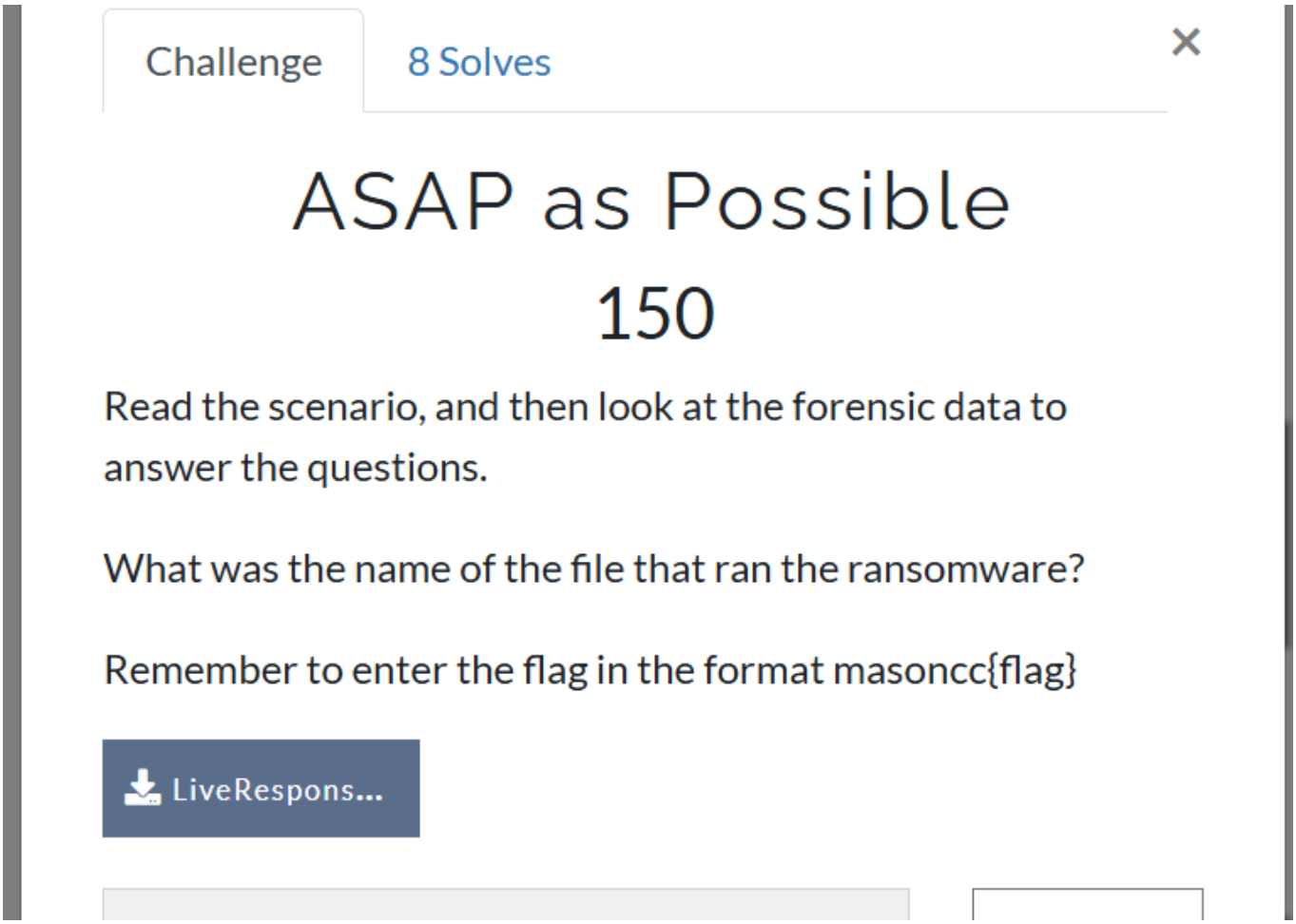
Writeup For The Office (PatriotTCTF)

This is a quick write-up for my CCI Round 2. I have a flight tomorrow and I'm going on a trip to Qatar and Turkey, so I had to quickly grab a CTF problem, solve it, and write this up lol, so here it is.

Looks like a interesting CTF that comes from the famous TV series The Office

Problem 1:



We're given a zip file.

After downloading and extracting it, you'll find a folder named `LinuxResponse` and looks like the files were already extracted for us.
I tried solving it using **Midnight Commander (CLI)** and **FTK Imager** : two different approaches depending on whether you're using **Linux or Windows**.
I'll walk you through both methods because it's important to understand them from a **forensics perspective** cause you never know which OS you'll be working with during an investigation.

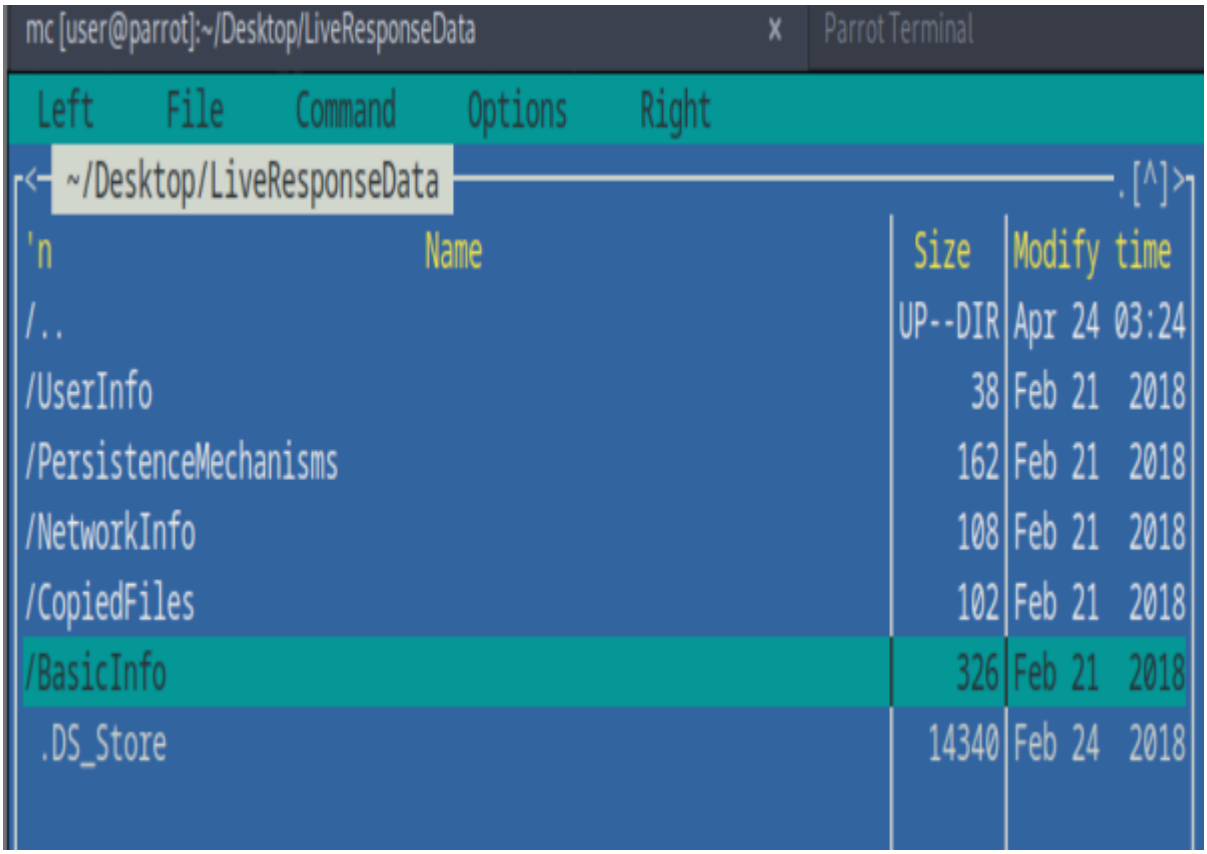
Like for this problem Midnight Commander helped me traverse files quickly and open text files while FTK helped me find the csv files which can be opened easily with Linux

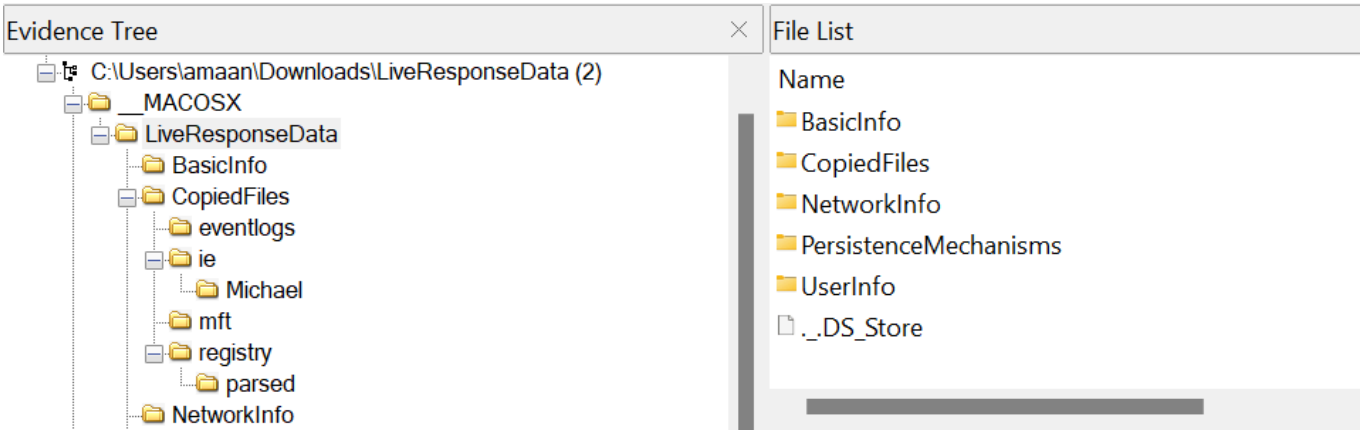
So what are Midnight and FTK?

Midnight Commander (mc) is a text-based file manager for Linux that lets you navigate and analyze file systems in the terminal.
FTK Imager is a forensic tool for Windows used to preview, extract, and analyze data from disk images.

Anyways lets stop beating around the bush and dive in!!!..

After opening **LiveResponseData**, we are met with four subdirectories, both in Linux and Windows.





i will start by using MC on Linux, then switch to FTK, because as we go further into the CTF, we see there are event logs and CSV files of MFTs, which are more easily visible on a Windows machine.

Since the question asks us to find **ransomware**,
my first guess is to check the running software, which can be found at `./BasicInfo/running_processes.txt`.

```
~/Desktop/LiveResponseData/BasicInfo
'n                    Name                    Size   Modify time
/..                                         UP--DIR Feb 21  2018
 .DS_Store                                    6148 Feb 21  2018
*system_info.txt                              2357 Feb 21  2018
*Running_processes.txt                       18251 Feb 21  2018
*List_hidden_directories.txt                 22109 Feb 21  2018
*LastActivityView.html                      664234 Feb 24  2018
*Installed_software_wmic.txt                  2298 Feb 21  2018
*Full_file_listing.txt                      10873K Feb 21  2018
*DiskDriveList_wmic.txt                        340 Feb 21  2018
```

At first, while reading through `./running_process.txt`, I wasn't able to find anything suspicious (though later I realized we could have found it here!).

Hence i decided why don't i look at LastActivity.html?...

Scrolling down i was able to find it!!....

```
nowrap>C:\Windows\System32\VSSVC.exe<td bgcolor=#FFFFFF nowrap> <td bgcolor=#FFFFFF nowrap>exe
<tr><td bgcolor=#FFFFFF nowrap>2/21/2018 2:13:06 PM<td bgcolor=#FFFFFF nowrap>Run .EXE file<td bgcolor=#FFFFFF nowrap>PAYLOAD_133MMK.EXE<td
bgcolor=#FFFFFF nowrap>C:\Users\Kevin\DOWNLOADS\PAYLOAD_133MMK.EXE<td bgcolor=#FFFFFF nowrap> <td bgcolor=#FFFFFF nowrap>EXE
```

C:\Users\Kevin\DOWNLOADS\PAYLOAD_133MMK.EXE.

Luckily for us, the adversary hadn't changed the file name 😅 (which doesn't usually happen in real situations, since adversaries aren't this dumb and typically rename the file to obfuscate it).

So what did we find?:

User: Kevin
File directory: Downloads ---(mostly from the internet then)
Filename: PAYLOAD_133MMK.EXE.

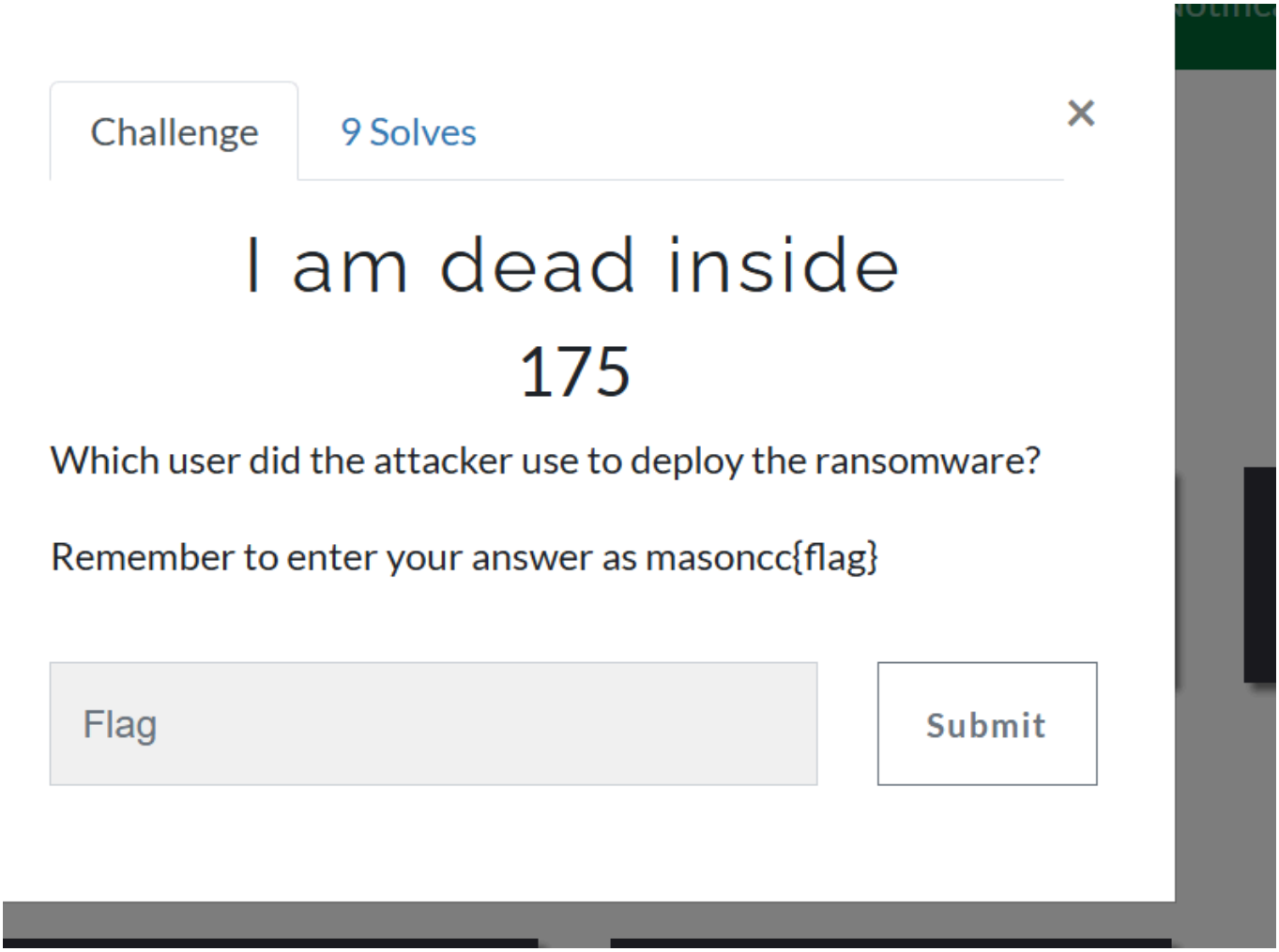
Coming from my previous sleuthing, where I hadn't found it in `./running_processes.txt`, looking back and using Ctrl+F, I was able to find it...

Yup The same file with a PID of 540 running for estimated CPU Time Window Title of 0:01:07.

Hence the first answer was

masoncc{PAYLOAD_133MMK.EXE}

Problem 2:



Ok, this one was easy...but I initially misread it and thought we had to find the command that ran the payload. That led me to stumble upon the `.evtx` files, which is why I switched to a Windows device to check the Security logs. I couldn't find any command execution logs, and then I re-read the question and realized… we just needed the user 😅. Felt kinda dumb since in the previous problem, we had already found that Kevin downloaded the file.

the evtx files are as below:

Yesterday			
Application.evtx	5/12/2025 11:15 PM	Event Log	2,116 KB
HardwareEvents.evtx	5/12/2025 11:15 PM	Event Log	68 KB
Internet Explorer.evtx	5/12/2025 11:15 PM	Event Log	68 KB
Kaspersky Event Log.evtx	5/12/2025 11:15 PM	Event Log	68 KB
Key Management Service.evtx	5/12/2025 11:15 PM	Event Log	68 KB
Media Center.evtx	5/12/2025 11:15 PM	Event Log	68 KB
Microsoft-Windows-Application Server-Applica...	5/12/2025 11:15 PM	Event Log	68 KB
Microsoft-Windows-Application Server-Applica...	5/12/2025 11:15 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4...	5/12/2025 11:15 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4...	5/12/2025 11:15 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4...	5/12/2025 11:15 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4...	5/12/2025 11:15 PM	Event Log	1,028 KB
Microsoft-Windows-Application-Experience%4...	5/12/2025 11:15 PM	Event Log	68 KB

maybe going threw the etvx files was a blessing in disguise and help us in further problems?....Lets see!!..

masoncc{Kevin}

Problem 3:

Challenge 3 Solves

Dwight U Ignorant

300

What is the name of the decryptor that will work on the ransomware'd files?

Remember to enter your answer in the format masoncc{flag}

Flag

Submit

Looks like we have a good question here : we need to find the **decrypter** that was used on the ransomware-encrypted files. You might be wondering what a decrypter is. Basically, when an adversary gains access to your laptop, they encrypt your files and then demand payment in exchange for the method to decrypt them — classic ransomware XD. Later, we come across a wallet address and a `.txt` file with instructions on how to decrypt the files.

Okay, so the first thing I did was look through the MFT file. Why would the MFT be useful for finding the decrypter?

Well, **I figured the decrypter must have been executed or created at some point**, so checking the MFT (Master File Table) could help reveal any newly created or recently accessed files — especially ones with suspicious names or unusual execution paths. I think I searched for terms like “decrypter” or similar keywords to track it down.

Below is what I found in the MFT CSV provided (also why I used Windows—since Excel makes it so much easier to go through a CSV file!!)

```
10|2|48081|10|GAMEEX~1|:\Users\Kevin\AppData\Local\Microsoft\Windows\GameExplorer|FOLDER|ALLOCATED|||not_indexed|directory|DOS|||2018-02-21 19:07:26.6161258|2
17|2|48069|10|EASEOF~1.WAL|:\Users\Kevin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk.[Mkliukang@india.com].w
16|2|48070|10|DESKTO~2.WAL|:\Users\Kevin\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink.[Mkliukang@india.com].wallet|FILE|ALLOCATED
13|2|48068|10|DESKTO~1.WAL|:\Users\Kevin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ini.[Mkliukang@india.com].wallet|F
14|2|48069|10|DESKTO~1.WAL|:\Users\Kevin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini.[Mkliukang@india.com].wallet|FI
```

Ooooo looks like i found something interesting ....

We see clear signs that Kevin's files have been encrypted — several file names now include the `.wallet` extension and contain the ransomware tag `[Mkliukang@india.com]`. This indicates that the attacker’s payload successfully ran and encrypted files in Kevin's user profile, confirming the impact of the ransomware.

So I dig deeper by searching "Kevin" to see if I could find something interesting. Since this is something I haven't worked with before, I found it tricky to make sense of it.

```
0x044AC400|GOOD|OK||70321|3|2|48071|10|INFORM~1.LNK|:\Users\Kevin\AppData\Roaming\Microsoft\Windows\Recent\INFORMATION HOW DECRYP our FI.lnk|F
```

Looking more i see a text file with a information how to decrypt the file??...maybe this is the key to find the decrypter?...so i went back on ftk to search for it...maybe i might find a suitable .dat file where i can extract it

Kevin_NTUSER.txt	62,904 (6...	Regular F...	2/21/2018 3:35...
Michael_NTUSER.txt	61,960 (6...	Regular F...	2/21/2018 3:37...
Pam_NTUSER.txt	58,294 (5...	Regular F...	2/21/2018 3:37...

```
Software\RealVNC\VNCViewer4\MRU not found.
----------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Feb 21 19:14:37 2018 (UTC)
  2 = INFORMATION HOW  DECRYP our FI.txt
  1 = paper_numbers.txt
  0 = sensitive_document.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
LastWrite Time Wed Feb 21 19:14:37 2018 (UTC)
MRUListEx = 1,0
  2 = INFORMATION HOW  DECRYP our FI.txt
  1 = paper_numbers.txt
  0 = sensitive_document.txt

----------------------------------------
recentdocs_timeline v.20161112
(NTUSER.DAT) Gets contents of user's RecentDocs key and place last write times into timeline based on MRUListEx

RecentDocs
Wed Feb 21 19:14:37 2018                :       INFORMATION HOW  DECRYP our FI.txt

The last write times are now placed in line with the values in the MRUListEx value
        Wed Feb 21 19:14:37 2018                2 = INFORMATION HOW  DECRYP our FI.txt
                                        1 = paper_numbers.txt
        Wed Feb 21 01:22:21 2018                0 = sensitive_document.txt
```

Oooo I found something! Not gonna lie, I'm super confused right now since I don't know what to do — but CTFs are meant to be a learning experience, so I dive forth... and then, BAM! A light bulb goes off in my head — *WOOOH!* What if I open the `./KEVIN/Desktop` directory and try extracting it? Could that actually work??

i found this https://www.youtube.com/watch?v=gLAyejgJ3Qs which speaks abt extracting NTUSER DAT to use registry explorer and thought maybe it would help..registry explorer if your wondering is a tool to read registry stuff and dat stuff by Eric Zukerman the goat of forensics.

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders... I looked it up and was like maybe it's here?.. hmm uhh?.. and then I looked at the MFT image again and went like oh shoot, it's gonna be on

NTUSER.DAT > Software > Microsoft > Windows > CurrentVersion > Explorer > RecentDocs

Hence, I locked in and went looking again lol — and there I found it on Registry Editor.

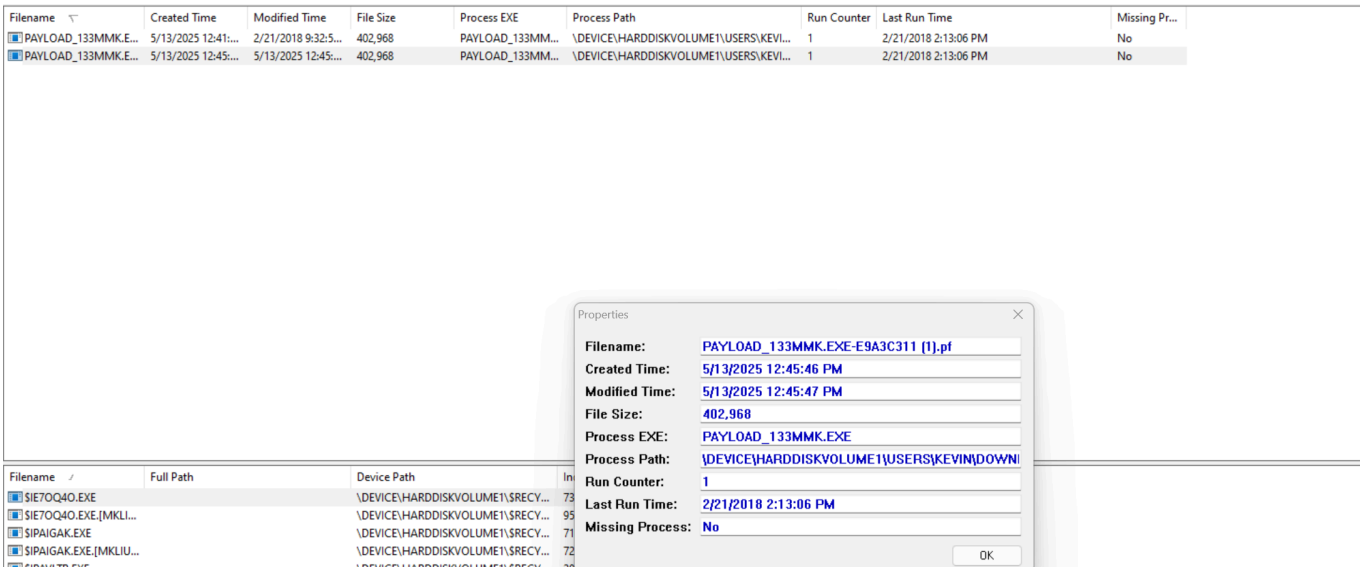
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
.txt	1	INFORMATION HOW DECRYP our FI.txt	INFORMATION HOW DECRYP our FI.lnk	0	2018-02-21 19:14:37	
.txt	0	paper_numbers.txt	paper_numbers.lnk	1		

Lmao I was still stuck, not really sure how to pull the file out—felt like I hit a roadblock 😭. But then I realized… **you can actually open files directly from the registry editor?!** Wild.

Earlier I figured out that you **can't extract** the actual `.txt` file **directly** from the NTUSER.DAT or `RecentDocs` view, which meant I had to somehow access `C:\Users\Kevin\AppData\Roaming\Microsoft\Windows\Recent\` —but I couldn't find that anywhere in the LinuxResponse files.

Then it hit me—**WAIT**, what if I check the `.pf` file for the payload ransomware? Maybe that would give me some lead or trace on where it was executed from or who ran it.

A `.pf` file, if you're not familiar, is a **Windows prefetch file**. It's basically a tracking file that logs how often and when a program was executed. So yeah, diving into that might just point us to the actual decryptor or at least confirm Kevin's involvement.**Kind of realized it might not help since it just a tracking file**



However we are able to see that it ran once which helps us to realize that the executable might have ran once and put stuff somewhere.

At this point i was about to give up then by chance i searched the wallet name on google [mkliukang@india.com] thinking it would help
No way—it's 1:08, my flight is at 1:30 and **boarding**, and I **found it**!! Apparently, this type of ransomware follows a specific format... Reading this blog showed that it's a strain of the **Dharma** virus, which is decryptable using **Kaspersky RakhniDecryptor.**

masoncc{RakhniDecryptor}.

Learning Outcome:

What I Learned from the this CTF

Alright , this CTF was a real ride. Here's a quick breakdown of what I learned while rushing through the challenge. 😂

1. **Importance of Environment (Linux vs Windows)**

- Knowing when to use **Midnight Commander (Linux)** vs **FTK Imager (Windows)** helped a lot. MC made it super quick to traverse folders and open text files, while FTK was amazing for viewing .csv (MFT) and .evtx logs.
- Lesson? Be comfortable switching environments based on the type of data you're analyzing.

2. **Running Processes & Activity Tracking**

- The `running_process.txt` file was useful but only if I paid attention. At first, I didn't see anything, but later I ctrl+F'd and found the payload.
- Also learned about checking `LastActivity.html` to see recent user activity. Super useful for tracking file executions.

3. **Registry Analysis**

- Learned how to check the `NTUSER.DAT` file using **Registry Explorer**.
- Found paths like `RecentDocs` which gave clues on recently accessed files.
- Even though you can't extract files directly from the registry, it points you in the right direction.

4. **.pf Files (Prefetch Files)**

- These are gold in Windows Forensics. They show what files were run, how many times, and when.
- Though it didn't give me the decryptor directly, it confirmed that the payload was run and reinforced Kevin's involvement.

5. **Searching Strings in MFT / CSVs**

- The MFT file gave away that `.wallet` ransomware extension and even included the attacker email.
- Helps in attribution, and confirms that encryption actually happened.
- Made me realize how useful it is to keyword search for stuff like `@india.com`, `wallet`, etc.

6. **Open-Source Intelligence (OSINT)**

- Googled the attacker email and found it's linked to Dharma ransomware.
- Then, using Elastio's blog, learned that **Kaspersky RakhniDecryptor** can decrypt old Dharma variants.
- Boom. Found the flag literally while boarding. Felt like a hacker in a movie fr.

Gona board the flight now hope i get threw the 2nd round of CCI with this one !!.