**GENUINENESS STUDY ON VIDEO USING CYBER FORENSICS**

**An Internship Report**

###### ***Submitted by***

**FATHIMA JEMINA M**

**(210181601014)**

***in partial fulfilment for the award of the degree of***

**BACHELOR OF TECHNOLOGY**

in

**COMPUTER SCIENCE AND ENGINEERING**



**JUNE 2023**



**BONAFIDE CERTIFICATE**

Certified that this project report “**GENUINENESS STUDY ON VIDEO USING CYBER FORENSICS**” is the bonafide work of “**FATHIMA JEMINA M(210181601014)**” who carried out the project work under my supervision. Certified further, that to the best of our knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

*SIGNATURE SIGNATURE*

**Dr. C HEMA Dr. AISHA BANU W.**

Associate Professor Professor and Head

Department of CSE Department of CSE

B.S. Abdur Rahman Crescent B.S. Abdur Rahman Crescent

Institute of Science and Technology Institute of Science and Technology

Vandalur, Chennai – 600 048 Vandalur, Chennai – 600 048





**VIVA VOCE EXAMINATION**

The viva voce examination of the project work titled **“GENUINENESS STUDY ON VIDEO USING CYBER FORENSICS”,** submitted by **FATHIMA JEMINA M(210181601014)** is held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**INTERNAL EXAMINER EXTERNAL EXAMINER**

**ACKNOWLEDGEMENT**

We sincerely express our heartfelt gratitude to **Dr. T. Murugesan**, Vice Chancellor,

B.S. Abdur Rahman Crescent Institute of Science and Technology, for providing us an environment to carry out our course successfully.

We sincerely thank **Dr. N. Raja Hussain,** Registrar, for furnishing every essential facility for doing our internship project.

We thank **Dr. Sharmila Sankar**, Professor and Dean, School of Computer, Information and Mathematical Sciences for her motivation and support.

We thank **Dr. Aisha Banu W,** Professor and Head, Department of Computer Science and Engineering, for providing strong oversight of vision, strategic direction and valuable suggestions.

We obliged our class advisor **Dr. C. Hema,** Associate Professor,Department of Computer Science and Engineering for her professional guidance and continued assistance during our internship.

We thank our internship mentor **Dr. Suthendran,** Cybersecurity Professional, SaiTechops LLP, Coimbatore for his inputs and guidance throughout the internship period.

We thank our internship coordinator, **Dr. Arunkumar Thangavelu,** Director, SaiTechOps LLP, Coimbatore for providing the internship opportunity.

We thank all the **Faculty members** and the **System Staff** of the Department of Computer Science and Engineering for their valuable support and assistance at various stages of project development.

**(FATHIMA JEMINA M)**

**ABSTRACT**

Ensuring the genuineness and integrity of video content has become a critical concern with the exponential growth in digital media and wide usage of videos in various domains. This study explores into the area of cyber forensics to establish strong methodologies for the authentication and verification of video content, addressing the escalating challenges posed by deepfakes, video manipulations, and other malicious activities.

The project employs a both theoretical frameworks and practical applications of cyber forensics techniques. By examining the digital evidence left during the creation, transmission, and storage of video files, the study aims to develop a comprehensive understanding of the vulnerabilities and potential points of exploitation within the video authentication process.

The investigation focuses on the identification and analysis of common video manipulation techniques and exploration of metadata and digital signatures associated with the video.

In conclusion, this internship project contributes to the evolving field of cyber forensics by providing a comprehensive framework for ensuring the genuineness of video content. The proposed methodologies and tools aim to mitigate the risks associated with video manipulation techniques thereby supporting the reliability of video evidence in legal proceedings, journalism, and other critical applications. This internship project also highlights the caution of analysing a video before forwarding to avoid being caught in the act of forgery.

**TABLE OF CONTENTS**

**CHAPTER NO TITLE PAGE NO**

[1. INTRODUCTION 5](#_Toc150540553)

[2. LITERATURE SURVEY 6](#_Toc150540554)

[3. PROBLEM STATEMENT 7](#_Toc150540555)

[4. METHODOLOGY 7](#_Toc150540556)

[4.1 Existing methodology 7](#_Toc150540557)

[4.2 Proposed Methodology 8](#_Toc150540558)

[5. HARDWARE ENVIRONMENT SETUP 9](#_Toc150540559)

[6. TOOL SELECTION 10](#_Toc150540561)

[6.1 Autopsy 10](#_Toc150540562)

[6.2 FTK Imager 11](#_Toc150540563)

[6.3 WinMD5 12](#_Toc150540564)

[6.4 Encase 13](#_Toc150540565)

[7. VIDEO FORENSIC APPROACH 14](#_Toc150540566)

[8. IDENTIFICATION 15](#_Toc150540567)

[9. VERIFICATION OF FILE INTEGRITY 15](#_Toc150540568)

[10. ANALYSIS AND EXAMINATION 16](#_Toc150540569)

[10.1 FTK Imaging 16](#_Toc150540570)

[10.1.1 Add Digital Evidence 16](#_Toc150540571)

[10.1.2 Create Disk Image 17](#_Toc150540572)

[10.2 Autopsy 18](#_Toc150540573)

[10.2.1 Create a case 18](#_Toc150540574)

[10.2.2 Data Acquisition and Processing 20](#_Toc150540575)

[10.2.3 Examining the evidence 22](#_Toc150540576)

[10.2.4 Findings 23](#_Toc150540577)

[10.3 Encase 24](#_Toc150540578)

[10.3.1 Examining the Evidence 24](#_Toc150540579)

[10.3.2 Findings 25](#_Toc150540580)

[11. GENUINE VIDEO ANALYSIS 25](#_Toc150540581)

[12. RESULT & CONCLUSION 26](#_Toc150540582)

[REFERENCES 27](#_Toc150540583)

[TECHNICAL BIOGRAPHY 28](#_Toc150540584)

**LIST OF FIGURES**

**FIGURE NO TITLE PAGE NO**

[Figure 1: Process of investigation 9](file:///I:\Intership\Internship_Report.docx#_Toc150540698)

[Figure 2: Stages of Digital Forensics 14](#_Toc150540699)

[Figure 3: Identification of Video source 15](#_Toc150540700)

[Figure 4: MD5 Verification 15](#_Toc150540701)

[Figure 5:Adding Evidence in FTK Imager 16](#_Toc150540702)

[Figure 6: Video to JPG converted evidence 17](#_Toc150540703)

[Figure 7: Create Image in FTK imager 17](#_Toc150540704)

[Figure 8: Viewing FTK imager analysis 18](#_Toc150540705)

[Figure 9: FTK imager process 18](#_Toc150540706)

[Figure 10: Autopsy 19](#_Toc150540707)

[Figure 11: Entering case details in Autopsy 19](#_Toc150540708)

[Figure 12: Additional case details 19](#_Toc150540709)

[Figure 13: Selecting Host in Autopsy 20](#_Toc150540710)

[Figure 14: Select Data Source 20](#_Toc150540711)

[Figure 15: Select Data Source 21](#_Toc150540712)

[Figure 16: Configure Ingest module 21](#_Toc150540713)

[Figure 17: Add Data Source 22](#_Toc150540714)

[Figure 18: Last Modified Time 23](#_Toc150540715)

[Figure 19: Video Handler 23](#_Toc150540716)

[Figure 20: AVC Coding 24](#_Toc150540717)

[Figure 21: Conversion of video to frames 24](#_Toc150540718)

[Figure 22: Copyleft 25](#_Toc150540719)

[Figure 23: Scene cut 25](#_Toc150540720)

[Figure 24: Intra-Refresh 25](#_Toc150540721)

[Figure 25: Genuine Video Analysis 25](#_Toc150540722)

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | **TITLE** | **PAGE NO.** |
| 5.1 | PC Setup | 9 |
| 5.2 | Pendrive Setup | 10 |
| 5.3 | Tool Selection | 10 |

# INTRODUCTION

Video manipulation is a very challenging domain that deals with the tampering and manipulation of digital images. The rise of easy-to-use video manipulation tools has placed unprecedented power in the hands of individuals. It has become a major concern for the whole society. Serious cases of Video Manipulation are increasing, and this alarms the law and order systems of the world. There are numerous video editing, enhancing, correction, modification, and recreation tools readily available, which encourages the commission of criminal acts.

A wide variety of tools for video forensic analysis have been developed. These tools can be used to attribute a video to the originating device, to reconstruct the past video compression history, and even to detect video manipulations. The applications of these methods range from educational videos to videos aimed at (mass) manipulation and [propaganda](https://en.wikipedia.org/wiki/Propaganda), a straightforward extension of the long-standing possibilities of [photo manipulation](https://en.wikipedia.org/wiki/Photo_manipulation).

These fake videos go viral leading to misinterpretations. Since fake videos go viral in minutes, one cannot differentiate between a genuine video and forged video. This form of computer-generated misinformation has contributed to [fake news](https://en.wikipedia.org/wiki/Fake_news), and there have been instances when this technology was used during political campaigns.

The metadata are used for video decoding and indicating other information such as the date, time, and location of the video when created. Because video editing tools tend to cause large structural changes in metadata, it is difficult for one to alter a video file without leaving any metadata traces.

The main objective of this project is to identify the genuineness of a video using meta data analysis for video forensic of the MP4 video format sent through social media. In this report, the results of using the metadata in MP4 files is examined for video forensic scenarios. Also, the main objective is to inform the users to be cautious of any video before forwarding it to others through social media.

# 2. LITERATURE SURVEY

In the modern society, videos are manipulated by wrong-doers to create a false statement about the victim. Most of the videos which become viral have a large opportunity of bring fake. These video manipulations are mostly commonly found in military and politics which lead to false rumours about certain aspects. Although, the political party or military may have referenced a different topic, the wrong doer’s forge the video to make it resemble the political or military said the statement in the forged video.

Few examples include the video of military jets posted on TikTok during Ukraine-Russia War[[1],](#RussiaWar) ‘Dhakka Start’ train push from Jawans[[2]](#Jawan) and Rahul Gandhi[[3]](#RahulGandhi) Targeted in Clipped Video on Loan Waivers.

In the military jets video, it was actually the historical footage captured as live video which lead to misleading information. The video was edited to make the visuals look real to mislead people into believing the launch of missiles.

In the ‘Dhakka Start’ train push, the video was edited such that it seemed Jawans and railway staff helped to push start the train. But in reality, it was the railway personnel and police who helped detached the coaches to avoid spread of fire.

In Rahul Ghandi’s case, a viral video spread on social media which contained mixing of two clips of Congress president making contradictory claims on farm loan waivers. In the first few seconds of the clip, Rahul Ghandhi makes a statement about not waiving farmer’s loan. This clip was from 2013 which was merged with the 2018 clip where Rahul Gandhi promises to waive off farmer loans leading to mislead information.

Some approaches proposed for Video forgery analysis are usage of Deep Learning for Deep Fake Detection, Atom structure analysis. Tools like Autopsy and Encase are also used to analyse and find the genuineness of a video.

# 3. PROBLEM STATEMENT

Videos are easily manipulated and edited to mislead and spread false information. Manipulation of video causes certain evidence to be proven false. For example, cctv footages or video recordings which are edited cannot be used as alibi unless it is completely analysed and declared as genuine or forged video. Hence it is important to analyse the video and its contents before declaring it as an evidence of the case.

In this project, we are analysing the genuineness of a video and determine the factors to find if it is a genuine video. The main objectives of this project are:

* To find the genuineness of the video
* To determine the factors which identify whether a video is fake or genuine
* To analyse the metadata of the video
* Using tools to analyse the contents of the video

# 

# 4. METHODOLOGY

In this section the different methodologies used to approach the problem are mentioned. The idea proposed to solve the problem is also mention.

## **4.1 Existing methodology**

One of the existing methodologies is to use the Exiftool method, by comparing 2 MP4 format videos. This method analyses the authenticity of a video not only through metadata analysis techniques but also using hash analysis techniques contained in videos.

Analysis of the hash contained in the video will use the Forevid tool which is expected to facilitate the detection of the authenticity of a video. [[4]](#Methodology)

In this paper, they’ve only analysed the metadata and verified the hash value. Hash comparison require the original video to be present as well. This is one of the drawbacks of this project.

## **4.2 Proposed Methodology**

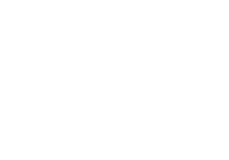
In this project, the video is analysed using Autopsy and Encase to find whether it is genuine or fake. The metadata of the video file is taken into analysis. From the hex dump of the video, if the video is forged we can obtain evidence like video editing tools used, copyright information and other software used to manipulate the video. The metadata of the video can also be analysed to find out the date of creation, MD5 hash value etc.

In this project, we have also analysed the video by converting it into frames. Each frame’s metadata is analysed to find any difference between the frames of the video as mentioned in Figure 1.

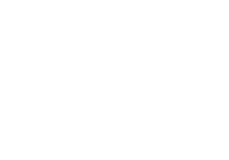
Firstly, the image of the video is taken using FTK imager. Then the metadata of the video is analysed using Autopsy and Encase. If any suspicious information is found, then the video is declared as forged or fake. The video is converted into frames using online converter. The frames are imaged and analysed to find any suspicious metadata.

To find the genuineness of the video, a normal video is taken and compared with the forged video. The difference of metadata information can be used to declare that the video is not genuine and it is forged.

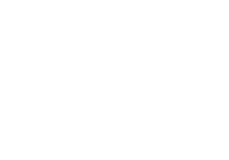
**Process of the Investigation:**



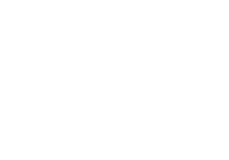
Identification of video



Preservation and generation of hash value

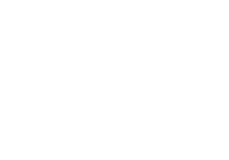


Converting video into frames and copying it, obtained video and genuine vide into a pen drive



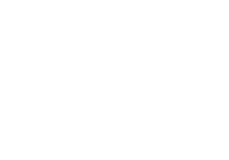
Data Acquisition & Processing using

FTK imager



Examination and Analysing using Autopsy,

Encase



Report & Conclusion

Figure 1: Process of investigation

# 5. HARDWARE ENVIRONMENT SETUP

|  |  |
| --- | --- |
| **Device Model** | PC |
| **OS Version** | Windows 10 |
| **Usage** | Used to create and analyze the disk image of pen drive created using Autopsy and Encase |

*Table 5.1: PC Setup*

|  |  |
| --- | --- |
| **Device Model** | SanDisk Cruzer Pen drive |
| **Capacity** | 8GB |
| **Usage** | Used for copying video |

*Table 5.2: Pendrive Setup*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool Name** | Autopsy | Encase | FTK Imager |
| **Version** | 4.20.0 | 22.3 | 4.7.1.2 |

*Table 5.3: Tools*

# 6. TOOL SELECTION

In this section, the tools used to analyse the genuineness of a video are listed. The reason for choosing the specific tool is also mentioned.

## **6.1 Autopsy**

Autopsy[[5]](#autopsy)is computer software that makes it simpler to deploy many of the open source programs and plugins used in [The Sleuth Kit](https://en.wikipedia.org/wiki/The_Sleuth_Kit). 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. It is an open source tool.

The tool is largely maintained by [Basis Technology Corp.](https://en.wikipedia.org/wiki/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 analyse all or part of the underlying data source.
* **Centralized** — 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.

**Features:**

Beyond standard features such as hash analysis, keyword search, and registry analysis, Autopsy offers advanced features not found in commercial tools:

* Enhanced timeline analysis. Parallel file analysis in multi-core systems, enabling fast results.
* Multiple examiners working on the same case at the same time.
* Python scripting support allows users to add custom features at any time.
* These features, or modules, are shared throughout the forensics community and at the annual Open Source Digital Forensics Conference (#OSDFCon).

**Why Autopsy?**

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

## **6.2 FTK Imager**

FTK Imager[[6]](#ftk) is a data preview and imaging tool used to acquire digital evidence in a forensically sound manner by creating copies of data without changing the original in any way. The latest version supports the AFF4 format and execution on portable drives. It is an open source tool.

**Features:**

* Create forensic images of entire local hard drives, CDs and DVDs, thumb drives and other USB devices–or just the files and folders you need.
* Preview the contents of forensic images stored on local machines or network drives.
* Create hashes of files to verify data integrity using either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA-1).
* Another unique feature of FTK is its use of a shared case database. Rather than having multiple working copies of data sets, FTK uses only a single, central database for a single case.

**Why FTK imager?**

FTK Imager allows you to perform memory capture or registry capture on a live device, to recover passwords or other data stored in memory on the active device.

## **6.3 WinMD5**

WinMD5Free[[7]](#winmd5)is a tiny and fast utility to compute MD5 hash value for files. WinMD5 is a small and easy tool to calculate md5 hash or checksum for different files. It is an open source tool.

**Features:**

* Supports almost all Windows platforms including Microsoft Windows XP, Vista, Windows 7, 8, 10, and Windows 11.
* Fast and multi-threaded. It can compute a 2 GB file less than 1 minute.
* Supports big files larger than 4 GB.
* Low resource usage. It uses less than 5 MB RAM.
* Don’t require .NET runtime installed. It is a standalone EXE file and the start-up is speedy. There are MD5 tools for Windows on the market, but most of them requires .NET runtime and they may take a few seconds to start. This is also the reason I wrote the program.
* Supports “Drag & Drop”. You may either select a file, or drag and drop a file to the program window to get the MD5 hash value.
* Supports verification of original MD5 value and current MD5 value.
* Most important, it is FREE. No spyware or adware bundle.
* Small size, an effective and tiny tool for data security.

**Why WinMD5?**

As an Internet standard (RFC 1321), MD5 has been used in a wide variety of security applications, and is also commonly used to check the integrity of file, and verify download.

## **6.4 Encase**

EnCase[[8]](#encase) is the shared technology within a suite of digital investigations products by Guidance Software (acquired by OpenText in 2017). The software comes in several products designed for forensic, cyber security, security analytics, and e-discovery use.

EnCase is traditionally used in forensics to recover evidence from seized hard drives. It allows the investigator to conduct in-depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry. It is a licensed software.

**Features:**

* Acquire from Almost Anywhere
* Forensically Sound Acquisition
* Advanced Analysis
* Improved Productivity
* Automated de-NISTing Capabilities
* Multiple File Viewer Support

**Why Encase?**

* Unmatched performance
* Court-accepted evidence format
* Superior efficiency
* In-depth evidence investigation

# 7. VIDEO FORENSIC APPROACH

Cyber Forensics deals with the extraction and recovery of data as evidence against a crime. A cyber forensic investigation can help to identify and prove different types of thefts committed by a criminal.

The stages followed in digital forensics (Figure 2):

* Identification
* Preservation
* Analysis
* Documentation
* Presentation

Figure 2: Stages of Digital Forensics

# 8. IDENTIFICATION

Identification is the first stage of digital forensics. In this process, the video is obtained through social media(Whatsapp) and the data about video is analysed.

Source of video (Figure 3): <https://www.pexels.com/>



Figure 3: Identification of Video source

# 9. VERIFICATION OF FILE INTEGRITY

The hash value of the video is noted before imaging and analysis using winMD5. If any tampering occurs during Autopsy or Encase analysis, it can be used to verify the integrity of the analysed video.

The MD5 (message-digest algorithm) hashing algorithm as shown in Figure 4, is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message. It is one of the most commonly used hash algorithms.

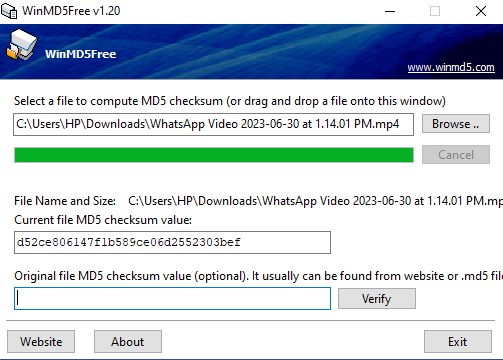


Figure 4: MD5 Verification

# 10. ANALYSIS AND EXAMINATION

In this section the data is analysed through tools like Autopsy and Encase for evidence. The metadata is analysed and the result is documented. The result of the analysis is noted down.

The following analysis method is executed:

* Obtained Video Analysis using Autopsy and Encase
* Genuine Video Analysis using Autopsy and Encase
* Conversion of Video to Frames analysis

## **10.1 FTK Imaging**

The following files are copied into the pen drive: obtained video, converted frames of video and genuine video. The image of the pen drive is taken using FTK imager and the evidence is analysed.

### **10.1.1 Add Digital Evidence**

Install FTK imager and add the digital evidence for which the image will be captured as shown in Figure 5 and Figure 6.

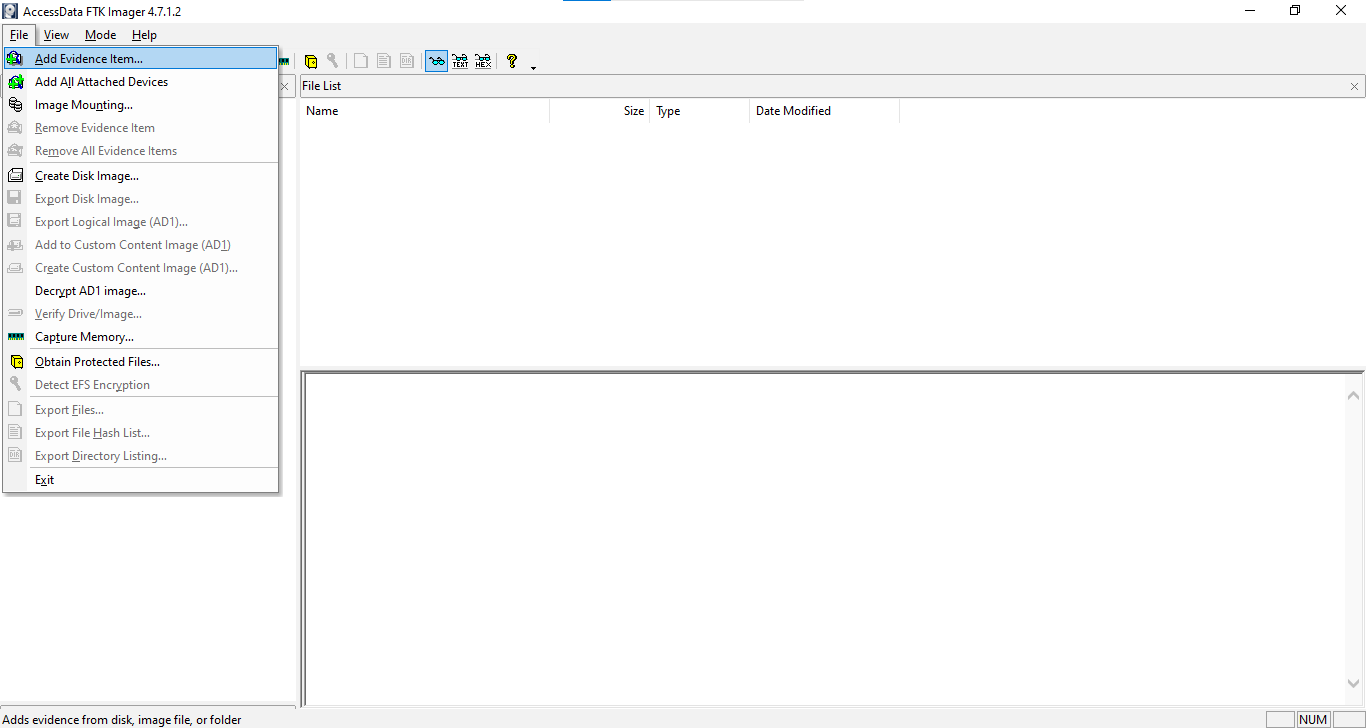


Figure 5:Adding Evidence in FTK Imager

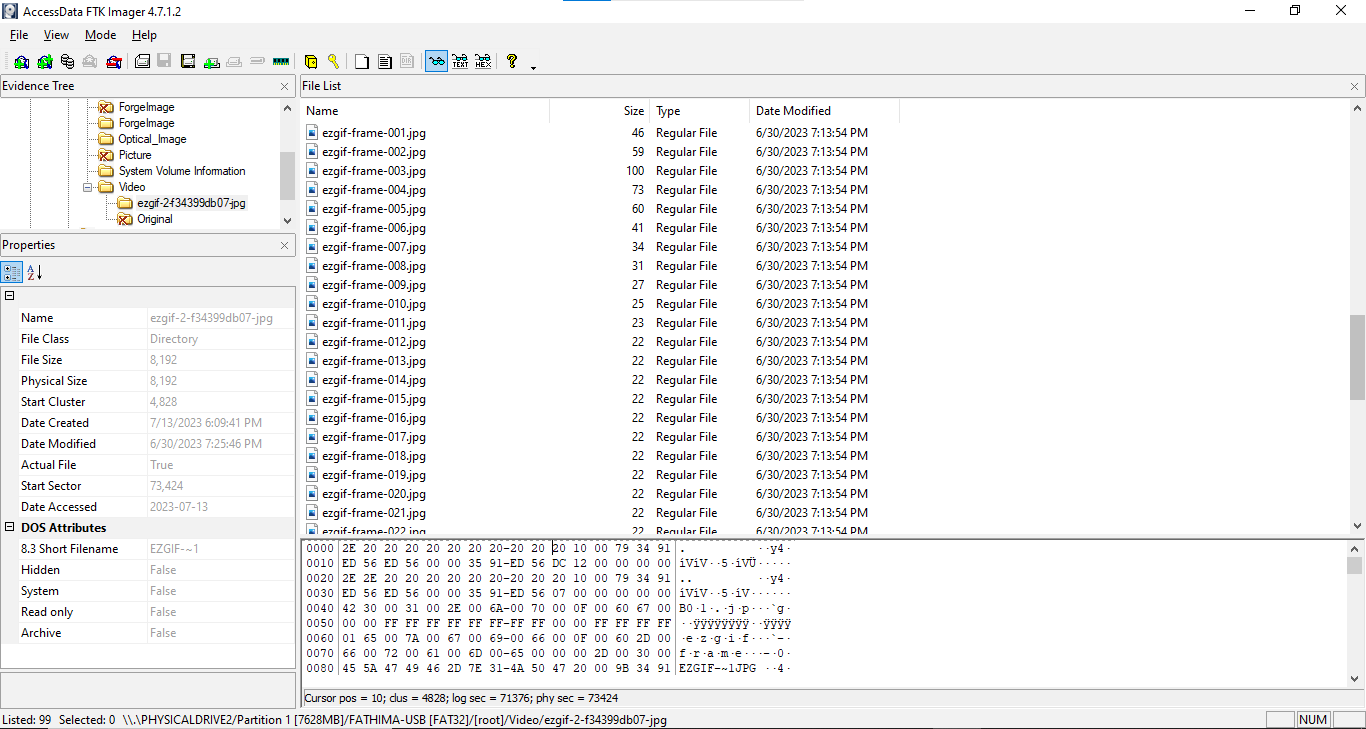


Figure 6: Video to JPG converted evidence

### **10.1.2 Create Disk Image**

Create a disk image of the pen drive. Steps to be followed:

1) Click on create image and fill in the details to proceed (Figure 7).

2) Image will be stored in the desired location. You can check for the progress of the image in that location (Figure 8).

3) FTK imager also generates hash value for the imaged pen drive (Figure 9).

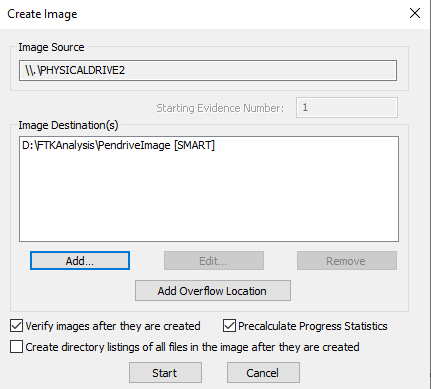


Figure 7: Create Image in FTK imager

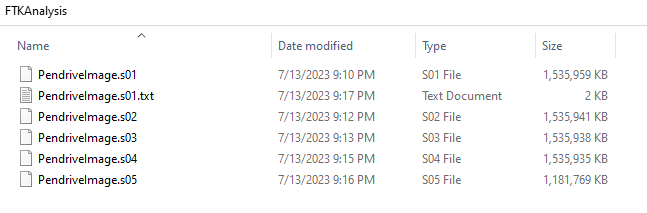


Figure 8: Viewing FTK imager analysis

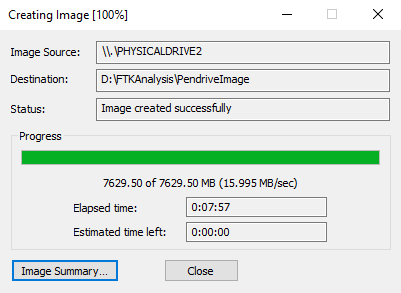


Figure 9: FTK imager process

## **10.2 Autopsy**

In this section, the imaged pen drive is analysed using Autopsy. Autopsy has ingest modules to find evidence about the investigation. Any suspicious file will be marked under the ‘S’ column. Any file that occurs in other case which is included in the current case will be counted under the ‘O’ column. Any file that has comments will be notified under the ‘C’ column.

### **10.2.1 Create a case**

After installing Autopsy, open the extension. You will see a dialogue box asking whether to create a case, open a case or open recent case.

**STEP 1:**

Click on ‘New Case’ and proceed as shown in Figure 10.



Figure 10: Autopsy

**STEP 2:**

Enter the case information and choose the base directory of the case and click “Next” as shown in Figure 11.

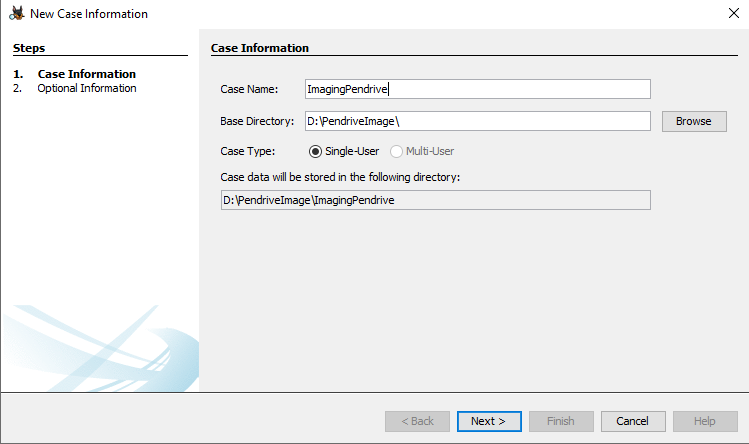


Figure 11: Entering case details in Autopsy

**STEP 3:**

Enter case details and click “Next” as shown in Figure 12.

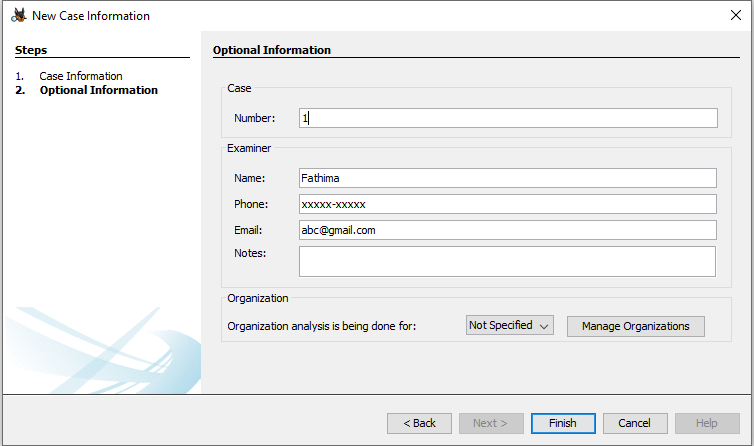


Figure 12: Additional case details

**STEP 4:**

Select the Host and click ‘Next’ as shown in Figure 13.

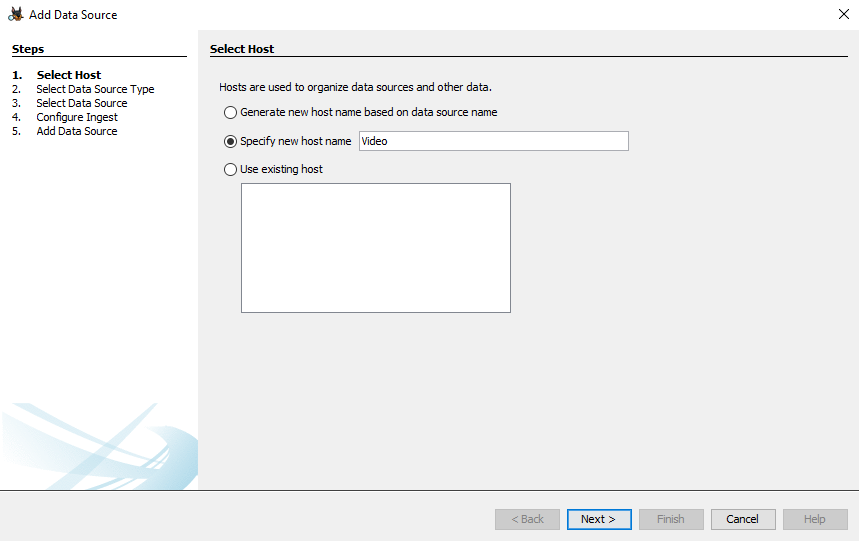


Figure 13: Selecting Host in Autopsy

### **10.2.2 Data Acquisition and Processing**

In this section, the imaged pen drive is acquired and processed for the forensic analysis

**STEP 1:**

Select Data Source Type and click ‘Next’ as shown in Figure 14.

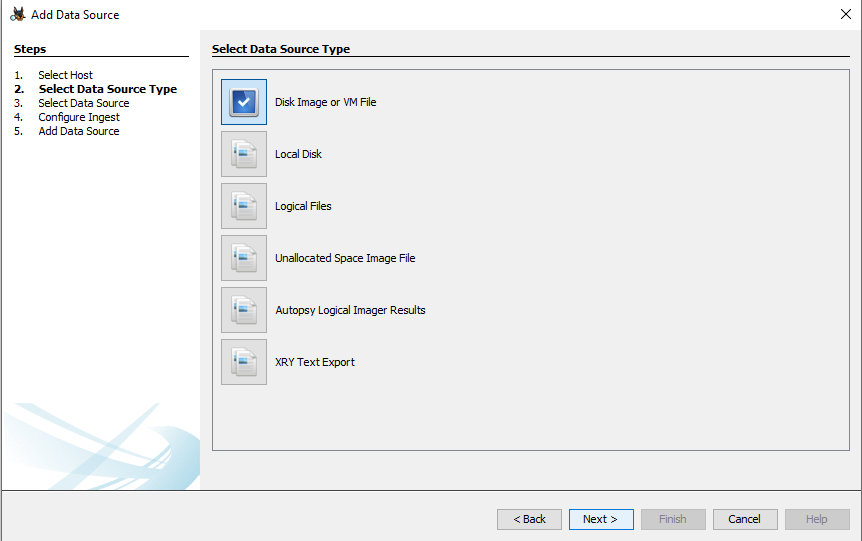


Figure 14: Select Data Source

**STEP 2:**

Select the data source, select the path to point to the first image in the FTK image destination folder and click ‘Next’ as shown in Figure 15.

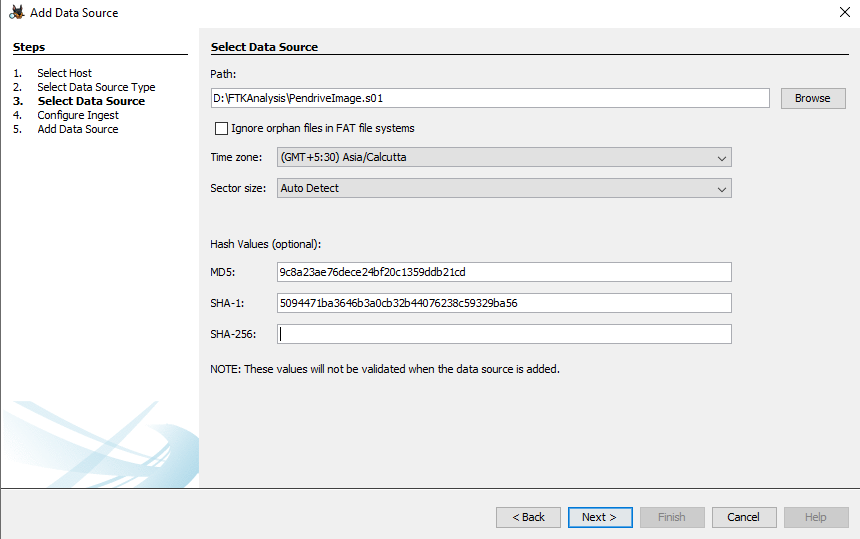


Figure 15: Select Data Source

**STEP 3:**

Configure the ingest modules and click ‘Next’ as shown in Figure 16.

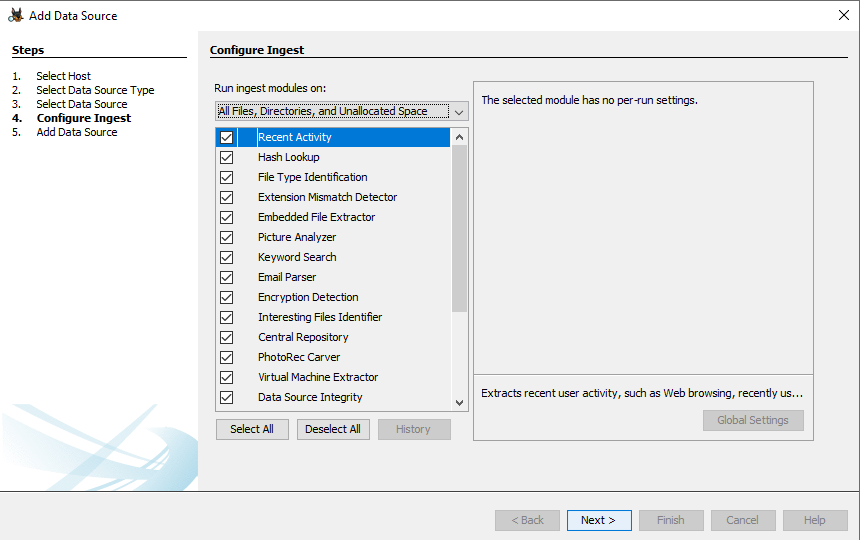


Figure 16: Configure Ingest module

**STEP 4:**

Wait until the data sources are added and analysed then click ‘Finish’ as shown in Figure 17.

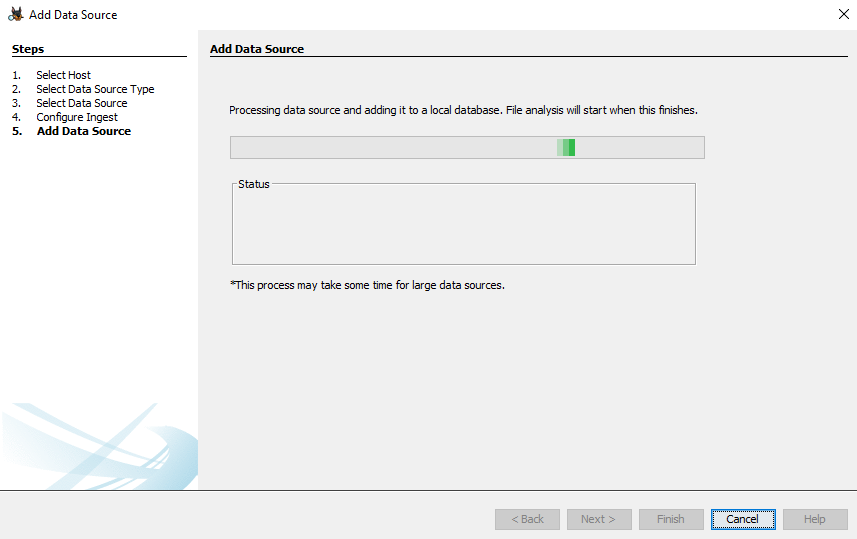


Figure 17: Add Data Source

### **10.2.3 Examining the evidence**

While analysing the video, we can find the format of the video which is ftyp, date of creation can also be found from last modified time (Figure 18).

While examining the evidence it can be found that copyleft was used in the video.

***Ftyp*** is designed as a flexible, extensible format that facilitates interchange, management, editing and presentation of the media.

***Video Handler:*** Video media handlers are responsible for interpreting and manipulating video data. It is used for uploading video in any format and make them play in any browser (Figure 19)

***AVC coding:*** Advanced Video Coding, also referred to as H.264 or MPEG-4 Part 10, is a video compression standard based on block-oriented, motion-compensated coding. This type of coding can only be found in videos that are edited or forged (Figure 20).

While analysing the converted frames of video, we can find that the format of the frames is lavc58.134 (Figure 21)

Also, we can find that the size of the first 11 frames differ whereas from 12th frame the size is constant.

### **10.2.4 Findings**

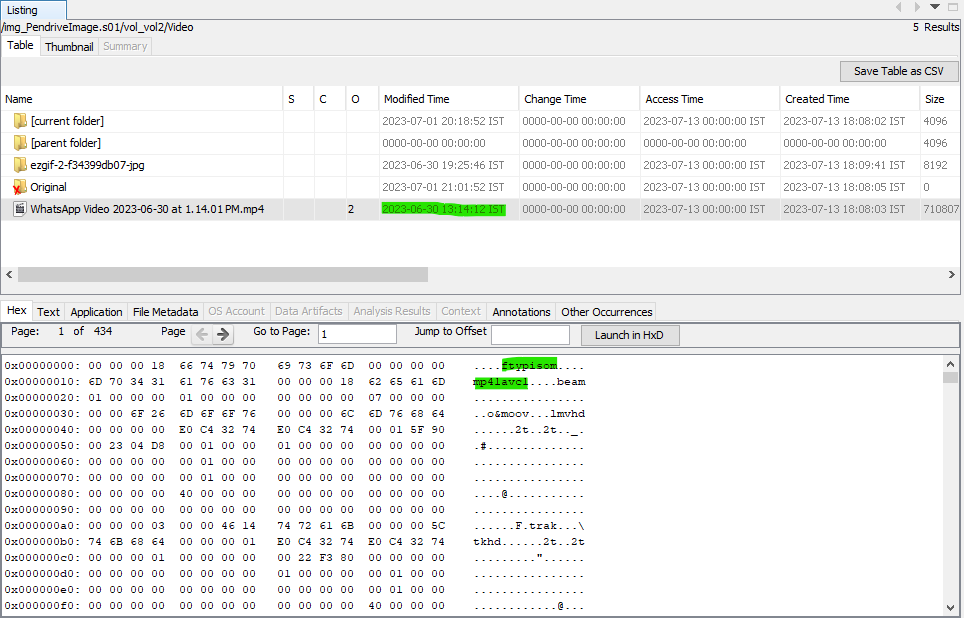


Figure 18: Last Modified Time

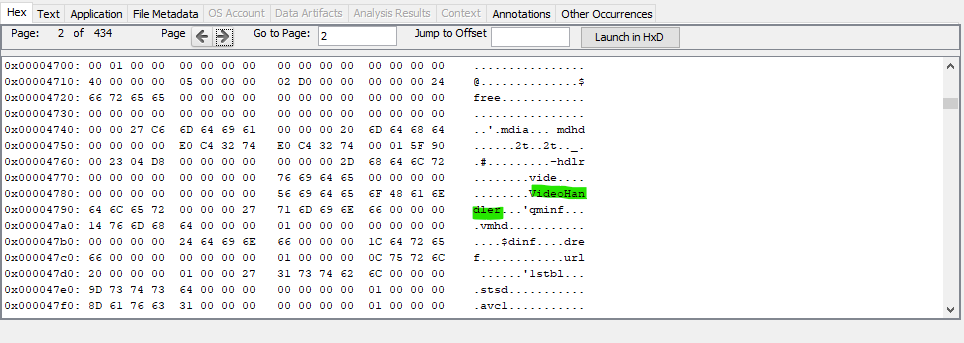


Figure 19: Video Handler

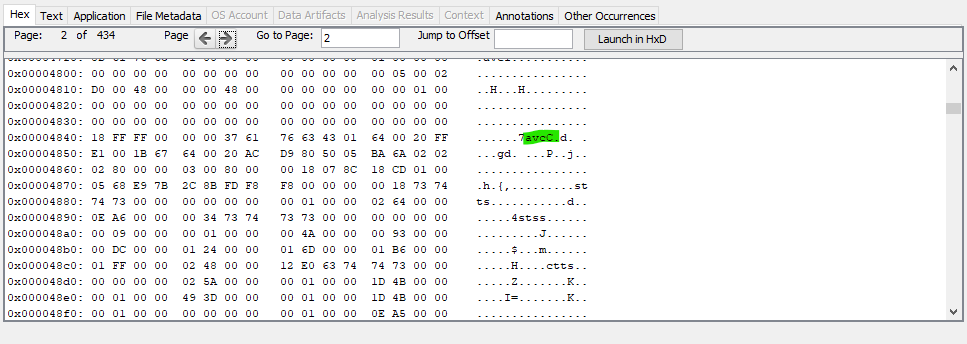


Figure 20: AVC Coding

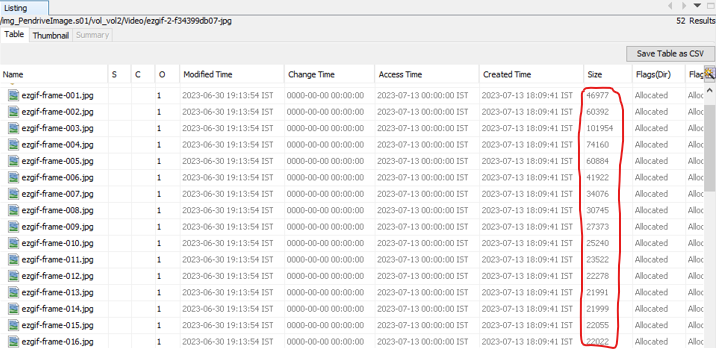


Figure 21: Conversion of video to frames

## **10.3 Encase**

In this section, the imaged pen drive is analysed using Encase. Encase has ingest modules to find evidence about the investigation.

### **10.3.1 Examining the Evidence**

While analysing the video, the following factors can be found:

***Copyleft:*** is the legal technique of granting certain freedoms over copies of copyrighted works with the requirement that the same rights be preserved in derivative works. It is collaboration of two companies. This video was created with the partnership of [www.videolan.org](http://www.videolan.org). (Figure 22)

***Scene cut:*** It splits an entire video into individual clips which can be used to create edited videos for forgery purpose. (Figure 23)

***Intra refresh:*** An intra refresh algorithm is presented which enables low-delay video communication at the efficiency of standard IP-coding schemes. (Figure 24)

### **10.3.2 Findings**



Figure 22: Copyleft



Figure 23: Scene cut



Figure 24: Intra-Refresh

# 

# 11. GENUINE VIDEO ANALYSIS

In an ordinary video file, the format is ftypmp4. Also, ordinary video file does not contain copyleft, scene cut or intra fresh as shown in Figure 25.

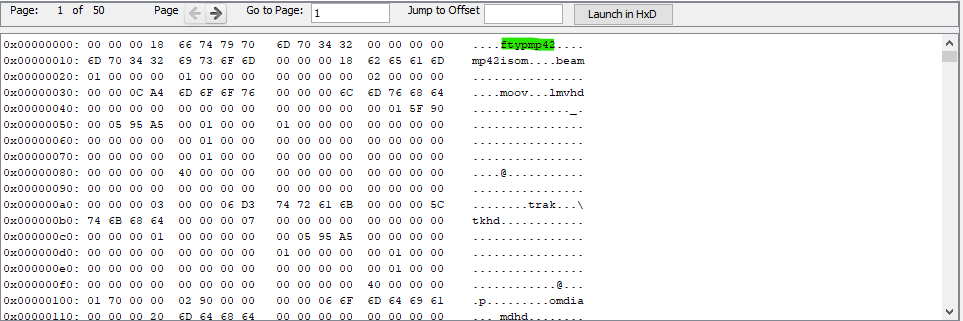


Figure 25: Genuine Video Analysis

# 

# 12. RESULT & CONCLUSION

After analysis of the video, it can be found that it is not original. It is an edited video and copyleft rights were used. Also, the video was edited using scene cut and low delay video communication was applied using Intra refresh. Also, the original date of creation of the video can be found while analysing the metadata of the video.

While comparing the forged video with an ordinary video, we can find that the ordinary video does not contain any of the editing tools or copyleft rights. It can also be found that the ordinary video is of mp4 format whereas the forged video is in isom format.

With these findings, it can be concluded that the video is not genuine and it has been manipulated. Thus, this also proves the importance of analysing a video before coming to a conclusion about its genuineness.

If videos are analysed, misinterpretation of information could be avoided and information can be verified of its genuineness. It should also be noted that one should not forward a video without knowing it’s genuineness. This will make it harder for the offenders to spread false information by manipulation of videos.

# REFERENCES

[1] Live capture of military jets during Russia-Ukraine War. <https://www.bbc.com/news/60867414>

[2] Train Push act by Jawans actually fake. <https://timesofindia.indiatimes.com/videos/viral-videos/fake-news-alert-dhakka-start-viral-train-video-flagged-jawans-didnt-push-start-train-says-railway/videoshow/101636547.cms>

[3] Rahul Gandhi Targeted in Clipped Video on Loan Waivers

<https://www.thequint.com/news/webqoof/rahul-gandhi-targeted-clipped-video-loan-waivers#read-more>

[4] FORENSIC ANALYSIS VIDEO METADATA AUTHENTICITY DETECTION USING EXIFTOOL <https://bajangjournal.com/index.php/JIRK/article/view/2227/1605>

[5] Autopsy Slueth Kit:

<https://en.wikipedia.org/wiki/Autopsy_(software)>

<https://www.autopsy.com/>

<http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/>

<https://www.sleuthkit.org/autopsy/features.php>

[6] FTK imager: <https://www.exterro.com/ftk-imager>

<https://go.exterro.com/l/43312/2023-05-03/fc4b78>

[7] WinMD5: <https://www.winmd5.com/>

[8] Encase: <https://encase-forensic.software.informer.com/7.0/>

***Other references:***

Copyleft:<https://en.wikipedia.org/wiki/Copyleft#:~:text=Copyleft%20is%20the%20legal%20technique,be%20preserved%20in%20derivative%20works>.

Scene-cut: <https://twister-scenecut-hd.software.informer.com/>

Intra-refresh:<http://www.apsipa.org/proceedings_2014/data/paper/1018.pdf>

Ftyp: <https://dev.to/alfg/a-quick-dive-into-mp4-57fo>

Video Handler: <https://www.drupal.org/project/video_handler>

AVC Coding: <https://en.wikipedia.org/wiki/Advanced_Video_Coding>

# TECHNICAL BIOGRAPHY

**MEMBER 1**



**FATHIMA JEMINA M**  was born in Chennai, India in 2003. She is currently pursuing her B.Tech in Computer Science and Engineering (with specialization in Cyber Security) degree at B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai. She aspires to pursue a career in the domain of Cyber Security.

**Contact:** +91 9385435611 **| Email:** [fathijem1510@gmail.com](mailto:fathijem1510@gmail.com)