Open the notes

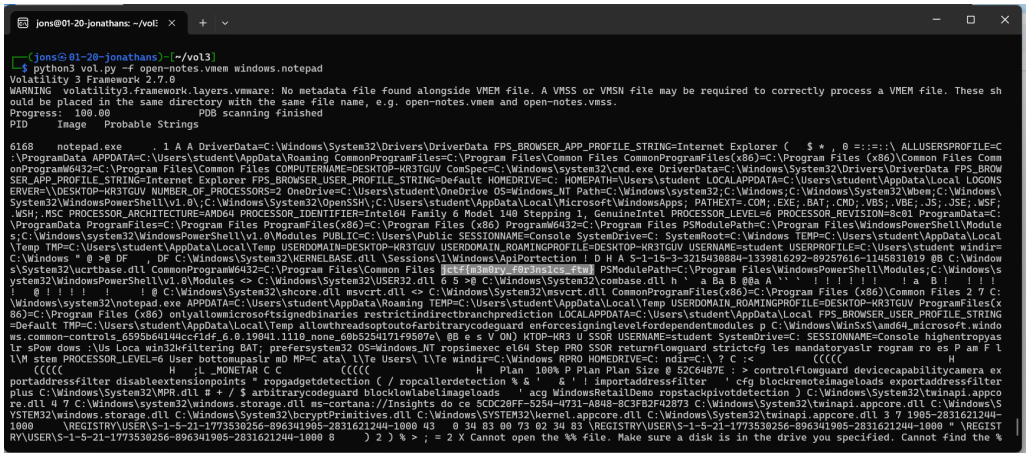
open-notes

331

forensics easy

A workstatiobn we are examining had some open files at the time of the memory capture. Examine the memory image at open-notes.vmem to find the flag.

Given vmem file (VMWare memory capture) to be analyzed using volatility. Because the question told us to check at notepad, so we're just gonna use windows volatility notepad plugin (https://medium.com/@rifqiaramadhan/volatility-3-plugin-kusertime-notepad-sticky-evtxlog-f0e8739eee55) and use it to view the memory



Sticky-situation

sticky-situation

991

forensics hard

- Somebody found this laptop running in the basement of Cullimore - right by the mailroom.
- Normally we'd just turn it in, but with all of the cyberattacks and cyberpsychosis going on - we're not about to throw away evidence without examining it first.
- Examine this ad1, and see if anything sticks out to you.
- I find it useful to write down my thoughts and findings on whatever I have nearby - paper, sticky notes, etc.
- Once I have evidence, I put it on a wall or lay it on the table and start connecting the dots.
- Yes, I'm crazy with strings all over the wall - but it helps!
- Maybe you'll find my approach useful, too?

File download: sticky-situation.ad1

Flag Format: `jctf{exactly_as_1t_@ppears}`

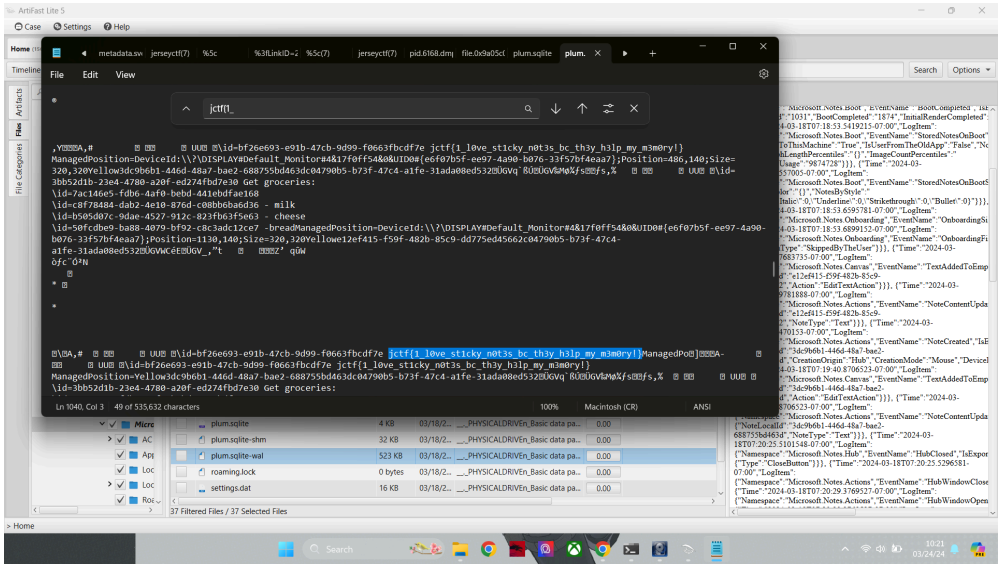
Pretty cool challs, given ad1 file we are tasked to find what the user store in sticky notes in his device. So we are gonna find out the artifact of the sticky notes.
First of all im just gonna mount it using FTK Imager and analyze it using ArtiFast Lite.
From this article (https://dingtoffee.medium.com/windows-sticky-notes-forensics-80ee31ab67ef) we know that there are some artifacts related to Sticky notes located at`%APPDATA%\Roaming\StickyNotes\`and `%LOCALAPPDATA%\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe`
We will check both of the directory

Transaction Log and Events :

`%LOCALAPPDATA%\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState\plum.sqlite-shm`

`%LOCALAPPDATA%\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState\plum.sqlite-wal`

Because of we are searching for what the user stored in the sticky notes, we will check at the “plum.sqlite-wal” file and open it using notepad



All along watchtower

All-Along-the-Watchtower

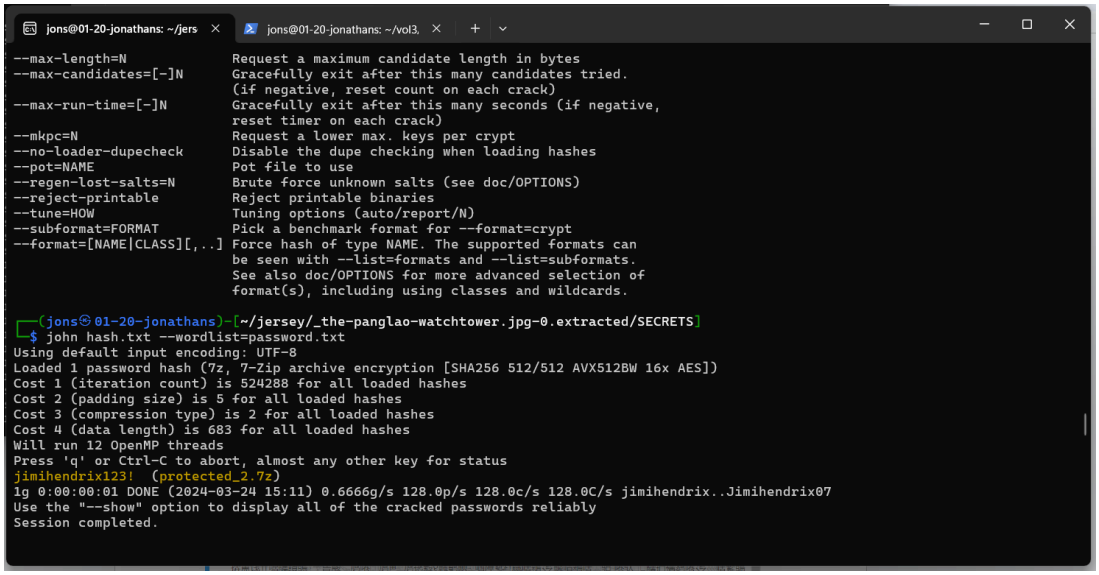
561

forensics medium

Our informant has met back with us at base. He has stolen a file from a suspect who's starting to show dangerous signs of cyberpsychosis. Aside from his unending lust for bloodshed, our informant noted that the suspect would not shut up about "rats making him crazy" as well as the term "Base FFFF+1" but that's probably just nonsense. Anyways, can you look beyond the layers of this corrupted file to extract the information that we need?

Developed by: BonsaiUmai

Given the file we're just gonna brute it using given password.txt and john



Extracting it using the password give us file “secrets.txt” contains some weird strings. Based on the chall description “Base FFFF+1” refers to Base65536 so we gonna decode it using that