ShadowCrypt

Proactive Ransomware Protection: Employing Camouflage and Concealment

Under the Guidance of

Ms. Sariya Jabeen Duriya

Assistant Professor, CSE - (IoT)

*****

Abdul Samad - 161021749020

Mohammed Abdul Raqeeb - 161021749035

Mohammed FasiUddin Arsalaan - 161021749041

Ransomware Description

- Malware encrypts files and demands ransom for decryption.
- Advanced variants of Ransomware evade traditional detection.

Example:

- LockBit operates as a "*Ransomware-as-a-Service*"
- "*Double Extortion*" - Encrypt data and also threaten to publish confidential information on DarkWeb

Objective

"Ransomware Protection through File Concealment"

Existing Systems (*Active*)

- Firewalls
- Intrusion Detection/Prevention Systems
- Endpoint Security solutions
- Backup and Recovery

Proposed System (*Proactive*)

- ✓ Minimize ransomware impact by hiding critical files.
- ✓ Ensure usability while preventing unauthorized encryption.

Key Concept

✓ Ransomware targets the user data (i.e. “C:\Users\”)

✗ Doesn’t target the system files with extensions “.dll” or “.exe”

Proposed Method

- This project presents a proactive defense strategy that minimizes damage even after ransomware attack.
- To protect user data from ransomware attack, we can -
  - User data ----> Rename & Move ----> System Directories
  - { .docx, .xlsx, .pptx, .pdf ....} ----> { .dll or .exe }
  - { .docx, .xlsx, .pptx, .pdf ....} <---- { .lnk }

Algorithm

Algorithm 1 Hiding and Recovery Function

Data: P, the list of included paths
Data: E, the list of included file extensions
Data: T, mapping table

```
1:  function HideFile(file)
2:      fileName ← RandomGenName()
3:      path ← RandomSelect(P)
4:      ext ← RandomSelect(E)
5:      hiddenFile ← path + fileName + ext
6:      MoveFile(file, hiddenFile)
7:      linkFile ← MakeLinkFile(file, hiddenFile)
8:      UpdateTable(T, hiddenFile, file, linkFile)
9:  end function
10: function RecoverFile(hiddenFile)
11:     file, linkFile ← PopTable(T, hiddenFile)
12:     MoveFile(hiddenFile, file)
13:     Delete(linkFile)
14: end function
```

Project Overview

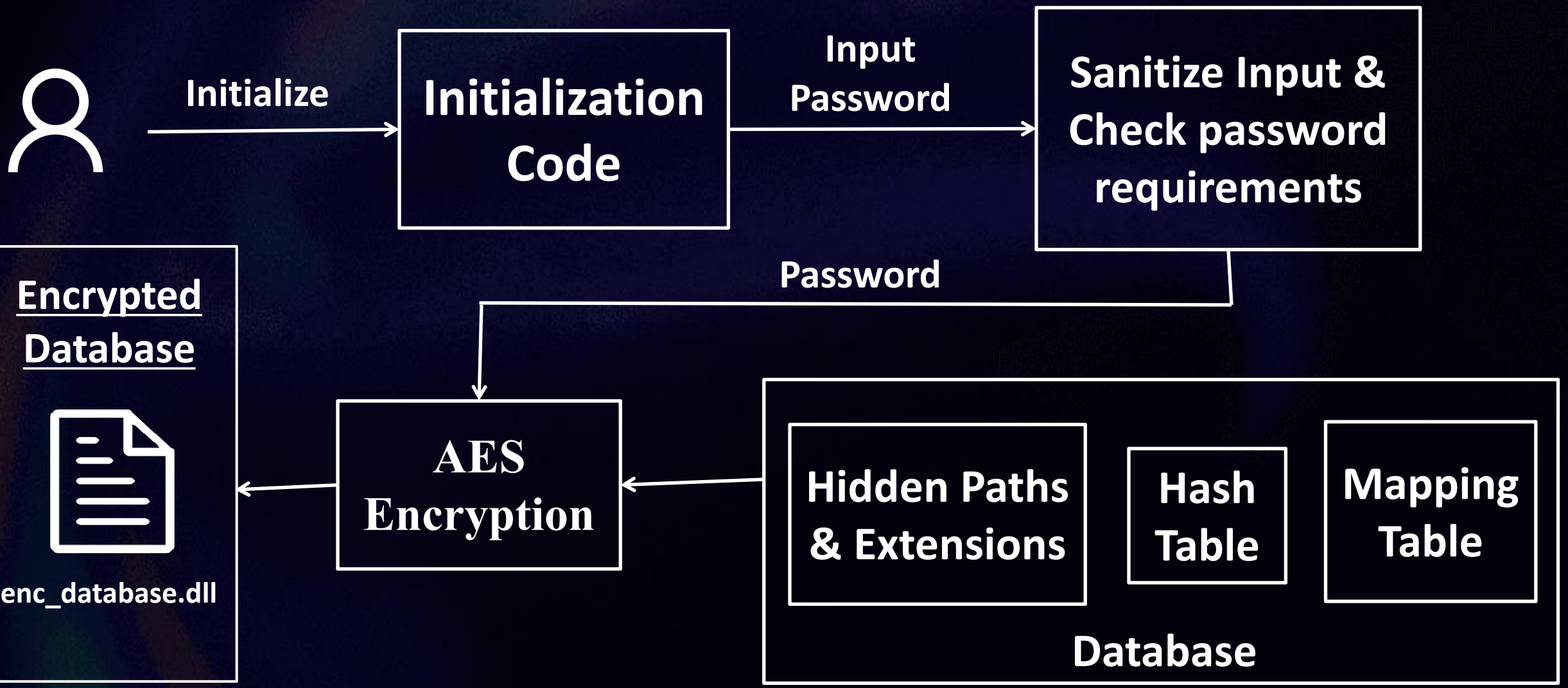
- **File Concealment**: Hide User files in System directories.
- **Encrypted Database**: Secures data for safe file tracking (Confidentiality)
- Store **Hashes** of Filepaths (Integrity)
- **Linker Mechanism**: Allows access to hidden files securely (Availability)
- **File Recovery**: Recover the hidden files back.

Tools and Technologies Used

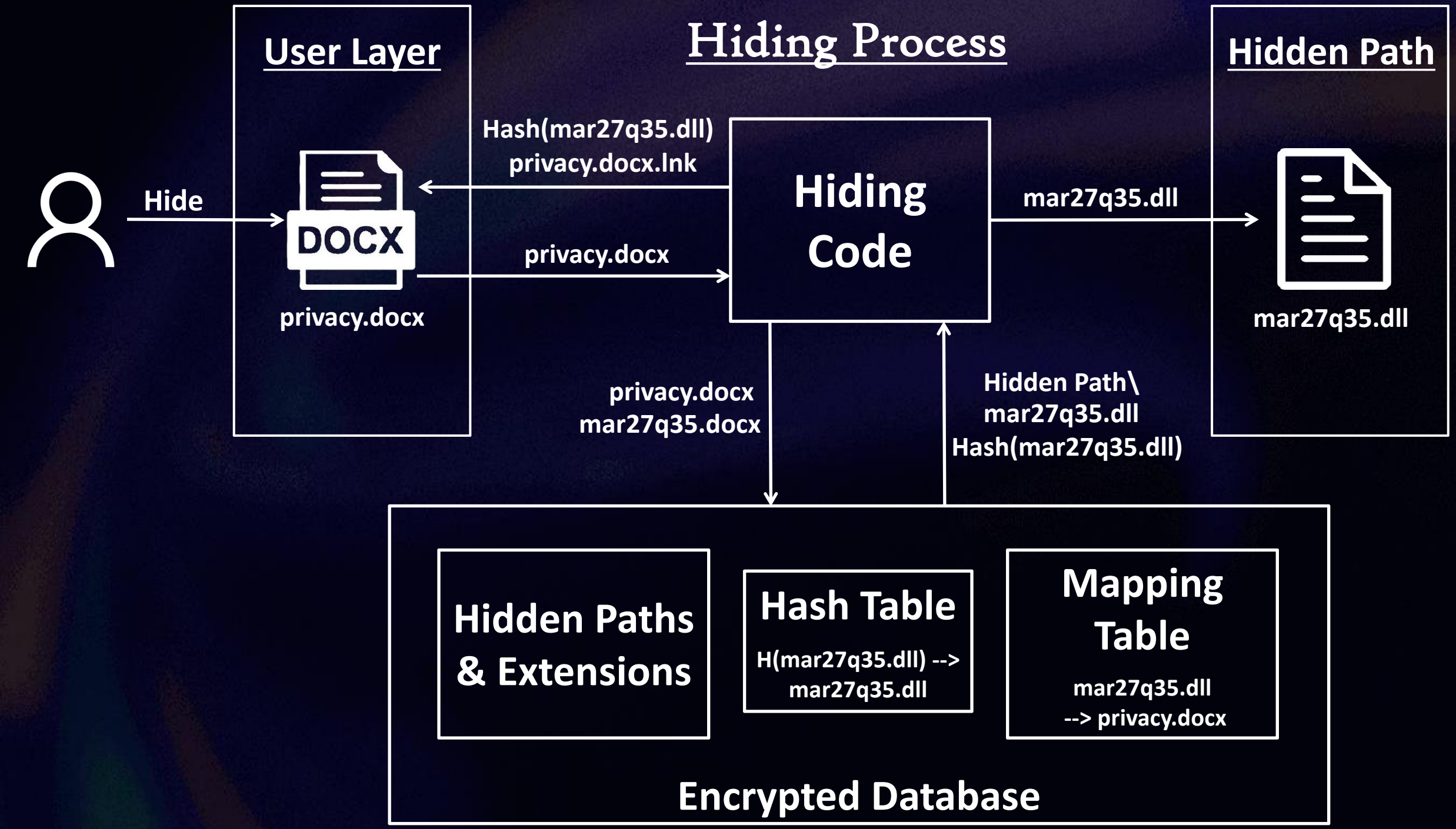
- **Target OS** : Windows
- **Languages** : Python, Powershell, Batch scripting
- **Python package manager** : UV
- **Encryption** : **AES**
- **Version Control** : Git, GitHub
- **Virtualization** : VirtualBox
- **Windows Installation builder software** : InstallForge

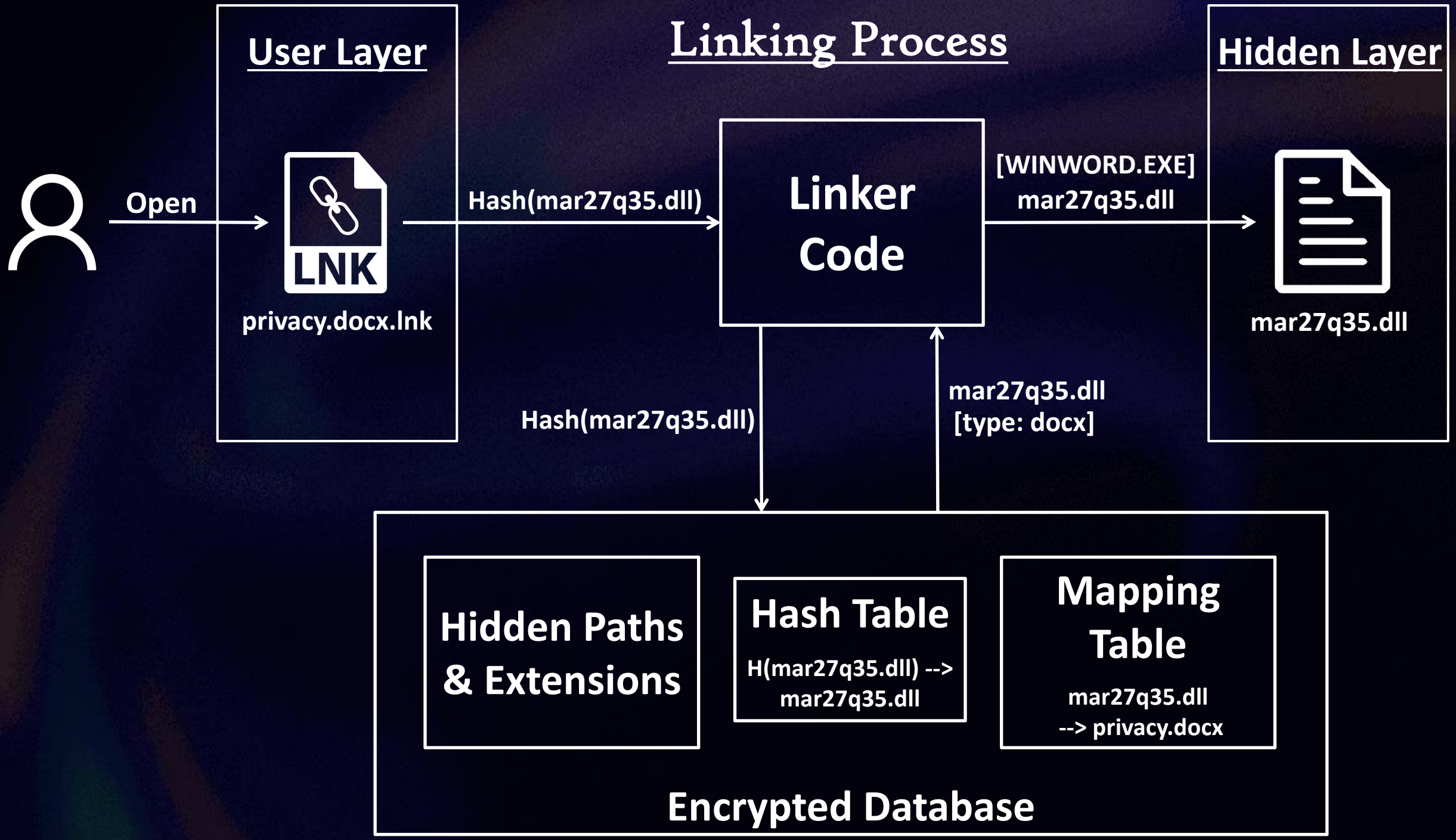
ARCHITECTURE

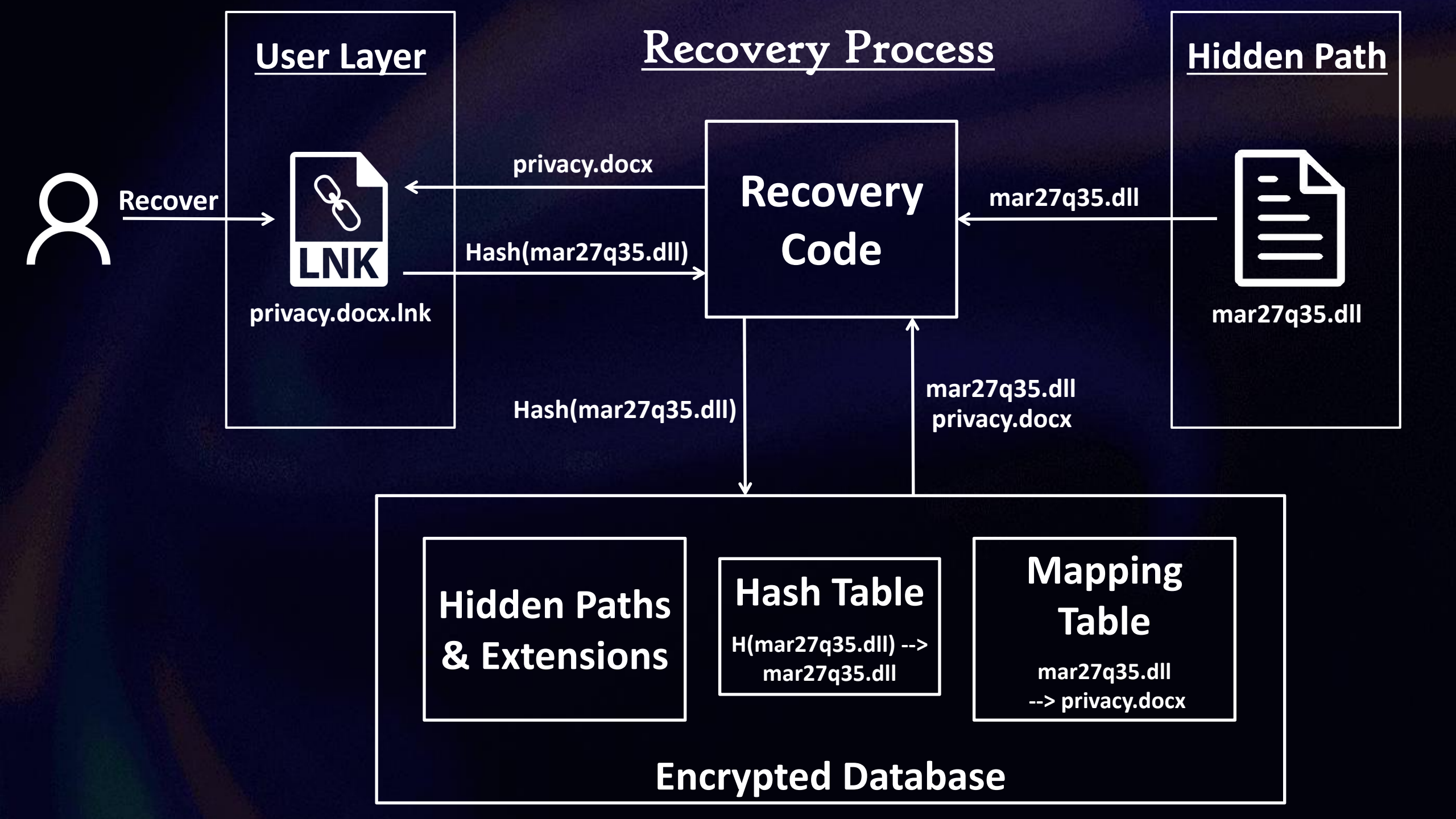
Database Initialization Process

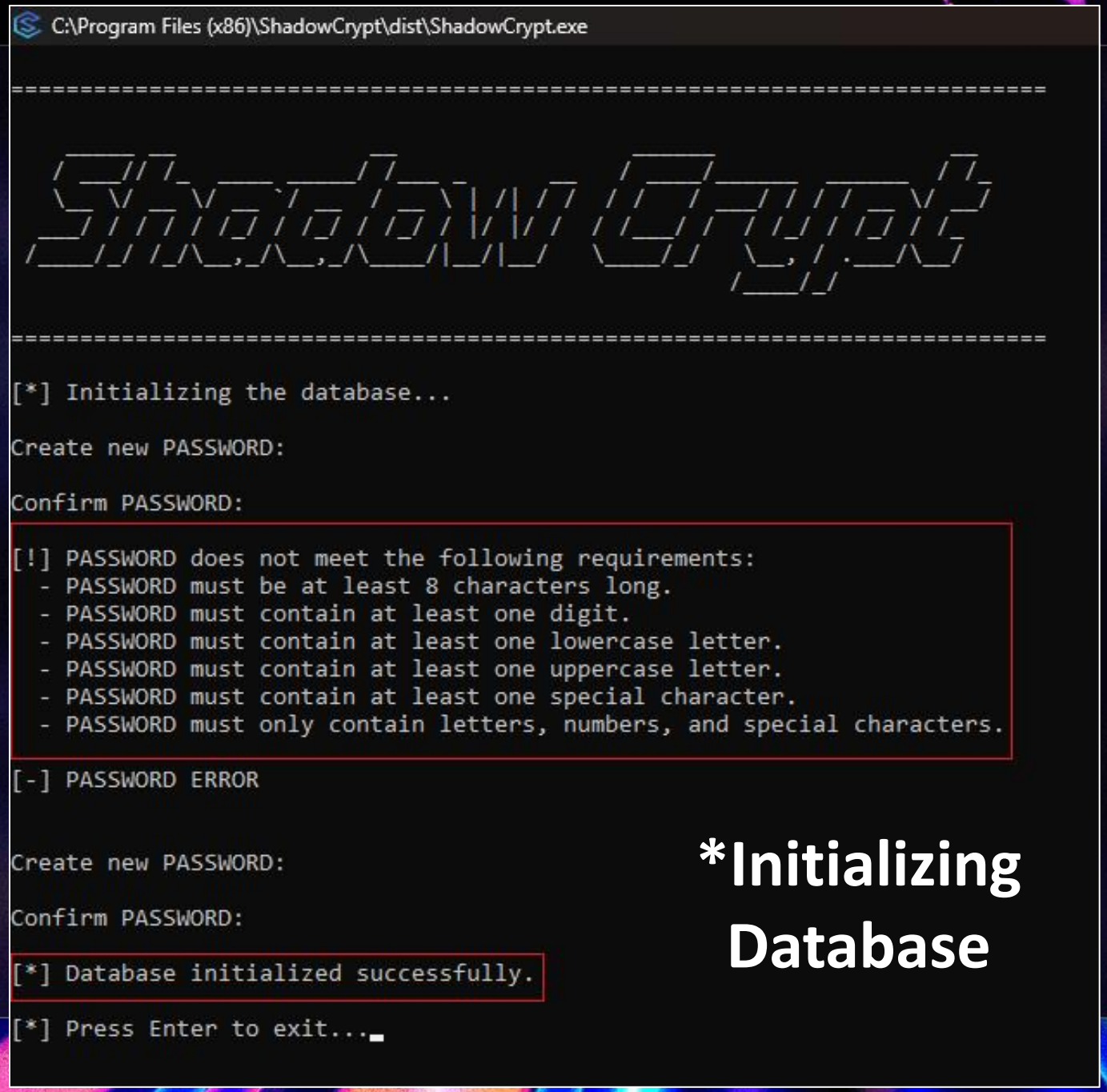


Hiding Process



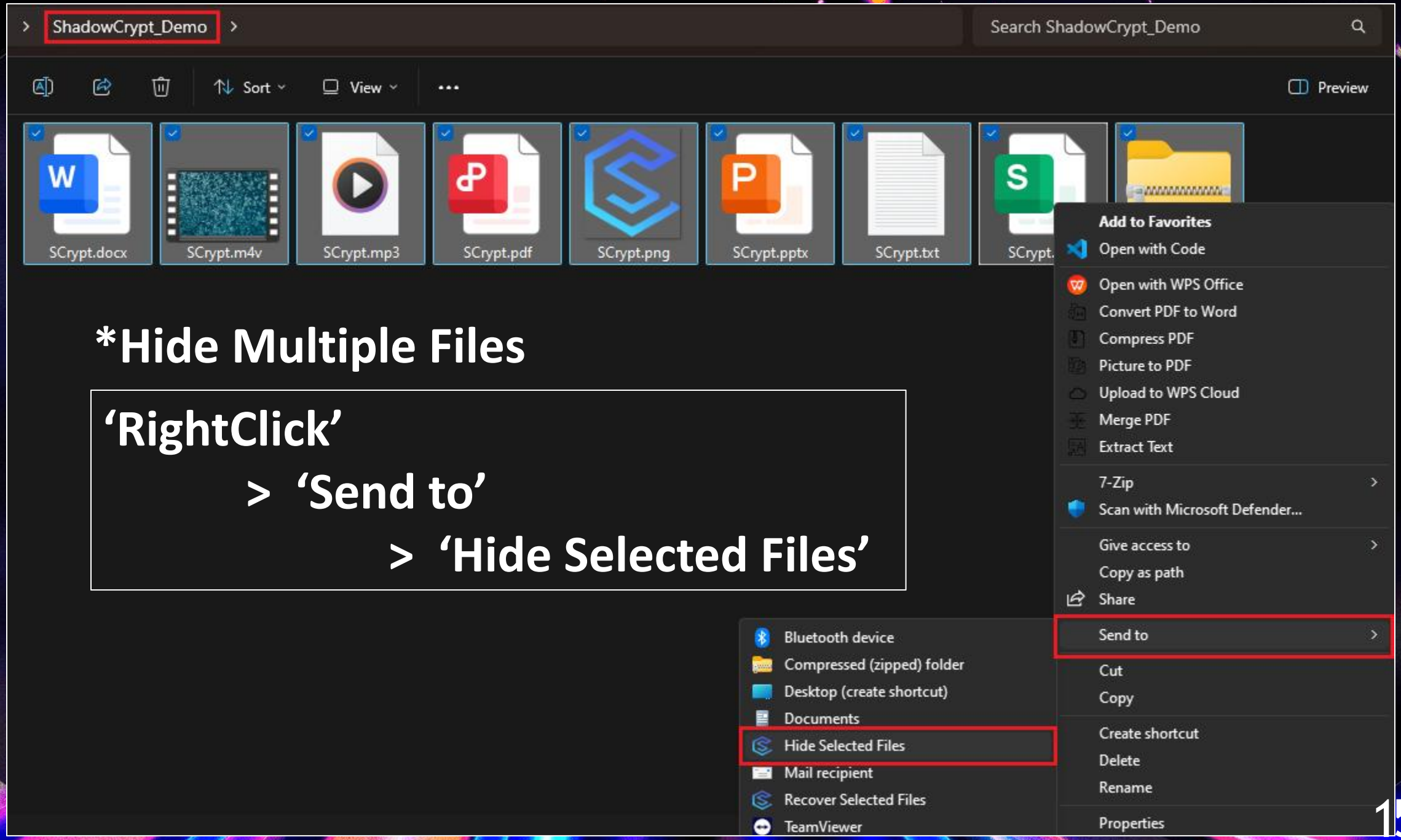

Linking Process
User Layer
Hidden Layer
Open
LNK
privacy.docx.lnk
Hash(mar27q35.dll)
Linker Code
[WINWORD.EXE]
mar27q35.dll
mar27q35.dll
Hash(mar27q35.dll)
mar27q35.dll
[type: docx]
Hidden Paths & Extensions
Hash Table
H(mar27q35.dll) --> mar27q35.dll
Mapping Table
mar27q35.dll --> privacy.docx
Encrypted Database


Recovery Process
User Layer
Hidden Path
Recover
LNK
privacy.docx.lnk
privacy.docx
Hash(mar27q35.dll)
Recovery Code
mar27q35.dll
mar27q35.dll
Hash(mar27q35.dll)
mar27q35.dll
privacy.docx
Hidden Paths & Extensions
Hash Table
H(mar27q35.dll) --> mar27q35.dll
Mapping Table
mar27q35.dll --> privacy.docx
Encrypted Database



*Initializing Database

Project Implementation



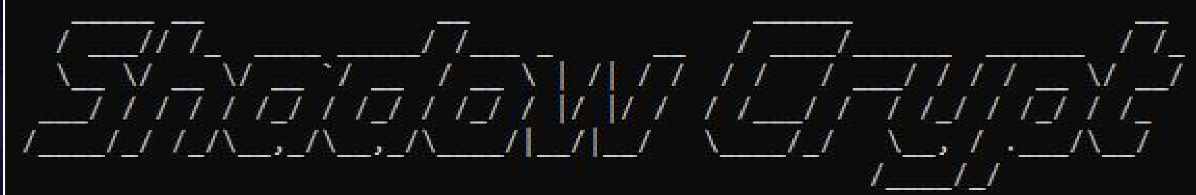
*Hide Multiple Files

‘RightClick’
> ‘Send to’
> ‘Hide Selected Files’

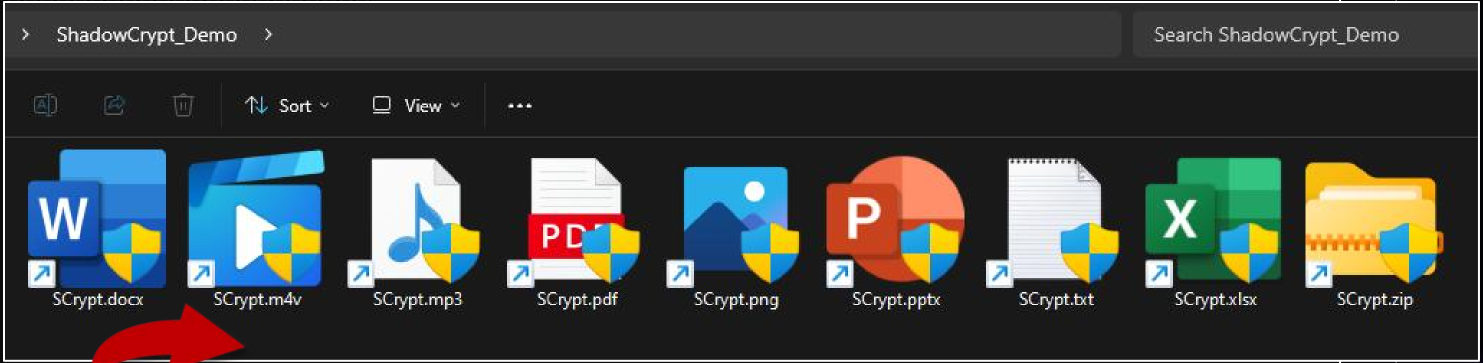
*Hiding Files

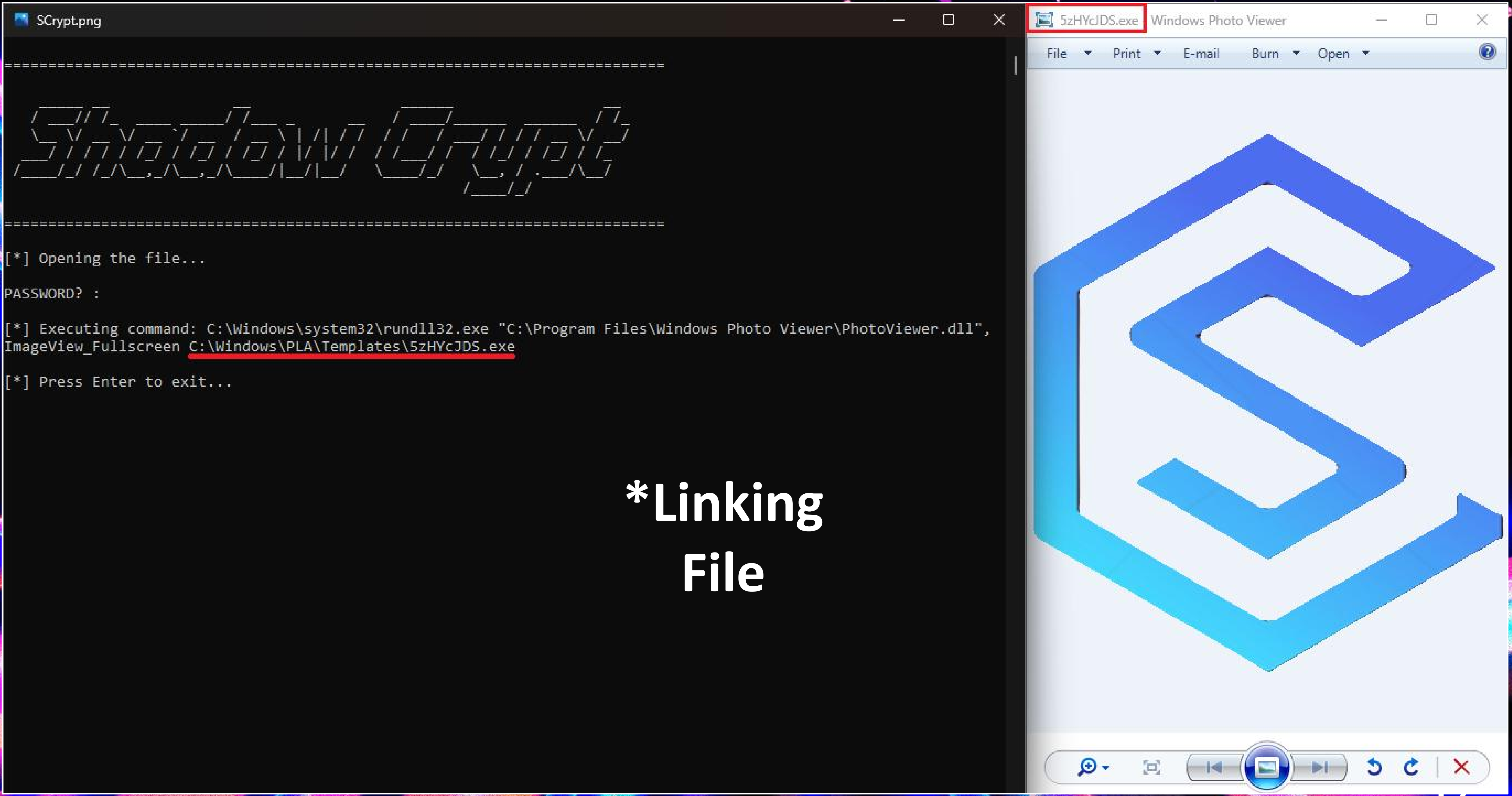
C:\Program Files (x86)\ShadowCrypt\dist\ShadowCrypt.exe

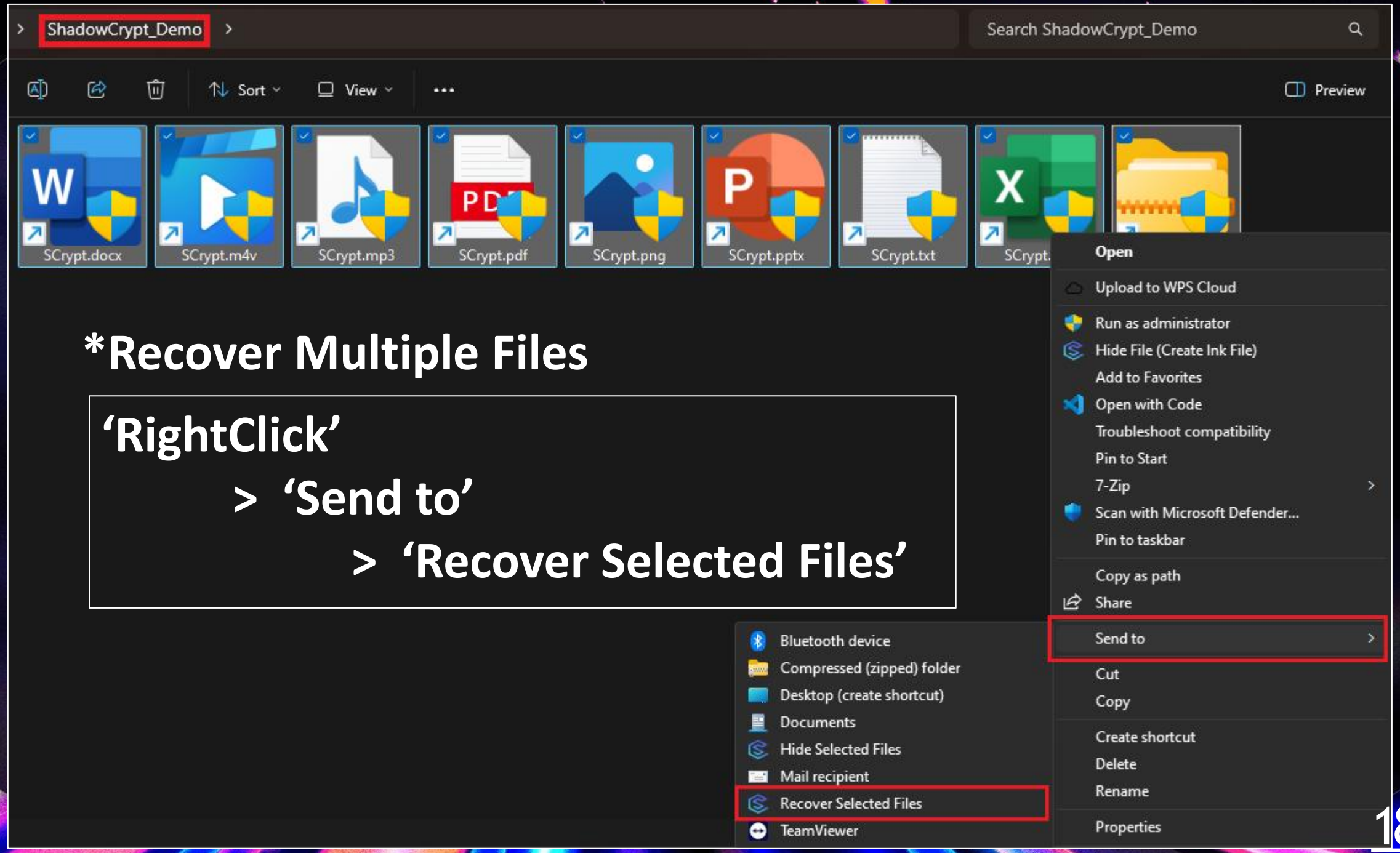
```
==========================================================================
```



```
==========================================================================

[*] Hiding files:
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.zip
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.docx
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.m4v
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.mp3
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pdf
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.png
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pptx
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.txt
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.xlsx

PASSWORD? :

[*] Supported Extensions:
['doc', 'docx', 'xls', 'xlsx', 'ppt', 'pptx', 'pdf', 'txt', 'zip', '7z', 'png', 'jpg', 'jpeg', 'mp3', 'wav', 'opus', 'mp4', 'm4v']

    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.zip -> C:\Windows\PLA\Templates\prFZaOIx.exe
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.docx -> C:\Windows\System32\Speech\Engines\wgN8sgQI.exe
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.m4v -> C:\Windows\System32\Speech\Engines\TDIy4mc2.dll
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.mp3 -> C:\Windows\PLA\Templates\5tbDq5hT.dll
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pdf -> C:\Windows\Help\ki4pJz39.exe
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.png -> C:\Windows\PLA\Templates\5zHYcJDS.exe
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pptx -> C:\Windows\Help\Windows\IndexStore\en-US\T9D1b0E7.dll
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.txt -> C:\Windows\PLA\Templates\FtbWKMxi.exe
    [+] Hiding success: C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.xlsx -> C:\Windows\System32\Speech\Engines\pf11mpZc.dll

[*] Press Enter to exit...
```




SCrypt.png
[*] Opening the file...
PASSWORD? :
[*] Executing command: C:\Windows\system32\rundll32.exe "C:\Program Files\Windows Photo Viewer\PhotoViewer.dll", ImageView_Fullscreen C:\Windows\PLA\Templates\5zHYcJDS.exe
[*] Press Enter to exit...
*Linking File
5zHYcJDS.exe Windows Photo Viewer
File Print E-mail Burn Open



*Recover Multiple Files

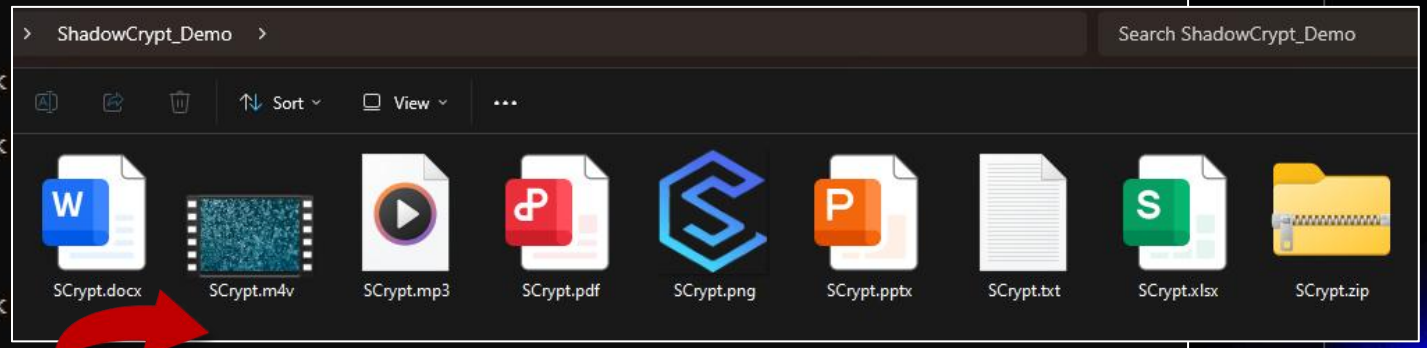
‘RightClick’

> ‘Send to’

> ‘Recover Selected Files’

C:\Program Files (x86)\ShadowCrypt\dist\ShadowCrypt.exe

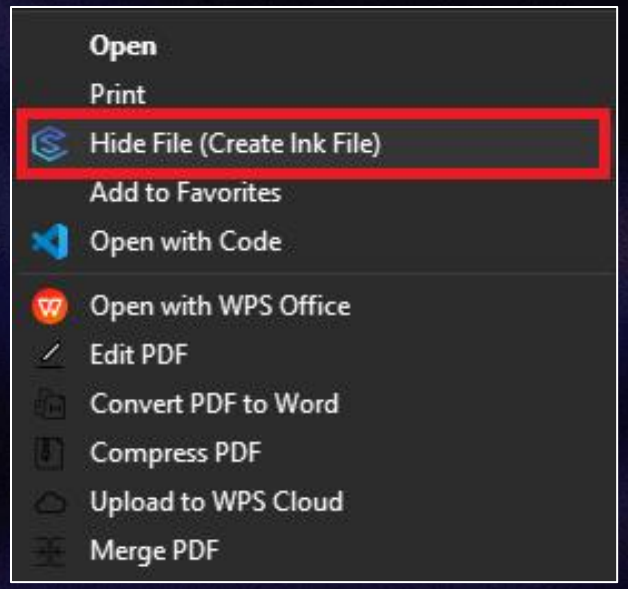
```
================================================================================

 ____  _               _            ____                       _
/ ___|| |__   __ _  __| | _____   _/ ___|_ __ _   _ _ __ | |_
\___ \| '_ \ / _` |/ _` |/ _ \ \ / / |   | '__| | | | '_ \| __|
 ___) | | | | (_| | (_| | (_) \ V /| |___| |  | |_| | |_) | |_
|____/|_| |_|\__,_|\__,_|\___/ \_/  \____|_|   \__, | .__/ \__|
                                                |___/|_|

================================================================================

[+] Recovering files:
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.txt.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.xlsx.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.zip.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.docx.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.m4v.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.mp3.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pdf.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.png.lnk
C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pptx.lnk

PASSWORD? :

    [+] Recovered: C:\Windows\PLA\Templates\FtbWKMxi.exe -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.txt
    [+] Recovered: C:\Windows\System32\Speech\Engines\pf11mpZc.dll -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.xlsx
    [+] Recovered: C:\Windows\PLA\Templates\prFZaOIx.exe -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.zip
    [+] Recovered: C:\Windows\System32\Speech\Engines\wgN8sgQI.exe -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.docx
    [+] Recovered: C:\Windows\System32\Speech\Engines\TDIy4mc2.dll -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.m4v
    [+] Recovered: C:\Windows\PLA\Templates\5tbDq5hT.dll -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.mp3
    [+] Recovered: C:\Windows\Help\ki4pJz39.exe -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pdf
    [+] Recovered: C:\Windows\PLA\Templates\5zHYcJDS.exe -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.png
    [+] Recovered: C:\Windows\Help\Windows\IndexStore\en-US\I9D1b0E7.dll -> C:\Users\Abdul\Desktop\ShadowCrypt_Demo\SCrypt.pptx

[*] Press Enter to exit...
```

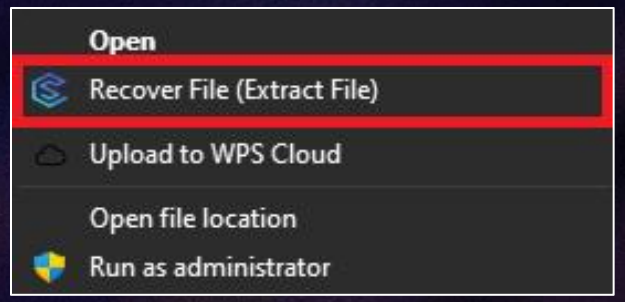


*Recovering Files

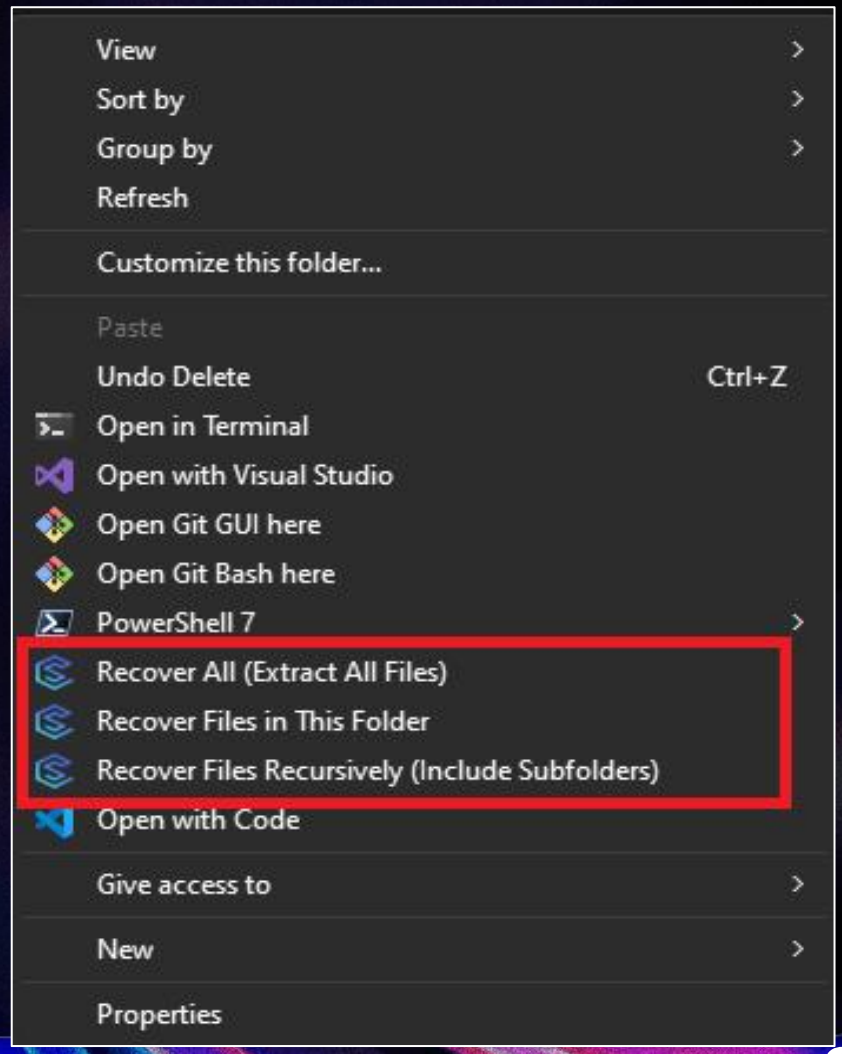
Other Features

*Single File Operations





*Recovery Features



FEATURES

- Proactive Defense
- Strong Password Policy
- Secure File Hiding
- Encrypted Mappings (Confidentiality)
- Identify files without exposing their contents (by Hashing --> Integrity)
- Access via Smart Shortcuts (Availability)
- Ease of access:
  - Rightclick Menu options
  - Installation with `.exe`

REFERENCES

➢ Research Paper

S. Lee, S. Lee, J. Park, K. Kim and K. Lee, "Hiding in the Crowd: Ransomware Protection by Adopting Camouflage and Hiding Strategy With the Link File," IEEE Access, vol. 11, pp. 92693-92704, 2023, doi: 10.1109/ACCESS.2023.3309879


Thank You !