TASK (TSK-000-183)

Incident Response Procedures

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Digital Forensics Techniques:

Evidence Collection

Preservation

Analysis

Documentation and Reporting

Let's dive into each section.

Incident Response Procedures

1. Preparation

Objective: To establish an incident response plan and equip the team with necessary tools and knowledge.

Key Activities:

Develop an Incident Response Plan (IRP) with clear roles and responsibilities.

Train the incident response team and conduct regular drills.

Set up monitoring and alerting systems.

Maintain an inventory of critical assets and prioritize based on their importance.

2. Identification

Objective: To detect potential security incidents as early as possible.

Key Activities:

Monitor network and system activity using SIEM (Security Information and Event Management) systems.

Use intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Analyze logs and alerts to identify suspicious activity.

Classify incidents based on severity and type.

3. Containment

Objective: To limit the damage and prevent the incident from spreading.

Key Activities:

Isolate affected systems or networks.

Implement temporary fixes or workarounds.

Preserve evidence for further investigation.

4. Eradication

Objective: To eliminate the root cause of the incident.

Key Activities:

Identify and remove malware or unauthorized access.

Patch vulnerabilities and update systems.

Verify that systems are clean and secure.

5. Recovery

Objective: To restore normal operations while ensuring the security of systems.

Key Activities:

Gradually restore systems and networks to their normal state.

Monitor systems for any signs of residual issues.

Validate that all security measures are in place and effective.

6. Lessons Learned

Objective: To improve future incident response efforts.

Key Activities:

Conduct a post-incident review and analysis.

Document findings and recommendations.

Update the incident response plan and security measures.

Digital Forensics Techniques

1. Evidence Collection

Objective: To gather digital evidence in a forensically sound manner.

Key Activities:

Collect data from computers, servers, mobile devices, and networks.

Use write blockers to prevent alteration of evidence.

Document the collection process meticulously, including timestamps and methodologies.

2. Preservation

Objective: To ensure the integrity of collected evidence.

Key Activities:

Store evidence in a secure environment.

Maintain a chain of custody log to track the handling of evidence.

Use checksums to verify data integrity.

3. Analysis

Objective: To interpret the evidence and extract meaningful information.

Key Activities:

Use forensic tools to analyze file systems, logs, and network data.

Reconstruct timelines of events based on evidence.

Identify signs of unauthorized access, data exfiltration, or other malicious activities.

4. Documentation and Reporting

Objective: To document findings and provide clear, actionable reports.

Key Activities:

Create detailed reports that include methodologies, findings, and conclusions.

Provide recommendations for improving security and preventing future incidents.

Ensure that reports are clear and understandable for both technical and non-technical stakeholders.

Digital Forensics on evidence:

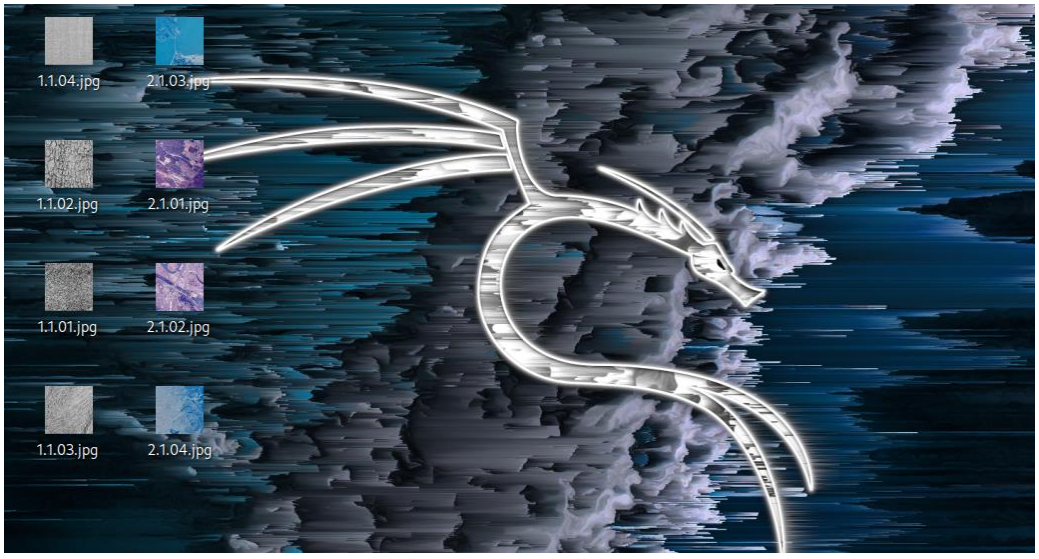
Description: Perform forensics on

- **Steganography**
- **Images**
- **Videos**
- **Audio**

The increasing reliance on digital media and the surge in cybercrimes have emphasized the need for advanced forensic techniques. This project aims to investigate image files with a primary focus on data forensics, steganography, and disk images. The goal is to develop methodologies and tools to uncover hidden information, detect tampering, and extract valuable data for legal and investigative purposes.

- Conduct an in-depth analysis of image files, including popular formats such as JPEG, PNG, and BMP.

-Simple photos.



- Explore data forensics techniques to recover deleted or hidden information within image files.

-Pictures Extracted through Steghide:

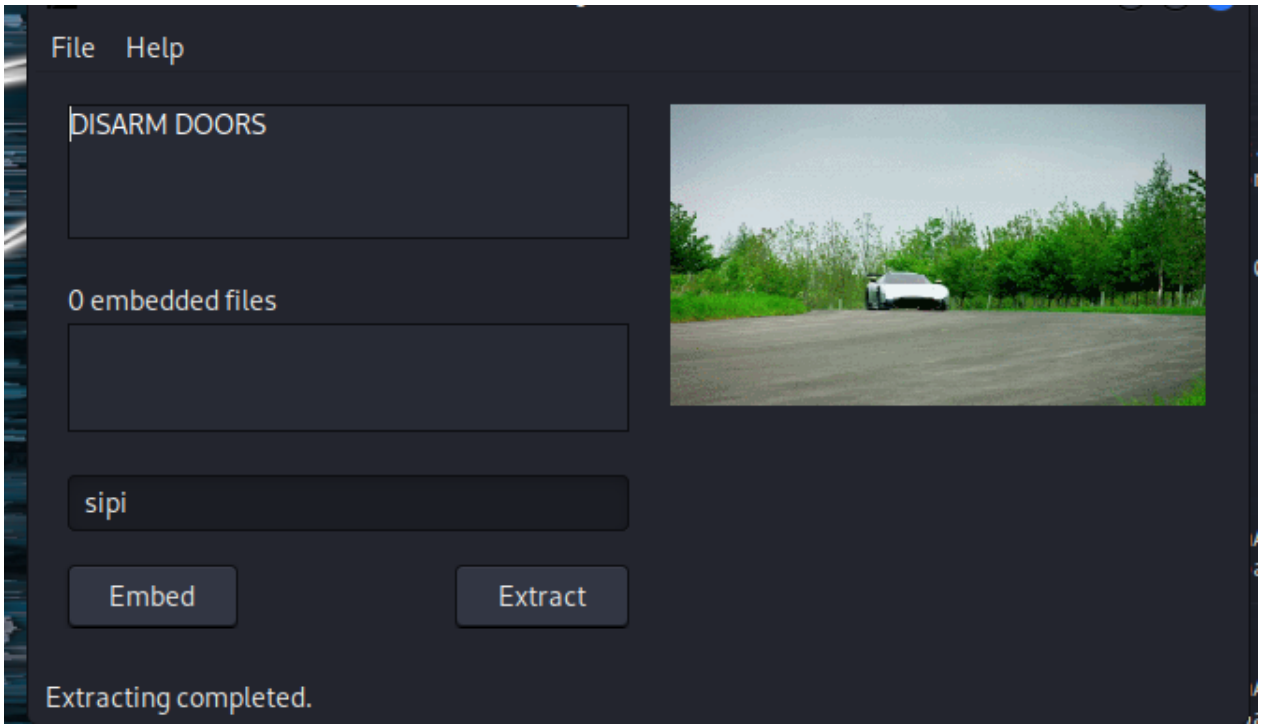
```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf 1.1.01.jpg -xf 01ext.txt  -p sipi
wrote extracted data to "01ext.txt".

┌──(kali㉿kali)-[~/Downloads]
└─$ cat 01ext.txt
12&32$
```

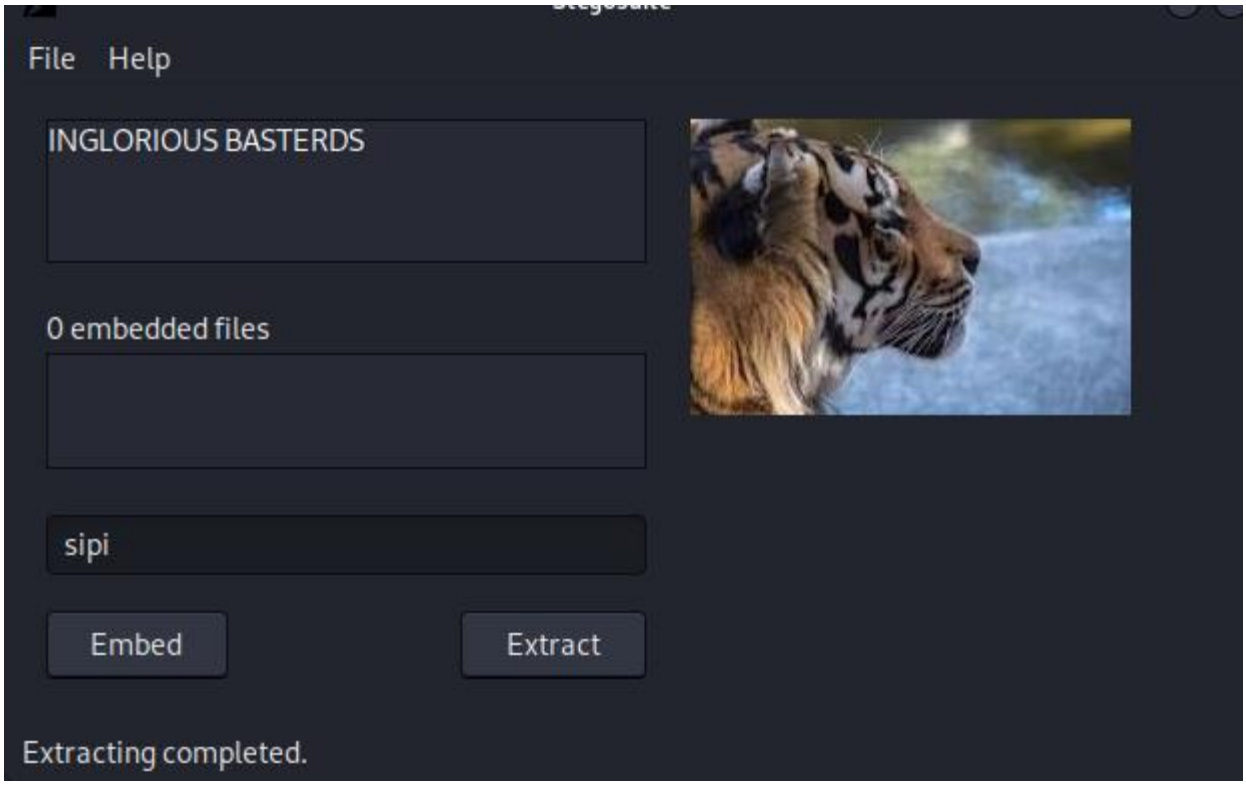
```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf 1.1.02.jpg -xf 02ext.txt  -p sipi
wrote extracted data to "02ext.txt".

┌──(kali㉿kali)-[~/Downloads]
└─$ cat 02ext.txt
Ab129AX
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf 2.1.01.jpg -xf 03ext.txt  -p sipi
wrote extracted data to "03ext.txt".

┌──(kali㉿kali)-[~/Downloads]
└─$ cat 03ext.txt
LAST MINUTE PAPERWORK
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf 2.1.02.jpg -xf 04ext.txt  -p sipi
wrote extracted data to "04ext.txt".

┌──(kali㉿kali)-[~/Downloads]
└─$ cat 03ext.txt
LAST MINUTE PAPERWORK
```

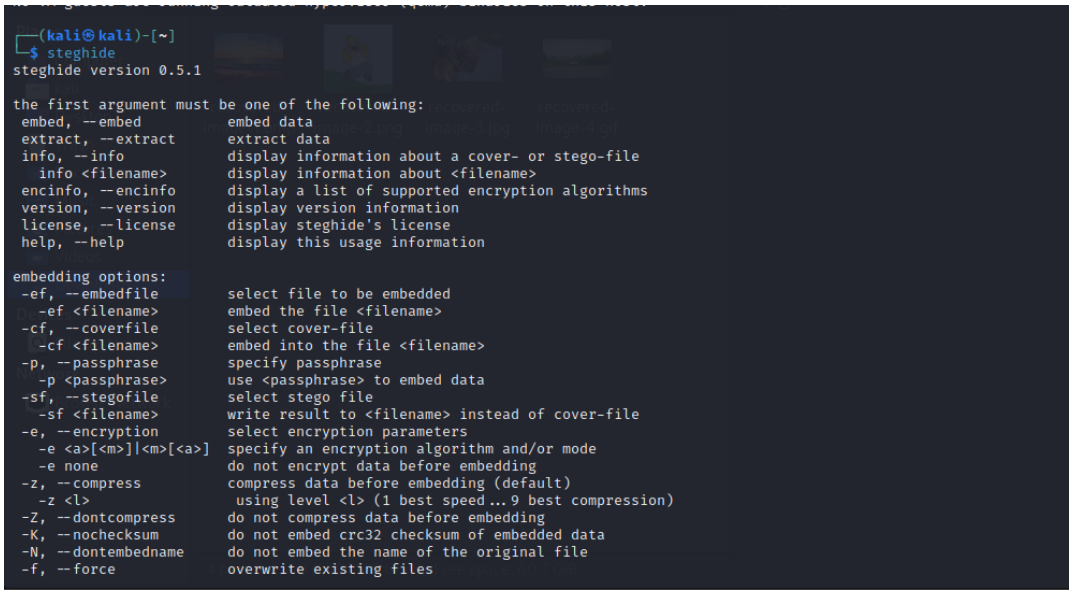
-Now Pictures extracted through StegoSuite:





- Investigate steganography methods and develop tools to detect and extract concealed data from images.

-Steghide

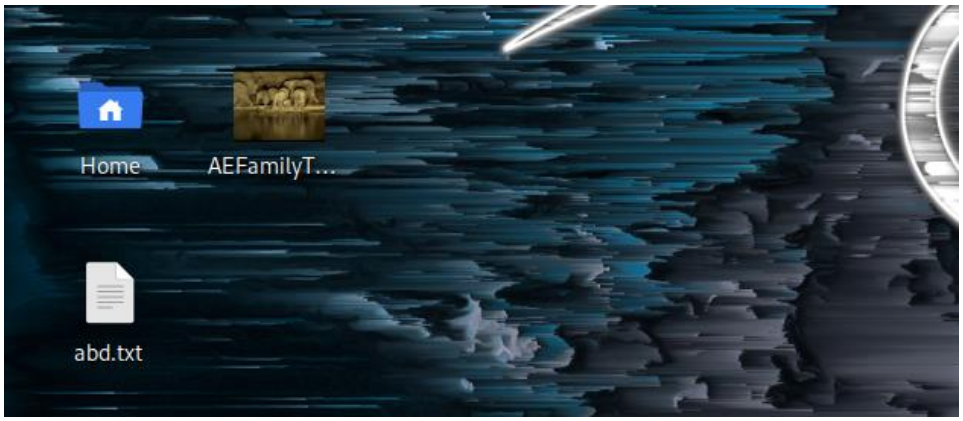


-Stegosuite:

```
┌──(kali㉿kali)-[~]
└─$ stegosuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Steganography tool to hide information in image files

Usage: stegosuite [-hV] [COMMAND]

Options:
  -h, --help      Show this help message and exit.
  -V, --version   Print version information and exit.

Commands:
  help      Displays help information about the specified command
  gui       Starts the GUI
  embed     Embeds data into image
  extract   Extracts data from image
  capacity  Shows the maximum amount of embeddable data

Example:
  stegosuite help embed           Displays help for stegosuite embed
```

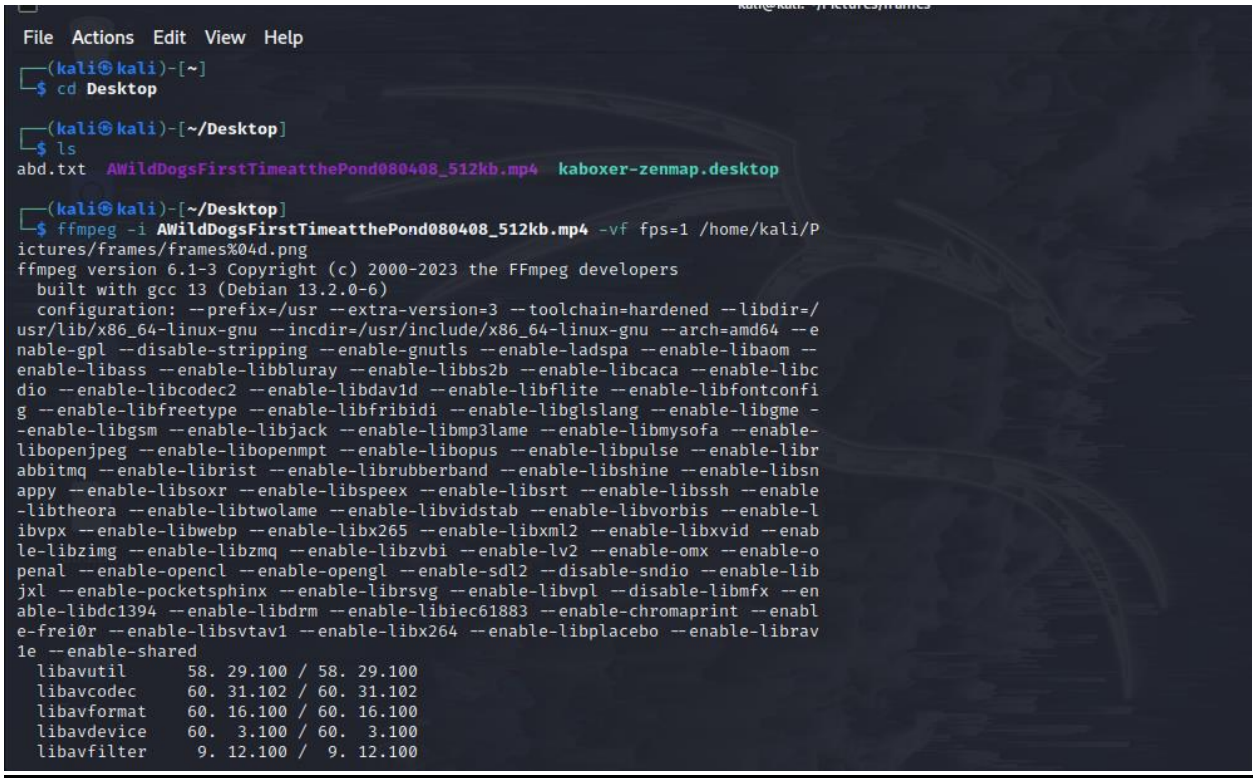
- Conduct an in-depth analysis of video files provided by website “nist”.

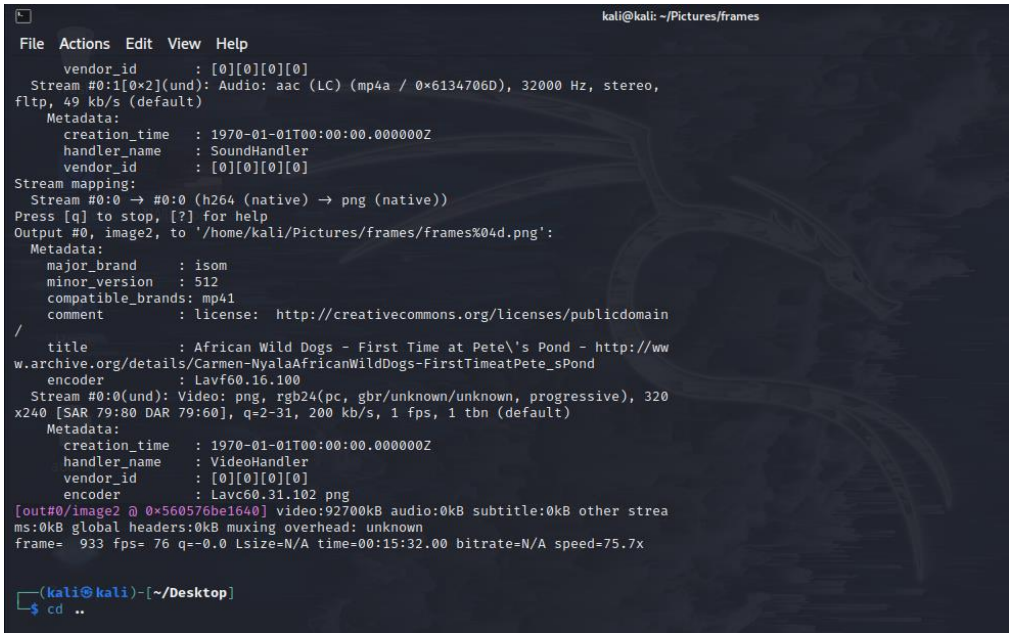
-Drag and Drop videos from Windows to kali:

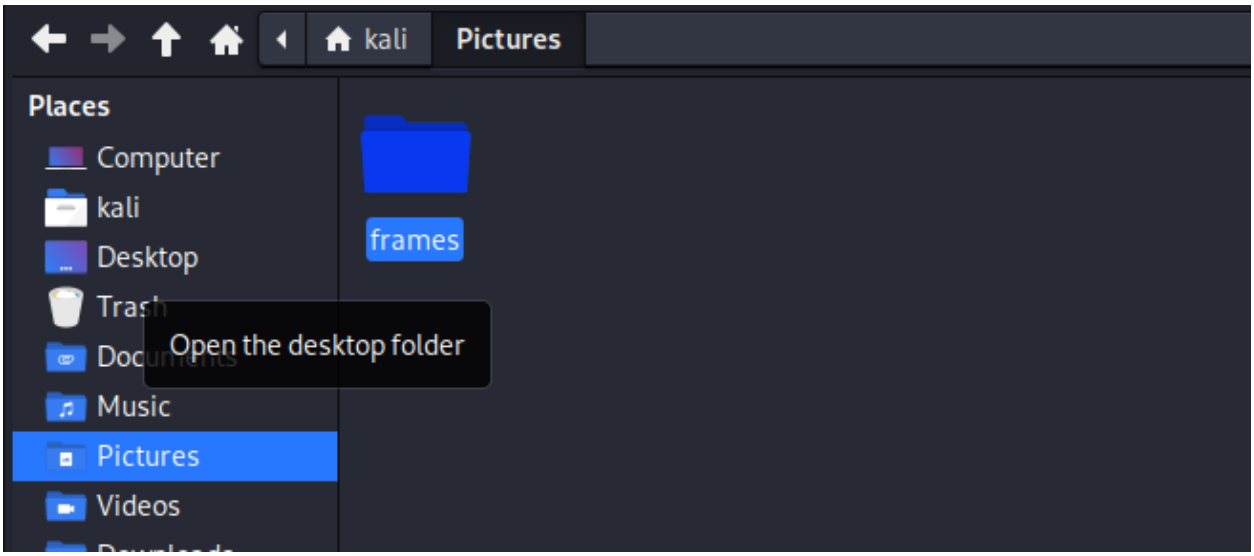


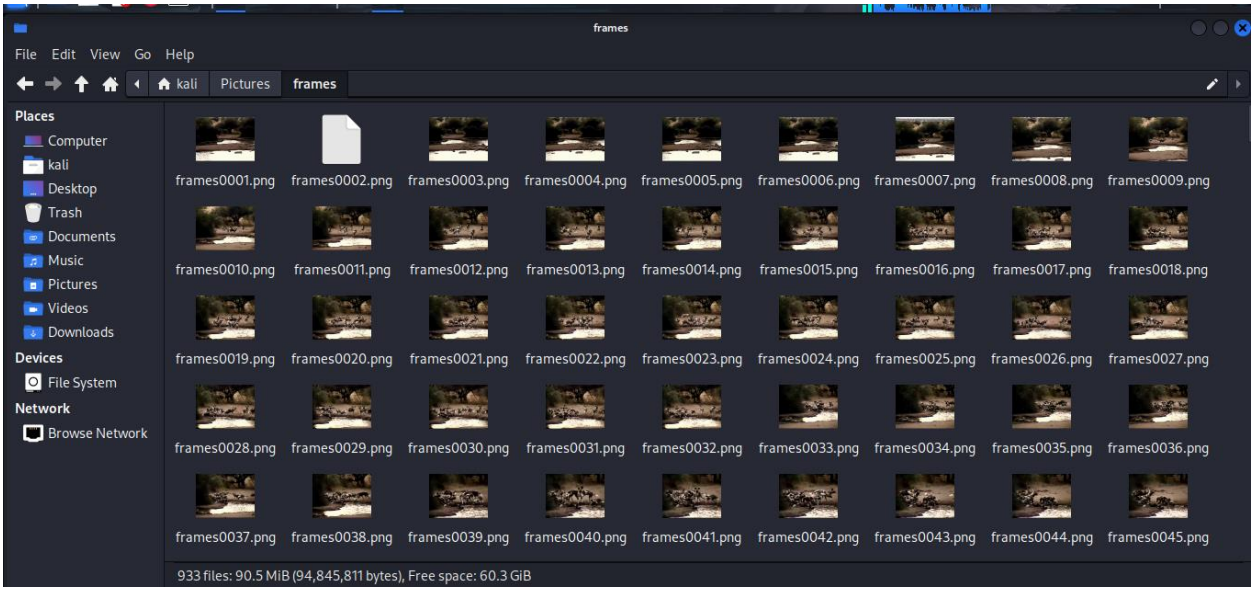
- Explore data forensics techniques to recover deleted or hidden information within videos and do steganalysis on it.

-Video 1:

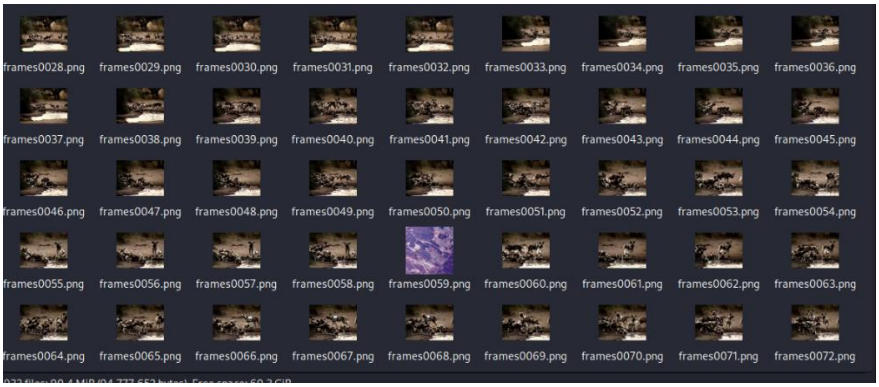






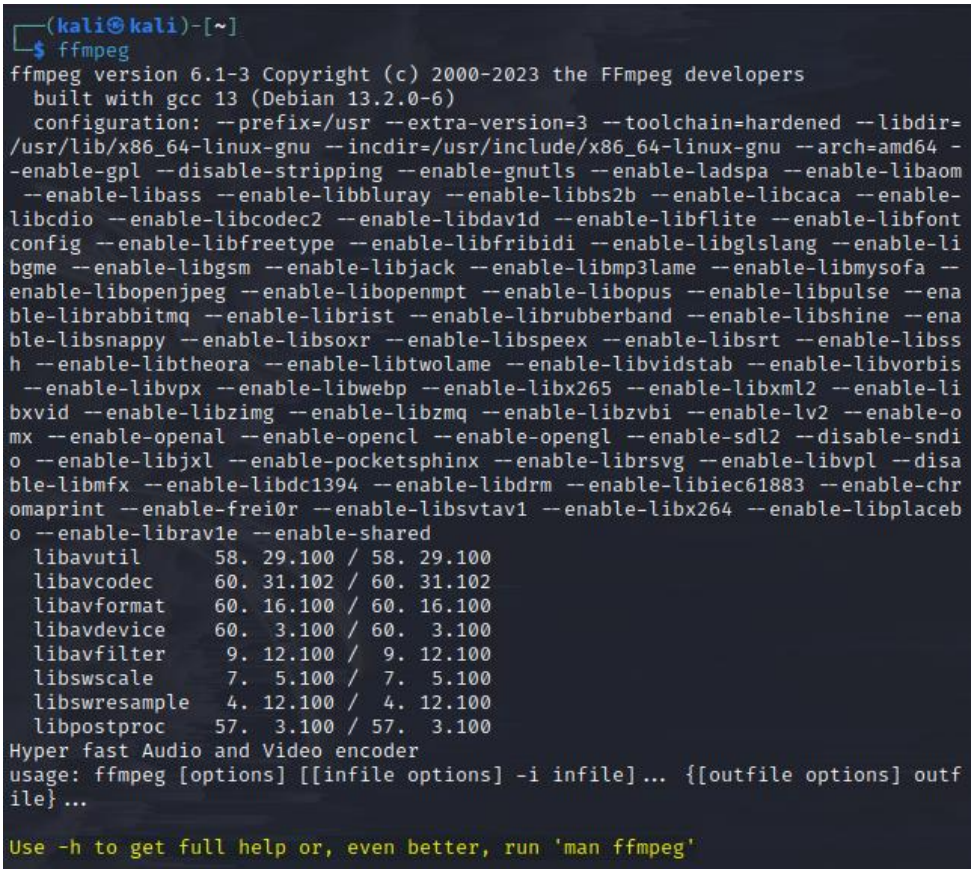


Embedded image:



- Show which steganography tools are used to detect and extract concealed data from videos.

  - ffmpeg:



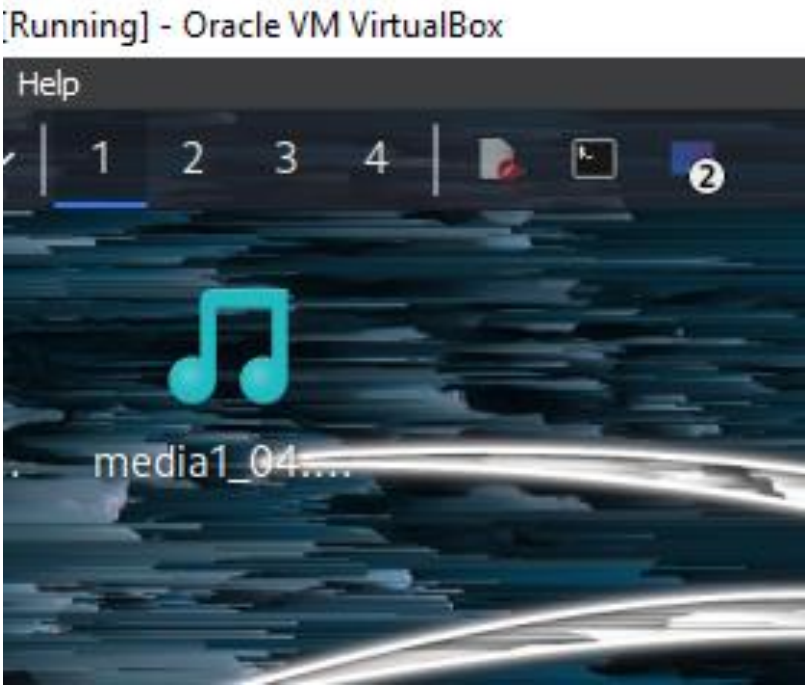
  - Steghide:

```
┌──(kali㉿kali)-[~]
└─$ steghide
steghide version 0.5.1

the first argument must be one of the following:
 embed, --embed          embed data
 extract, --extract      extract data
 info, --info            display information about a cover- or stego-file
   info <filename>       display information about <filename>
 encinfo, --encinfo      display a list of supported encryption algorithms
 version, --version      display version information
 license, --license      display steghide's license
 help, --help            display this usage information

embedding options:
 -ef, --embedfile        select file to be embedded
   -ef <filename>        embed the file <filename>
 -cf, --coverfile        select cover-file
   -cf <filename>        embed into the file <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to embed data
 -sf, --stegofile        select stego file
   -sf <filename>        write result to <filename> instead of cover-file
 -e, --encryption        select encryption parameters
   -e <a>[<m>]|<m>[<a>]  specify an encryption algorithm and/or mode
   -e none               do not encrypt data before embedding
 -z, --compress          compress data before embedding (default)
   -z <l>                 using level <l> (1 best speed ... 9 best compression)
 -Z, --dontcompress      do not compress data before embedding
 -K, --nochecksum        do not embed crc32 checksum of embedded data
 -N, --dontembedname     do not embed the name of the original file
 -f, --force             overwrite existing files
```

-I have gained password access through brute force attack and password for all video and image files is “sipi”:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ stegcracker recovered-image-3_embed.jpg
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2023 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

No wordlist was specified, using default rockyou.txt wordlist.
Counting lines in wordlist..
Attacking file 'recovered-image-3_embed.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
241728/14344392 (1.69%) Attempted: josine2006ngwww
```

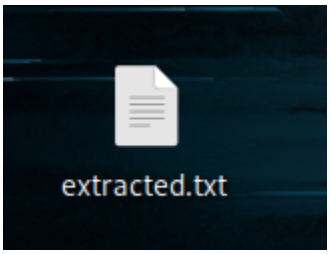
- Conduct an in-depth analysis of audio files, including popular formats such as .wav, .mp3 etc.



-file embedded in audio is retrieved:

```
┌──(kali㉿kali)-[~/Desktop/AudioStego/build]
└─$ ./hideme output.wav -f
Doing it boss!
Looking for the hidden message ...
File detected. Retrieving it ...
Message recovered size: 511 bytes
File has been saved as: output.txt G
Recovering process has finished successfully.
Cleaning memory ...

┌──(kali㉿kali)-[~/Desktop/AudioStego/build]
└─$ cat output.txt\ G$'\177'
Korean airliner has been hijacked.
, "Jim: DEPLOY TO MT. WEATHER NOW!,"
"CALL OFICE (sic) AS SOON AS POSSIBLE. 4145 URGENT."
"SITUATION LOCK DOWN ALL AT&T LOCATIONS HAVE BEEN EVACUATED."
"National Master Console has been re-routed to Merrimack."
message said: "#2 MCLL EXEC WAS ABOARD ONE OF THE PLANES. 1 OF THE ONES WHO BETR
AYED HARRY. NO TEARS HERE." Metrocall founder Harry Brock had been ousted as pre
sident six years earlier. Metrocall chief operating officer Steven Jacoby died o
n Flight 77 that day.

┌──(kali㉿kali)-[~/Desktop/AudioStego/build]
└─$
```

-File in which embedded data is stored:

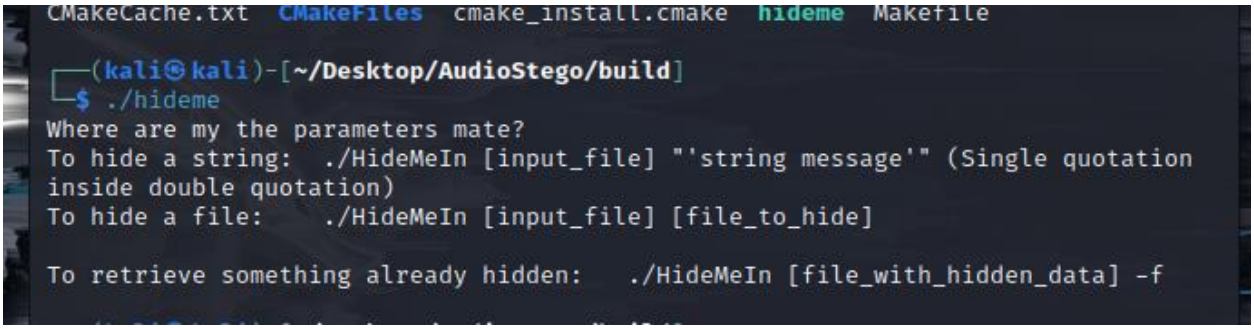


-THE AUDIO HAS SOME ENCRYPTED MESSAGE WHICH IS RETRIEVED:

```
┌──(kali㉿kali)-[~/Desktop/AudioStego/build]
└─$ ./hideme output.wav -f
Doing it boss!
Looking for the hidden message ...
String detected. Retrieving it ...
Message recovered size: 45 bytes
Message: 'The US goverment had taken control over 911'
Recovering process has finished successfully.
Cleaning memory ...
```

- Show which steganography tools are used to detect and extract concealed data from audio.

-The tool which is used to carried out audio steganography is.**/hideme**



In this way I have done Steganography in all file formats and my required goals have been achieved.