"2023-01-15 20:22:03 IST"	"2022-11-17 01:00:33 IST"	"2023-01-15 20:22:03 IST"	"41"			
"GeneratedPluginRegistrant.swift-slack"	".swift-slack"	"r"	"yes"	"2023-01-15 20:22:03 IST"	"2022-11-17 01:00:33 IST"	"2023-01-15 20:22:03 IST"	"41"			
"AppDelegate.swift"	".swift"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:17 IST"	"21"			
"app_icon_1024.png"	".png"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"102994"	"71"		
"app_icon_1024.png-slack"	".png-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"5680"	"71"		
"app_icon_128.png"	".png"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"520"	"71"		
"app_icon_128.png-slack"	".png-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"14142"	"71"		
"app_icon_16.png"	".png"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"520"	"71"		
"app_icon_256.png"	".png"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"14142"	"71"		
"app_icon_256.png-slack"	".png-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"1066"	"71"		
"app_icon_32.png"	".png"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"36406"	"71"		
"app_icon_32.png-slack"	".png-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"36406"	"71"		
"app_icon_512.png"	".png"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"36406"	"71"		
"app_icon_512.png-slack"	".png-slack"	"r"	"yes"	"2023-08-02 19:26:21 IST"	"2022-11-17 01:00:29 IST"	"2022-09-07 20:38:32 IST"	"36406"	"71"		

Link to the Report File:

https://drive.google.com/file/d/1xhpwReG7HT8wVtVLe51NzDcmByb1dM2J/view?usp=drive_link

-----END of ASSIGNMENT-----