TRAINING DAY 23 REPORT:

STEGANOGRAPHY TOOLS :

- ## Find Hidden Information from Sound

Definition: Extracting hidden messages embedded within sound files (WAV, MP3, etc.) using steganographic techniques or audio analysis.

Techniques:

1. LSB (Least Significant Bit): Data is hidden in the quietest (least significant) bits of audio samples.

2. Echo Hiding: Tiny delays (echoes) carry data in timing.

3. Spectrogram Analysis: Visualizing audio to find image/text patterns.

4. Frequency Injection: Hidden tones or modulated signals carry secret messages.

Tools:

- Audacity

- Sonic Visualiser

- Steghide (if embedded using hybrid methods)

Process:

1. Load the audio file into a visual/audio tool.

2. Zoom into waveforms or spectrograms.

3. Analyze for suspicious patterns, noise, or text encoding.

- ## Find Hidden Information from Sound – Using Audacity

Audacity: A free, open-source audio editor used for analyzing and manipulating sound files.

How It Helps in Steganography:

- Spectrogram view reveals visual traces of hidden content (e.g., images or binary text).

- Effect Filters: Reveal modulations or waveform changes.

- Time Stretching/Amplifying: Make subtle changes more visible.

Steps:

1. Open the audio file in Audacity.

2. Switch to **Spectrogram View** (from the track dropdown).

3. Look for strange patterns, QR codes, text, etc.

4. Apply filters or adjust frequency range to clarify.

Example Use:

If a hacker hides an image in audio using **Photosounder**, Audacity can reveal it by displaying frequency patterns.

- ## Steganography – Use of OGR Tool

OGR Tool (OutGuess GUI Runner):

- A GUI-based steganographic tool for embedding/extracting hidden messages in media.

- Uses **OutGuess**, a command-line stego tool that embeds data in JPEGs using statistical steganography.

Features:

- Hide/extract text or files in JPEG images.

- Preserve statistical characteristics to avoid detection.

- GUI simplifies the complex command-line operations.

How to Use:

1. Choose a carrier image (e.g., `cover.jpg`).

2. Select a secret file or text to embed.

3. Run the hide command.

4. Later, use "Extract" to retrieve the hidden content.

Use Case:

Useful for **secure messaging**, **CTFs (Capture The Flag)** challenges, and **forensic analysis**.

- ## Steganography – Deepsound Tool

DeepSound:

A **Windows-based audio steganography tool** used to **embed secret files into WAV or FLAC files**.

Features:

- Hide documents, archives, or any file in audio.

- Encrypts data with password protection.

- Outputs natural-sounding audio (no distortion).

- Supports **AES-256 encryption**.

How to Use:

1. Open DeepSound.

2. Import a `.wav` file as carrier.

3. Add secret files.

4. Optionally set password.

5. Export stego audio.

Extraction:

Use DeepSound again to open the stego audio and extract hidden files.

Good for covert transmission of files or for **digital forensics training**.

- ## Steganography – DeEgger Tool

DeEgger Embedder:

- Lightweight tool for **steganography in images and audio**.

- Capable of embedding data inside JPG, WAV, etc.

- Focuses on **simplicity and stealth**.

Features:

1. Hide multiple files inside a single carrier.

2. Uses **basic obfuscation**, not strong encryption.

3. No visual/audio degradation of the carrier.

4. Drag-and-drop UI for quick use.

Use Cases:

- Ethical hacking practice

- Red-team steganography

- Educational stego labs

Steps:

1. Select a carrier file (image or audio).

2. Choose file(s) to hide.

3. Embed and export stego file.

4. Later use the tool to extract the hidden data.

By : Brahmjot Kaur URN : 2302501 CRN : 2315045