الجامعة الاسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يونيبرسيتي اسلام انتارابغسا مليسيا
Garden of Knowledge and Virtue

KULLIYYAH OF INFORMATION AND TECHNOLOGY
CSCI 2304 INTELLIGENT SYSTEMS
SEMESTER I, 2024/2025

PROJECT REPORT
SUBMISSION DATE: 20/1/2025

Project Team Name: **Nasi Kandar**

Crime Case of Investigation: **Identity Theft**

Team members:

Name	Matric No	Responsibility in the project
MOHAMAD WAZIR BIN NORDIN	2215353	1. Coordination with all team members as the Project Leader. 2. Discovery of white-hat evidence. 3. Coming up with innovative ideas for black-hat. 4. Encoding and encrypting evidence for submission. 5. Compiling all evidence for submission.
MOHAMAD HAFIZ BIN MOHD JAIS	2218827	1. Discovery of white-hat evidence. 2. Documenting the appendix for both black hat and white hat. 3. Implementation of ICECTF skills for blackhat(html). 4. Updating the master plan of the project for more comprehension. 5. Completed the report writing, and revision of appendixes.
MUHAMMAD AMIRUL HAZIQ BIN MUHAMAD HASMAHADI	2319959	1. Discovery of white-hat evidence. 2. Collaborating with Wazir and Hafiz to come up with creative black hat ideas. 3. Double-checking report writing and appendix. 4. Keeping the project on track. 5. Evaluate and test all evidence.
MUHAMMAD AMMAR BIN MOHD ASRI	2114617	1. Contribution to report writing.

TABLE OF CONTENTS

1. Introduction **2**
1.1 Background 2
1.2 Case Overview 2
2. Objectives **2**
3. Methodology **2**
3.1 Investigation Tools 2
3.2 Investigation Process 3
4. Findings **3**
4.1 White Hat Investigation Results 3
4.2 Black Hat Implementation 5
5. Conclusion **9**
5.1 Summary of Findings 9
5.2 Challenges and Solutions 10
5.3 Recommendations 10
6. Appendices **11**

1. Introduction

1.1 Background

This is the group project report done by group Nasi Kandar of section 3 for the course CSCI 2303 Principles of IT security. The project is divided into two main components. The first part is the White Hat Investigation which consists of applying techniques learned from class in order to unravel hidden information by decrypting and finding hidden messages. The second part of the project is the Black Hat activity where the group utilizes encryption, steganography, and obfuscation techniques learned from class in order to conceal information and digital evidence according to the scenario.

1.2 Case Overview

Case Scenario:

You are at a crime scene, which is the home of a suspected cybercriminal named Eddy. According to the police, Eddy as an imposter obtains key pieces of personally identifiable information (PII), such as Social Security or driver's license numbers, to impersonate someone else. The chief police officer tells you that Eddy used his email to get the instruction from an unknown friend. They also communicate by using hidden tactics known as steganography to hide the information.

By examining Eddy's laptop, you find out that there are many suspicious files and steganography installed on the laptop including S-Tools, Quick Stego, SNOW, and Oursecret. There is one suspicious file named arjVqragvgl.zip saved on the computer Desktop.

Overview from case scenario: Eddy is the name of a suspected cybercriminal, is under investigation for identity theft and impersonation. Eddy's laptop contains multiple steganography tools (S-Tools, Quick Stego, SNOW, Oursecret). A suspicious file named arjVqragvgl.zip located on the Desktop. The investigation centers around analyzing a provided artifact (.ZIP file) containing multiple pieces of hidden evidence using various steganographic and forensic techniques.

2. Objectives

The main objectives of this project are to :

1. To identify and analyze at least five pieces of hidden evidence within the provided artifact
2. To demonstrate proficiency in using digital forensic tools and techniques
3. To create five challenging pieces of hidden evidence using various concealment techniques
4. To enhance practical understanding of digital forensics methodologies

3. Methodology

3.1 Investigation Tools

These are the tools utilized in order to unravel hidden messages.

Name of Tool	Purpose	Tool link(file)
1. S-tools	Analyzing and extracting data hidden in image files.	None (S-tools software)
2. QuickStego	Examining file structures and hidden data	None (Quickstego software)
3. MorseCode Translator	Decode messages in Morse code into understandable messages.	https://morsecode.world/international/translator.html

3.2 Investigation Process

Part 1: White Hat Investigation

1. Initial Assessment
2. Performed preliminary analysis of the ZIP file
3. Identified file types and potential areas of investigation
4. Evidence Discovery
5. Applied systematic analysis using various tools
6. Documented each step and finding

Part 2: Black Hat Implementation

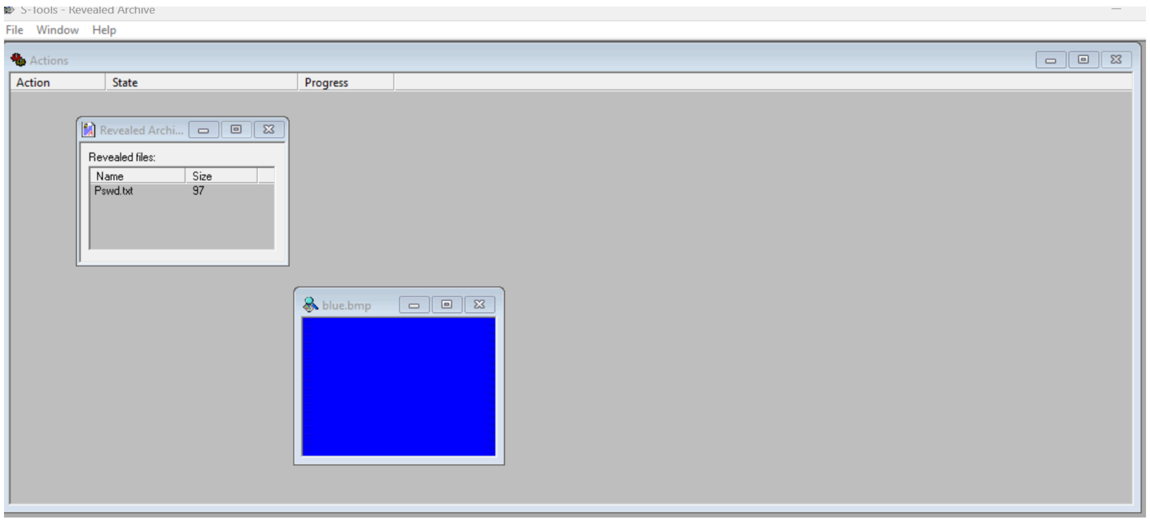
1. Evidence Creation
2. Selected appropriate concealment methods
3. Implemented various hiding techniques
4. Solution Documentation
5. Created step-by-step recovery guides
6. Verified solution reproducibility

4. Findings

4.1 White Hat Investigation Results

These are the results of the investigation that we extracted from 6 hidden messages.

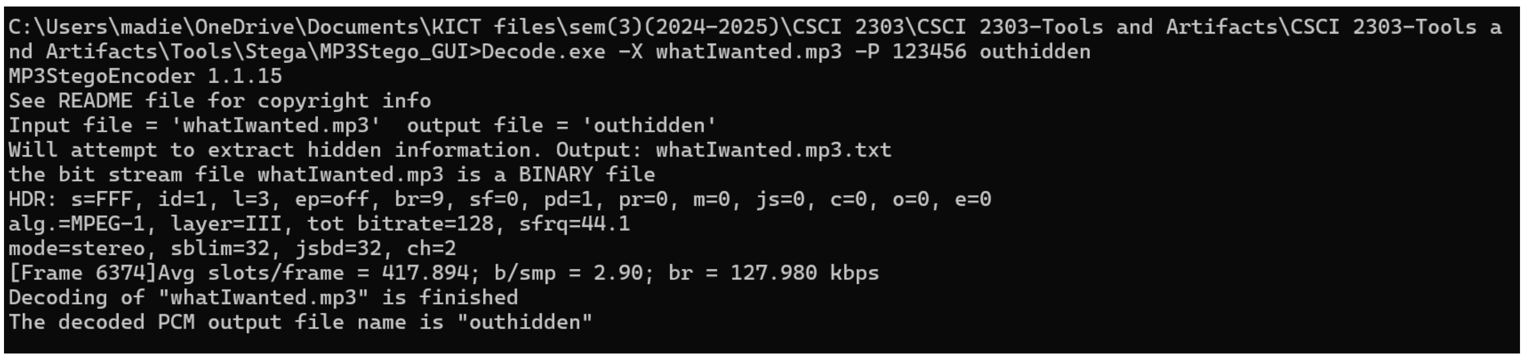
1. Utilizing s-tools to uncover the hidden message in blue.bmp which revealed pswrd.txt.



Revealed files:

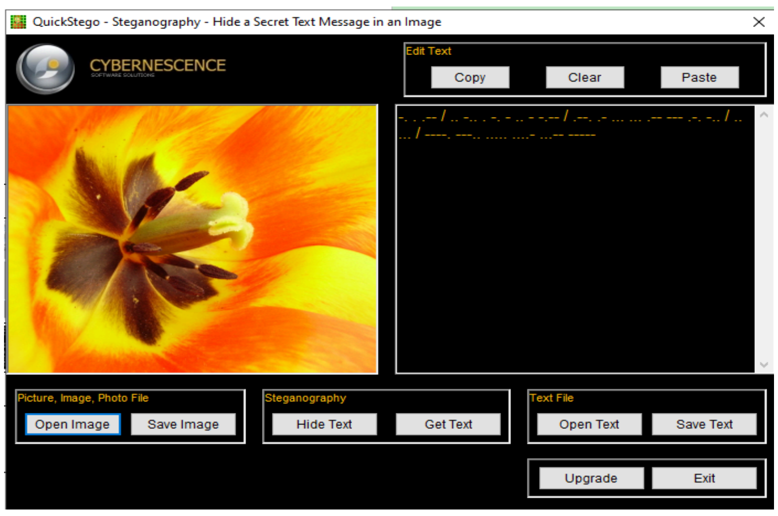
Name	Size
Pswd.txt	97

2. The use of mp3steno and cmd in order to reveal the hidden message in whatIwanted.mp3. In addition, it was discovered that the decryption password of the mp3 is 12345 in ch14.pptx/



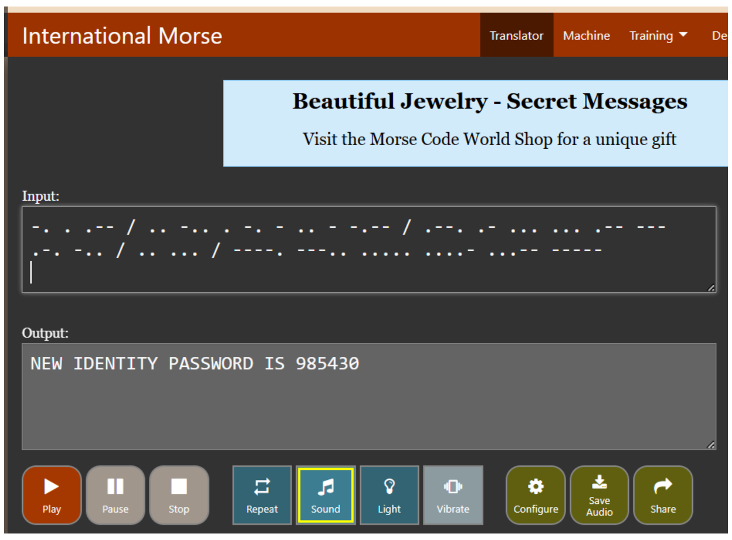
```
C:\Users\madie\OneDrive\Documents\KICT files\sem(3)(2024-2025)\CSCI 2303\CSCI 2303-Tools and Artifacts\CSCI 2303-Tools a
nd Artifacts\Tools\Stega\MP3Stego_GUI>Decode.exe -X whatIwanted.mp3 -P 123456 outhidden
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'whatIwanted.mp3'  output file = 'outhidden'
Will attempt to extract hidden information. Output: whatIwanted.mp3.txt
the bit stream file whatIwanted.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 6374]Avg slots/frame = 417.894; b/smp = 2.90; br = 127.980 kbps
Decoding of "whatIwanted.mp3" is finished
The decoded PCM output file name is "outhidden"
```

3. The hidden message in flower-1193218 was simple to find since it did not require any passphrase, therefore QuickStego was used in order to unravel the morse code for “NEWIDENTITYPASSWORDIS985430” in the image. This step required mp3 quickStego and morse code translator.



QuickStego - Steganography - Hide a Secret Text Message in an Image

```
-. . .-- / .. -.. . -. - .. - -.-- / .--. .- ... ... .-- --- .-. -.. / ..
... / ----. ---.. ..... ....- ...-- -----
```



International Morse

Beautiful Jewelry - Secret Messages

Visit the Morse Code World Shop for a unique gift

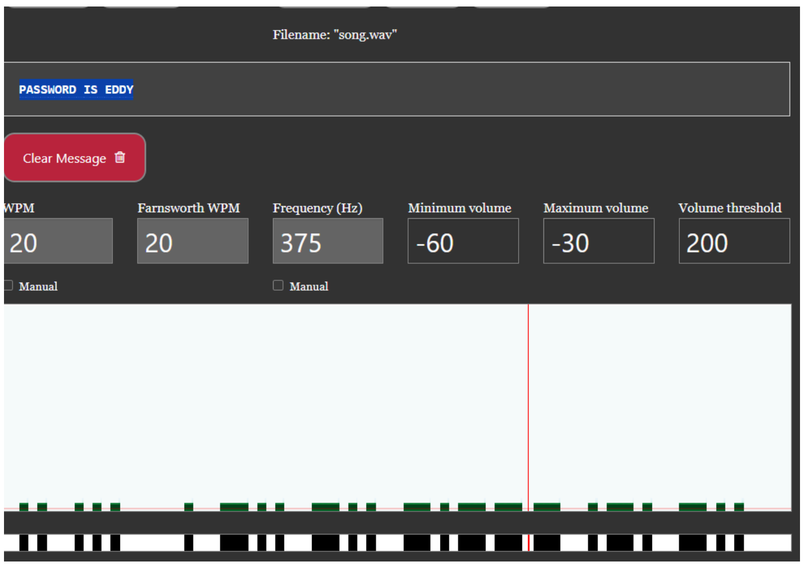
Input:

```
-. . .-- / .. -.. . -. - .. - -.-- / .--. .- ... ... .-- ---
.-. -.. / .. ... / ----. ---.. ..... ....- ...-- -----
```

Output:

```
NEW IDENTITY PASSWORD IS 985430
```

4. song,wav is a morse code audio which revealed “PASSWORD IS EDDY” after decryption. the password is extracted using Morse Code Translator

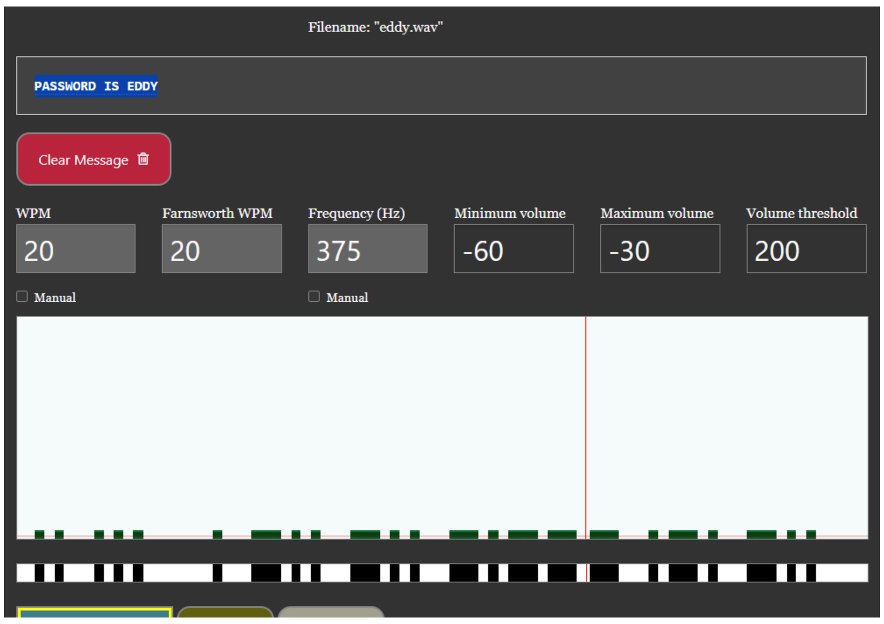


Filename: "song.wav"

```
PASSWORD IS EDDY
```

WPM: 20
Farnsworth WPM: 20
Frequency (Hz): 375
Minimum volume: -60
Maximum volume: -30
Volume threshold: 200

5. like song.wav, Eddy.wav is also a morse code audio which revealed “PASSWORD IS EDDY” after decryption. the password is extracted using Morse Code Translator

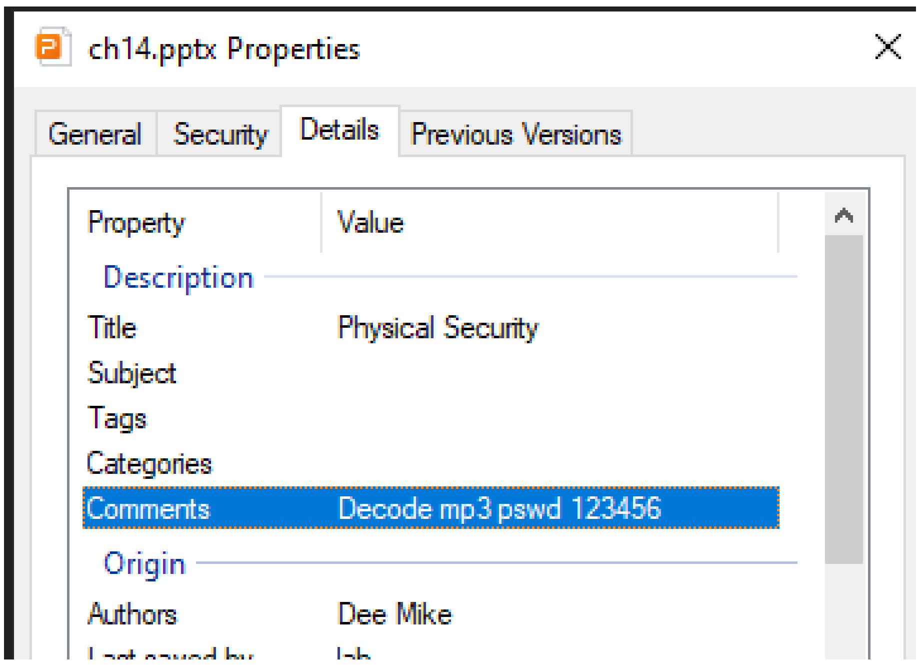


Filename: "eddy.wav"

```
PASSWORD IS EDDY
```

WPM: 20
Farnsworth WPM: 20
Frequency (Hz): 375
Minimum volume: -60
Maximum volume: -30
Volume threshold: 200

6. ch14.pptx was a case of obfuscation, where the hidden information was not in the file but actually hidden in the file properties, where it revealed Decode mp3 pswd 123456

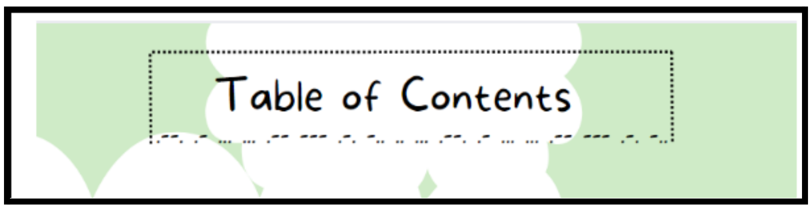


ch14.pptx Properties

Property	Value
Description	
Title	Physical Security
Subject	
Tags	
Categories	
Comments	Decode mp3 pswd 123456
Origin	
Authors	Dee Mike
Last saved by	lab

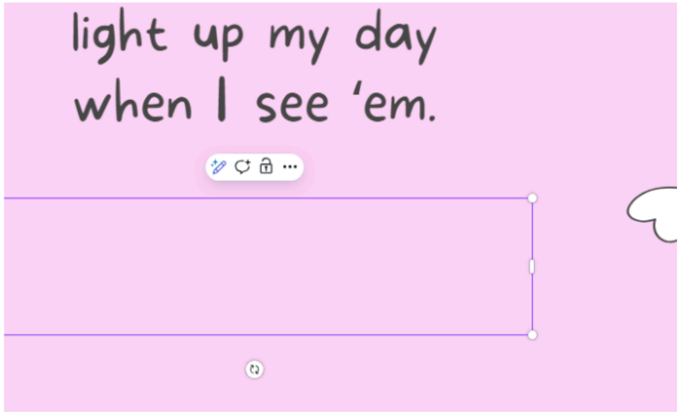
4.2 Black Hat Implementation

1. We use the morse code as a conceal method to hide the evidence of Passlove file using the morse code encoder.The hidden message which is PASSWORDISPASSWORD is located at the title header of the third slide.



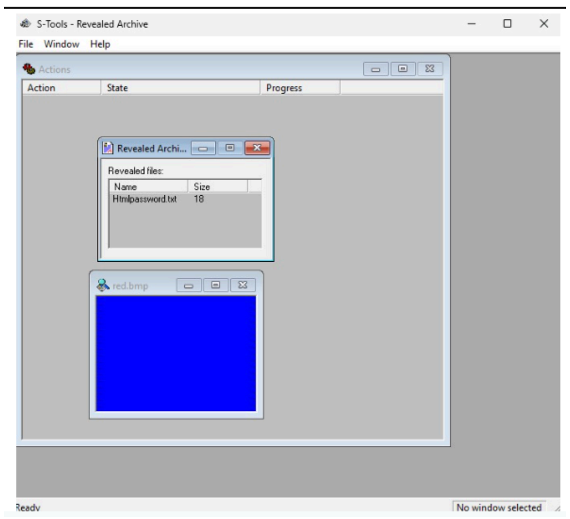
Concealment Steps	Recovery Steps
1. Create a canva slide to hide the secret message 2. hidden text is hidden in morse code located around the border	1. victim analyse the content and look carefully what hidden in the particular slide and the morse code is hidden along the border of "Table of Contents" 2. then the morse code is copied and paste into Morse Code Translator.

2. Stega and Rot13 have been implemented for self made Youtube link using stenography. The message hidden is the link itself that is located at the blank space of under text in the fifth slide. this is called as Obfuscation Technique



Concealment Steps	Recovery Steps
1. set the color of the text same as background	1. copy the blank hidden text in the box as shown. 2. paste the plain text in Rot13

3. Steganography technique has been applied using S-tools for red.bmp. The hidden message contained is Htmlpassword.txt located in the image. User needs to discover the pass key which is “ PASSWORD “.

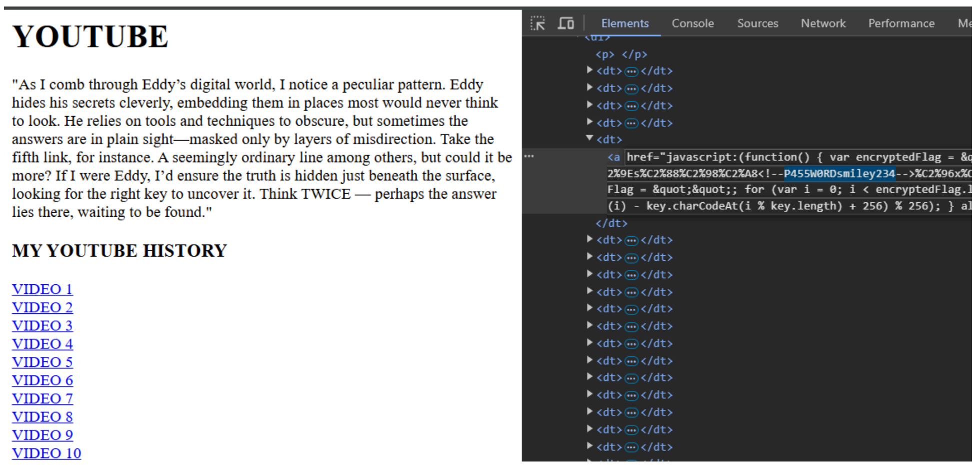


Revealed files:

Name	Size
Htmlpassword.txt	18

Concealment Steps	Recovery Steps
1. Using S-Tools, the **Htmlpassword.txt** file was embedded into **red.bmp** 2. The hidden message can be retrieved by loading the steganographed image into S-Tools and entering the correct passkey ("PASSWORD")	1. load the ‘red.bmp’ file in the steganography 2. upload image in Quick Stego and click the button ‘Get Text’ button to reveal the hidden text in the image file

4. MyYoutubeHistory.html is also Obsfucation Technique where the password is hidden in the inspect element. user has to find the password from listed youtube links. one of the twenty links provided is not working and user will get the hint from header in the html. the 5th link is the crashed URL and user has to get the password from that particular link in the inspect element.



YOUTUBE

"As I comb through Eddy’s digital world, I notice a peculiar pattern. Eddy hides his secrets cleverly, embedding them in places most would never think to look. He relies on tools and techniques to obscure, but sometimes the answers are in plain sight—masked only by layers of misdirection. Take the fifth link, for instance. A seemingly ordinary line among others, but could it be more? If I were Eddy, I’d ensure the truth is hidden just beneath the surface, looking for the right key to uncover it. Think TWICE — perhaps the answer lies there, waiting to be found."

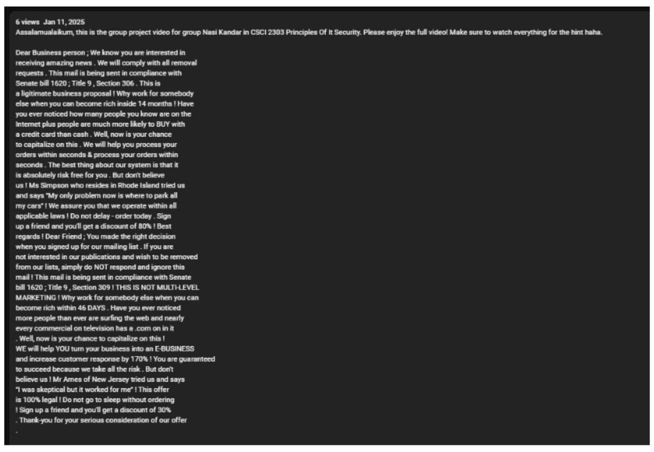
MY YOUTUBE HISTORY

VIDEO 1
VIDEO 2
VIDEO 3
VIDEO 4
VIDEO 5
VIDEO 6
VIDEO 7
VIDEO 8
VIDEO 9
VIDEO 10

```
<p> </p>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>
  <a href="javascript:(function() { var encryptedFlag = &q
  2%9Es%C2%88%C2%98%C2%A8<!--P455W0RDsmiley234-->%C2%96x%C
  Flag = &quot;&quot;; for (var i = 0; i < encryptedFlag.l
  (i) - key.charCodeAt(i % key.length) + 256) % 256); } al
</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
<dt>…</dt>
```

Concealment Steps	Recovery Steps
1. Create a list of youtube links and provide hint to navigate the 5th link as the location of hidden password 2. Hide the password in the navigated of the 5th link in inspect element	1. right click on the html file to open the inspect element 2. navigate to the 5th link in the inspect element and analyse the hidden password between the strings hidden in the element

5. We use encryption and steganography to conceal the descriptive file using spam mimic tools. to hide the evidence of Passlove slide using the morse code encoder.The hidden message which is eddyStinks is located in the description of the video.

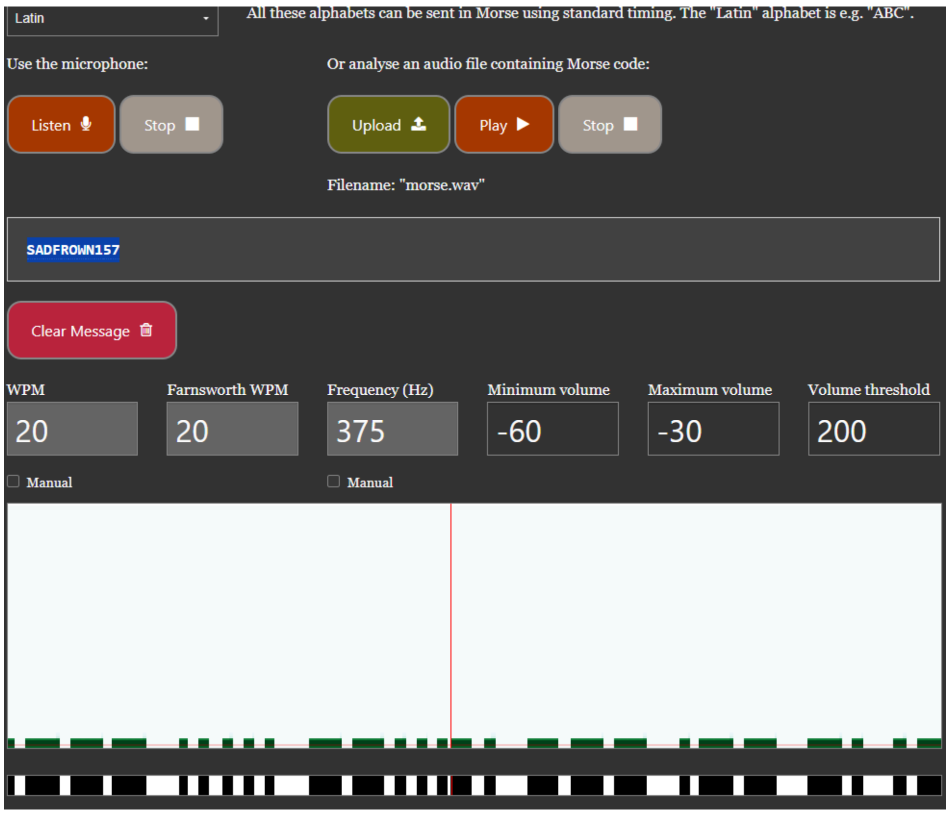


6 views Jan 11, 2025
Assalamualaikum, this is the group project video for group Nasi Kandar in CSCI 2303 Principles Of It Security. Please enjoy the full video! Make sure to watch everything for the hint haha.

Dear Business person ; We know you are interested in
receiving amazing news . We will comply with all removal
requests . This mail is being sent in compliance with
Senate bill 1620 ; Title 9 , Section 306 . This is
a ligitimate business proposal ! Why work for somebody
else when you can become rich inside 14 months ! Have
you ever noticed how many people you know are on the
Internet plus people are much more likely to BUY with
a credit card than cash . Well, now is your chance
to capitalize on this . We will help you process your
orders within seconds & process your orders within
seconds . The best thing about our system is that it
is absolutely risk free for you . But don't believe
us ! Ms Simpson who resides in Rhode Island tried us
and says "My only problem now is where to park all
my cars" ! We assure you that we operate within all
applicable laws ! Do not delay - order today . Sign
up a friend and you'll get a discount of 80% ! Best
regards ! Dear Friend ; You made the right decision
when you signed up for our mailing list . If you are
not interested in our publications and wish to be removed
from our lists, simply do NOT respond and ignore this
mail ! This mail is being sent in compliance with Senate
bill 1620 ; Title 9 , Section 309 ! THIS IS NOT MULTI-LEVEL
MARKETING ! Why work for somebody else when you can
become rich within 46 DAYS . Have you ever noticed
more people than ever are surfing the web and nearly
every commercial on television has a .com on in it
. Well, now is your chance to capitalize on this !
WE will help YOU turn your business into an E-BUSINESS
and increase customer response by 170% ! You are guaranteed
to succeed because we take all the risk . But don't
believe us ! Mr Ames of New Jersey tried us and says
"I was skeptical but it worked for me" ! This offer
is 100% legal ! Do not go to sleep without ordering
! Sign up a friend and you'll get a discount of 30%
. Thank-you for your serious consideration of our offer
.

Concealment Steps	Recovery Steps
1. Create a password with a SpamMimic tools(Website) to create a fake Spam Messages 2. Hide it inside the Description down below in Youtube Videos	1. Copy all the spam messages and paste it into the Spammimic decoder tools(Website) 2. You will get the password to unlock the RAR file

6. We used Morse Code wav file to hide the password inside an audio file.

7. 

Latin

All these alphabets can be sent in Morse using standard timing. The "Latin" alphabet is e.g. "ABC".

Use the microphone:

Or analyse an audio file containing Morse code:

Filename: "morse.wav"

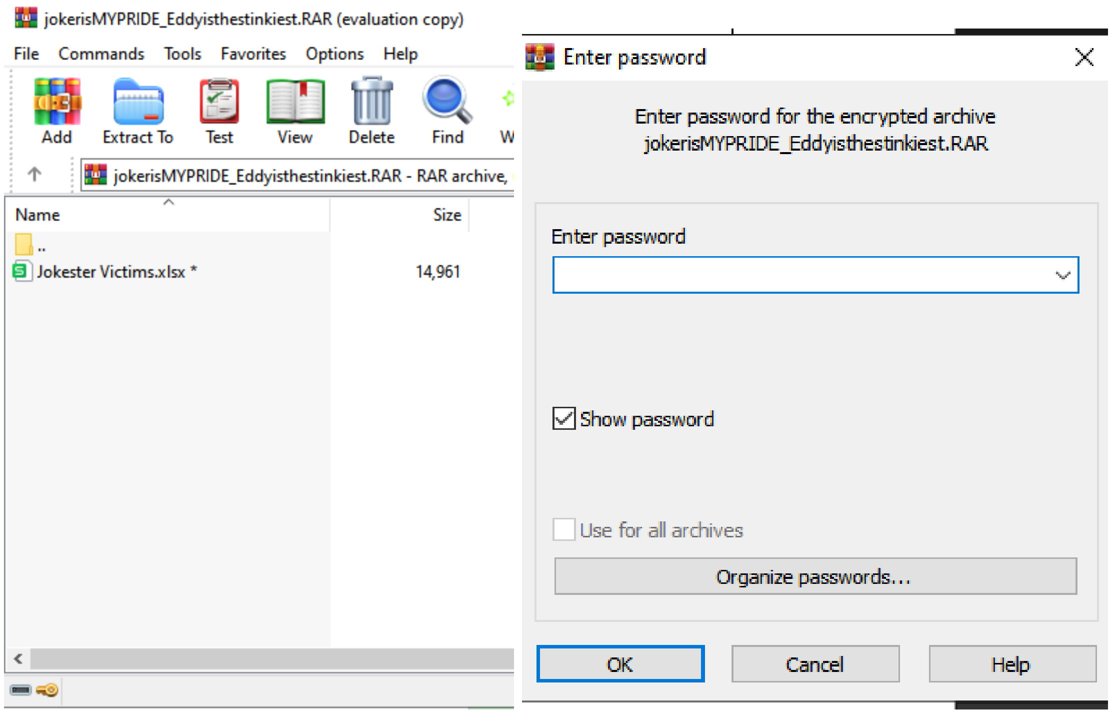
SADFROWN157

WPM: 20
Farnsworth WPM: 20
Frequency (Hz): 375
Minimum volume: -60
Maximum volume: -30
Volume threshold: 200

□ Manual
□ Manual

Concealment Steps	Recovery Steps
1. Make a custom Morse Code file using Morse Code Encoder to encode the message intended 2. Download the Morsecode audio File	1. Put the Morse Code audio file into the Decoder ones and let it play 2. Password will be shown as “SADFROWN157”

8. We locked both the Excel file in different Winrar so that User will have to solve the riddles first and try to find their way to find 2 keys which can unlock both of the RAR file


jokerisMYPRIDE_Eddyisthestinkiest.RAR (evaluation copy)

jokerisMYPRIDE_Eddyisthestinkiest.RAR - RAR archive,

Name	Size
..	
Jokester Victims.xlsx *	14,961

Enter password

Enter password for the encrypted archive jokerisMYPRIDE_Eddyisthestinkiest.RAR

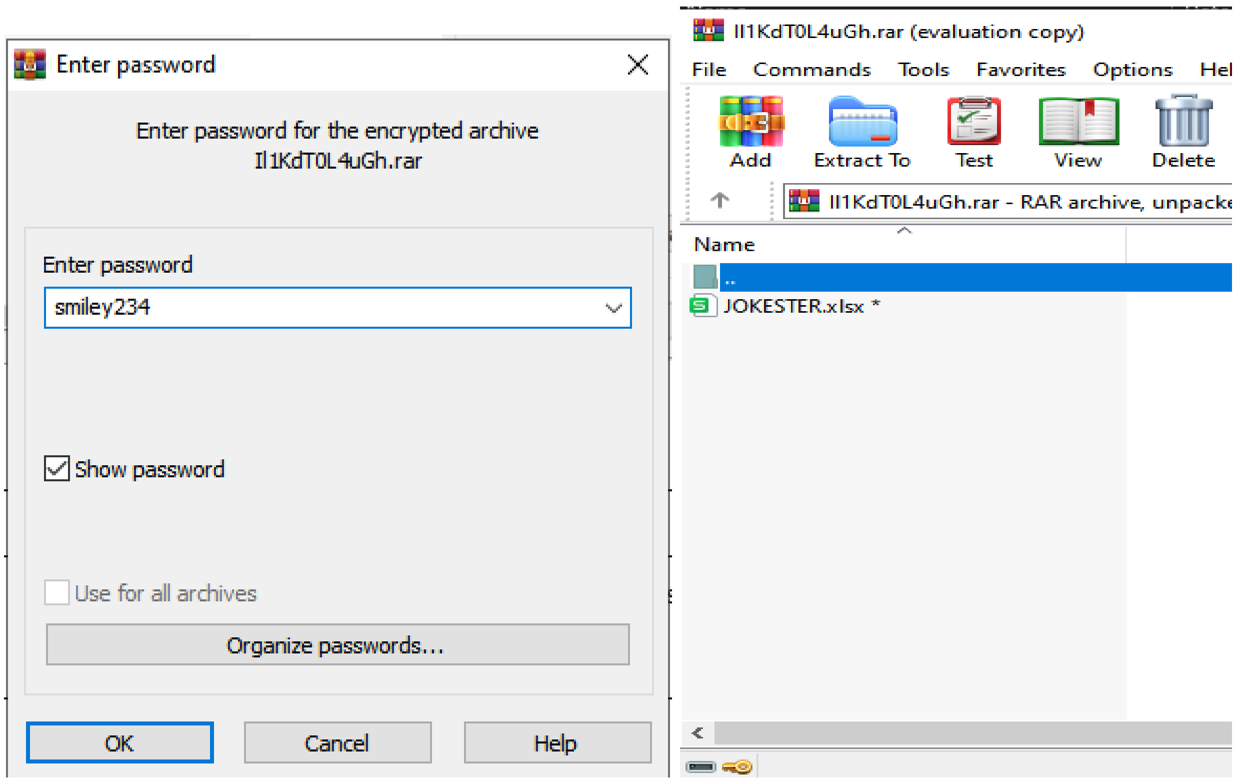
Enter password

☑ Show password

□ Use for all archives

Concealment Steps	Recovery Steps
1. create a rar file, locate the file, right-click, choose “Set password,” and enter chosen password	1. Put the password ‘SADFROWN157’ to unlock the files

9. Same goes to this Excel file which will expose the second part of the Black Hat evidence


Enter password

Enter password for the encrypted archive Il1KdT0L4uGh.rar

Enter password: smiley234

☑ Show password

□ Use for all archives

Il1KdT0L4uGh.rar (evaluation copy)

Il1KdT0L4uGh.rar - RAR archive, unpacke

Name

..

JOKESTER.xlsx *

Concealment Steps	Recovery Steps
1. create a rar file, locate the file, right-click, choose “Set password,” and enter chosen password	1. Put the password ‘smiley234’ to unlock the 2nd part of the evidence

5. Conclusion

5.1 Summary of Findings

1. White Hat Investigation:

During the investigation, six hidden pieces of evidence were successfully identified, revealing critical information. A hidden message within blue.bmp was extracted using S-tools, leading to the discovery of pswrd.txt. Similarly, whatIwanted.mp3 concealed a message decoded with MP3Steno using the password 12345. A visual examination of the flower-1193218 image uncovered a Morse code message, "NEWIDENTITYPASSWORDIS985430." Additionally, two audio files, song.wav and Eddy.wav, both encoded with Morse code, revealed the phrase "PASSWORD IS EDDY." Finally, obfuscated information within the metadata of ch14.pptx provided the MP3 decode password, further unlocking crucial data. These findings collectively contributed significant evidence to the case.

2. Black Hat Implementation:

A variety of data concealment techniques were employed to create eight pieces of hidden evidence, showcasing advanced methods of information hiding. A Morse code message embedded in the PassLove file revealed "PASSWORDISPASSWORD," while steganography combined with ROT13 encoding concealed a YouTube link. S-tools steganography was used in red.bmp to hide Htmlpassword.txt. Additional hidden content was stored within a RAR file, and an HTML file was protected by the password smiley234. Spam Mimic encryption in a descriptive file encoded the message "eddyStinks." MP3 steganography, secured with the password sadFrown157, provided another layer of concealment, and an Excel file contained further hidden content. These diverse techniques demonstrate a comprehensive approach to securing and obscuring sensitive information.

5.2 Challenges and Solutions

Challenges	**Solutions**
Multiple layers of encryption and passwords requiring sequential solving	● Create a systematic password management system ● Implement a structured unlocking workflow
Various tools and techniques needed for different file types	● Standardize the toolkit ● Tool management
Complex implementation of different steganography methods	● Create implementation templates ● Testing procedures ● Practice scenario first and gradually increase complexity
Need to maintain comprehensive documentation of all steps	● Standardize documentation ● Documentation management ● regular review of documentation accuracy
Coordination between white hat discovery and black hat implementation	● Project management improvements ● Workflow optimization ● regular review session between teams

5.3 Recommendations

1.Process Improvements:

To ensure consistency and efficiency in steganography projects, a standardized template for documenting implementations should be developed, detailing the tools, techniques, and parameters used. A comprehensive checklist for testing hidden evidence recovery will help verify successful extraction and integrity of concealed data. Clear naming conventions for files and passwords must be established to maintain clarity and organization. Additionally, implementing version control for different stages of evidence creation will allow for better tracking, management, and refinement of processes throughout the project lifecycle.

2.Technical Enhancements:

To enhance data concealment strategies, exploring more advanced steganography tools will provide improved functionality and security. Implementing multi-layer encryption techniques can add additional protection to hidden information. Developing more sophisticated password schemes will increase resistance to unauthorized access. Additionally, creating automated testing procedures for evidence verification will streamline the process of ensuring data integrity and successful recovery, improving overall efficiency and reliability.

3. Documentation Updates:

To improve the efficiency and clarity of recovery procedures, detailed flowcharts should be created to visually map each step. Implementing standardized screenshot documentation will ensure consistent visual records for reference. Clear step-by-step guides for each technique will enhance reproducibility and understanding for users. Additionally, maintaining a central repository of all tools and methods used will provide easy access and organization, fostering better management and collaboration in future projects.

4. Security Improvements:

To strengthen data security and obfuscation, implementing more complex password combinations will increase resistance to brute-force attacks. Using multiple encryption layers adds additional barriers against unauthorized access. Creating decoy files and false paths can mislead intruders and protect real data. Additionally, implementing time-based or sequential unlocking mechanisms will enhance control and make unauthorized recovery more challenging, providing a robust and multi-faceted approach to secure information concealment.

5. Training Recommendations:

To enhance skills and adaptability, regular practice with new steganography tools is essential for staying current with evolving technologies. Cross-training team members on different techniques will build a more versatile and knowledgeable team. Documenting best practices and lessons learned will provide a valuable reference for continuous improvement. Additionally, creating training scenarios for new techniques will foster hands-on learning and better prepare the team for real-world applications and challenges.

6. Appendices

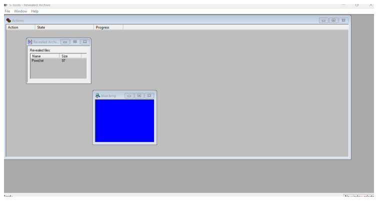
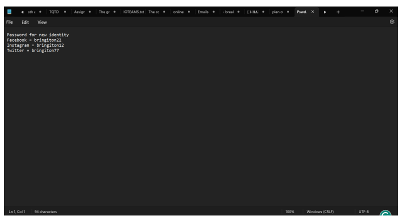
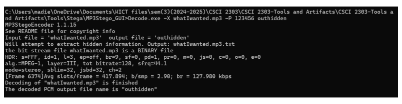
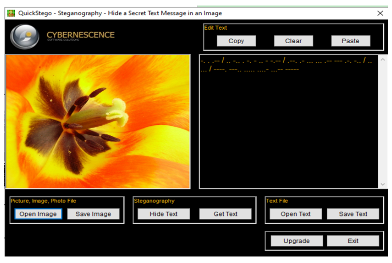
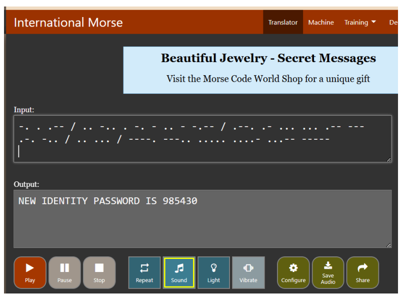
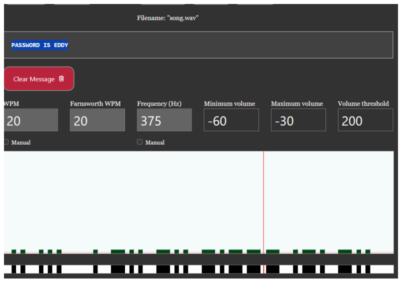
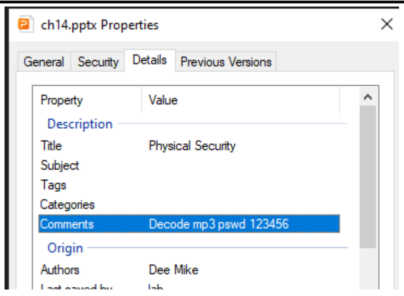
DIGITAL EVIDENCE SUMMARY

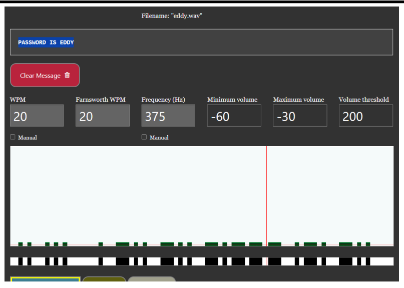
PART 1 [WHITE HAT]:INSPECTING DIGITAL EVIDENCE

Case ID:14

Case Name: Identity Theft

Analyzed By: Nasi Kandar

No	Evidence Name	Technique Used	Tools Utilized	Hidden message	Hidden message Location	Passphrase (if any)	Screenshot	Remarks
1	blue.bmp	Steganography (Reveal message)	S-tools	pswrd.txt	inside blue.bmp	eddy	 S-Tools - Revealed Archive Revealed files: Name Size Pswd.txt 97  Password for new identity Facebook = bringiton22 Instagram = bringiton12 Twitter = bringiton77 Ln 1, Col 1 94 characters 100% Windows (CRLF) UTF-8	
2	whatIwanted.mp3	Steganography	mp3 steno, cmd	eddy IDEA	-	Using the "123456" from the ch14.pptx	 C:\Users\madie\OneDrive\Documents\KICT files\sem(3)(2024-2025)\CSCI 2303\CSCI 2303-Tools and Artifacts\CSCI 2303-Tools and Artifacts\Tools\Stega\MP3Stego_GUI>Decode.exe -X whatIwanted.mp3 -P 123456 outhidden MP3StegoEncoder 1.1.15 See README file for copyright info Input file = 'whatIwanted.mp3' output file = 'outhidden' Will attempt to extract hidden information. Output: whatIwanted.mp3.txt the bit stream file whatIwanted.mp3 is a BINARY file HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0 alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1 mode=stereo, sblim=32, jsbd=32, ch=2 [Frame 6374]Avg slots/frame = 417.894; b/smp = 2.90; br = 127.980 kbps Decoding of "whatIwanted.mp3" is finished The decoded PCM output file name is "outhidden"	
3	flower-1193218	Steganography	QuickStego,Morse code translator	NEW IDENTITY PASSWORD IS 985430	Inside the flower picture	-	 QuickStego - Steganography - Hide a Secret Text Message in an Image  International Morse Beautiful Jewelry - Secret Messages Visit the Morse Code World Shop for a unique gift Input: -. . .-- / .. -.. . -. - .. - -.-- / .--. .- ... .-- --- .-. -.. / .. ... / ----. ---.. ....- ...-- ----- Output: NEW IDENTITY PASSWORD IS 985430	
4	song.wav	Morse Code Decoding(Steganography)	Morse Code Translator	PASSWORD IS EDDY	Secret message encrypted using morse code	-	 Filename: "song.wav" PASSWORD IS EDDY WPM 20, Farnsworth WPM 20, Frequency (Hz) 375, Minimum volume -60, Maximum volume -30, Volume threshold 200 □ Manual □ Manual	
5	ch14.pptx	Obfuscation technique	none	Decode mp3 pswd 123456	Inside the comments of the file when you clicked properties	-	 ch14.pptx Properties General Security Details Previous Versions Property Value Description Title Physical Security Subject Tags Categories Comments Decode mp3 pswd 123456 Origin Authors Dee Mike Last saved by lab	

No	Evidence Name	Technique Used	Tools Utilized	Hidden message	Hidden message Location	Passphrase (if any)	Screenshot	Remarks
6	Eddy.wav	Morse Code Decoding	Morse Code Translator	PASSWORD IS EDDY	Secret message encrypted using morse code	-	 Filename: "eddy.wav" PASSWORD IS EDDY WPM: 20 Farnsworth WPM: 20 Frequency (Hz): 375 Minimum volume: -60 Maximum volume: -30 Volume threshold: 200 	

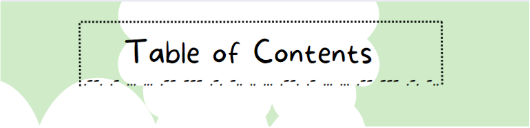
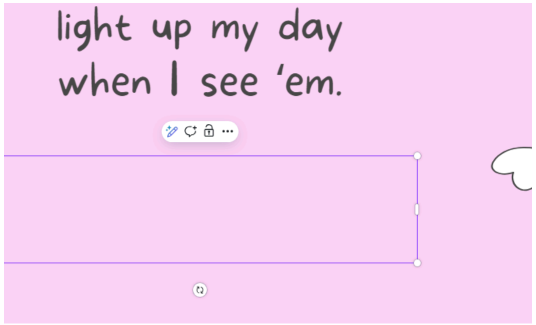
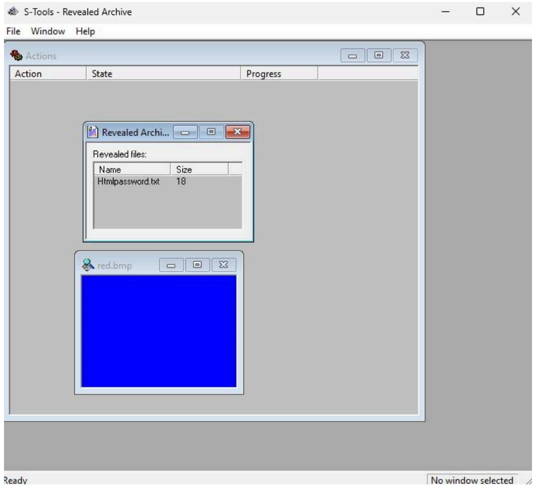
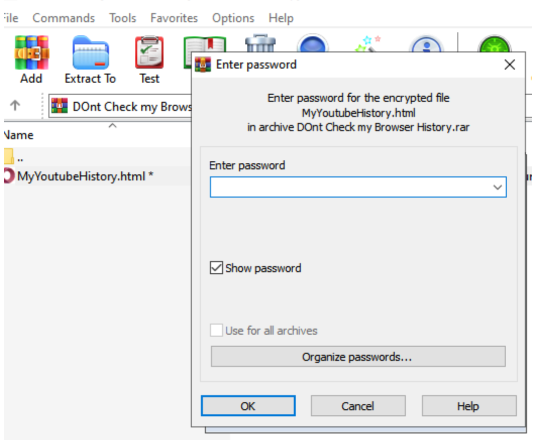
DIGITAL EVIDENCE SUMMARY

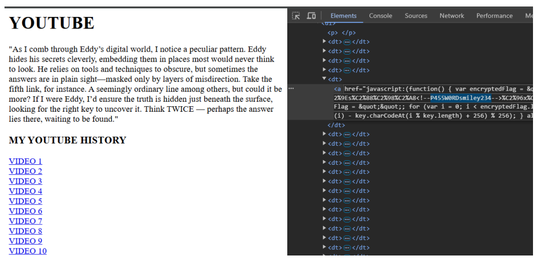
PART 2 [BLACK HAT]: HIDING DIGITAL EVIDENCE

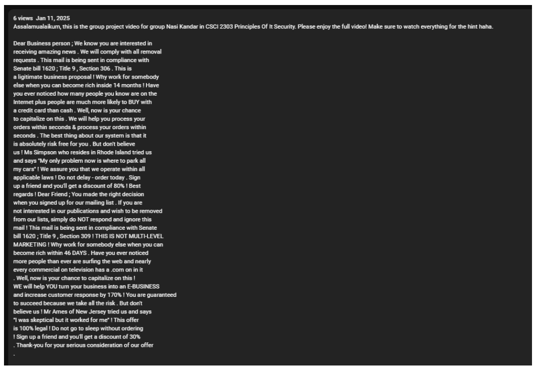
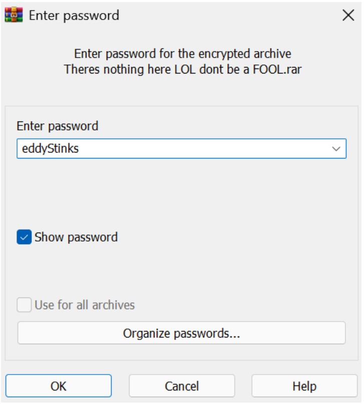
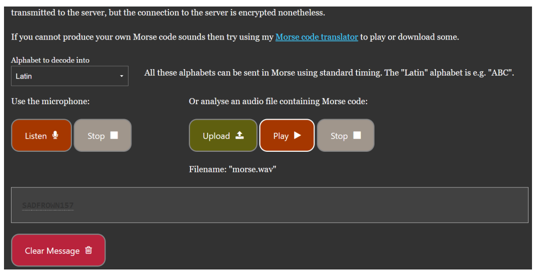
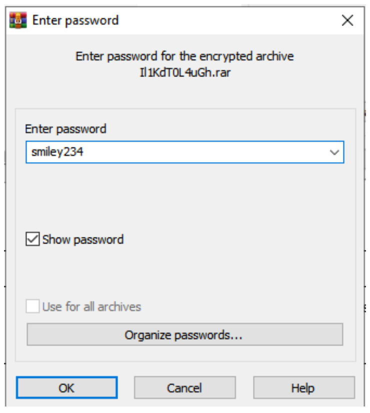
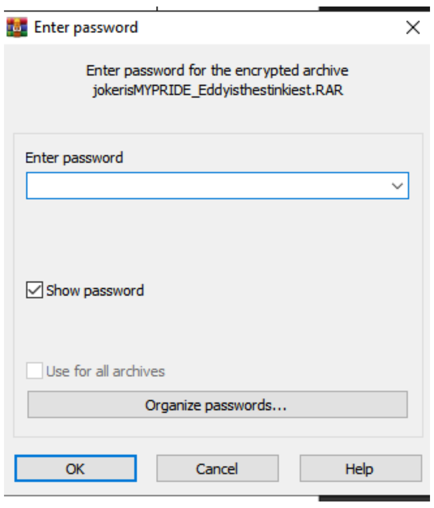
Case ID:14

Case Name: Identity Theft

Created By: Nasi Kandar

No	Evidence Name	Technique Used	Tools Utilized	Hidden message	Hidden message Location	Passphrase (if any)	Screenshot	Remarks
1	PassLove(The thing I love about you)	Morse Code	Morse code encoder	PASSWORDISPASSWORD	Title header of third slide	-	 Table of Contents	
2	Youtube Link (The thing I love about you)	Stega, rot13	Steno	https://youtu.be/OiJwcljdYqk	Blank Space of slide under text in fifth slide	-	 light up my day when I see 'em.	
3	red.bmp	Steganography	S-tools	Htmlpassword.txt	in the image	PASSWORD	 S-Tools - Revealed Archive File Window Help Actions Action State Progress Revealed Archi... red.bmp Ready No window selected Revealed files: Name: Htmlpassword.txt Size: 18	
4	DOnt Check my Browser History	-	-	-	-	hafizEncem	 ile Commands Tools Favorites Options Help Add Extract To Test DOnt Check my Brows Name .. MyYoutubeHistory.html * Enter password Enter password for the encrypted file MyYoutubeHistory.html in archive DOnt Check my Browser History.rar Enter password ☑ Show password □ Use for all archives Organize passwords... OK Cancel Help	

5	MyYoutubeHistory.html	Obsfucation Technique	Inspect	part1 password which is smiley234	in the inspect element	smiley234	 YOUTUBE
							"As I comb through Eddy's digital world, I notice a peculiar pattern. Eddy hides his secrets cleverly, embedding them in places most would never think to look. He relies on tools and techniques to obscure, but sometimes the answers are in plain sight—masked only by layers of misdirection. Take the fifth link, for instance. A seemingly ordinary line among others, but could it be more? If I were Eddy, I'd ensure the truth is hidden just beneath the surface, looking for the right key to uncover it. Think TWICE — perhaps the answer lies there, waiting to be found."
							MY YOUTUBE HISTORY
							VIDEO 1
							VIDEO 2
							VIDEO 3
							VIDEO 4
							VIDEO 5
							VIDEO 6
							VIDEO 7
							VIDEO 8
							VIDEO 9
							VIDEO 10
							`<p> </p>`
							`<dt>…</dt>`
							`<dt>…</dt>`
							`<dt>…</dt>`
							`<dt>…</dt>`
							`<dt>`
							`<a href="javascript:(function() { var encryptedFlag = &q`
							`2%9Es%C2%88%C2%98%C2%A8<!--P455W0RDsmiley234-->%C2%96x%C`
							`Flag = &quot;&quot;; for (var i = 0; i < encryptedFlag.l`
							`(i) - key.charCodeAt(i % key.length) + 256) % 256); } al`
							`</dt>`
							`<dt>…</dt>`	

6	Descriptive	Encryption and steganography	Spam Mimic	eddyStinks	in the description of the video	-	 6 views Jan 11, 2025 Assalamualaikum, this is the group project video for group Nasi Kandar in CSCI 2303 Principles Of It Security. Please enjoy the full video! Make sure to watch everything for the hint haha. Dear Business person ; We know you are interested in receiving amazing news . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1620 ; Title 9 , Section 306 . This is a ligitimate business proposal ! Why work for somebody else when you can become rich inside 14 months ! Have you ever noticed how many people you know are on the Internet plus people are much more likely to BUY with a credit card than cash . Well, now is your chance to capitalize on this . We will help you process your orders within seconds & process your orders within seconds . The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Ms Simpson who resides in Rhode Island tried us and says "My only problem now is where to park all my cars" ! We assure you that we operate within all applicable laws ! Do not delay - order today . Sign up a friend and you'll get a discount of 80% ! Best regards ! Dear Friend ; You made the right decision when you signed up for our mailing list . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 1620 ; Title 9 , Section 309 ! THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich within 46 DAYS . Have you ever noticed more people than ever are surfing the web and nearly every commercial on television has a .com on in it . Well, now is your chance to capitalize on this ! WE will help YOU turn your business into an E-BUSINESS and increase customer response by 170% ! You are guaranteed to succeed because we take all the risk . But don't believe us ! Mr Ames of New Jersey tried us and says "I was skeptical but it worked for me" ! This offer is 100% legal ! Do not go to sleep without ordering ! Sign up a friend and you'll get a discount of 30% . Thank-you for your serious consideration of our offer .	
7	Theres nothing here LOL dont be a FOOL	Steganography	Morse Code Translator	part2 password which is SADFROWN157	in the morsecode file	eddyStinks	 Enter password Enter password for the encrypted archive Theres nothing here LOL dont be a FOOL.rar Enter password eddyStinks ☑ Show password □ Use for all archives Organize passwords... OK Cancel Help  transmitted to the server, but the connection to the server is encrypted nonetheless. If you cannot produce your own Morse code sounds then try using my Morse code translator to play or download some. Alphabet to decode into Latin All these alphabets can be sent in Morse using standard timing. The "Latin" alphabet is e.g. "ABC". Use the microphone: Listen Stop Or analyse an audio file containing Morse code: Upload Play Stop Filename: "morse.wav" SADFROWN157 Clear Message	
8	Excelfile	-	-	-	-	smiley234 SADFROWN157	 Enter password Enter password for the encrypted archive Il1KdT0L4uGh.rar Enter password smiley234 ☑ Show password □ Use for all archives Organize passwords... OK Cancel Help  Enter password Enter password for the encrypted archive jokerisMYPRIDE_Eddyisthestinkiest.RAR Enter password ☑ Show password □ Use for all archives Organize passwords... OK Cancel Help	