CBS 412 MULTIMEDIA SECURITY & FORENSICS:
Movie Piracy Case Study

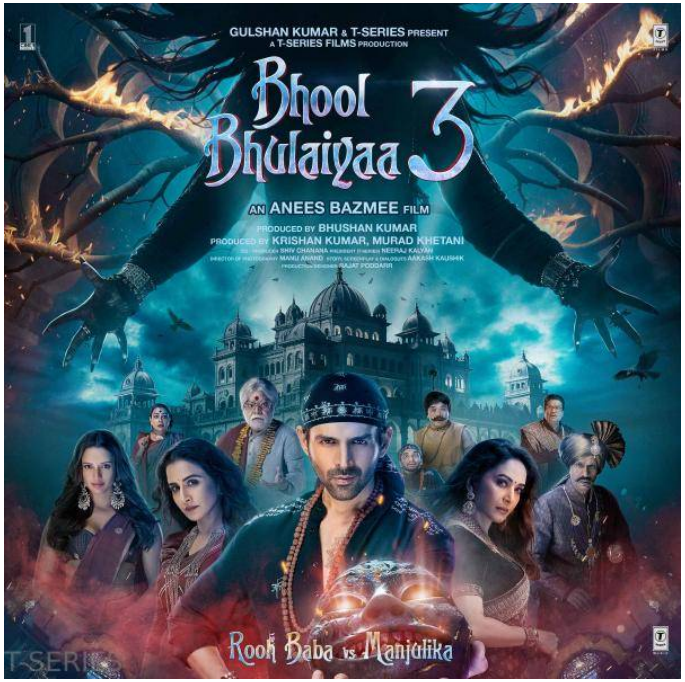
K. Revanth
Roll No: 2021BCY0037

Introduction

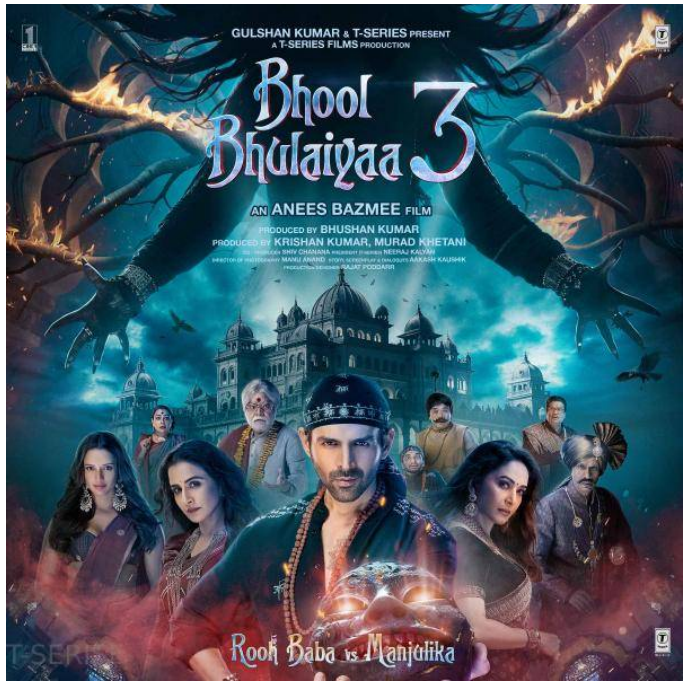
Scenario: Pramod Kumar, a cybersecurity analyst at T-Series Productions, was alerted that a pirated copy of the movie *Bhool Bhulaiyaa 3* was found online shortly after its release.

Objective: Investigate and identify how the piracy occurred using forensic techniques.

Investigating the Pirated Poster



Original Poster



Pirated Poster

Investigating the Pirated Poster

Metadata Analysis

Metadata analysis involves examining hidden data within files to authenticate them, track changes, identify origins, or gather forensic evidence.

- **Command used:** `exiftool <image.jpg>`
- **Result:** Discrepancies found in the `Software` and `Modify Date` fields of the pirated poster.

Investigating the Pirated Poster

```
revanth@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
```

Original Poster Metadata

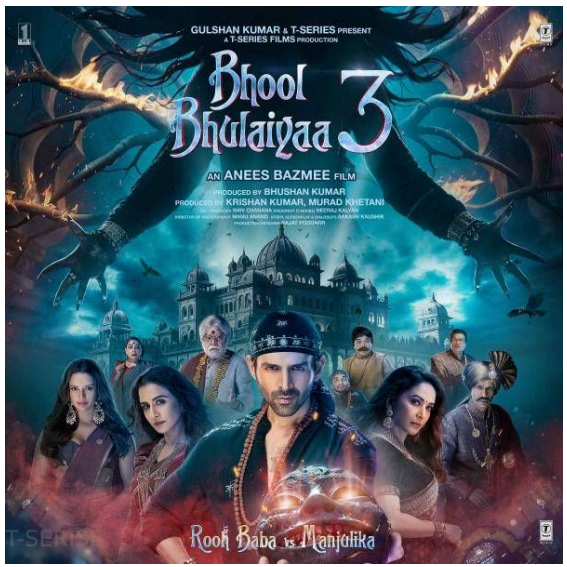
```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 exiftool bhool_bhulaiya_3_fake.jpg
ExifTool Version Number         : 12.40
File Name                       : bhool_bhulaiya_3_fake.jpg
Directory                       : .
File Size                       : 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
```

Pirated Poster Metadata

Investigating the Pirated Poster

ELA Analysis

- *Tool used:* FotoForensics
- **Analysis:** ELA (Error Level Analysis) detected inconsistencies in left bottom corner, indicating possible tampering around the watermark.

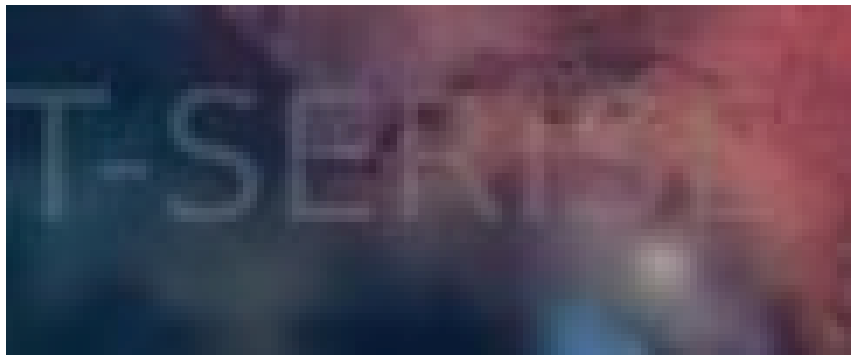


Investigating the Pirated Poster

Visual Anomalies

- **Discrepancies in the watermark:**
  - Blurred background near watermark
  - Misspelling: "T-Serise" instead of "T-Series"

Original Poster



Pirated Poster

Steganalysis of the Pirated Poster

Steganography Detection

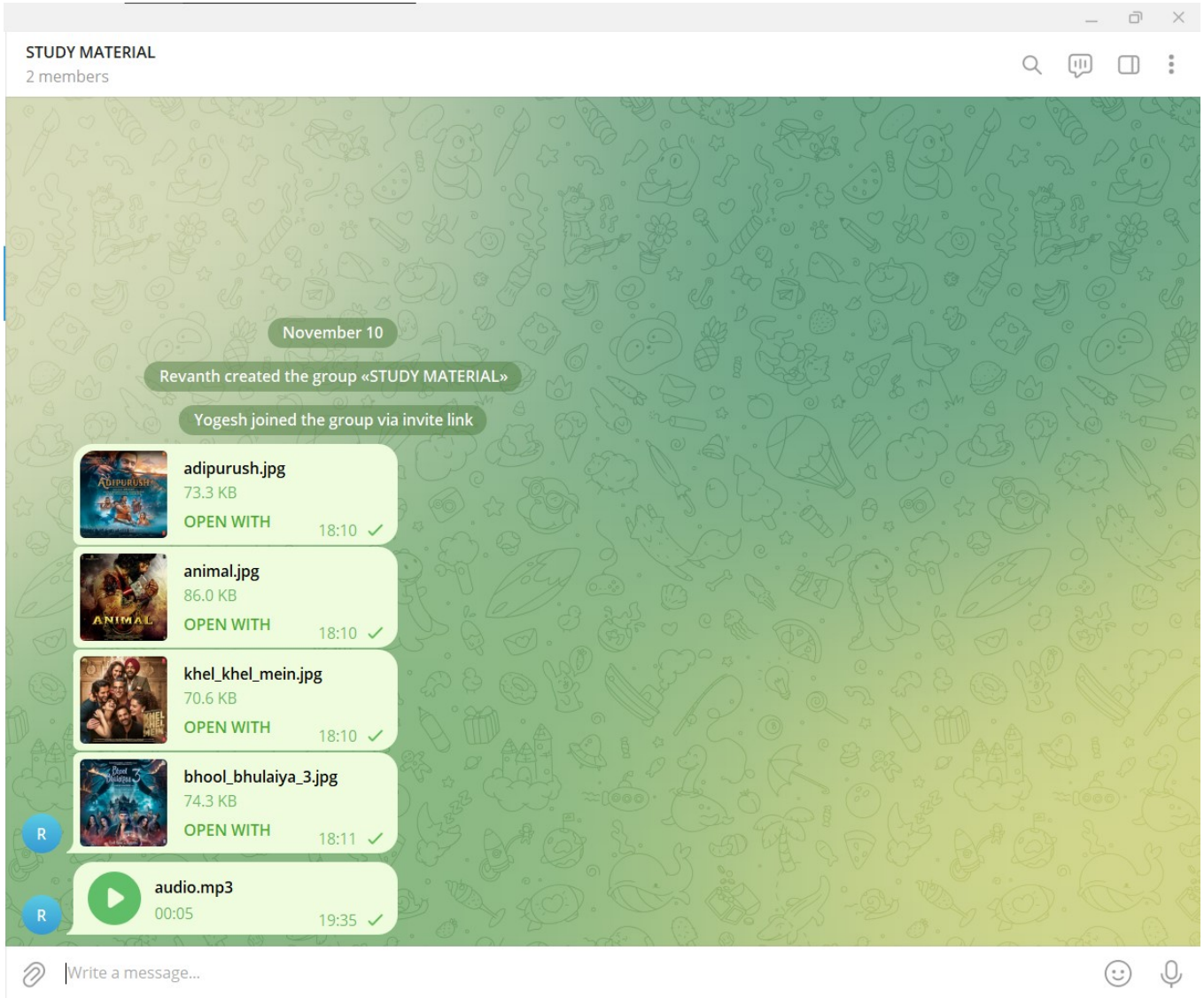
- *Tool used:* Steghide
- **Command:** `steghide extract <image.jpg>`

A hidden text file was extracted from the pirated poster using the passphrase "download". The file contained a link to a Telegram group sharing pirated content.

```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 steghide extract -sf bhool_bhulaiya_3_fake.jpg
Enter passphrase:
wrote extracted data to "link.txt".
```

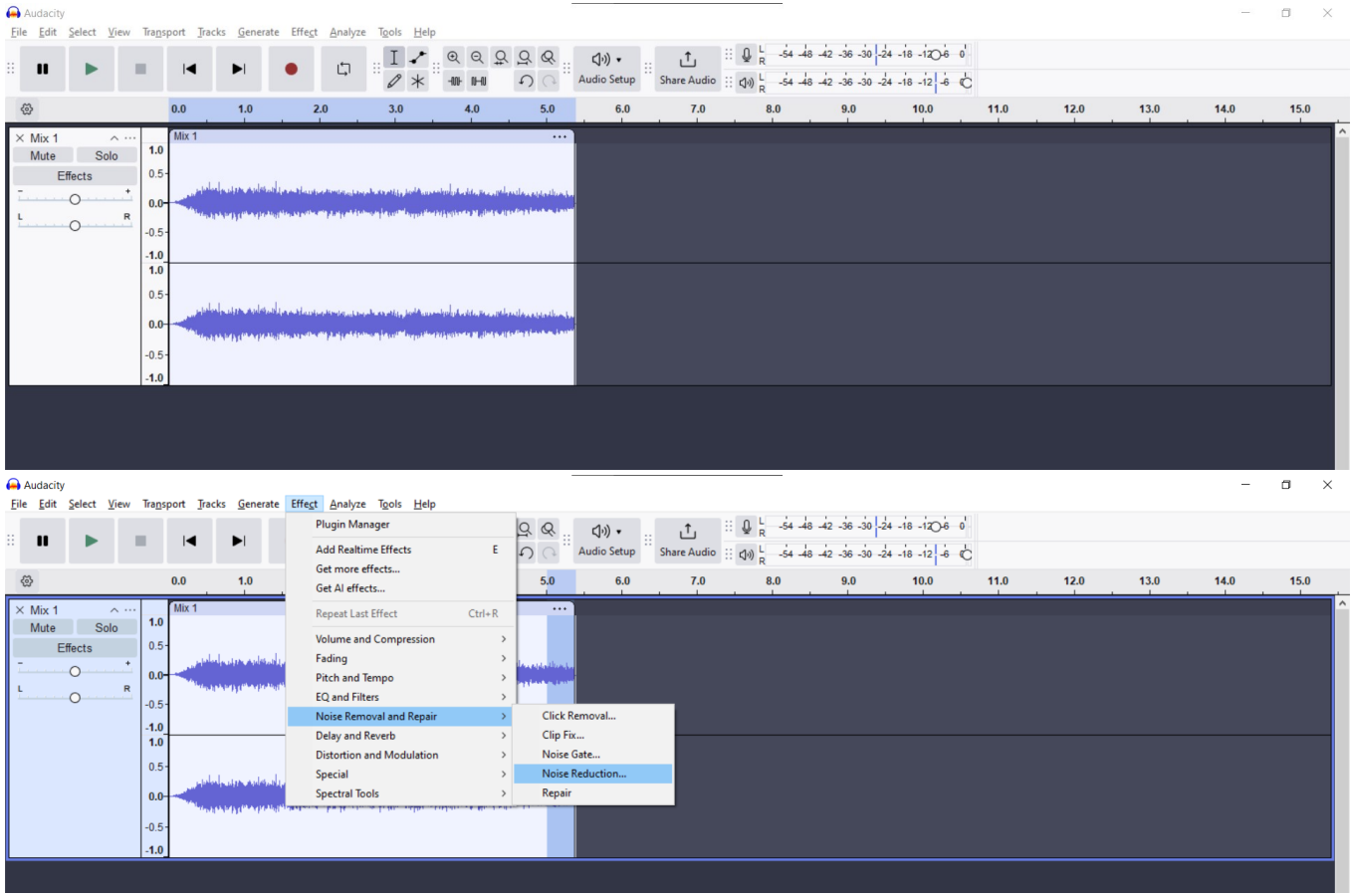
```
revanth@DESKTOP-75PL99T:/mnt/d/IIIT K/SEM-7/CBS 412 MULTIMEDIA SECURITY & FORENSICS/LABS/LAB EXAM$
 cat link.txt
https://t.me/+eSqbmNksg1M5OTll
```

Analyzing Telegram Group Files

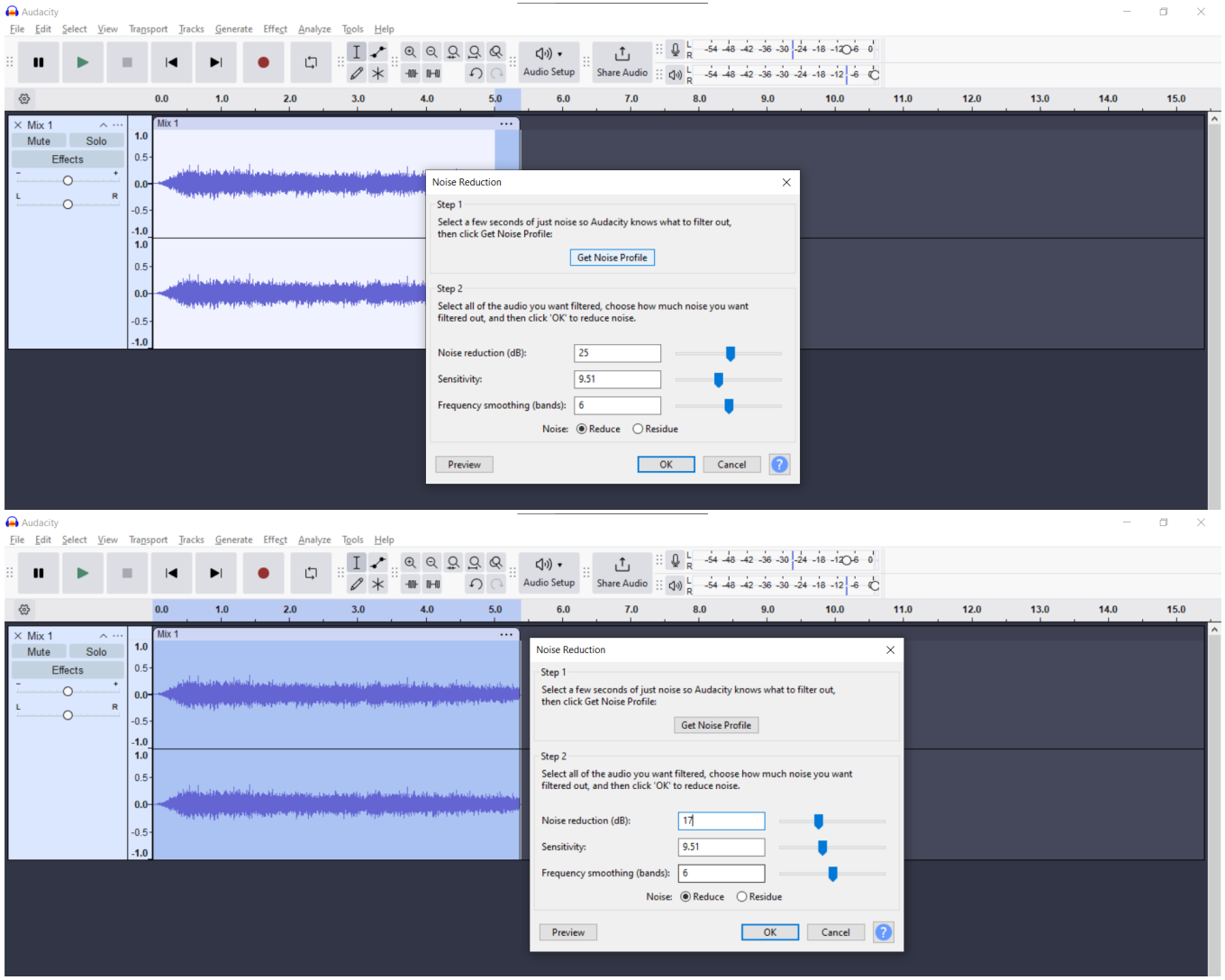


Analyzing Telegram Group Files

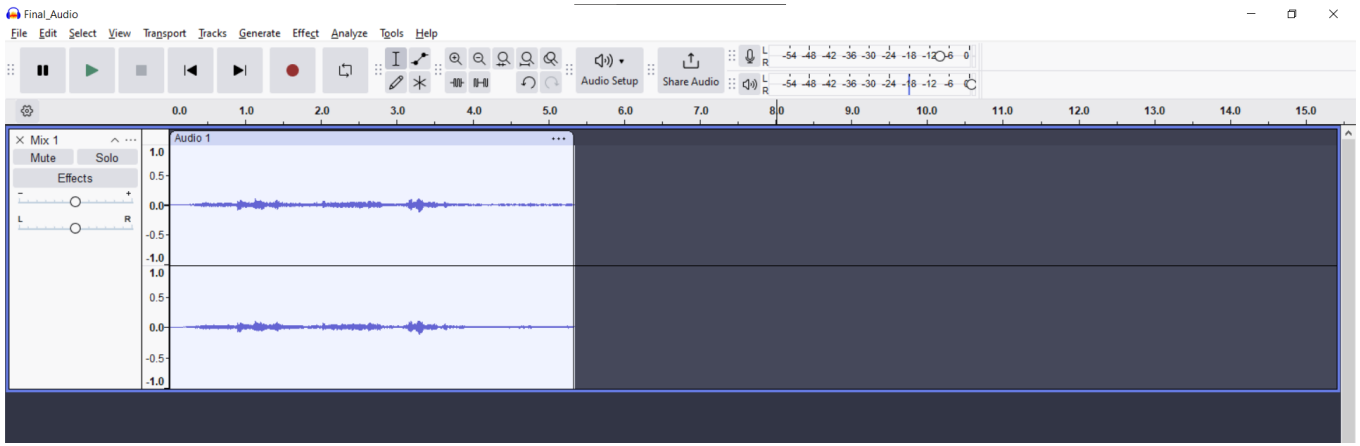
Forensic Analysis of Audio An audio file from the group was analyzed using Audacity to reveal hidden speech.



Analyzing Telegram Group Files



Analyzing Telegram Group Files



Audio Analysis

- Initial audio file was analyzed, and noise reduction was applied in Audacity.

Analyzing Telegram Group Files

Audio Files:

- Click here to play initial audio file (before noise reduction)
- Click here to play processed audio file (after noise reduction)

Extracted Phrase:

- "I am a movie lover and I love new content."

Possible code words:

- "movie", "lover", "movielover", "love", "content"

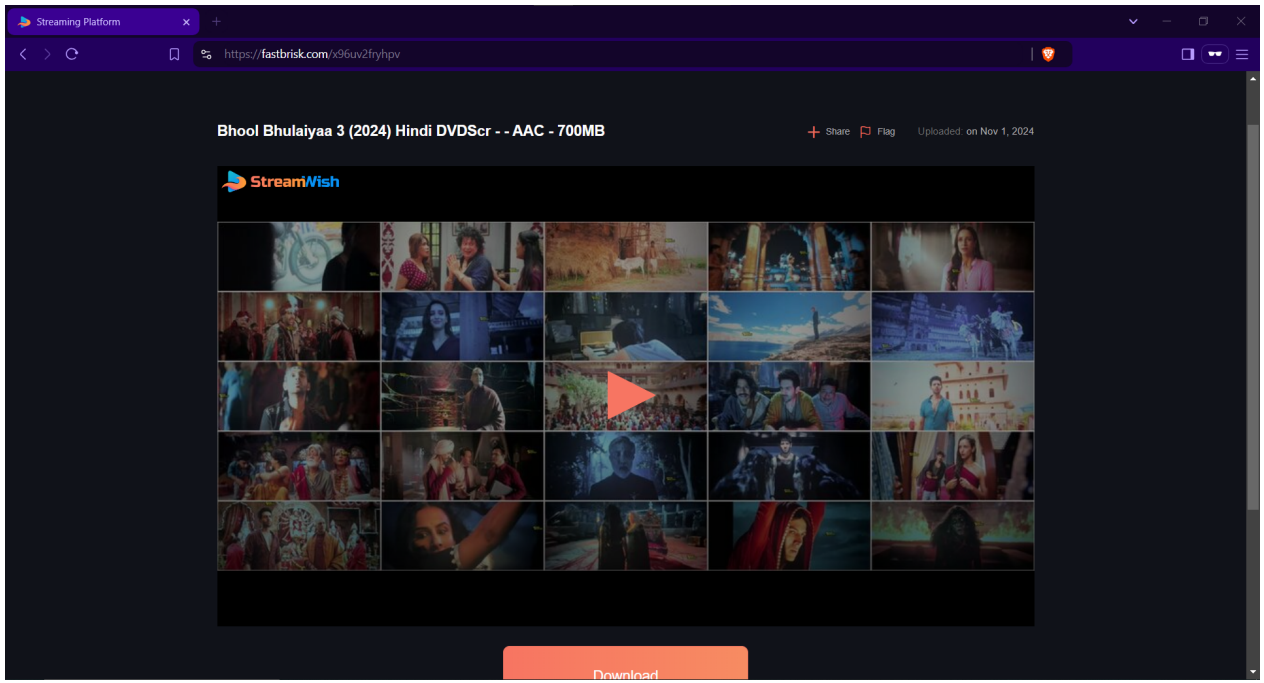
Analyzing Telegram Group Files

Hidden Links in Posters Steghide was used to extract hidden files from movie posters. Each poster had a unique passphrase:

- **Bhool Bhulaiyaa 3:** Passphrase - "content"

```
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
```

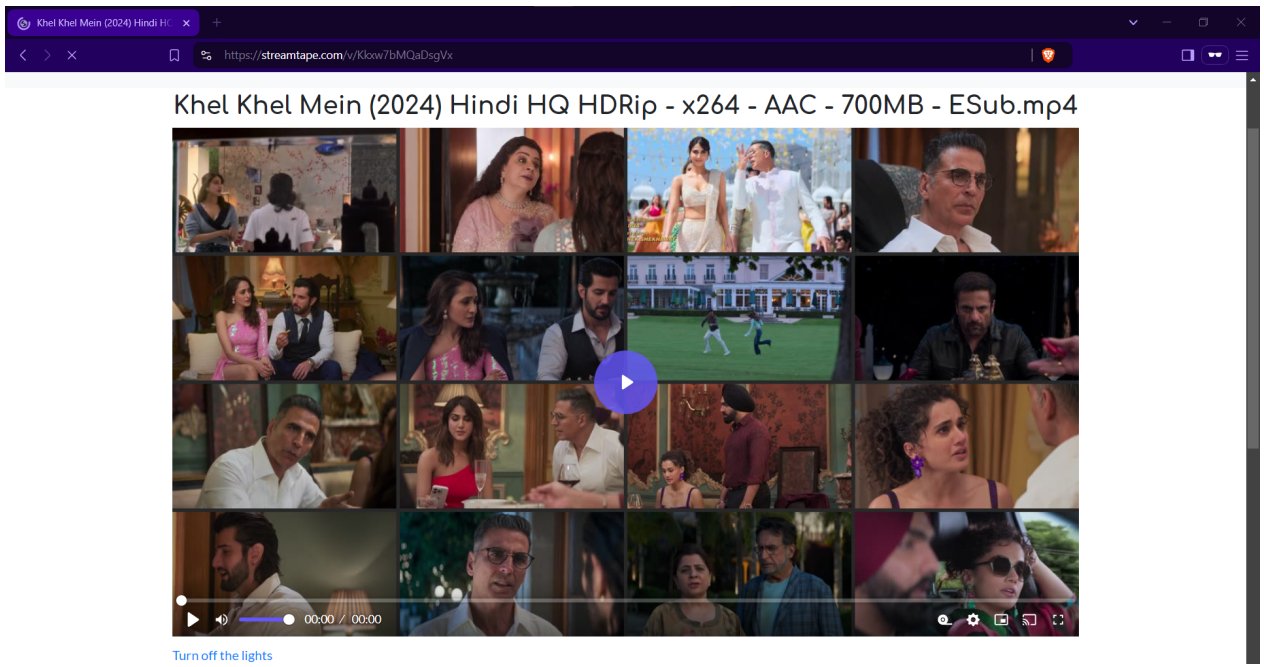


Analyzing Telegram Group Files

- **Khel Khel Mein:** 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
```

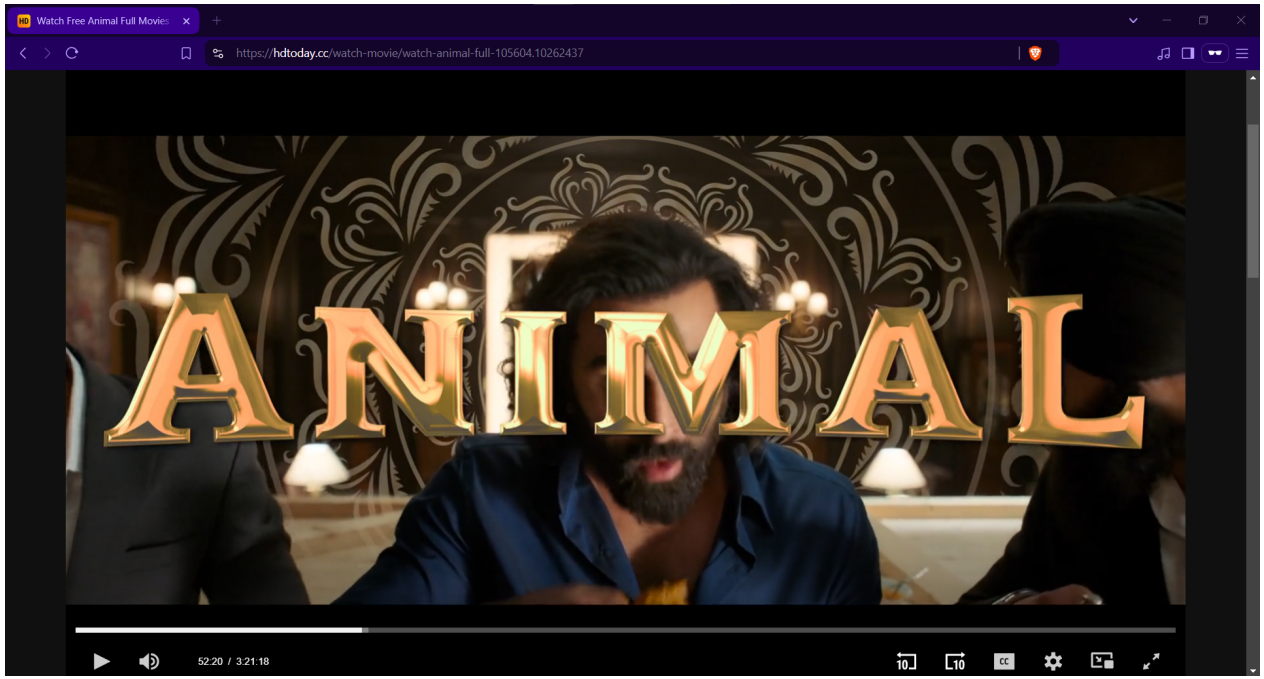


Analyzing Telegram Group Files

- **Animal:** 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
```

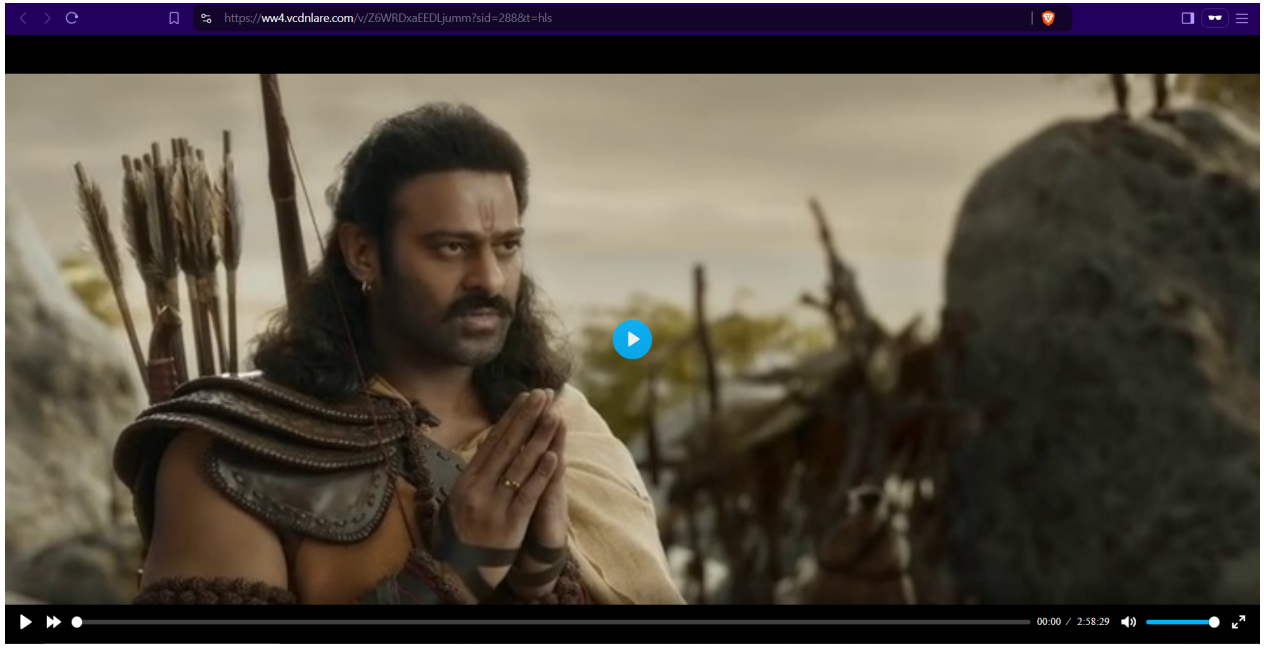


Analyzing Telegram Group Files

- **Adipurush:** 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
```



Mitigating Piracy

Steps taken:

- Blocked access to websites hosting pirated content.
- Reported the Telegram channel for shutdown.
- Requested removal of forged posters from Google search.

Conclusion

By combining metadata analysis, ELA, and steganography detection, the piracy operation was disrupted, safeguarding the intellectual property of T-Series Productions.

Tools Used

- **ExifTool:** Metadata analysis
- **FotoForensics:** Error Level Analysis (ELA)
- **Steghide:** Steganography operations
- **Audacity:** Noise reduction in audio files