CBS 412

Multimedia Security & Forensics

LAB REPORT

SCENARIO BASED WORK

NAME: K. REVANTH

ROLL NO: 2021BCY0037

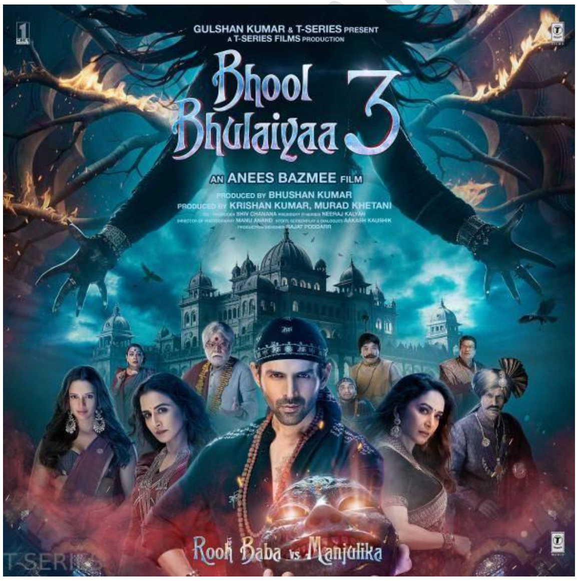
THE MOVIE PIRACY SYNDICATE

Pramod Kumar, a cybersecurity analyst at T-Series Productions, was alerted that their latest film, *Bhool Bhulaiyaa 3*, had been pirated and was available online shortly after its release, even before the film was released on OTT platforms. To investigate this breach, Pramod conducted a forensic audit using following techniques.

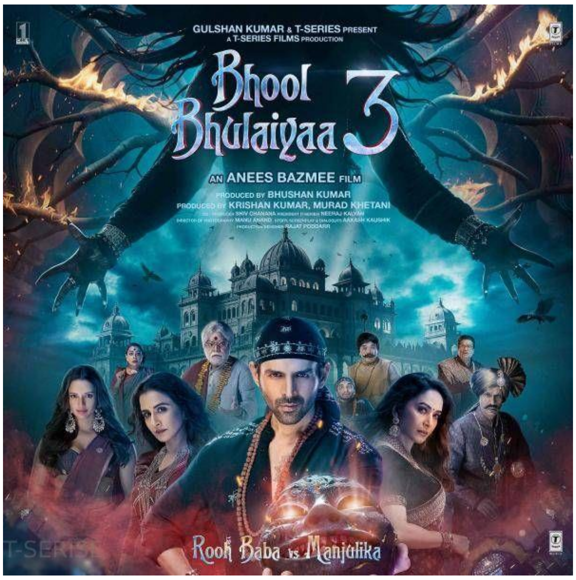
Step 1: Investigating the Pirated Poster

Pramod began by searching for pirated content online. He typed "*Bhool Bhulaiyaa 3 download*" into Google and found a suspicious poster for the film in the search results. He downloaded this poster and compared it to the official poster available on the T-Series website.

// Original poster



// Pirated poster



He followed the below ways to check the validity of the poster:

- **Metadata Analysis**

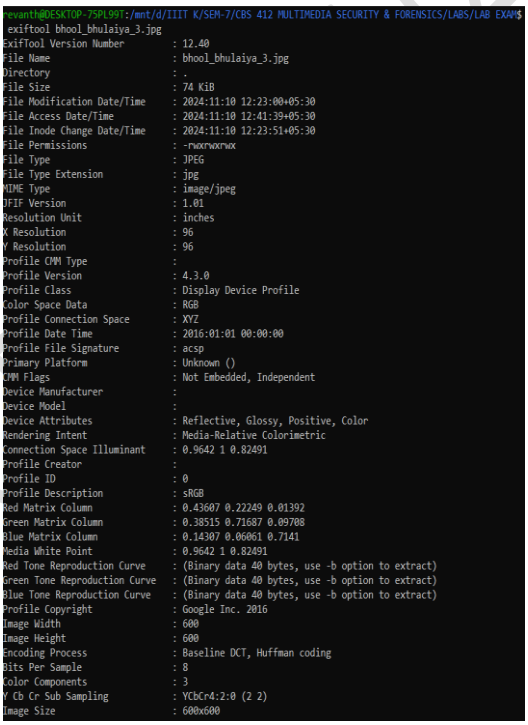
Metadata contains descriptive and technical information about the file itself, including details like creation date, modification history, file format, author information, device settings, and software used to create or edit the file. Metadata Analysis refers to the examination of the hidden data stored within digital files. Metadata analysis is used to authenticate files, identify file origins, track modifications, or extract forensic evidence.

Pramod used the following command to analyse the metadata of both posters:

```
exiftool bhool_bhulaiya_3.jpg
```

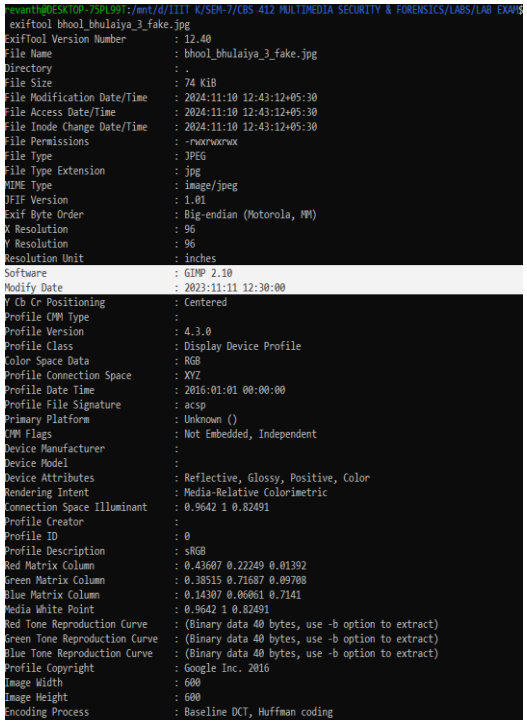
```
exiftool bhool_bhulaiya_3_fake.jpg
```

// Original poster metadata



```
evanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 exiftool bhool_bhulaiya_3.jpg
ExifTool Version Number         : 12.40
File Name                       : bhool_bhulaiya_3.jpg
Directory                       : .
File Size                       : 74 KiB
File Modification Date/Time     : 2024:11:10 12:23:00+05:30
File Access Date/Time           : 2024:11:10 12:41:39+05:30
File Inode Change Date/Time     : 2024:11:10 12:23:51+05:30
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Profile CMM Type                :
Profile Version                 : 4.3.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2016:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Unknown ()
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Media-Relative Colorimetric
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 :
Profile ID                      : 0
Profile Description             : sRGB
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Media White Point               : 0.9642 1 0.82491
Red Tone Reproduction Curve     : (Binary data 40 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 40 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 40 bytes, use -b option to extract)
Profile Copyright               : Google Inc. 2016
Image Width                     : 600
Image Height                    : 600
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 600x600
```

// Pirated poster metadata



```
evanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 exiftool bhool_bhulaiya_3_fake.jpg
ExifTool Version Number         : 12.40
File Name                       : bhool_bhulaiya_3_fake.jpg
Directory                       : .
File Size                       : 74 KiB
File Modification Date/Time     : 2024:11:10 12:43:12+05:30
File Access Date/Time           : 2024:11:10 12:43:12+05:30
File Inode Change Date/Time     : 2024:11:10 12:43:12+05:30
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 96
Y Resolution                    : 96
Resolution Unit                 : inches
Software                        : GIMP 2.10
Modify Date                     : 2023:11:11 12:30:00
Y Cb Cr Positioning             : Centered
Profile CMM Type                :
Profile Version                 : 4.3.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2016:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Unknown ()
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Media-Relative Colorimetric
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 :
Profile ID                      : 0
Profile Description             : sRGB
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Media White Point               : 0.9642 1 0.82491
Red Tone Reproduction Curve     : (Binary data 40 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 40 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 40 bytes, use -b option to extract)
Profile Copyright               : Google Inc. 2016
Image Width                     : 600
Image Height                    : 600
Encoding Process                : Baseline DCT, Huffman coding
```

By comparing the metadata, Pramod identified discrepancies in the pirated poster (bhool_bhulaiya_3_fake.jpg). Two additional fields, ***Software*** and ***Modify Date***, were present in the pirated

version, indicating it had been altered with external software after its creation.

To further verify tampering, Pramod used the below technique.

- **Error Level Analysis (ELA):**

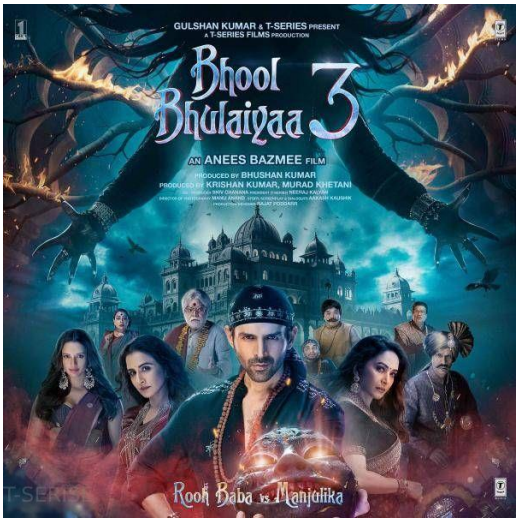
Error Level Analysis (ELA) is a forensic technique used to identify areas of an image that have been modified or tampered with. It works by analysing the compression levels in a digital image, particularly in JPEG files, which use lossy compression. When an image is saved as a JPEG, different areas of the image are compressed at various levels. ELA helps detect inconsistencies in the compression across different parts of the image. If an image has been altered (e.g., an object added, removed, or modified), the edited areas will have different compression characteristics than the rest of the image, as they may have been recompressed separately from the untouched areas.

Pramod used an external tool, **FotoForensics**, to perform ELA. He uploaded the pirated poster to see the results.

In the results obtained below, he noticed a clear anomaly in the lower-left corner of the image. The area surrounding the watermark

was inconsistent with the rest of the image, indicating that the watermark had likely been forged.

// ELA Output



To confirm it further, he tried to find Visual Anomalies as below.

- **Visual Anomalies**

Upon closely examining both the official and pirated posters, Pramod found more evidence of forgery. The background in the pirated poster was blurred near the watermark, the space between the watermark and the bottom edge had increased, and the company name was misspelled as **“T-Serise”** instead of **“T-Series”**.

// Original

// Pirated

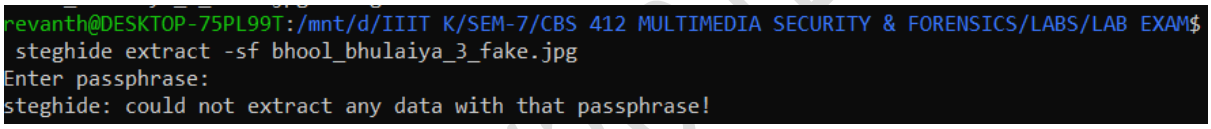
This confirmed that the watermark had been tampered with in the pirated poster.

<u>Step 2</u>: Steganalysis of the Pirated Poster

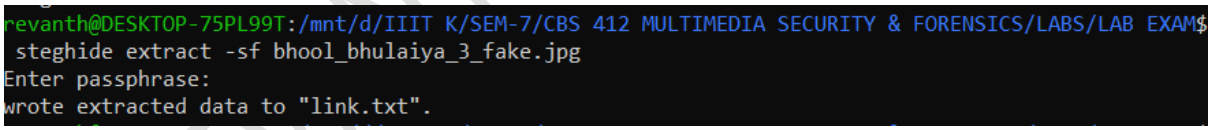
Steganalysis is the process of detecting and decoding hidden information (steganography) within digital media, such as images, audio, or text files. While steganography involves concealing data in seemingly harmless files, steganalysis focuses on uncovering these hidden messages or files by analyzing the media for irregularities or patterns that suggest data has been embedded covertly.

Next, Pramod suspected that the pirated poster might contain hidden data through steganography. To investigate, he used the **Steghide** tool and ran the following command to extract any concealed information:

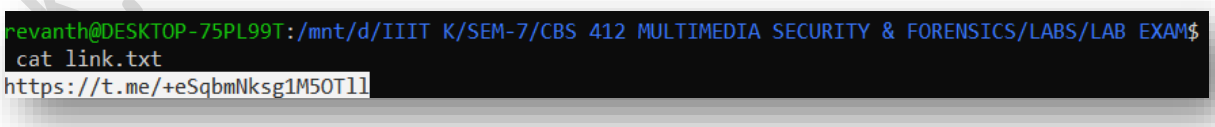
```
steghide extract -sf bhool_bhulaiya_3_fake.jpg
```



The tool prompted him for a passphrase. After trying several related terms, Pramod discovered that the word "***download***" was the correct passphrase.

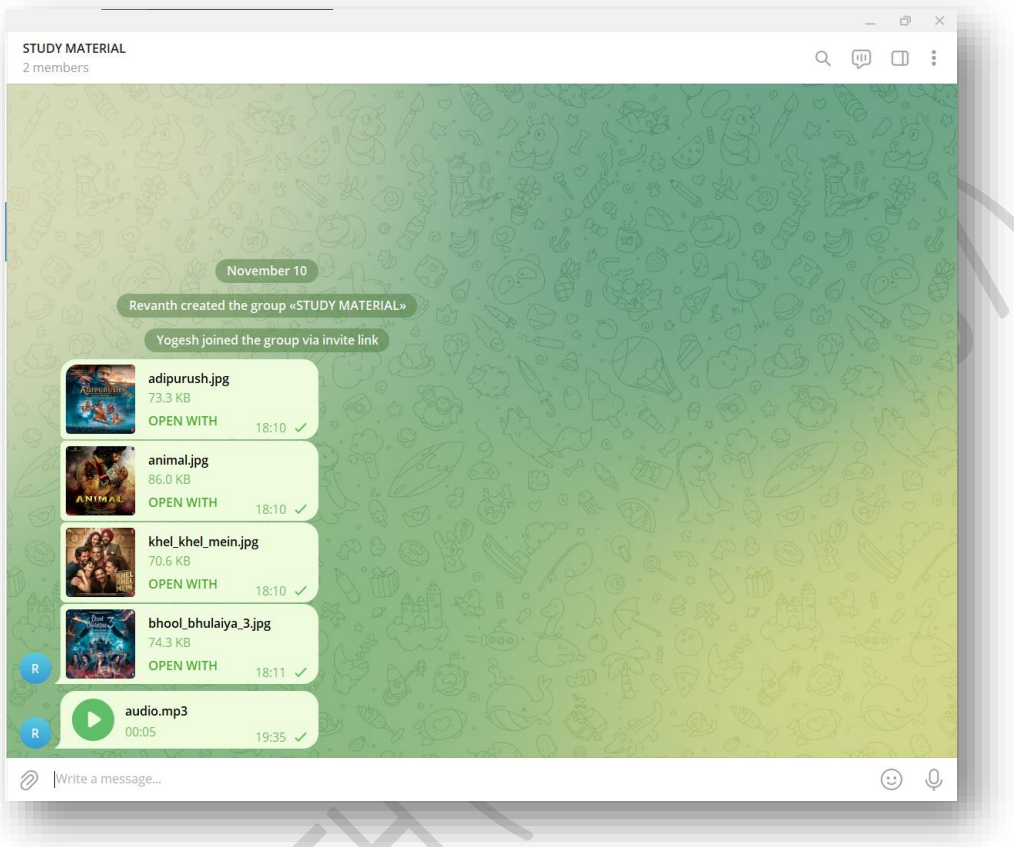


This allowed him to extract a hidden text file named *'link.txt'*.

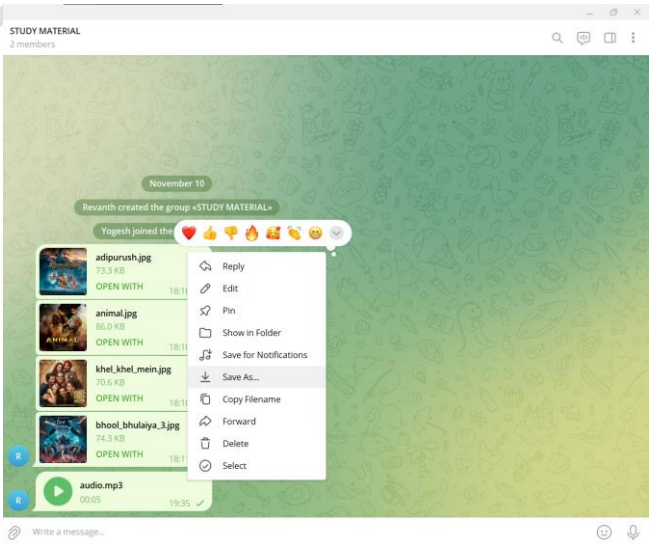


The text file contained a link (***https://t.me/+eSqbmNksg1M5OTll***) that redirected him to a Telegram group chat.

<u>Step 3</u>: Analysing the Telegram Group files

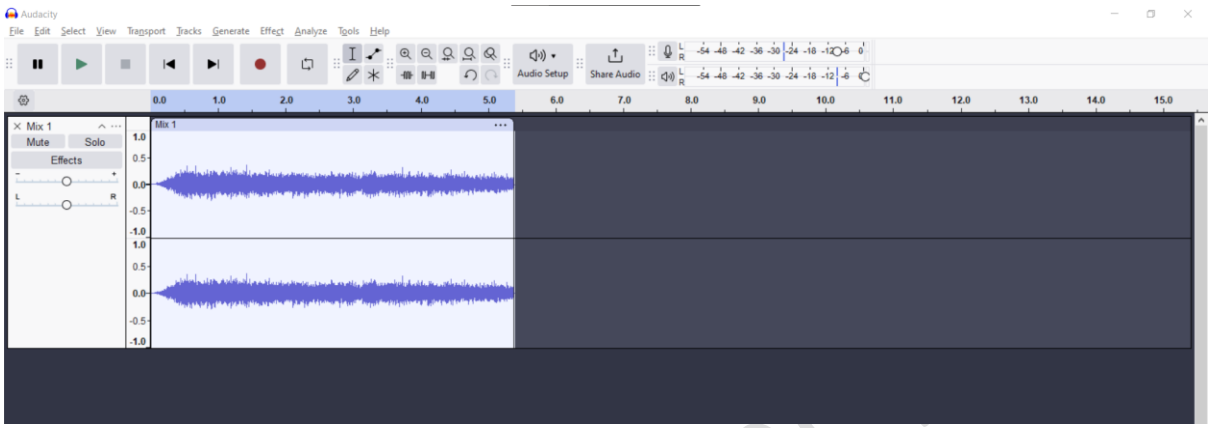


In the Telegram group, Pramod found four movie posters, including *Bhool Bhulaiyaa 3* poster, as well as an audio file. While the posters appeared normal at first glance, the audio clip was full of noise. Pramod downloaded the audio file and opened it in **Audacity** for further analysis.



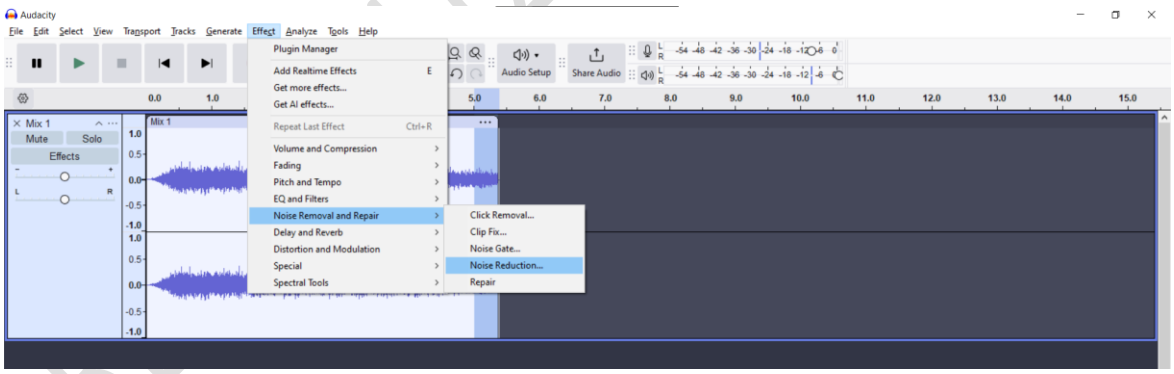
// Noisy audio

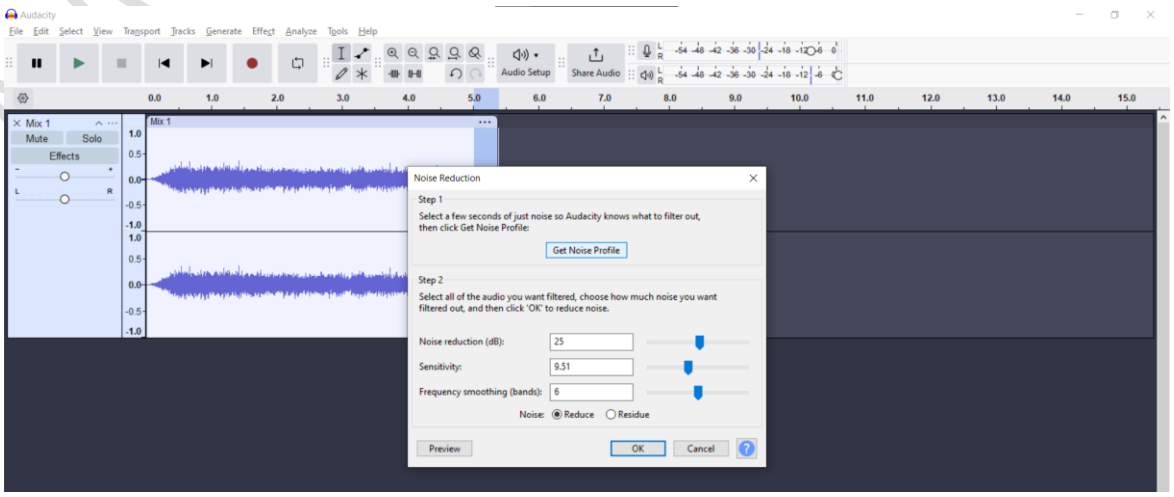
audio.mp3 (Double click to play the audio file)



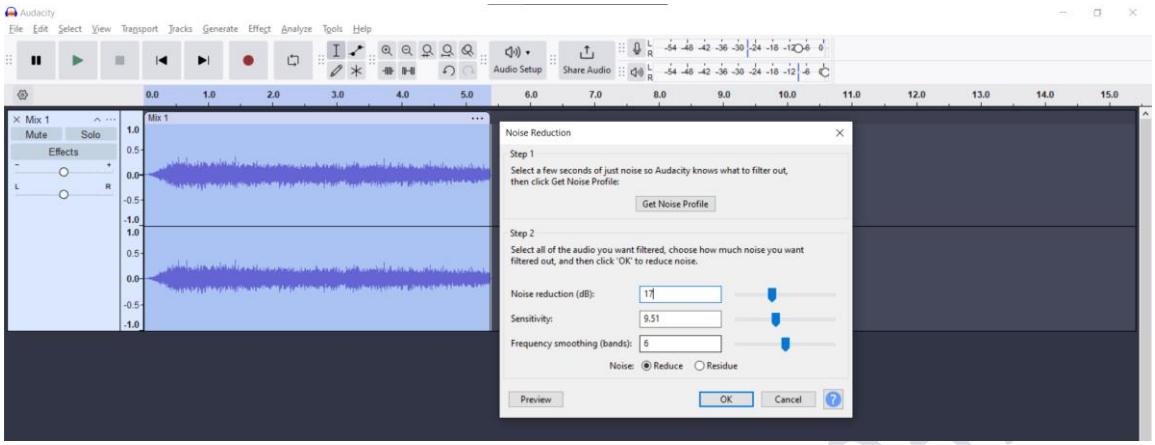
Noise Reduction in Audacity: Pramod applied noise reduction to the audio file using the following steps:

1. Created a noise profile from the noisy portion of the audio.



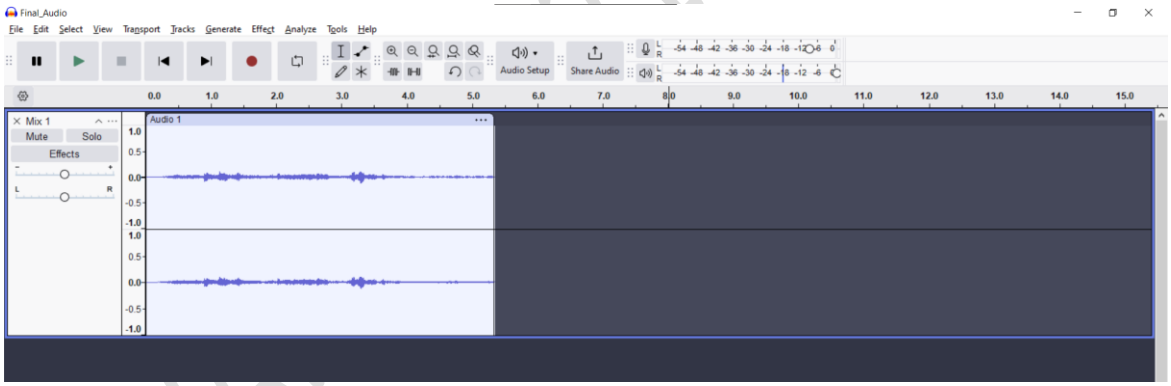


2. Applied noise reduction across the entire file.



// Final_audio

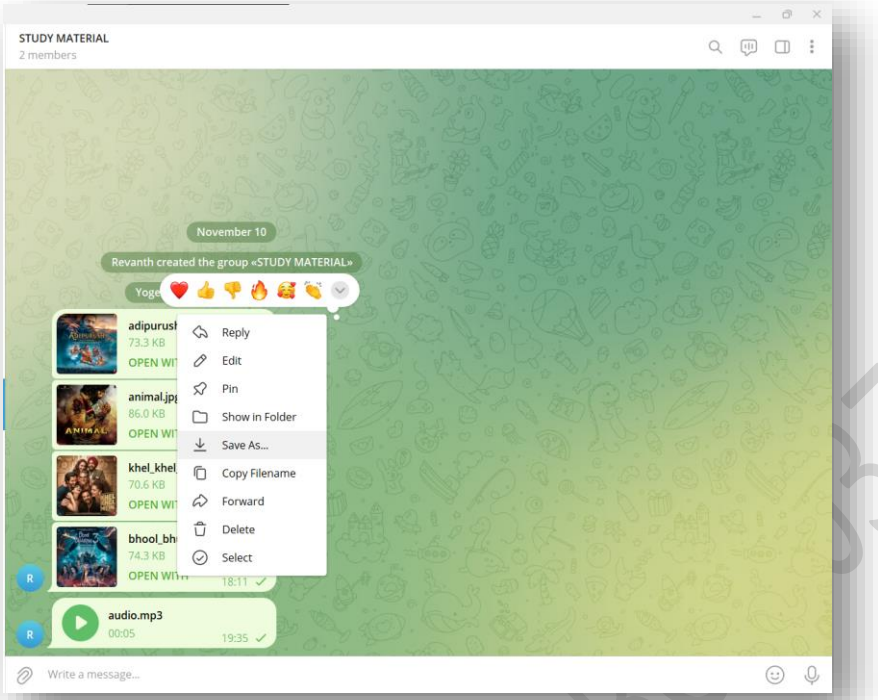
final_audio.mp3 (Double click to play the audio file)



After repeated processing, Pramod was able to clearly hear a voice saying, **"I am doing this because I am a movie lover and I love new content."** He noted key phrases from the audio: **'movie', 'lover', 'movielover', 'love', and 'content'.**

Step 4: Further Steganography Analysis

Pramod hypothesized that the audio file and the posters in the Telegram group were connected through hidden steganographic content. He downloaded all the posters from the group and used **Steghide** to analyze each one.



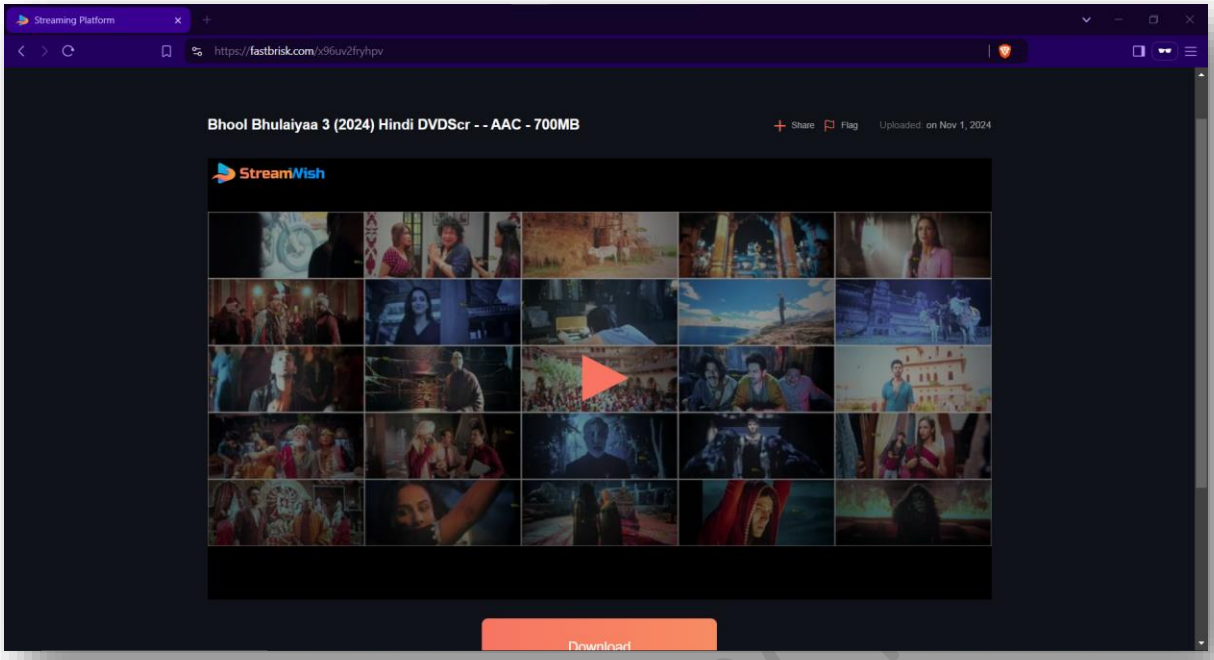
Starting with the *Bhool Bhulaiyaa 3* poster, he used the keywords extracted from the audio to attempt a brute-force attack.

```
steghide extract -sf bhool_bhulaiya_3.jpg
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 steghide extract -sf bhool_bhulaiya_3.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

The passphrase **"content"** successfully revealed a hidden file, '*bhool_bhulaiya_3_link.txt*', which contained a link to a webpage where the pirated movie could be streamed.

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 steghide extract -sf bhool_bhulaiya_3.jpg
Enter passphrase:
wrote extracted data to "bhool_bhulaiya_3_link.txt".
```

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 cat bhool_bhulaiya_3_link.txt
https://fastbrisk.com/x96uv2fryhpv
```



He repeated this process for the other three movie posters, each of which required different passphrases.

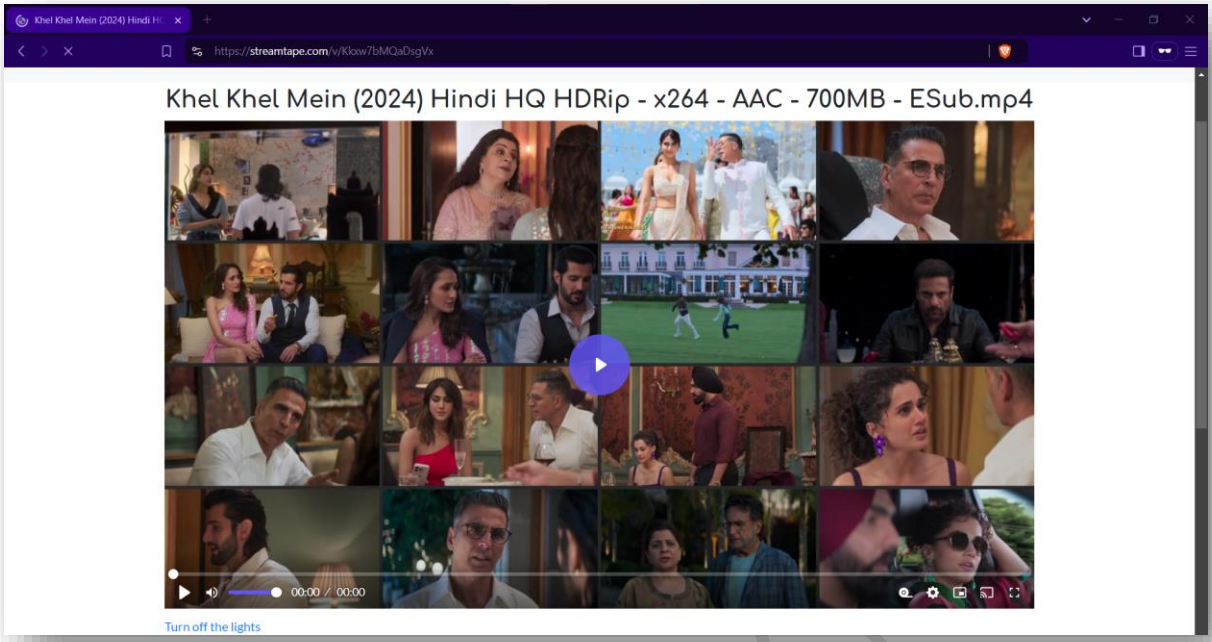
Khel Khel Mein:

```
steghide extract -sf khel_khel_mein.jpg
```

Passphrase: ***movielover***

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 steghide extract -sf khel_khel_mein.jpg
Enter passphrase:
wrote extracted data to "khel_khel_mein_link.txt".
```

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 cat khel_khel_mein_link.txt
https://streamtape.com/v/Kkxw7bMQaDsgVx
```



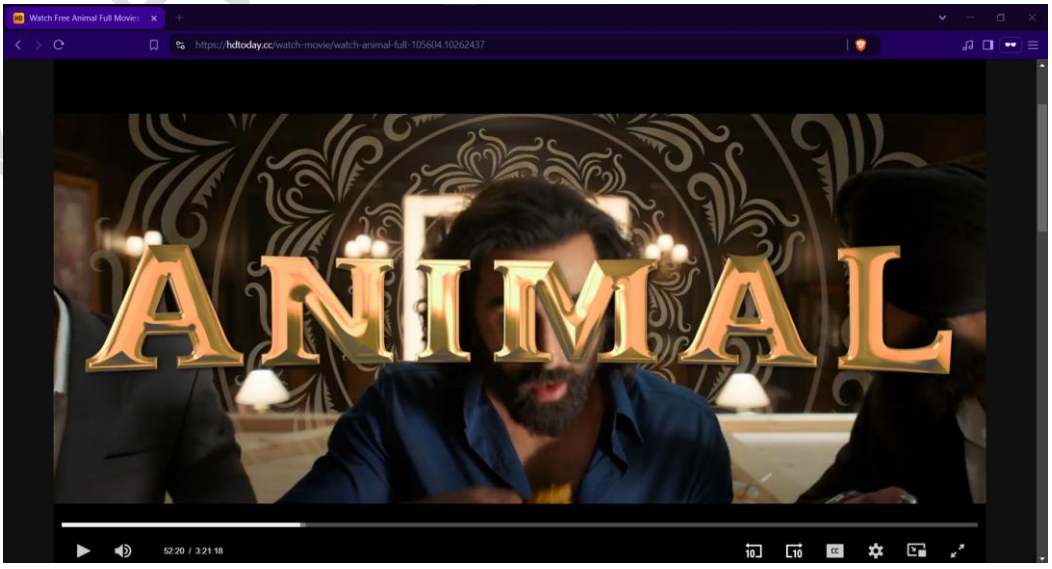
Animal:

```
steghide extract -sf animal.jpg
```

Passphrase: ***content***

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 steghide extract -sf animal.jpg
Enter passphrase:
wrote extracted data to "animal_link.txt".
```

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 cat animal_link.txt
https://hdtoday.cc/watch-movie/watch-animal-full-105604.10262437
```



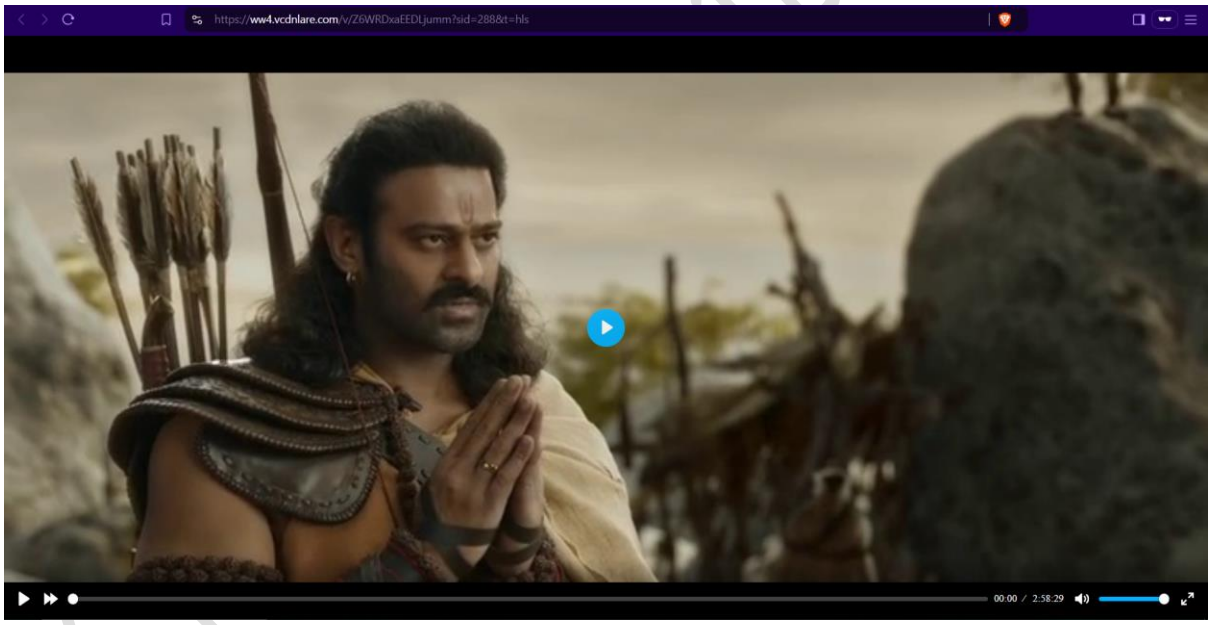
Adipurush:

```
steghide extract -sf adipurush.jpg
```

Passphrase: ***movielover***

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 steghide extract -sf adipurush.jpg
Enter passphrase:
wrote extracted data to "adipurush_link.txt".
```

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 cat adipurush_link.txt
https://ww4.vcdnlare.com/v/Z6WRDxaEEDLjumm?sid=288&t=hls
```



In each case, he was able to extract hidden links leading to pirated copies of the films.

Step 5: Mitigating the Piracy

Having identified the mechanism used to distribute pirated content, Pramod took swift action:

- He blocked access to the websites hosting the pirated movies.
- He identified and blocked the domains that could be used to host future pirated content.
- He reported the Telegram channel to the relevant authorities, resulting in it being shut down.
- Pramod also contacted Google to request the removal of the forged poster from search results.

Conclusion:

Through careful analysis of metadata, error level analysis, and steganography detection, Pramod Kumar successfully uncovered and disrupted a sophisticated movie piracy operation. His quick actions prevented further distribution of pirated T-Series content and safeguarded the company's intellectual property.

This case study demonstrates the importance of combining traditional forensic analysis with modern steganography techniques in combating digital piracy.

Tools Used:

- **ExifTool:** For ***metadata analysis*** to detect discrepancies in image files.
- **FotoForensics:** Website for conducting **Error Level Analysis (ELA)** to detect image tampering.
- **Steghide:** For performing **steganography** operations like embedding or extracting hidden data in images.
- **Audacity:** Open-source audio editor used for **noise reduction** and enhancing distorted audio files.