

CA3 Project report

For

[INT301] [Open Source Technologies]

Submitted in partial fulfilment of the requirements for the award of degree of

B.Tech. CSE

LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA, PUNJAB



Submitted By

Name of student: Sankalp Jadon

Registration Number: 11918858

Submitted To

Dr. Manjot Kaur

Task to be performed –

Use any open source software to generate your entire system's log report along with this find partial and full multimedia files(video files) in DataStream.

Chapter 1 - INTRODUCTION

1.1 Objective of the project

The objective of this project is to generate a comprehensive log report of the entire system using the open source forensic software Winaudit. The log report will contain detailed information about the system's activities, including the operating system, hardware, software applications, network connections, and user activities. Additionally, the project aims to identify and extract full and partial multimedia files, specifically video files, from the system's DataStream.

Winaudit is a powerful tool that enables forensic investigators to analyze and report on a wide range of system activities. It provides detailed information about hardware, software, network connections, user accounts, and system settings. By using Winaudit, we can gain a comprehensive understanding of the system's behavior, which can be helpful in identifying potential security issues, system vulnerabilities, and other critical information.

1.2 Description of the project

The project involves using Winaudit to collect and analyze data from a target system, including system configuration, software applications, network connections, and user activities. Once the data has been collected, we will use the software to generate a comprehensive log report, which will provide us with a detailed overview of the system's behavior.

In addition to the log report, we will also be identifying and extracting partial and full multimedia files from the system's DataStream, specifically video files. This will involve using Winaudit's advanced forensic analysis tools to locate and extract the relevant files from the system.

The project will provide us with valuable insights into the system's behavior, which can be used to identify potential security risks, system vulnerabilities, and other critical information. By using an open source forensic tool like Winaudit, we can ensure that our analysis is accurate, reliable, and unbiased.

1.3 Scope of the project

The scope of the project is to use Winaudit to collect and analyze data from a target system and generate a comprehensive log report that provides detailed information about the system's behavior. The log report will include information about the operating system, hardware, software applications, network connections, and user activities.

Additionally, we will be identifying and extracting partial and full multimedia files from the system's DataStream, specifically video files. This will involve using Winaudit's advanced forensic analysis tools to locate and extract the relevant files from the system.

The project's scope is limited to the use of Winaudit as the primary forensic analysis tool. We will not be using any other forensic software or tools during the project. However, we may use other open source tools to assist in the analysis or processing of the data collected by Winaudit.

The project's scope does not include any modifications to the target system, and we will not be altering any of the system's settings or configurations. The project is purely for analysis and reporting purposes and does not involve any changes to the system's behavior or operation.

Chapter 2 - SYSTEM DESCRIPTION

2.1 Target System Description

Target System is running Windows 10 Home operating system. Following are the system specification of the target system.

- Device name SankalpJadon
- Processor AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10 GHz
- Installed RAM 4.00 GB (3.45 GB usable)
- Device ID FA6C1A0C-283D-42E7-A989-33E67289D68C
- Product ID 00327-35851-58465-AAOEM
- System type 64-bit operating system, x64-based processor
- Edition Windows 10 Home Single Language
- Version 21H2
- Installed on 18-09-2021
- OS build 19044.2846
- Experience Windows Feature Experience Pack 120.2212.4190.0

Chapter 3 - Analysis Report

3.1 Project Flowchart

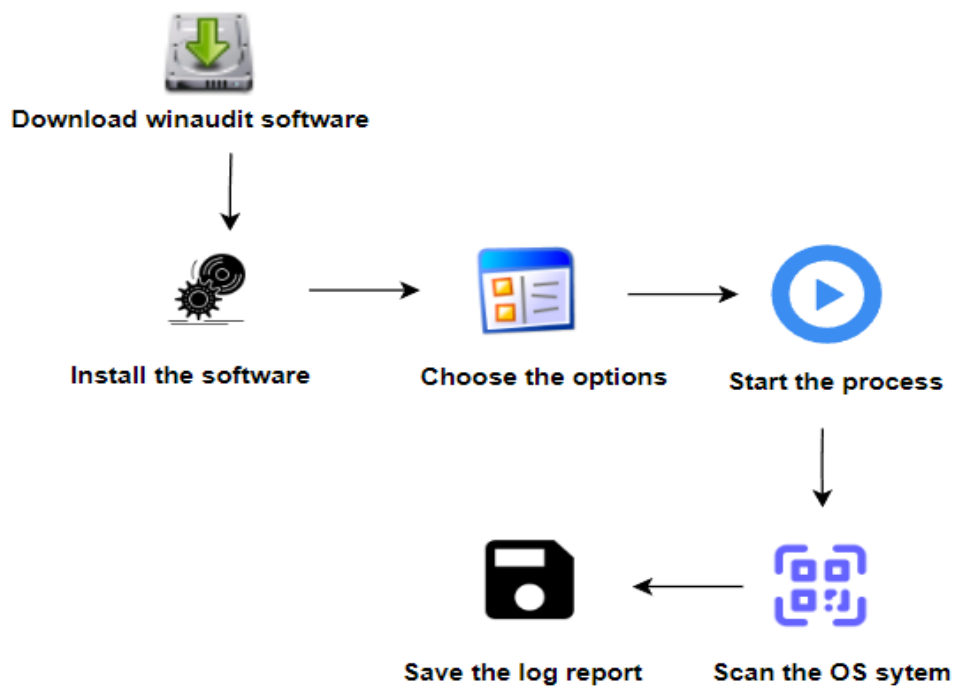


Fig 3.1 Project Flowchart

3.2 Downloading the software

Anyone can easily download the Winaudit Freeware v3.4.3 from internet . It is the most recent update, which was updated in 2022. Winaudit is a very light-weight software (0.7mb) . It comes as a zip file.

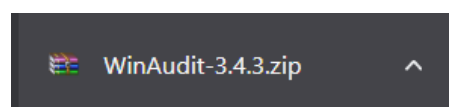


Fig 3.2 Downloaded zip file

3.3 Installing the software

Winaudit can easily be installed by following steps –

- Extract the Winaudit zip file


 WinAudit	24-10-2022 09:41	Application	1,956 KB
--	------------------	-------------	----------

Fig 3.3 Extracted Winaudit file

- And now it can run the software, as it is very light software which comes pre installed

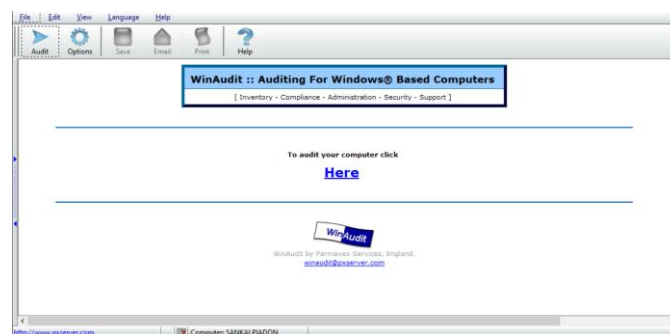


Fig 3.4 Application Interface

3.3 Editing and Choosing Options

Editing can be easily done using following steps –

- Go to Audit Options in **View -> Audit Options**

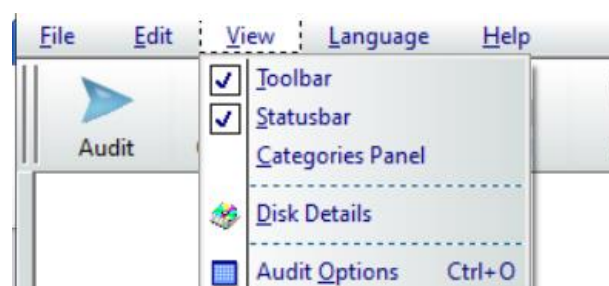


Fig 3.5 View Menu

- Now, choose the options needed in the log report

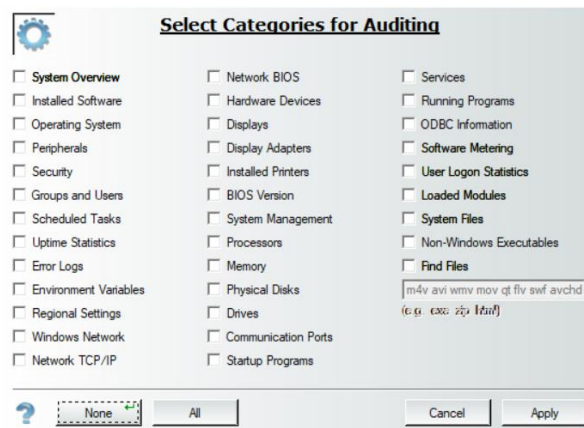


Fig 3.6 Categories Menu

- Select all the fields to create entire system log report .

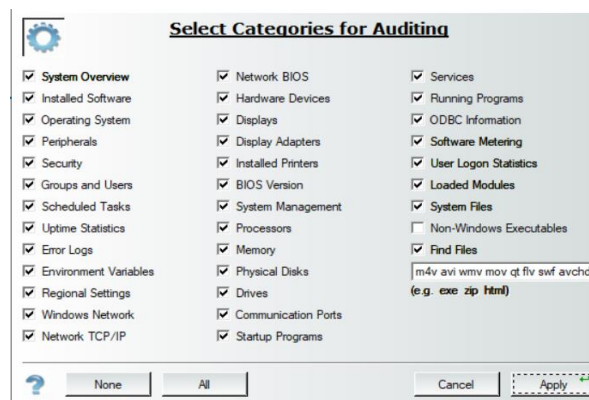


Fig 3.7 Selecting almost all the options

- Find files is the last option, which can be used to find the partial and full multimedia files (video) in the system. To search all the video files, we need to provide all video format extensions in the input field (.WEBM .MPG, .MP2, .MPEG, .MPE, .MPV .OGG .MP4, .M4P, .M4V .AVI .WMV .MOV, .QT .FLV, .SWF AVCHD)

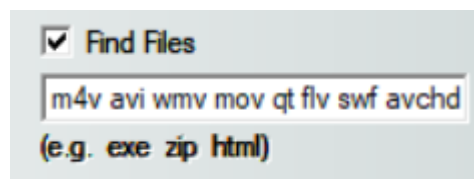


Fig 3.8 Inputting all the available video extensions

- Now , Click on apply to apply all the changes.

3.4 Start Scanning the System

- Now, click on Audit button in the tool bar.



Fig 3.8 Audit Button

- It will start scanning the system to create the log report. This process can also be stopped by clicking on the stop button.

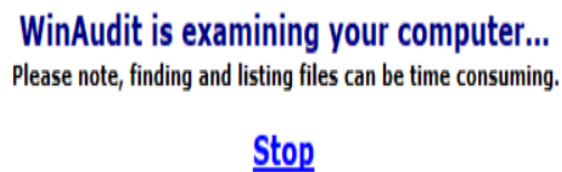


Fig 3.9 Winaudit started scanning the system to create a log report

3.5 Log Report

- After scanning, all the categories selected will be visible in the left panel

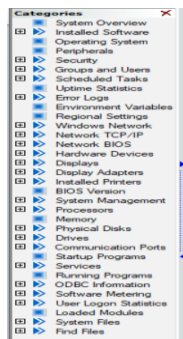


Fig 3.10 Categories Panel

- Video files will be available in the last under the find files name.

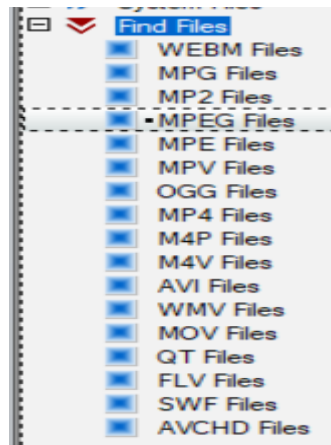


Fig 3.11 Video files in the category panel

- Any extension files can be easily viewed by selecting those files.

Name	File Size	Modified	Directory
I10BV39I.mp4	104 Bytes	05-04-2021 09:40:35	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I10OAL23.mp4	112 Bytes	04-04-2021 11:57:27	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I11RA92Q.mp4	104 Bytes	04-04-2021 11:57:27	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I13BFQZX.mp4	104 Bytes	04-04-2021 11:57:27	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1SEPK6.mp4	104 Bytes	05-04-2021 09:40:35	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I17W31NY.mp4	104 Bytes	04-04-2021 11:40:29	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I18KCPN6.mp4	104 Bytes	05-04-2021 09:40:35	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1CAG4CW.mp4	104 Bytes	04-04-2021 11:40:29	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1HHSH4O.mp4	104 Bytes	05-04-2021 09:40:35	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1IOPH69.mp4	104 Bytes	04-04-2021 11:40:29	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1LT9CKY.mp4	104 Bytes	04-04-2021 11:57:27	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1Q16WWA.mp4	104 Bytes	04-04-2021 11:40:29	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1QBTR7.mp4	104 Bytes	05-04-2021 09:40:35	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1TTU3K4.mp4	104 Bytes	04-04-2021 11:40:29	C:\\$Recycle.Bin\5-1-5-21-1580597 675-2918205653-3238981892-1001
I1V971QX.mp4	104 Bytes	05-04-2021 09:40:35	C:\\$Recycle.Bin\5-1-5-21-1580597

Fig 3.12 MP4 extension video files in the system

3.6 Saving the Log Report

- After generating the log report , it can be easily saved by clicking on the save button in the tool bar and selecting the destination

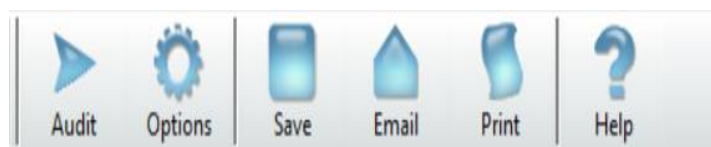


Fig 3.13 MP4 extension video files in the system

- Log report can be saved in different formats like csv, formatted text file or as a web page

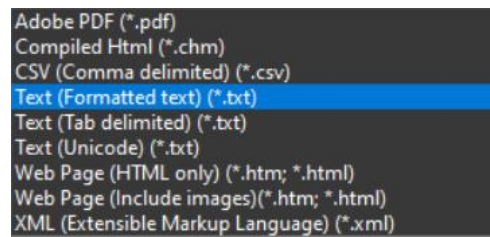


Fig 3.14 Different formats to save file

- Log report will then be saved in the destination



Fig 3.15 Save Log Report

References

- [1] <http://www.parmavex.co.uk/winaudit.html> (last accessed on 07-04-2023)
- [2] <https://app.diagrams.net/?src=about> (last accessed on 07-04-2023)
- [3] <https://www.portablefreeware.com/index.php?id=610> (last accessed on 06-04-2023)
- [4] <https://blog.filestack.com/thoughts-and-knowledge/complete-list-audio-video-file-formats/> (last accessed on 07-04-2023)