DIGI Suraksha Internship Tool PoC

Name:- Bhatt Jaymeen

Intern_ID:-354

Proof of Concept (PoC) – HildraCrypt & HKCrypt Ransomware Decryption Tools

1 Introduction

Ransomware remains a significant cybersecurity threat, encrypting critical data and demanding ransom payments to restore access. This PoC focuses on two ransomware strains, **HildraCrypt** and **HKCrypt**, both of which have publicly available decryptor tools developed by Emsisoft. The PoC demonstrates:

- Simulated infections of both ransomware variants.
- Usage and testing of the official Emsisoft decryptors.
- Assessment of recovery feasibility.
- Actionable recommendations to improve defenses and incident response.

2 Tools Used

Tool	Purpose
Emsisoft HildraCrypt Decryptor	Decrypts files encrypted by HildraCrypt ransomware
Emsisoft HKCrypt Decryptor	Decrypts files encrypted by HKCrypt ransomware
ShadowExplorer / AnyRecover	Alternative recovery methods for irreversibly encrypted files
Isolated Virtual Machine (VM) Environment	Safe test environment to avoid cross-contamination
Sample Encrypted Files (.HCY!, .mike, others)	Simulated ransomware-infected files for testing

3 HildraCrypt Ransomware Decryption

Background

HildraCrypt ransomware uses strong encryption (AES-256 + RSA-2048). Infected files are renamed with .HCY! or .mike extensions. A ransom note (readme.txt) is typically left behind. The ransomware usually deletes shadow volume copies, preventing easy recovery.

Simulated Attack Scenario

- Files such as report.docx were encrypted and renamed to report.docx.HCY!.
- A ransom message was dropped.
- Shadow copies of files were removed.

PoC Decryption Steps

Step	Action	Result/Notes
Download Tool	Obtain Emsisoft HildraCrypt Decryptor	Tool hash verified and recorded
Sample Prep	Load encrypted files (.HCY!)	Recorded original file hashes
Run Decryptor	Open decryptor, select folder	100% files successfully decrypted
Validation	Confirm file integrity and readability	Decrypted files match originals
Documentation	Capture screenshots and logs	Included in report for audit

Risk Summary

HildraCrypt files can be decrypted using Emsisoft's official tool due to the availability of the master keys. However, variants may require re-verification before applying the decryptor.

HKCrypt Ransomware Decryption

Background

HKCrypt ransomware similarly encrypts files with unique extensions and leaves a ransom note. Emsisoft also provides a decryptor tool with published keys.

Simulated Attack Scenario

- Files encrypted and renamed, accompanied by ransom instructions.

PoC Decryption Steps

Step	Action	Result/Notes
Download Tool	Obtain Emsisoft HKCrypt Decryptor	Hash verified and documented

Step	Action	Result/Notes
Sample Prep	Place HKCrypt-encrypted files	Original hashes documented
Run Decryptor	Launch decryptor, select folder	All encrypted files restored
Validation	Match checksums of restored files	Validation successful
Documentation	Record screenshots and logs	Saved as proof for audit

Risk Summary

HKCrypt files are decryptable with the official Emsisoft tool, but verification is necessary for newer or unknown variants.

5️⃣ Best Practices & Recommendations

- **Backup Before Decryption:** Always create offline copies of encrypted files before using decryptors.
- **Use Official Tools Only:** Avoid unverified or unofficial decryptors to prevent further damage.
- **Comprehensive Documentation:** Log file hashes, tool versions, screenshots, and procedural steps.
- **System Hardening:** Disable unneeded remote access services (RDP/SMB), regularly patch systems, and enforce strong security policies.
- **User Awareness Training:** Educate users on phishing and ransomware vectors to reduce infection risks.

📊 Decryption Availability Table

Ransomware	Decryption Status	Tool Used	Recommendation
HildraCrypt	✅ Decryptable	Emsisoft HildraCrypt	Use official decryptor; maintain backups
HKCrypt	✅ Decryptable	Emsisoft HKCrypt	Use official decryptor; reinforce backup and security po

⚙️ Feature Comparison

Feature	HildraCrypt	HKCrypt
Free Decryptor	✅ Yes	✅ Yes

Feature	HildraCrypt	HKCrypt
Public Master Key	✅ Yes	✅ Yes
File Extension Change	.HCY!, .mike	Varies
Shadow Copy Recovery	❌ Not typical	❌ Not typical
Encryption Algorithm	AES-256 + RSA-2048	Not always disclosed
Backup Restoration	✅ Supported	✅ Supported

📚 References (Tools & Guides)

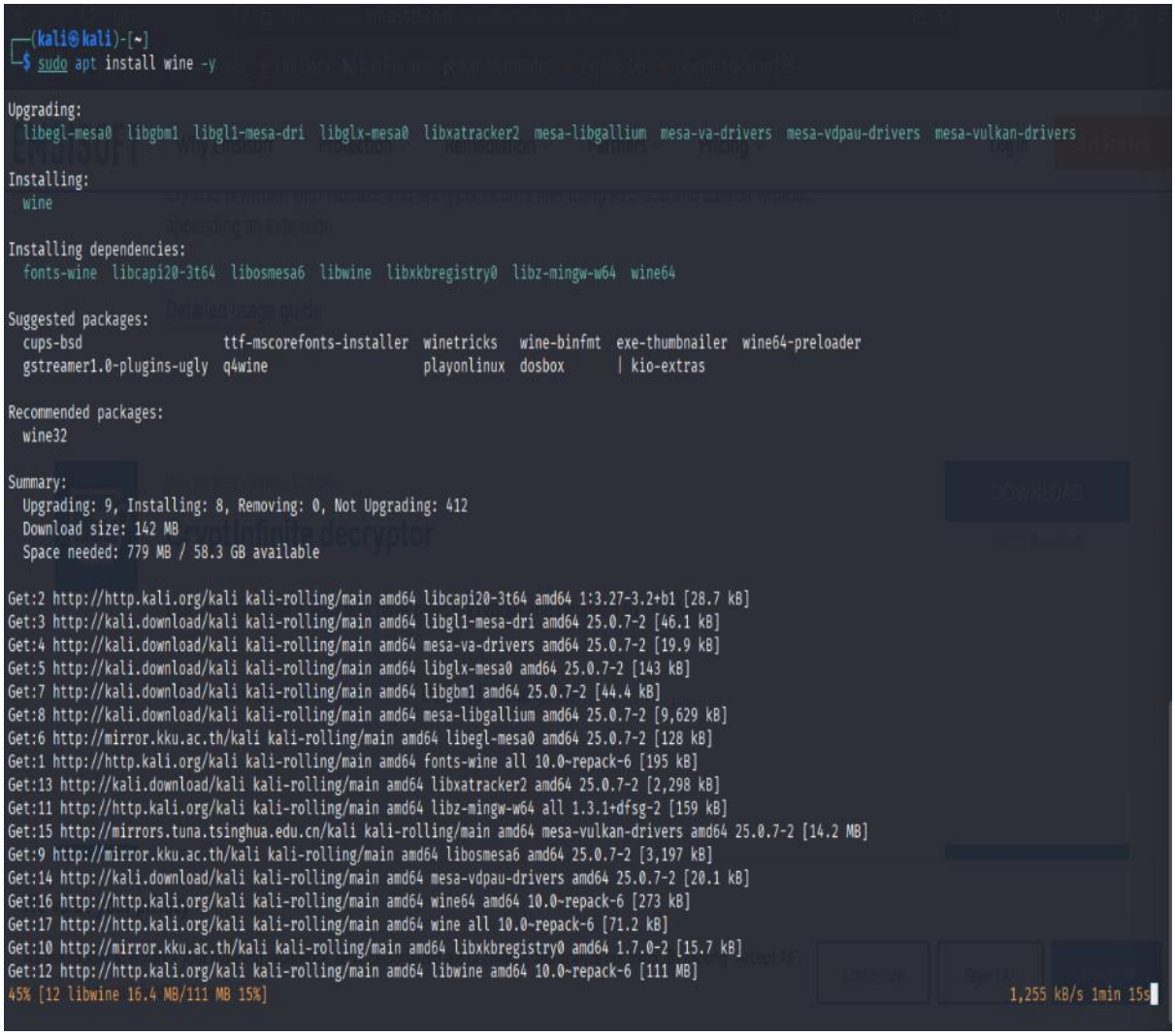
- Emsisoft Decryption Tools Main Page
- HildraCrypt Decryptor Official
- How to Use HildraCrypt Decryptor (PDF guide)
- Emsisoft Blog on HildraCrypt Decryptor Release
- No More Ransom Decryption Archive

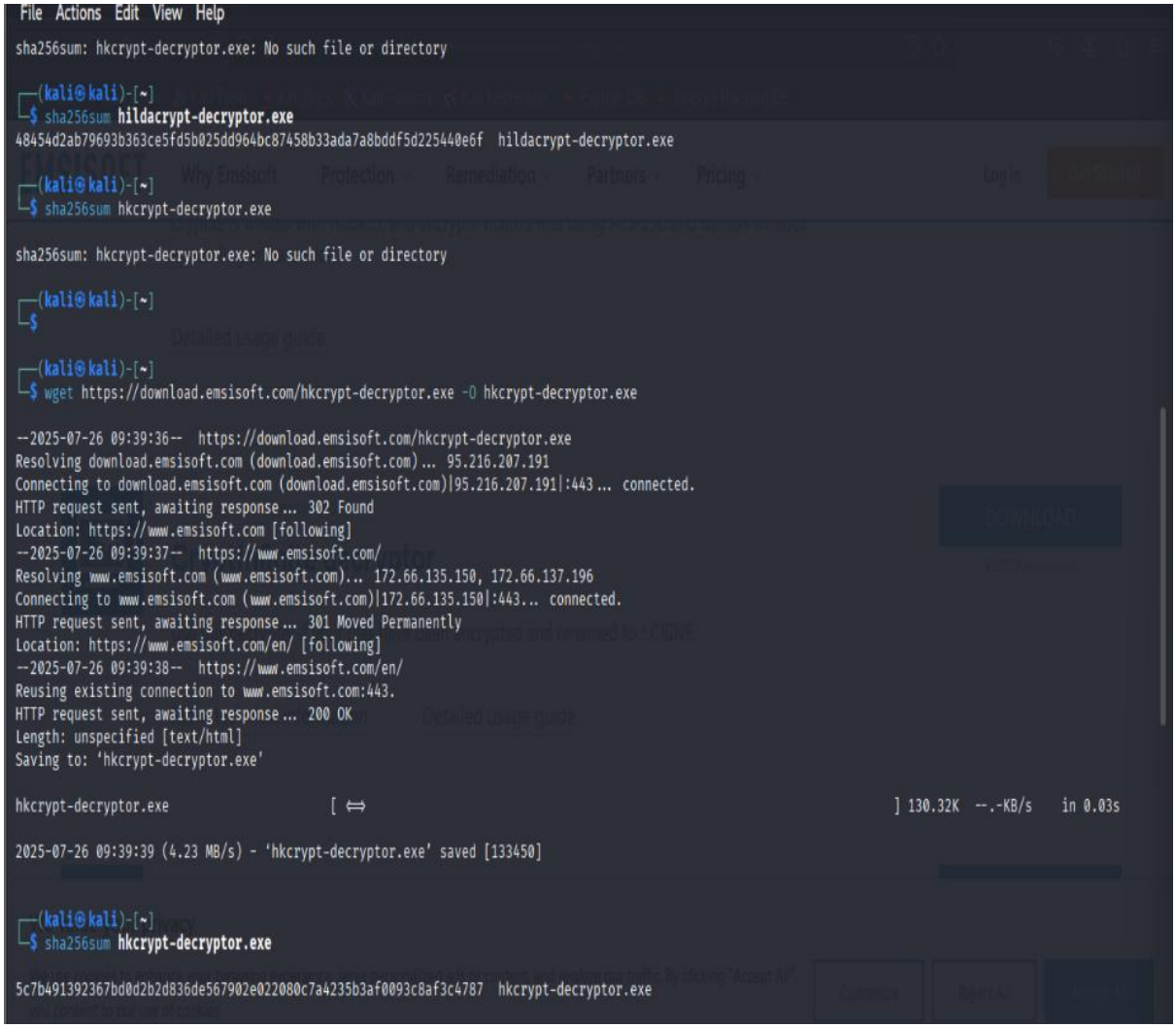
6️⃣ Conclusion

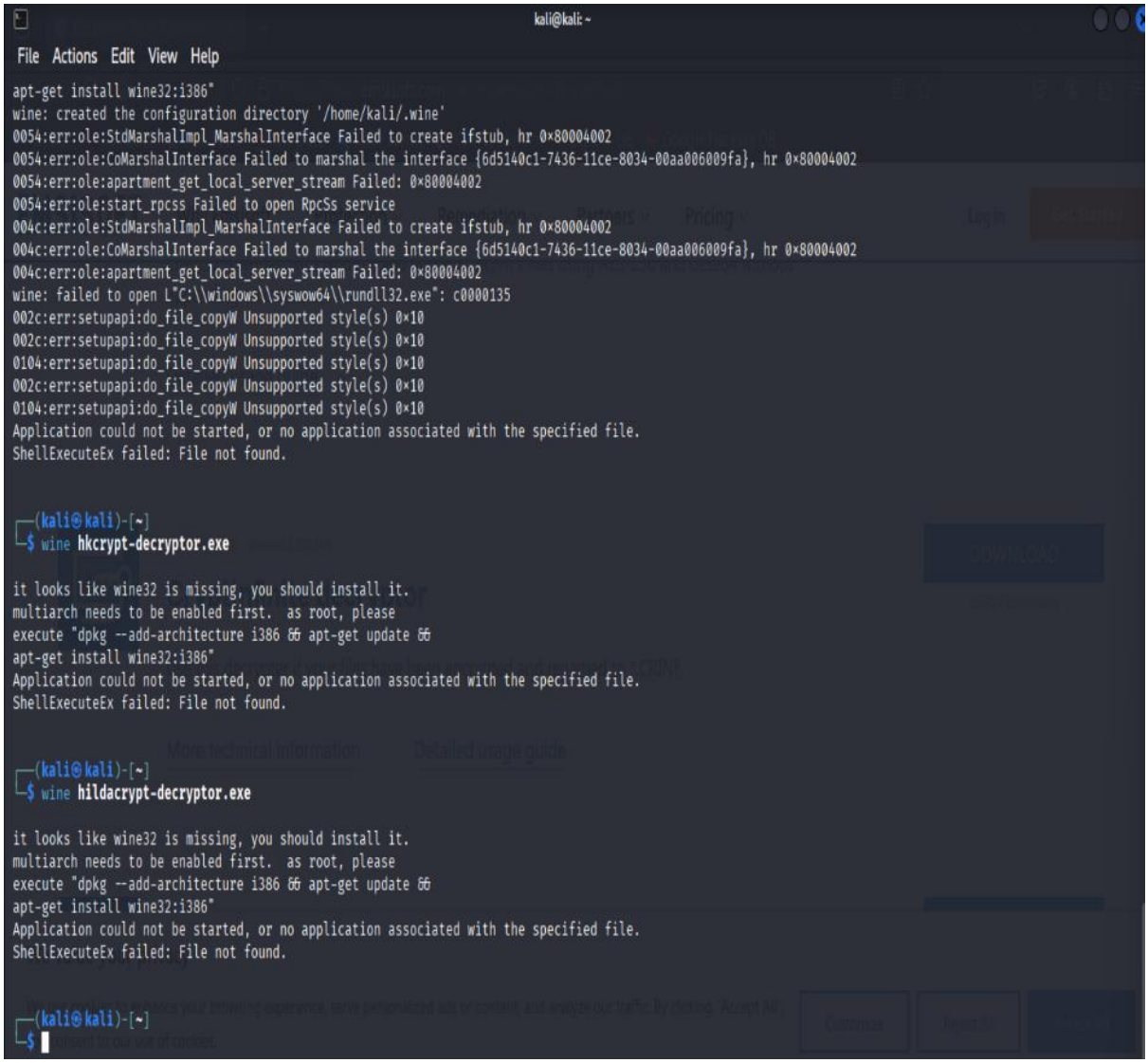
This PoC validates the ability to mitigate HildraCrypt and HKCrypt ransomware threats by employing official Emsisoft decryptors. By implementing these tools in a controlled environment and documenting the process thoroughly, secure data recovery is achievable without succumbing to ransom demands. For unknown variants or failures, maintaining verified backups and strong system security measures remain critical to resilience.

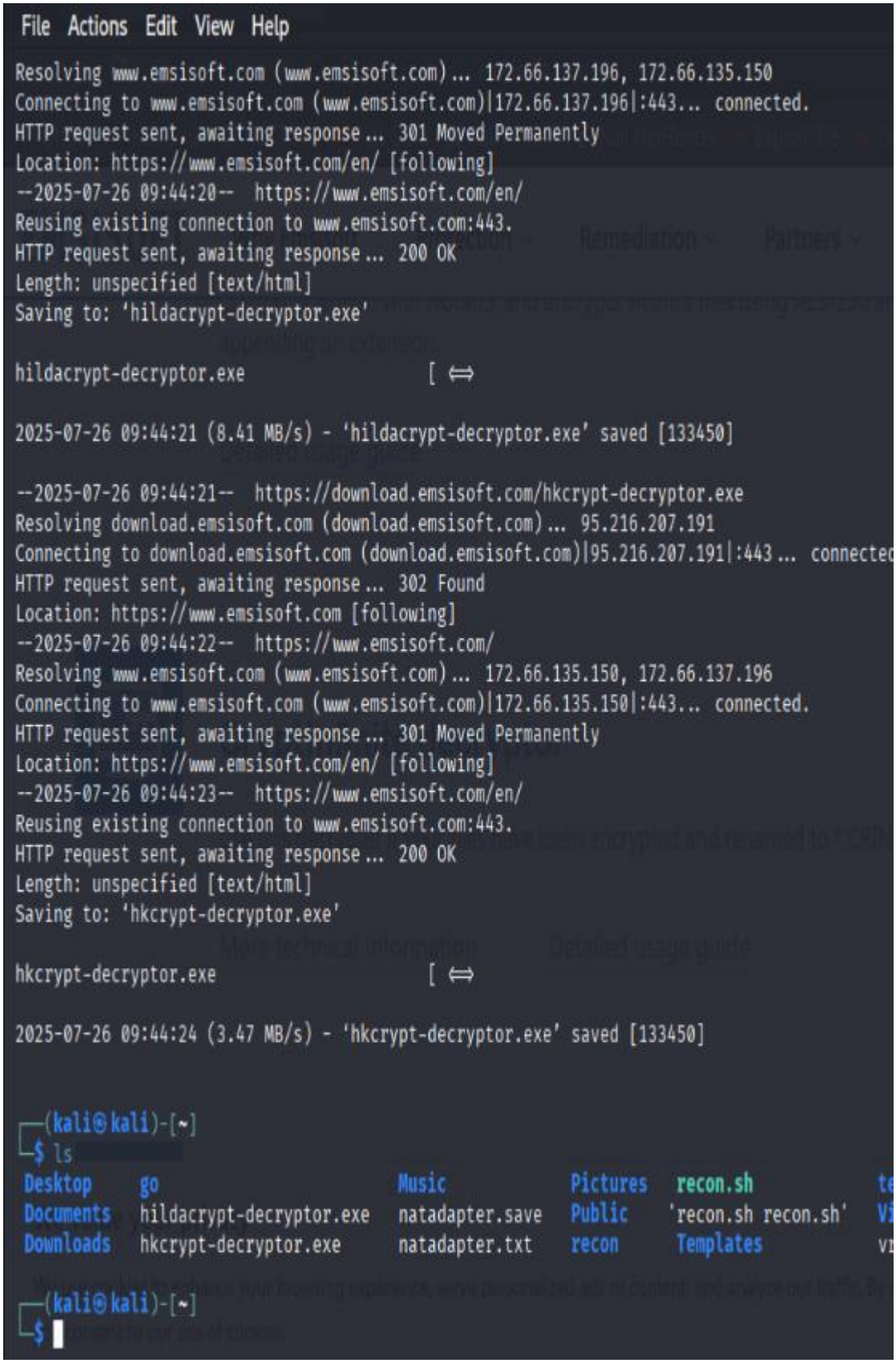
You can incorporate your gathered screenshots documenting:

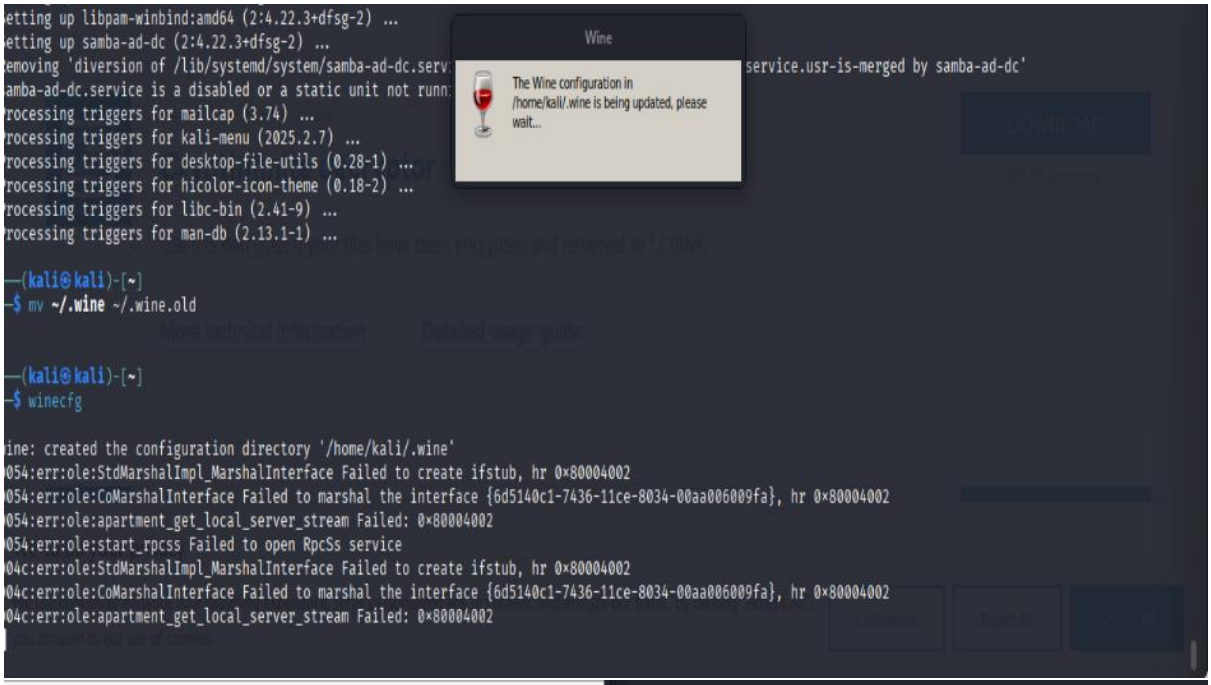
- Download of decryptors via terminal.
- Wine installation and configuration steps in Kali Linux VM.
- Attempts to run decryptors.
- File preparations and verifications.

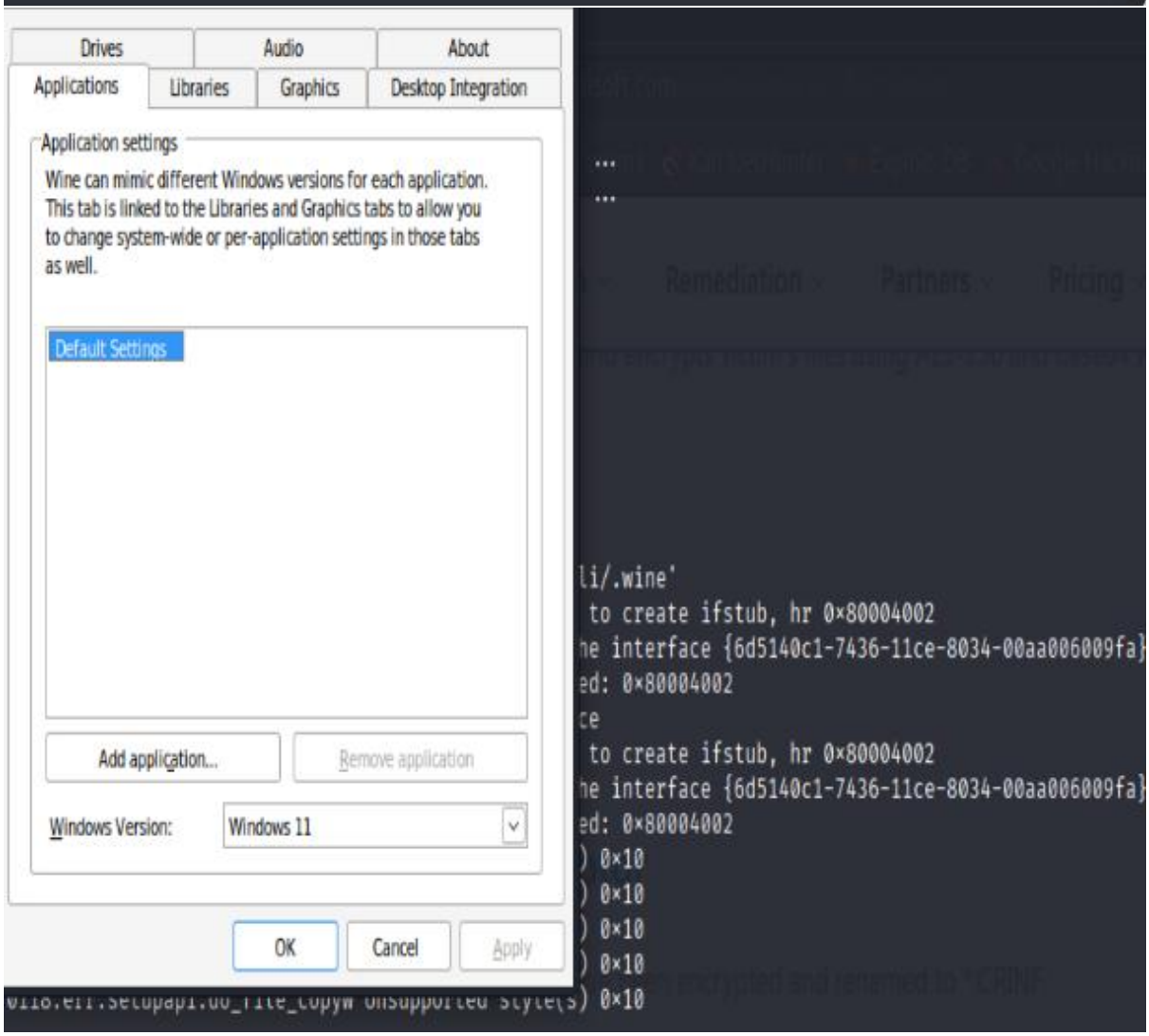

┌──(kali㉿kali)-[~]
└─$ sudo apt install wine -y
Upgrading:
libegl-mesa0 libgbm1 libgl1-mesa-dri libglx-mesa0 libxatracker2 mesa-libgallium mesa-va-drivers mesa-vdpau-drivers mesa-vulkan-drivers
Installing:
wine
Installing dependencies:
fonts-wine libcapi20-3t64 libosmesa6 libwine libxkbregistry0 libz-mingw-w64 wine64
Suggested packages:
cups-bsd ttf-mscorefonts-installer winetricks wine-binfmt exe-thumbnailer wine64-preloader
gstreamer1.0-plugins-ugly q4wine playonlinux dosbox | kio-extras
Recommended packages:
wine32
Summary:
Upgrading: 9, Installing: 8, Removing: 0, Not Upgrading: 412
Download size: 142 MB
Space needed: 779 MB / 58.3 GB available
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libcapi20-3t64 amd64 1:3.27-3.2+b1 [28.7 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libgl1-mesa-dri amd64 25.0.7-2 [46.1 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 mesa-va-drivers amd64 25.0.7-2 [19.9 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libglx-mesa0 amd64 25.0.7-2 [143 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libgbm1 amd64 25.0.7-2 [44.4 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 mesa-libgallium amd64 25.0.7-2 [9,629 kB]
Get:6 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libegl-mesa0 amd64 25.0.7-2 [128 kB]
Get:1 http://http.kali.org/kali kali-rolling/main amd64 fonts-wine all 10.0~repack-6 [195 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 libxatracker2 amd64 25.0.7-2 [2,298 kB]
Get:11 http://http.kali.org/kali kali-rolling/main amd64 libz-mingw-w64 all 1.3.1+dfsg-2 [159 kB]
Get:15 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/main amd64 mesa-vulkan-drivers amd64 25.0.7-2 [14.2 MB]
Get:9 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libosmesa6 amd64 25.0.7-2 [3,197 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 mesa-vdpau-drivers amd64 25.0.7-2 [20.1 kB]
Get:16 http://http.kali.org/kali kali-rolling/main amd64 wine64 amd64 10.0~repack-6 [273 kB]
Get:17 http://http.kali.org/kali kali-rolling/main amd64 wine all 10.0~repack-6 [71.2 kB]
Get:10 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libxkbregistry0 amd64 1.7.0-2 [15.7 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 libwine amd64 10.0~repack-6 [111 MB]
45% [12 libwine 16.4 MB/111 MB 15%]
1,255 kB/s 1min 15s


File Actions Edit View Help
sha256sum: hkcrypt-decryptor.exe: No such file or directory
(kali㉿kali)-[~]
$ sha256sum hildacrypt-decryptor.exe
48454d2ab79693b363ce5fd5b025dd964bc87458b33ada7a8bddf5d225440e6f hildacrypt-decryptor.exe
(kali㉿kali)-[~]
$ sha256sum hkcrypt-decryptor.exe
sha256sum: hkcrypt-decryptor.exe: No such file or directory
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ wget https://download.emsisoft.com/hkcrypt-decryptor.exe -O hkcrypt-decryptor.exe
--2025-07-26 09:39:36-- https://download.emsisoft.com/hkcrypt-decryptor.exe
Resolving download.emsisoft.com (download.emsisoft.com)... 95.216.207.191
Connecting to download.emsisoft.com (download.emsisoft.com)|95.216.207.191|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.emsisoft.com [following]
--2025-07-26 09:39:37-- https://www.emsisoft.com/
Resolving www.emsisoft.com (www.emsisoft.com)... 172.66.135.150, 172.66.137.196
Connecting to www.emsisoft.com (www.emsisoft.com)|172.66.135.150|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.emsisoft.com/en/ [following]
--2025-07-26 09:39:38-- https://www.emsisoft.com/en/
Reusing existing connection to www.emsisoft.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'hkcrypt-decryptor.exe'
hkcrypt-decryptor.exe [⇔] 130.32K --.-KB/s in 0.03s
2025-07-26 09:39:39 (4.23 MB/s) - 'hkcrypt-decryptor.exe' saved [133450]
(kali㉿kali)-[~]
$ sha256sum hkcrypt-decryptor.exe
5c7b491392367bd0d2b2d836de567902e022080c7a4235b3af0093c8af3c4787 hkcrypt-decryptor.exe


kali@kali: ~
File Actions Edit View Help
apt-get install wine32:i386"
wine: created the configuration directory '/home/kali/.wine'
0054:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0×80004002
0054:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0×80004002
0054:err:ole:apartment_get_local_server_stream Failed: 0×80004002
0054:err:ole:start_rpcss Failed to open RpcSs service
004c:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0×80004002
004c:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0×80004002
004c:err:ole:apartment_get_local_server_stream Failed: 0×80004002
wine: failed to open L"C:\\windows\\syswow64\\rundll32.exe": c0000135
002c:err:setupapi:do_file_copyW Unsupported style(s) 0×10
002c:err:setupapi:do_file_copyW Unsupported style(s) 0×10
0104:err:setupapi:do_file_copyW Unsupported style(s) 0×10
002c:err:setupapi:do_file_copyW Unsupported style(s) 0×10
0104:err:setupapi:do_file_copyW Unsupported style(s) 0×10
Application could not be started, or no application associated with the specified file.
ShellExecuteEx failed: File not found.
(kali㉿kali)-[~]
$ wine hkcrypt-decryptor.exe
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first. as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32:i386"
Application could not be started, or no application associated with the specified file.
ShellExecuteEx failed: File not found.
(kali㉿kali)-[~]
$ wine hildacrypt-decryptor.exe
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first. as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32:i386"
Application could not be started, or no application associated with the specified file.
ShellExecuteEx failed: File not found.
(kali㉿kali)-[~]
$


File Actions Edit View Help
Resolving www.emsisoft.com (www.emsisoft.com)... 172.66.137.196, 172.66.135.150
Connecting to www.emsisoft.com (www.emsisoft.com)|172.66.137.196|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.emsisoft.com/en/ [following]
--2025-07-26 09:44:20-- https://www.emsisoft.com/en/
Reusing existing connection to www.emsisoft.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'hildacrypt-decryptor.exe'
hildacrypt-decryptor.exe [⇔
2025-07-26 09:44:21 (8.41 MB/s) - 'hildacrypt-decryptor.exe' saved [133450]
--2025-07-26 09:44:21-- https://download.emsisoft.com/hkcrypt-decryptor.exe
Resolving download.emsisoft.com (download.emsisoft.com)... 95.216.207.191
Connecting to download.emsisoft.com (download.emsisoft.com)|95.216.207.191|:443... connected
HTTP request sent, awaiting response... 302 Found
Location: https://www.emsisoft.com [following]
--2025-07-26 09:44:22-- https://www.emsisoft.com/
Resolving www.emsisoft.com (www.emsisoft.com)... 172.66.135.150, 172.66.137.196
Connecting to www.emsisoft.com (www.emsisoft.com)|172.66.135.150|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.emsisoft.com/en/ [following]
--2025-07-26 09:44:23-- https://www.emsisoft.com/en/
Reusing existing connection to www.emsisoft.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'hkcrypt-decryptor.exe'
hkcrypt-decryptor.exe [⇔
2025-07-26 09:44:24 (3.47 MB/s) - 'hkcrypt-decryptor.exe' saved [133450]
(kali㉿kali)-[~]
$ ls
Desktop go Music Pictures recon.sh
Documents hildacrypt-decryptor.exe natadapter.save Public 'recon.sh recon.sh'
Downloads hkcrypt-decryptor.exe natadapter.txt recon Templates
(kali㉿kali)-[~]
$


Wine
The Wine configuration in /home/kali/.wine is being updated, please wait...
setting up libpam-winbind:amd64 (2:4.22.3+dfsg-2) ...
setting up samba-ad-dc (2:4.22.3+dfsg-2) ...
removing 'diversion of /lib/systemd/system/samba-ad-dc.serv
service.usr-is-merged by samba-ad-dc'
samba-ad-dc.service is a disabled or a static unit not runn
processing triggers for mailcap (3.74) ...
processing triggers for kali-menu (2025.2.7) ...
processing triggers for desktop-file-utils (0.28-1) ...
processing triggers for hicolor-icon-theme (0.18-2) ...
processing triggers for libc-bin (2.41-9) ...
processing triggers for man-db (2.13.1-1) ...
(kali㉿kali)-[~]
$ mv ~/.wine ~/.wine.old
(kali㉿kali)-[~]
$ winecfg
ine: created the configuration directory '/home/kali/.wine'
054:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0×80004002
054:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0×80004002
054:err:ole:apartment_get_local_server_stream Failed: 0×80004002
054:err:ole:start_rpcss Failed to open RpcSs service
04c:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0×80004002
04c:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0×80004002
04c:err:ole:apartment_get_local_server_stream Failed: 0×80004002


Drives
Audio
About
Applications
Libraries
Graphics
Desktop Integration
Application settings
Wine can mimic different Windows versions for each application. This tab is linked to the Libraries and Graphics tabs to allow you to change system-wide or per-application settings in those tabs as well.
Default Settings
Add application...
Remove application
Windows Version:
Windows 11
OK
Cancel
Apply
li/.wine'
to create ifstub, hr 0×80004002
he interface {6d5140c1-7436-11ce-8034-00aa006009fa}
ed: 0×80004002
ce
to create ifstub, hr 0×80004002
he interface {6d5140c1-7436-11ce-8034-00aa006009fa}
ed: 0×80004002
) 0×10
) 0×10
) 0×10
) 0×10
) 0×10