Disk Analysis & Autopsy

Disk Analysis & Autopsy is a Medium-difficulty forensics challenge on TryHackme. It involves analyzing a forensic disk image in Autopsy to determine what malicious software was installed, by which users, and uncover various other artifacts.

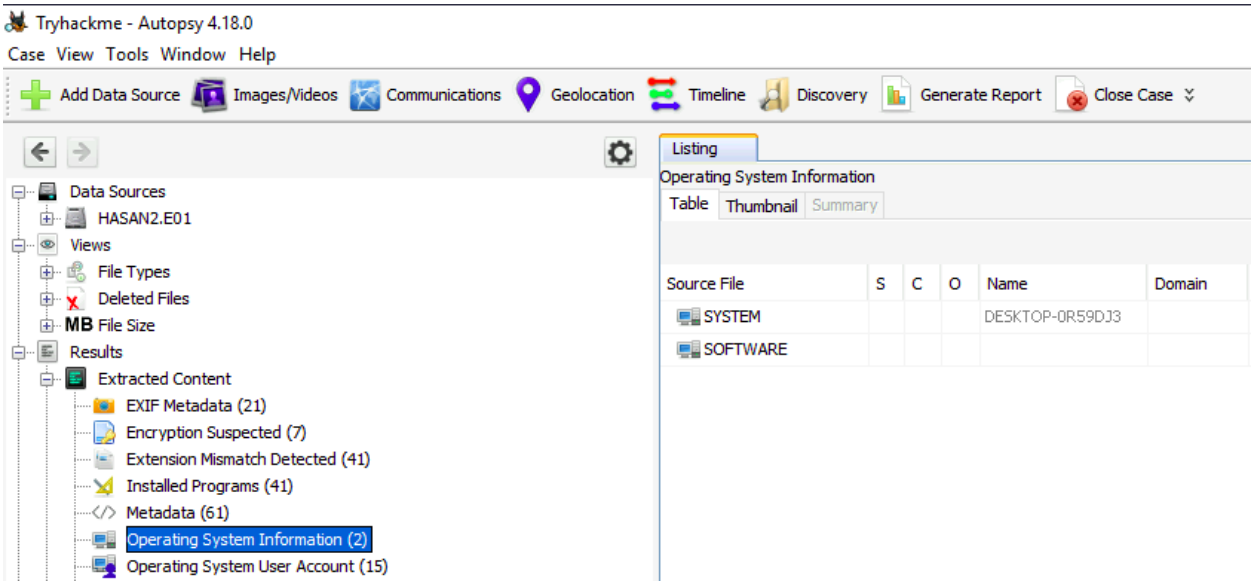
Here I will perform a manual analysis of the artifacts discovered by Autopsy to answer the module questions below.

1. What is the MD5 hash of the E01 image?

Select the E01 datasource in the Container tab under Summary.
Answer: 3f08c518adb3b5c1359849657a9b2079

2. What is the computer account name?

The computer name is under the results for “Operating System Information”.
Answer: DESKTOP-0R59DJ3

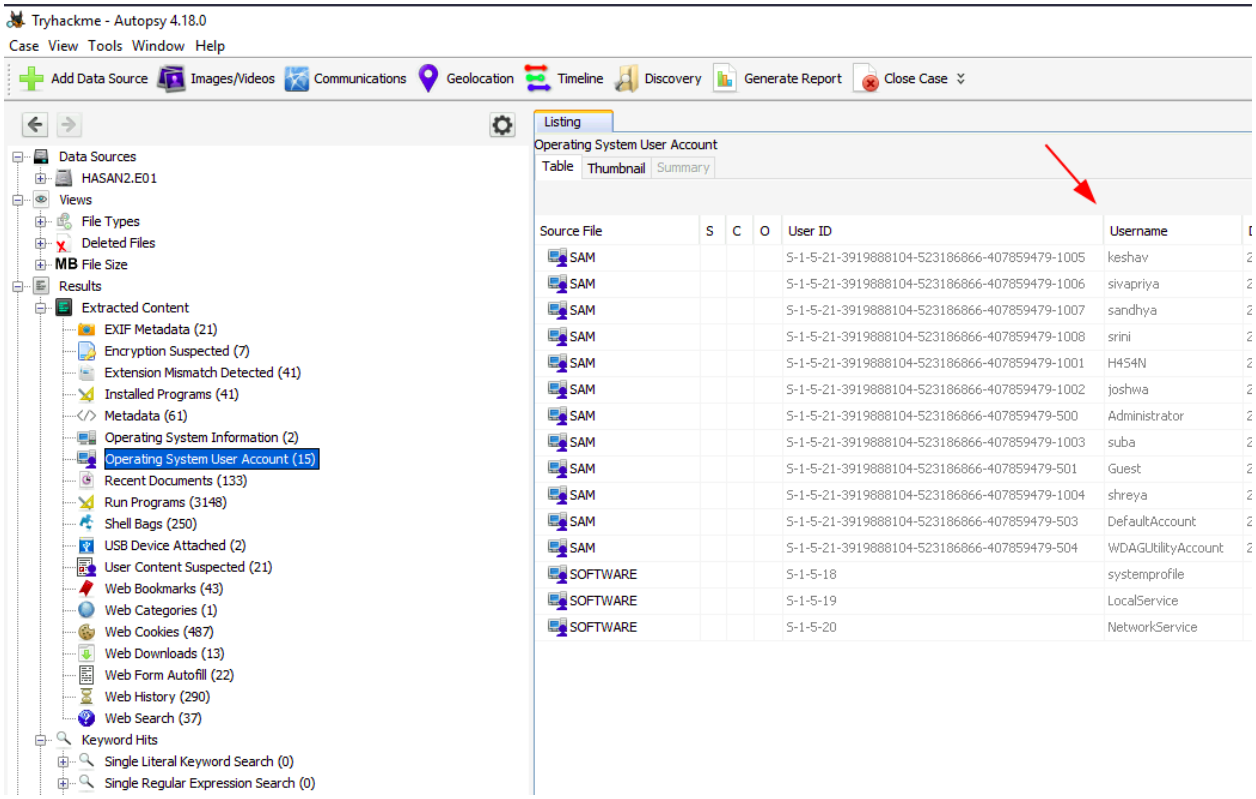


Disk Analysis & Autopsy

3. List all the user accounts

Below the Operating System Information results I see an option for Operating System User Accounts which is where the usernames are listed.

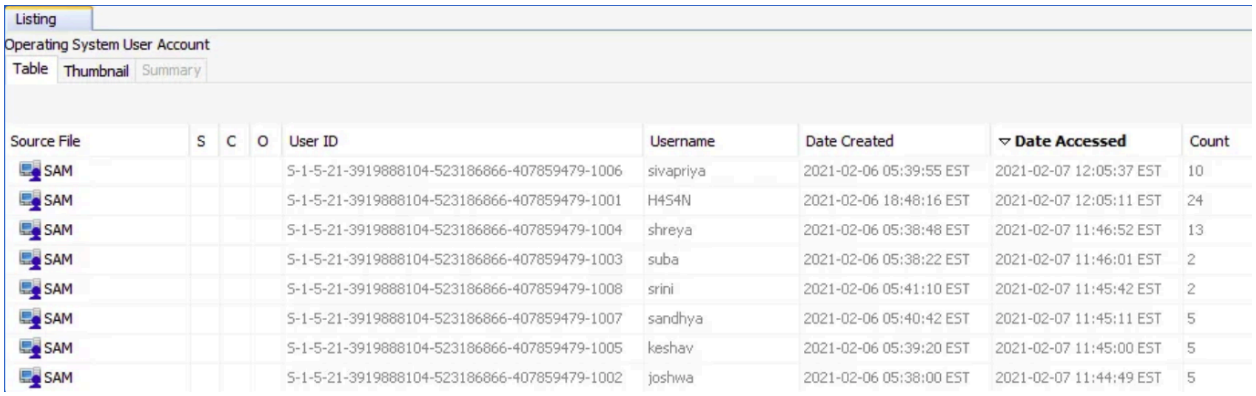
Answer: H4S4N,joshwa,keshav,sandhya,shreya,sivapriya,srini,suba



4. Who was the last user to log into the computer?

Sort the User Accounts by “Date Accessed” to get the answer.

Answer: sivapriya

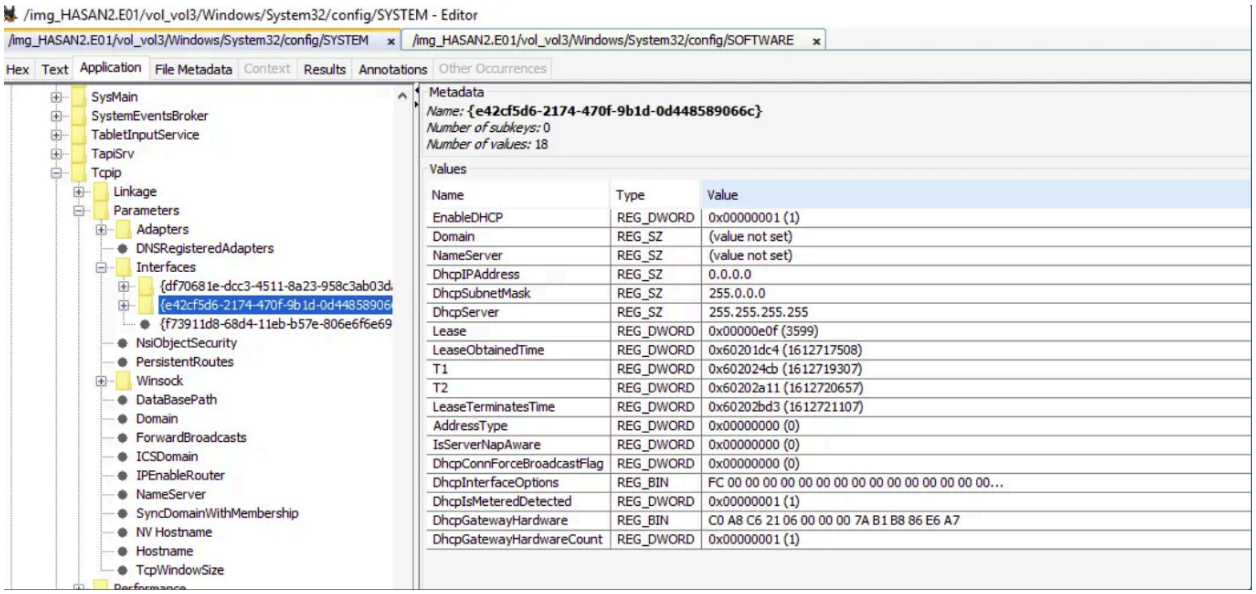


Disk Analysis & Autopsy

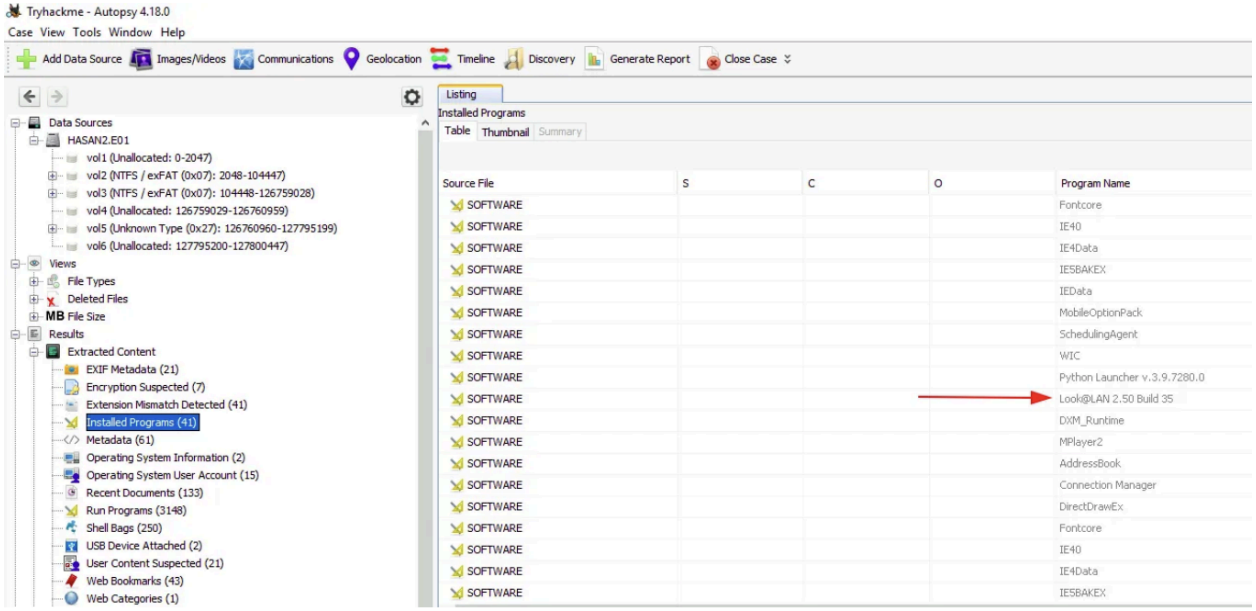
5. **What was the IP address of the computer?**

Answer: 192.168.130.216

With an image of a Windows machine, find the IP address associated with network adapters in the Windows Registry, which can also be accessed from the registry within Autopsy.

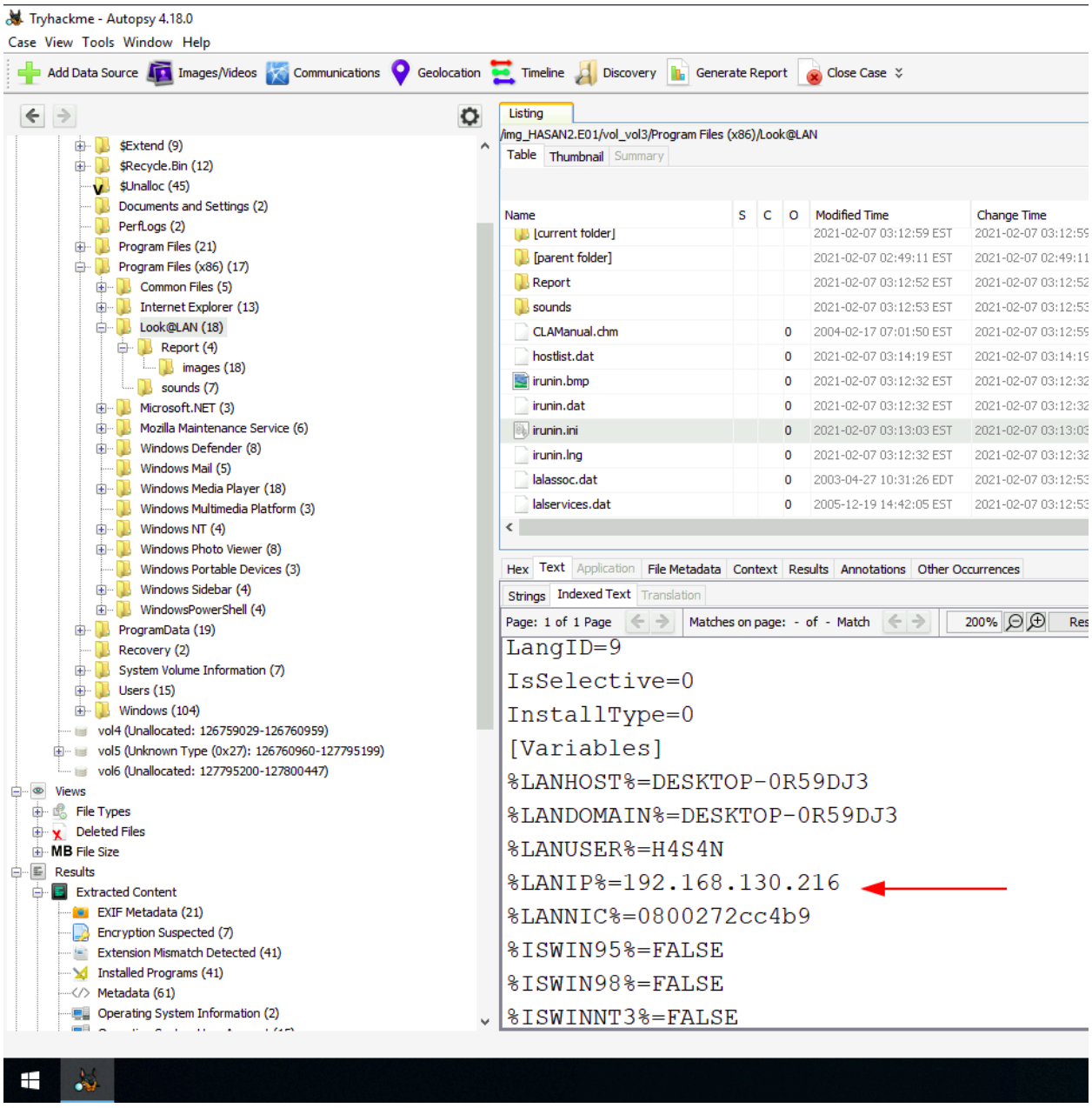


The IP address is listed as 0.0.0.0. While looking through Autopsy, I see an unusual application installed on the device.



Searching for the executable name tells me it is a network monitoring tool, so check for any generated logs. Finding its directory under Program Files (x86). Among the files in the folder, an .ini file appears (.ini files are used to set configurations).

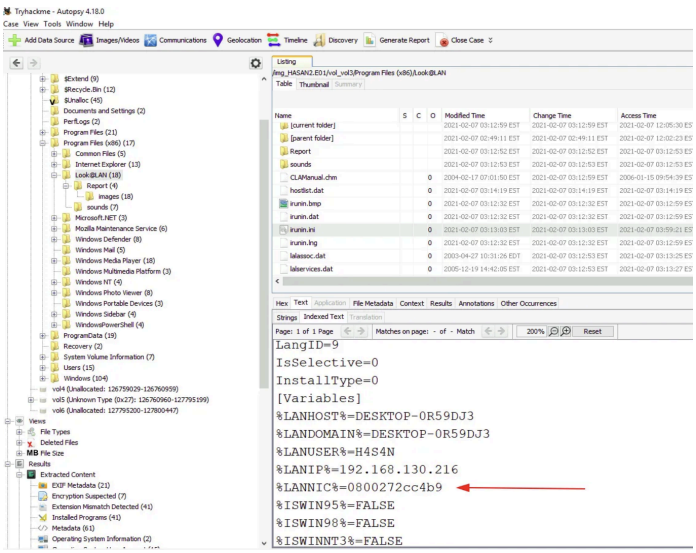
Disk Analysis & Autopsy



6. **What was the IP address of the computer?**

It wasn't present in the registry, and searching for the string "mac" within the .ini file returns no results. A second look at the fields surrounding the IP address, notice there is one for LANNIC.

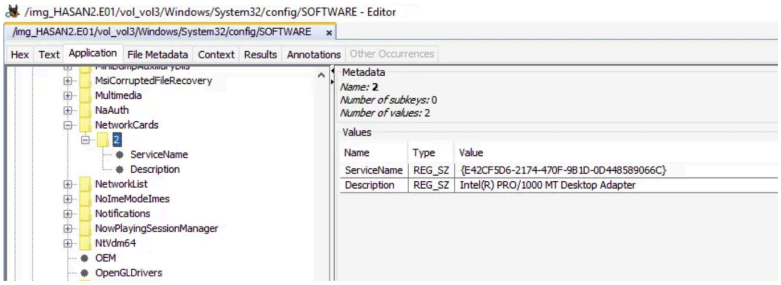
Answer: 08-00-27-2c-c4-b9



Disk Analysis & Autopsy

7. **What is the name of the network card on this computer?**

Return to the registry to get the name of the NIC, and find the name of the NIC under the following path: *SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards*



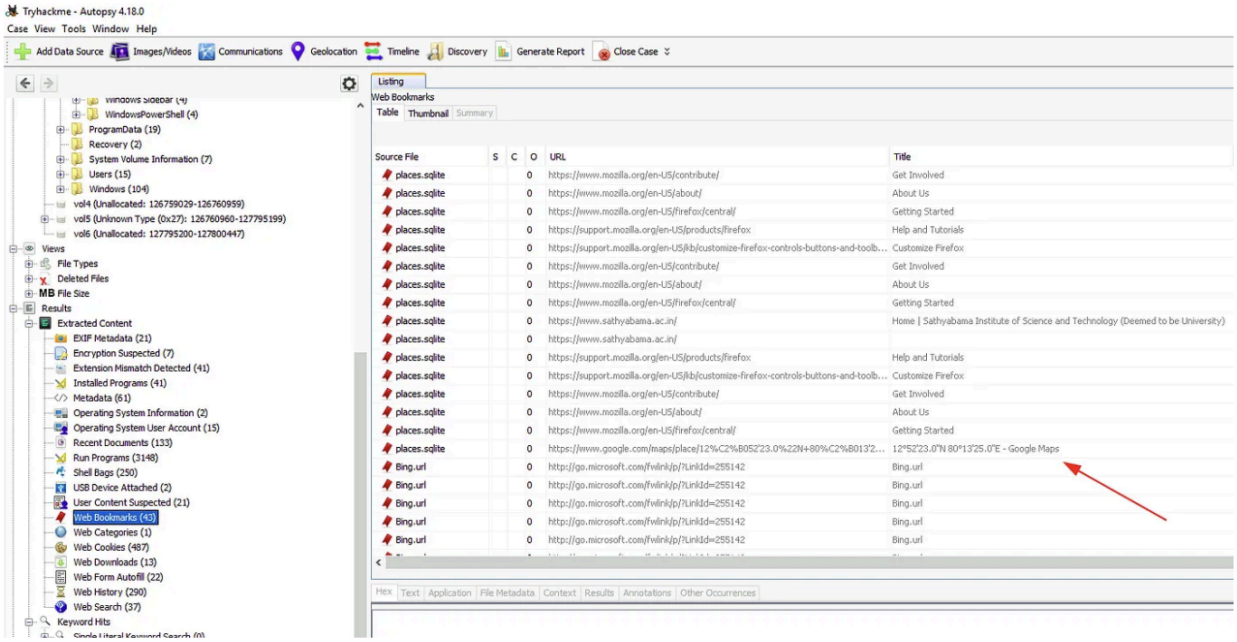
Answer: Intel(R) PRO/1000 MT Desktop Adapter

8. **What is the name of the network monitoring tool?**

Answer: Look@LAN

9. **A user bookmarked a Google Maps location. What are the coordinates of the location?**

Check Autopsy's Web Bookmarks results **Answer**: 12°52′23.0″N 80°13′25.0″E

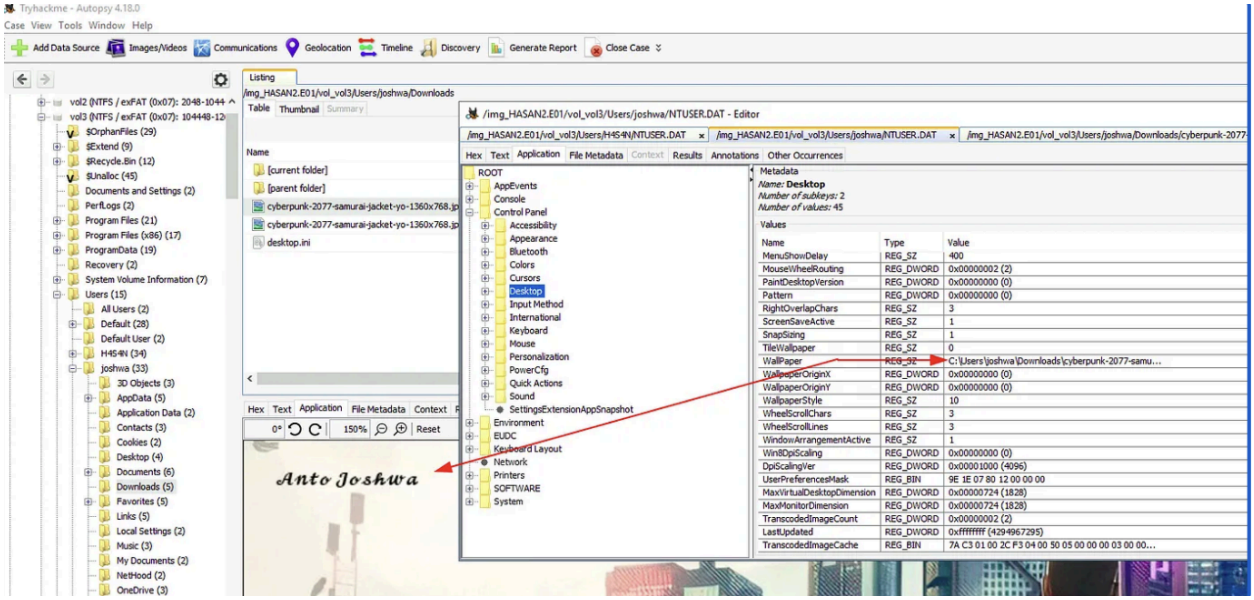


10. **A user has his full name printed on his desktop wallpaper. What is the user's full name?**

Windows stores user profile information in the NTUSER.dat file; located within their home directory. Knowing this, we can determine user wallpaper images and whether their name is visible in the image. We can see a name in the image and the last name matches the username, so this looks like our answer.

Answer: Anto Joshwa

Disk Analysis & Autopsy



11. **A user had a file on her desktop. It had a flag but she changed the flag using PowerShell. What was the first flag?**

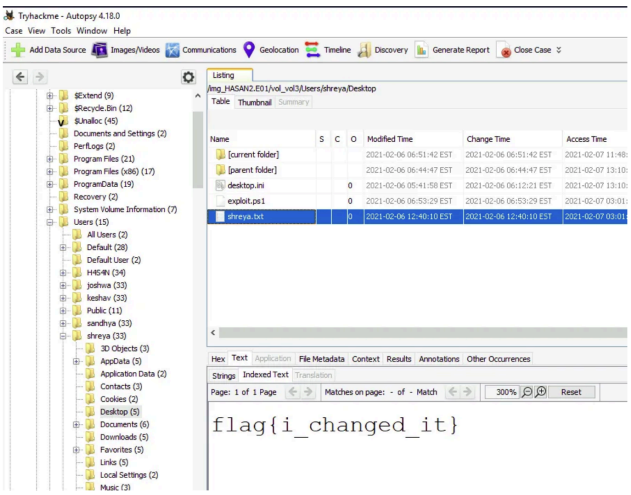
PowerShell command history is stored in *APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt*, so that will be the focus of the search. Firstly, determine what the file is named and who the user is.

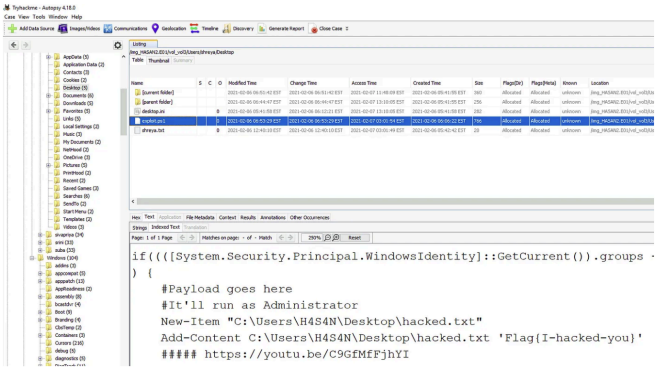
Answer: flag{HarleyQuinnForQueen}

12. **The same user found an exploit to escalate privileges on the computer. What was the message to the device owner?**

I took note of a PowerShell script named exploit in the previous question.

Answer: flag{I-hacked-you}





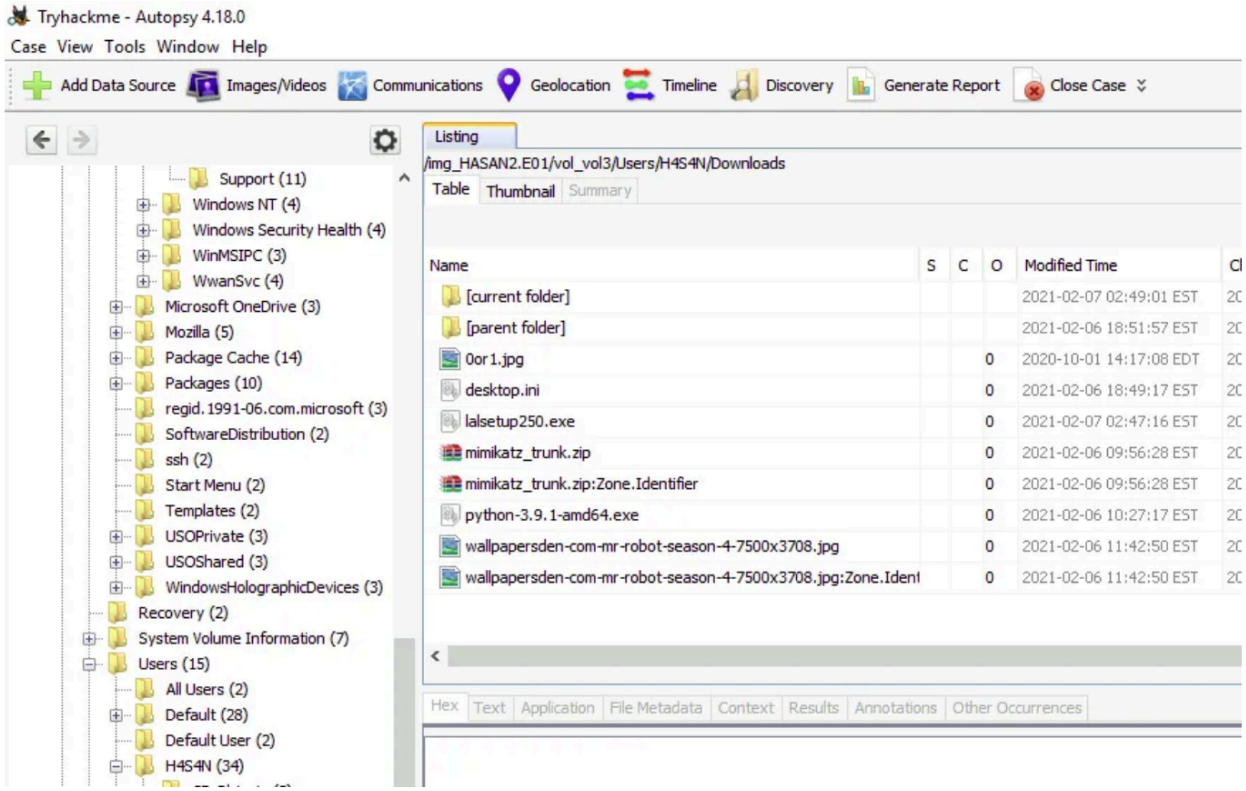
```
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups
) {
    #Payload goes here
    #It'll run as Administrator
    New-Item "C:\Users\H4S4N\Desktop\hacked.txt"
    Add-Content C:\Users\H4S4N\Desktop\hacked.txt 'Flag{I-hacked-you}'
    ##### https://youtu.be/C9GfMfFjhYI
```

Disk Analysis & Autopsy

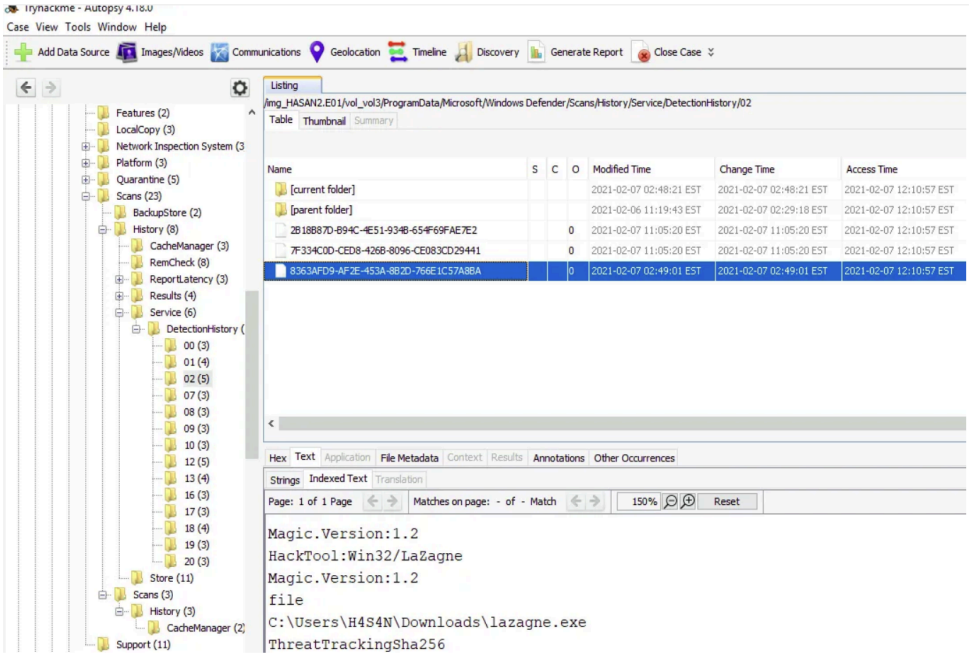
13. **2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)**

There are multiple signs of Mimikatz on the image, and the zip file is located in H4S4N's *\Downloads* folder.

Answer: Lazagne,Mimikatz



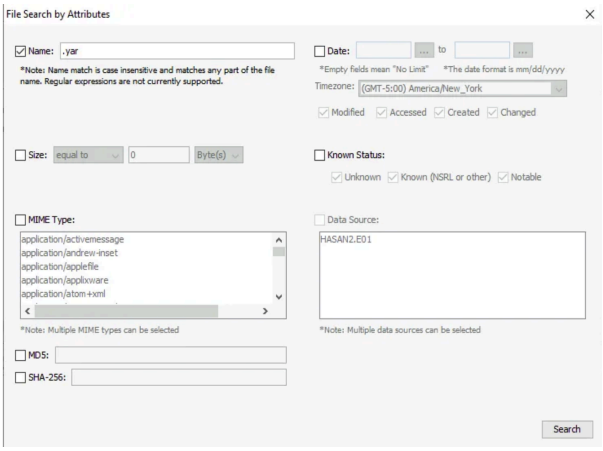
The other executable, however, is elusive. Checking the browser history, downloads, web searches, run programs, installed programs, recent documents, etc. leaves no clues. But there's a log source 'Windows Defender.' We'll have to determine where Defender records its alerts. Google finds a reference to

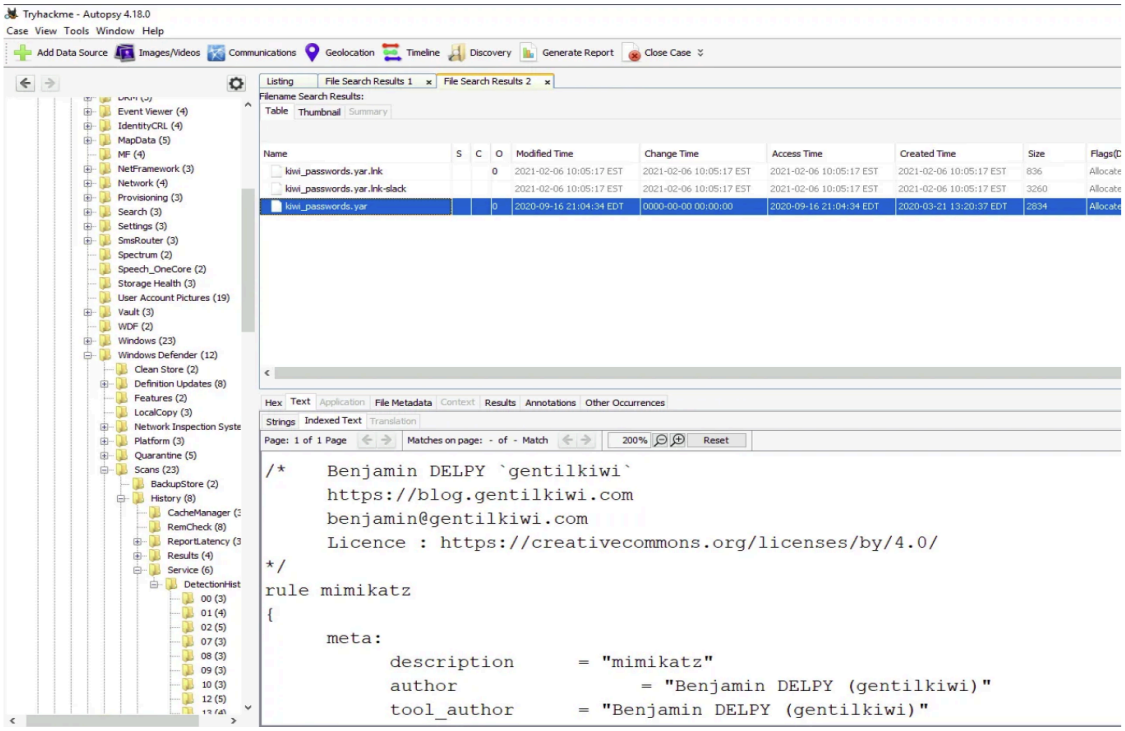


C:\ProgramData\Microsoft\Windows Defender\Scans\History. Multiple alerts for mimikatz preceding an alert for lazagne.exe. Google informs us it is another password-dumping tool.

14. **There is a YARA file on the computer. Inspect the file. What is the name of the author?**

Use the File Search By Attribute tool (located in the Tools drop-down menu) to search .yar and .yara files.
Answer: Benjamin DELPY (gentilkiwi)

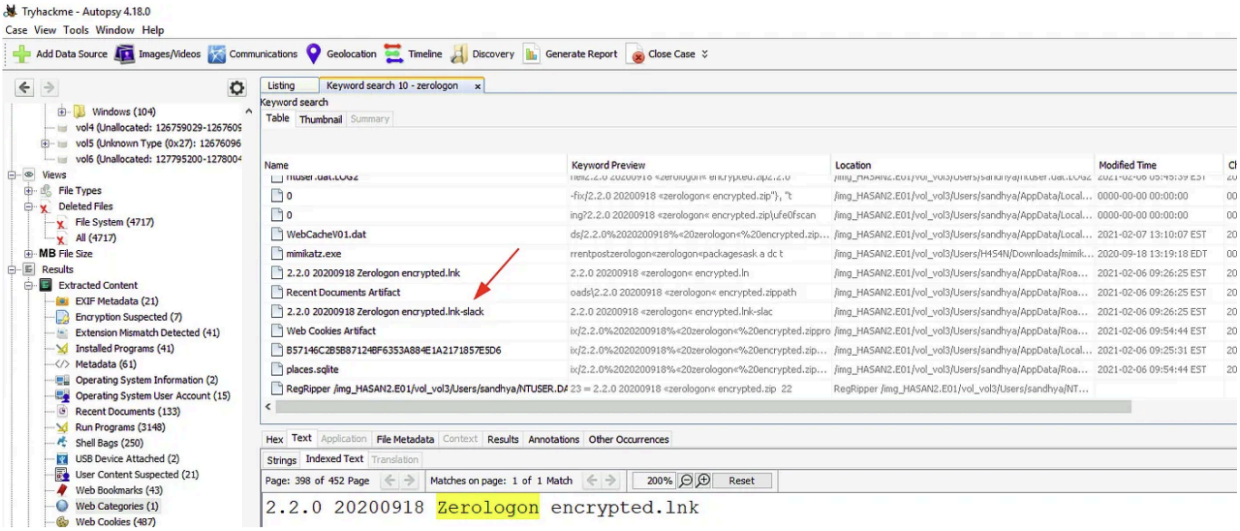




15. **One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found? (include the spaces in your answer)**

And we got a hit for a zipped Zerologon exploit. Though the file has been "deleted", there's evidence that it was located in sandhya's download folder.
Answer: 2.2.0 20200918 Zerologon encrypted.zip

Disk Analysis & Autopsy



Conclusion

This involved a deep dive into the user activity, registry, and additional sources of evidence. I learned in other walkthroughs to keep Windows Defender's scan history in mind for future investigations and incident response.