Home of CTF: https://ctf.idek.team/
Team: Obi0n3

Info

1. We will have two divisions: High School, and Open. High school teams are allowed to switch Open.
2. Each member must belong to exactly one team.
3. Teams may have any number of members.
4. For High School teams, all members must be enrolled in a High School.
5. During the CTF, sharing solutions or asking for outside help is prohibited.
6. Questions about challenges should be sent in the category chat or to the idekCTF ModMail. Please refrain from messaging challenge authors or any other participants. (If you're looking for a team use the team-search channel.)
7. Attacking the infrastructure or any attempt to disrupt the CTF is prohibited.
8. Report any bugs you find in the infrastructure or challenges directly to the organizers.
9. The flag format is `idek{[!-z]+}`.
10. Updates about challenges or the CTF will be announced in the announcements section in the

discord server.

11. Breaking any of the above rules may result in team disqualification

Forensics

Bquanman

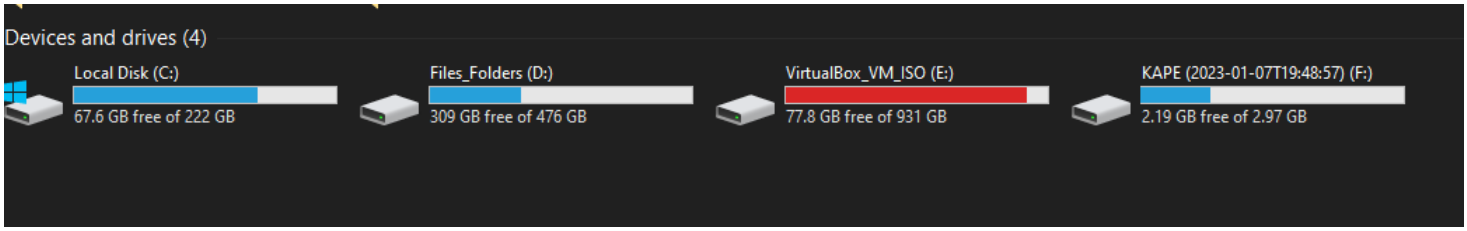
We're pretty sure there's been a hack into our system. The incident is suspected to be caused by an employee opening a document file received via email even though he deleted it shortly afterwards. We managed to do a logical acquisition of data from his hard drive. However, when we open the document file, it looks empty, can you analyze what it contains?

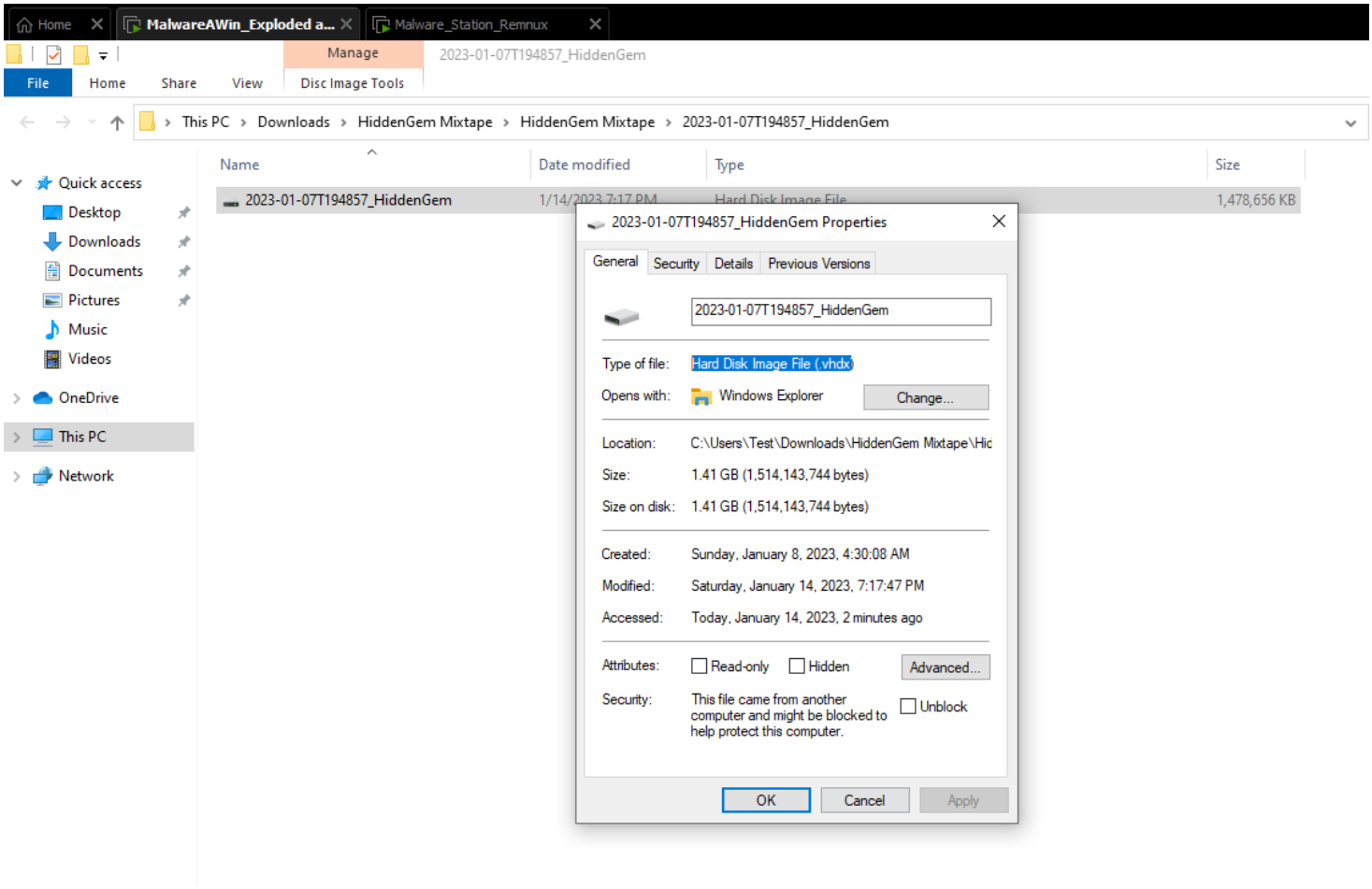
Tool: https://csilinux.com
Resource: https://csilinux.com/features
PS:csi

```
Update: powerup
Tools: wget csilinux.com/downloads/csitoolsupdate.sh -O -
| sh
```

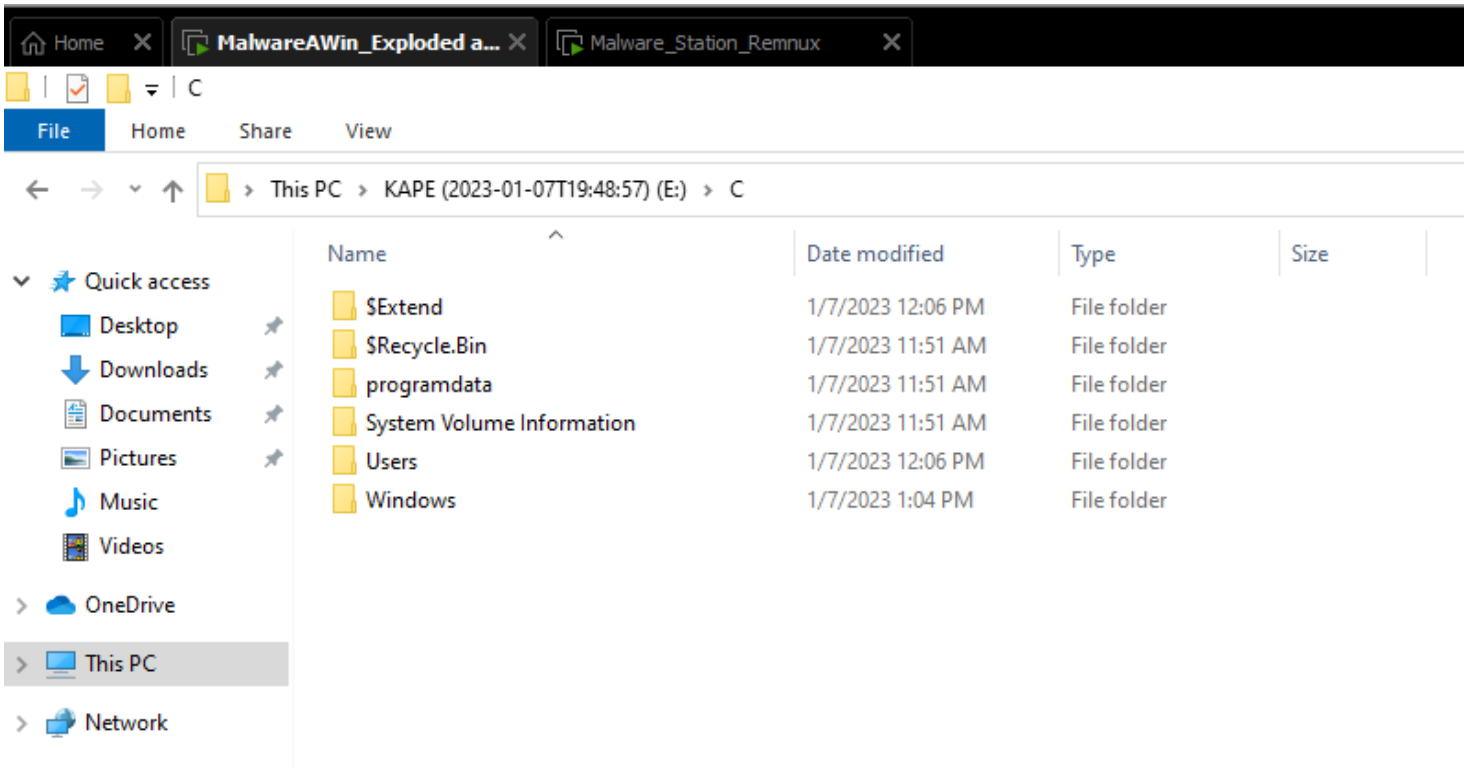
POC

```
- We get a link to download a zip file
- File was moved toa Win 10 sandboxed
- Unziped and was given a Hard Disk Image File (.vhdx)
- Mounted
- C:\
```

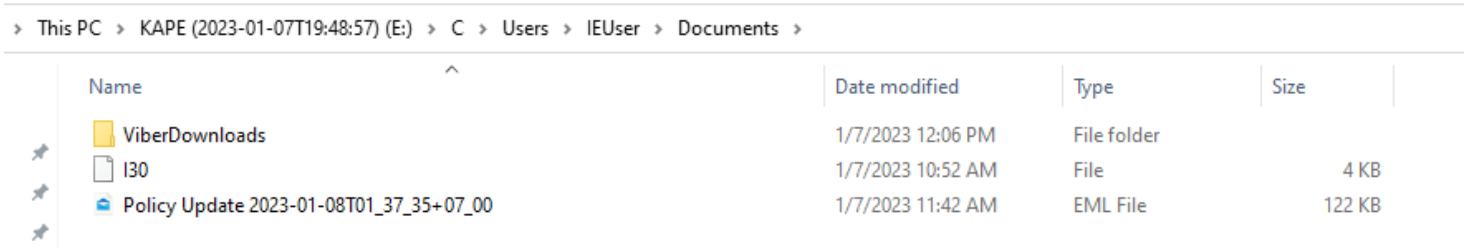




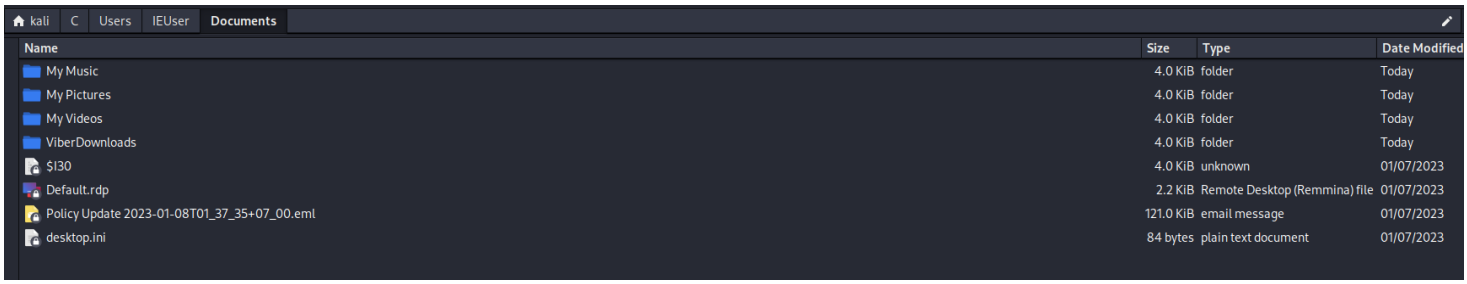
We get an interesting name convention for the drive and we are present to what looks like to be a windows directory.



From what are told this person clicked on an email and then deleted it. The file was an empty file. On the Documents folder of user IEUser I find an EML file



We are going to have to move the C:\ file to Kali manually so I can poke around.



We have more information here like an RDP drop and some other files. Lets look at the email

From Jake Weary <j4k3w34ry-pr0t0nm41l@protonmail.com>
To blu3dr490n@protonmail.com <blu3dr490n@protonmail.com>
Subject **Policy Update**

Reply | Reply All | Forward | Archive | Junk

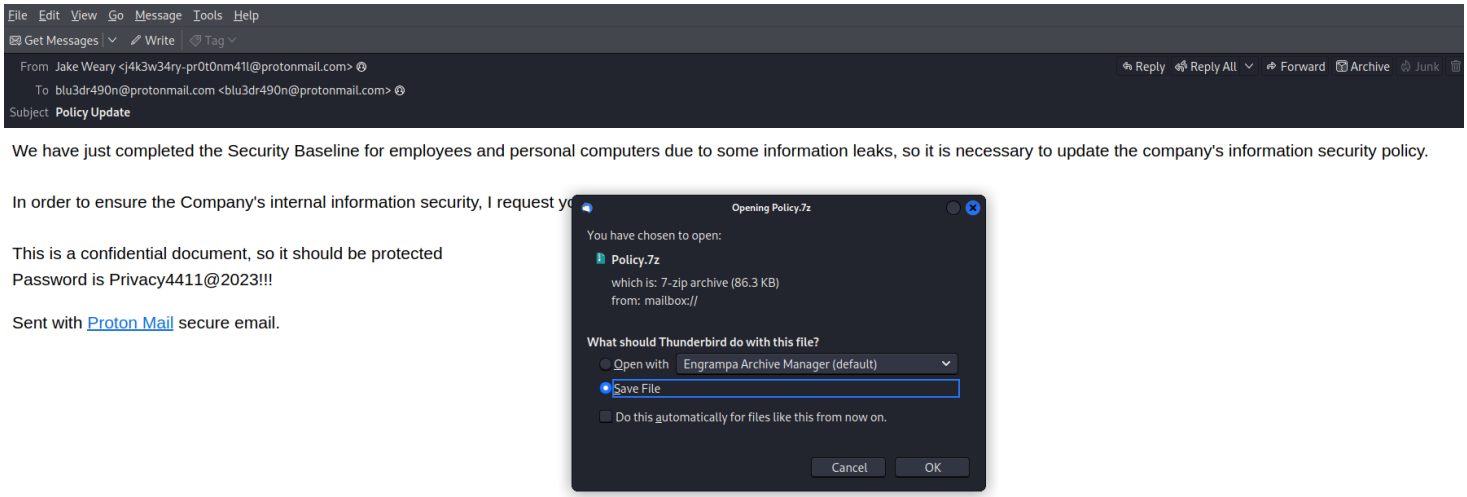
We have just completed the Security Baseline for employees and personal computers due to some information leaks, so it is necessary to update the company's information security policy.

In order to ensure the Company's internal information security, I request you to read and master the content of the policy

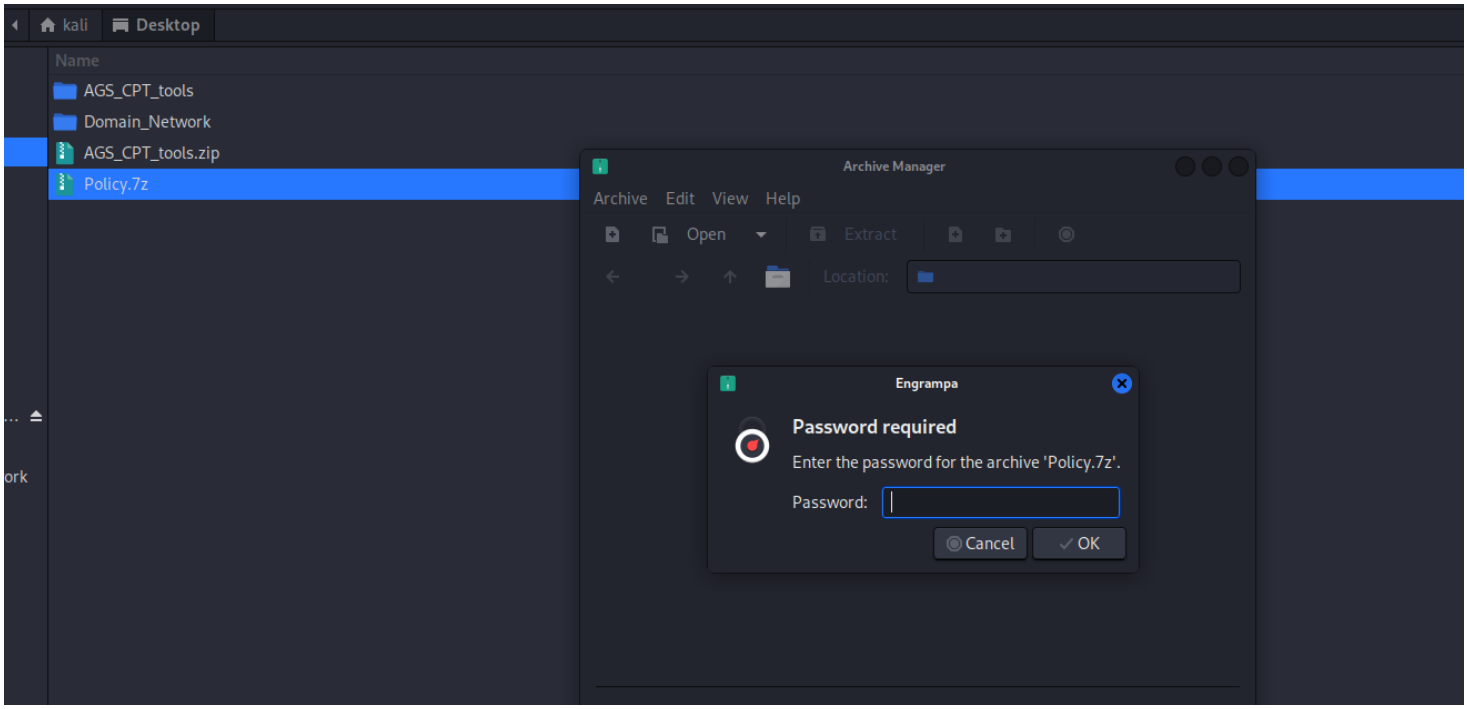
This is a confidential document, so it should be protected
Password is Privacy4411@2023!!!

Sent with Proton Mail secure email.

This could be the email the user click on. We also see an attachment

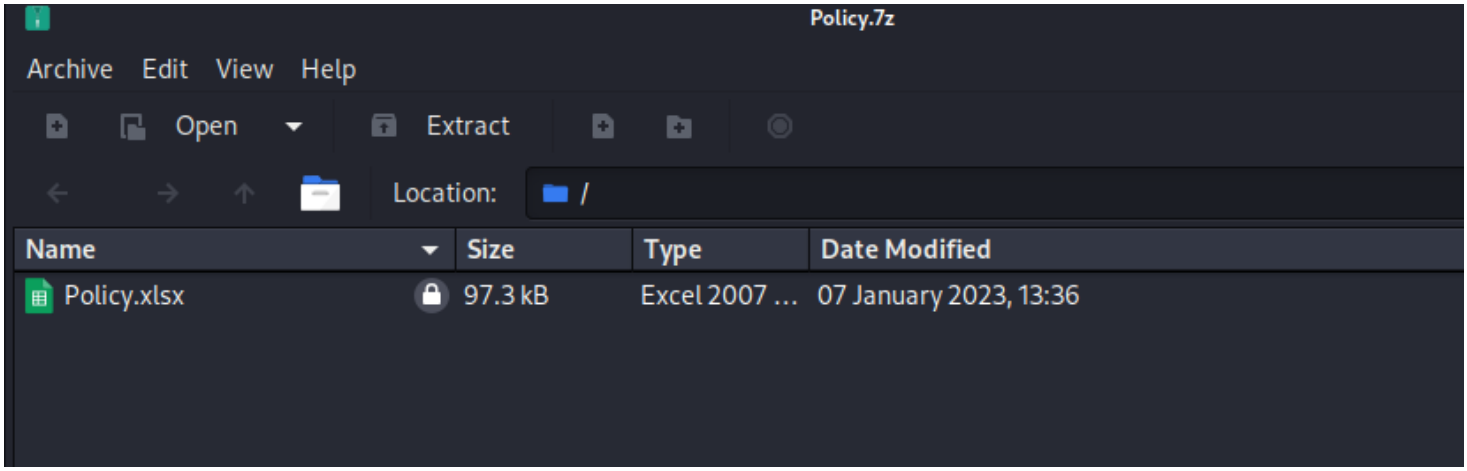


We try to unzip the file but it asked for the password, we use the one from the email



After we put in the password we find that is an xlsx

file format.

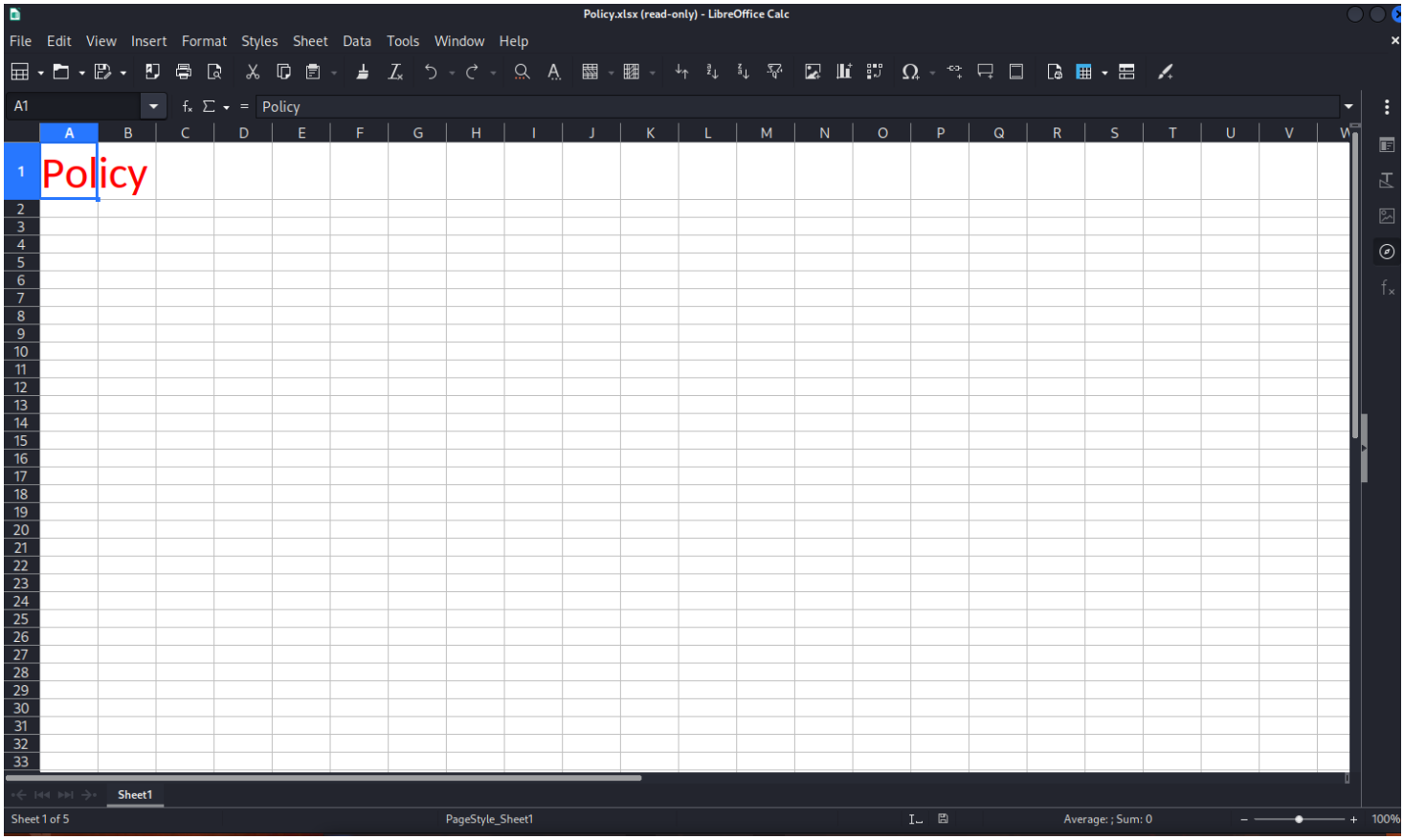


We Id the file as Microsoft Excel 2007 format

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -la Policy.xlsx
-rw-r--r-- 1 kali kali 95 KiB Sat Jan 7 13:36:17 2023 Policy.xlsx

┌──(kali㉿kali)-[~/Desktop]
└─$ file Policy.xlsx
Policy.xlsx: Microsoft Excel 2007+
```

I install libraoffice and try to look at the file



I wanted to see if we can find the file that the user tried to deleted.

```
┌──(kali㉿kali)-[~/C]
└─$ find ~/C -name "*.txt" 2> >(grep -v 'Permission denied' >&2)

/home/kali/C/Windows/System32/restore/MachineGuid.txt
/home/kali/C/Windows/Temp/VMWare/manifest.txt
/home/kali/C/Users/IEUser/AppData/Local/Microsoft/Windows/WER/ERC/queuepester.txt
/home/kali/C/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/brndlog.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_clwireg.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_vcredistUI6460.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/FXSAPIDebugLogFile.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_NDP471-KB4033341-x86-x64-ENU_decompression_log.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_SetupUtility.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/RDR81BE.tmp/empty.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_NDP40-KB2468871-v2-x64_decompression_log.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_wcf_CA_smci_20180306_213742_375.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_wcf_CA_smci_20180306_213741_953.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_vcredistUI63C3.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_dotNetFx40_Client_x86_x64_decompression_log.txt
/home/kali/C/Users/IEUser/AppData/Local/Temp/dd_NDP471-KB4054852-x64_decompression_log.txt

┌──(kali㉿kali)-[~/C]
└─$ ls -la /home/kali/C/Users/IEUser/AppData/Local/Temp/RDR81BE.tmp/empty.txt
r-xr--r--  1  kali  kali  0 B  Tue Dec 20 12:39:43 2022  empty.txt
```