



Mission Name

FindOutDeeply

History Context

The main objective for Claire and Ethan, is to check if the book provided was written by Claire's father.

Technical High-Level Overview

Player must analyse a book provided, named PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf. This book was written by Claire's father. Player's goal would be to locate a malicious PDF file.

Short Description

You're going to search for a book named PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf. Your goal is to analyse and detect any IP address related to the PDF file.

Mission Description

You're going to search for a book named PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf. To accomplish this goal, you're going to analyse a full image disk. Your goal is to analyse and detect any IP address related to the PDF file.

Location

SHANGHAI | BACKSTREET BAR

Tools

- FTK Imager
- Shadow Explorer
- Strings and findstr

Questions

Which is the name of network that was connected this evidence?

- Network

Which is the Security ID of “shangai” user?

- S-1-5-21-194084996-1766017298-4069487288-1000

Hints

1. Located PDF file in shadow copies.
2. Analyse PDF pdf with strings
3. Use strings command and grep so filter an IP Address.

Write Up

Player must mount image provided with Access Data FTK and they should detect three shadows copies::

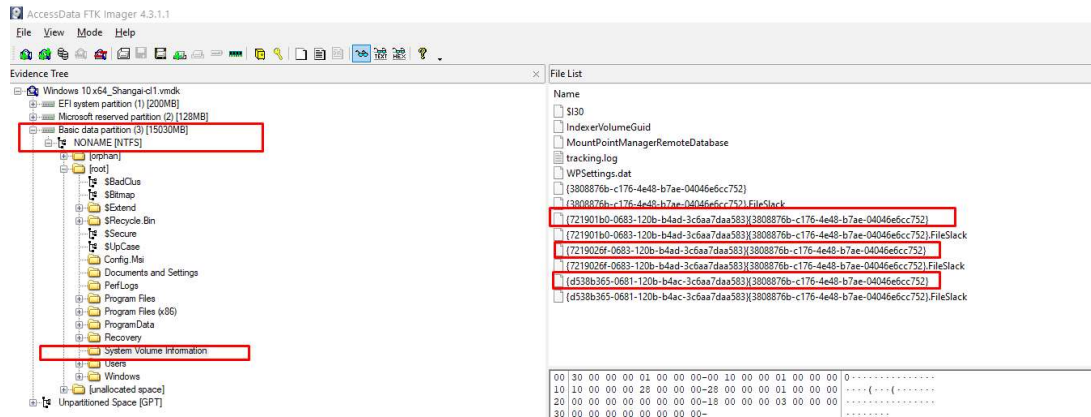


Figure 1

If player check the file system, they won't find any PDF file. So, the key is to search for inside a Shadow Copy. First of all, player must mount the imaged provided with Arsenal image mounter:

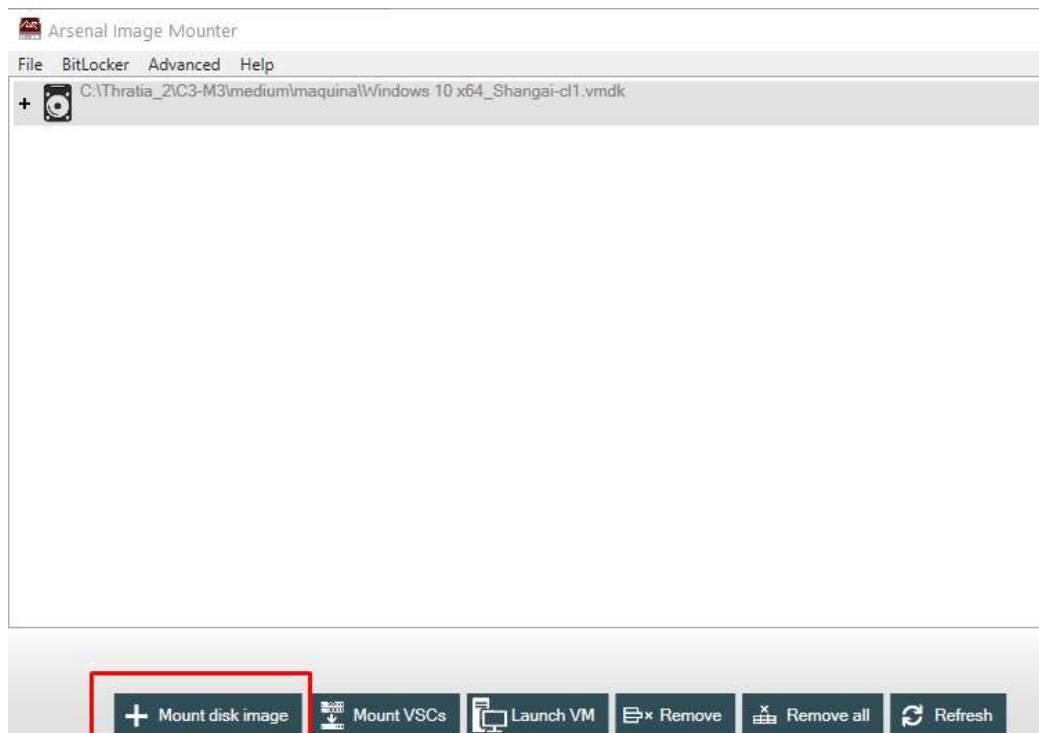


Figure 2

Once mounted, if player checks C:\Users\shangai\Documents, they won't see any PDF file:

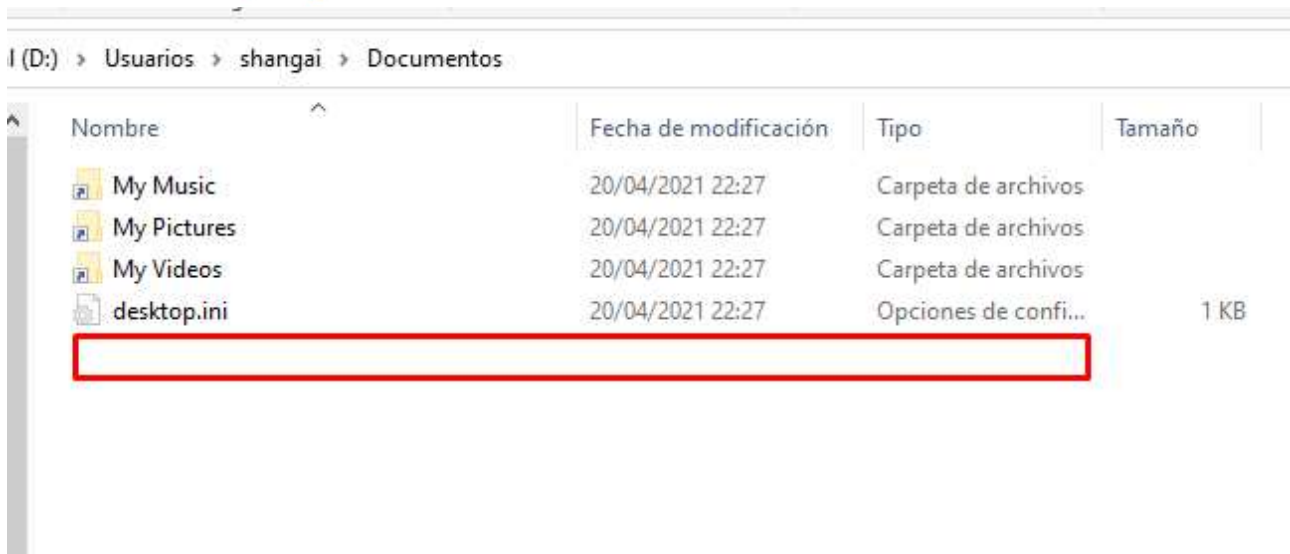


Figure 3

To locate the malicious PDF file, player must analyse shadows copies, using Shadow Explorer:

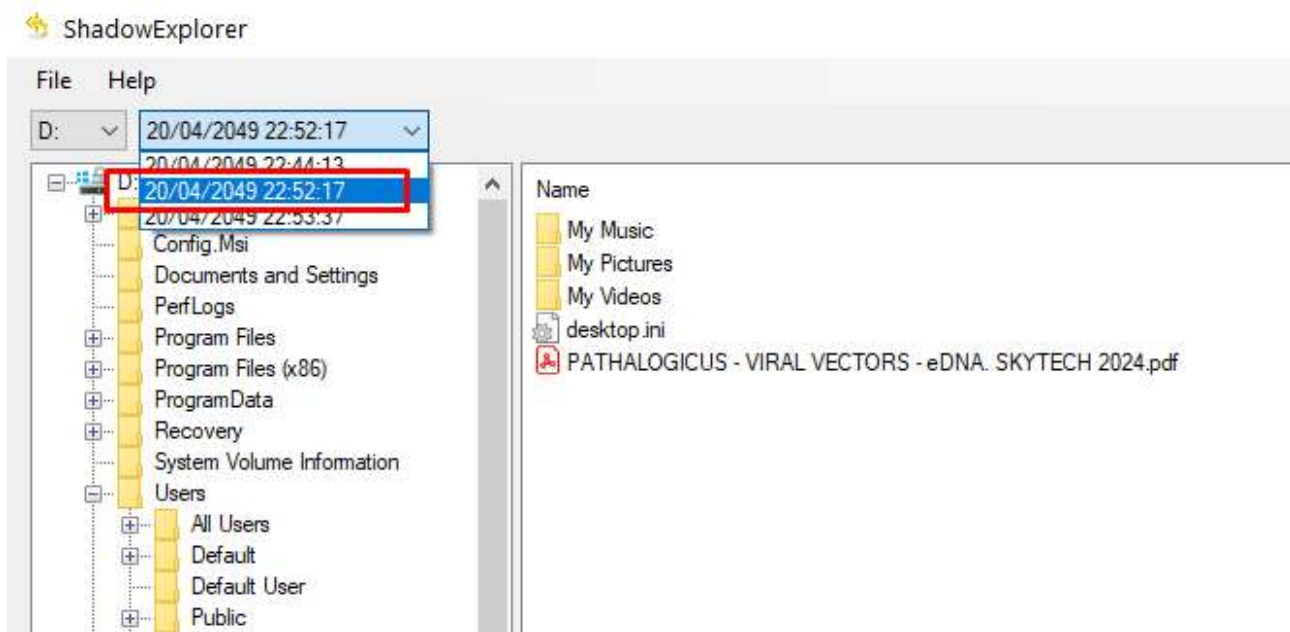


Figure 4

Once located, player should extract malicious PDF file to analyse.

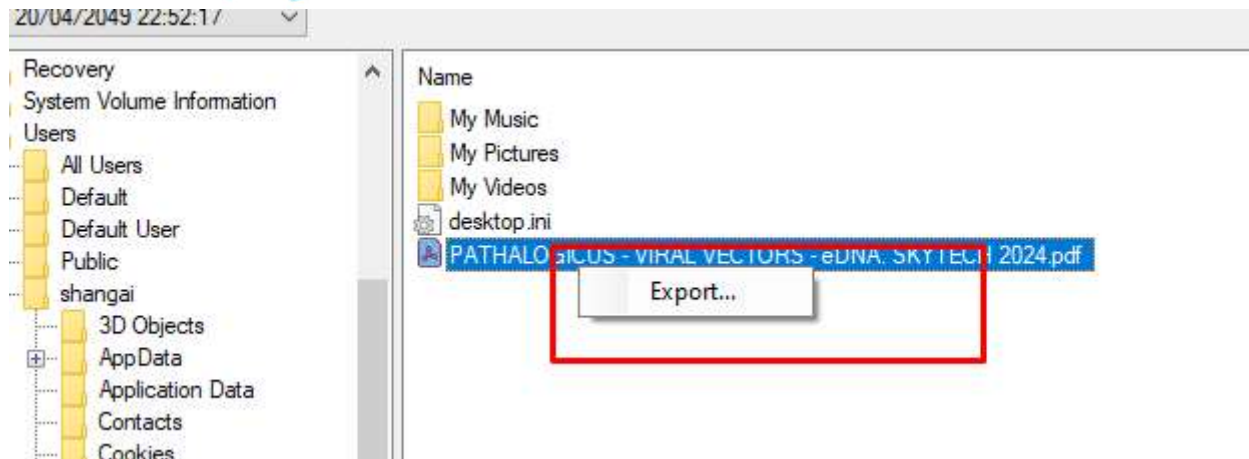


Figure 5

Once extracted, player could analyse to locate any IP address:

- `strings "C:\Users\recon\Desktop\PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf" | findstr /r "[0-9][0-9]*\.[0-9][0-9]*\.[0-9][0-9]*\.[0-9][0-9]*"`

```
C:\Users\recon\Desktop>strings "C:\Users\recon\Desktop\PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf"
| findstr /r "[0-9][0-9]*\.[0-9][0-9]*\.[0-9][0-9]*\.[0-9][0-9]*"
/X (\\10.21.41.4\Skyt)
```

Figure 6

Finally player will be able to get the IP address: 10.21.41.4

Flag Information

flag{10.21.41.4}