Forensic Investigation

The Case of Stolen Szechuan Sauce

By Rafi Islam

Tables of Content

Disk Mounting and Forensic Analysis

- Autopsy 4.21.0 - Autopsy is an open-source forensics platform that is fast, user-friendly, and capable of analyzing various mobile devices and digital media. It addresses computer data security, cyber theft, breaches, cyber-attacks, incident response, internal investigations, and fraud.
- AccessData FTK Imager4.7.1.2- FTK Imager is a tool for digital evidence analysis that can help you acquire, preview, and analyze data from various sources. It is widely used to gather and examine digital evidence.
- Network Packet Analyzer- Wireshark is an open source network packet analyzer that captures and displays network packets in real-time. It is useful for troubleshooting network issues and analyzing network protocols.
- Windows Registry Analyzer- is an open-source and easy-to-use graphical tool for working with Windows registry files called hives.
- Memory Analyzer- Volatility is a memory analysis tool that extracts information from memory dumps. It can perform tasks such as malware detection, timeline analysis, and memory carving.
-

Overview of files To be Analyzed

Domain Controller (DC01) Files:

- Disk Image (EO1)
- Memory and Page file
- Autoruns
- Protected Files
- PCAP file

Desktop Files:

- Disk Image (E01)
- Memory and Page file
- Autoruns
- Protected Files

Questions and Answers

1). What's the Operating System of the Server?

Answer- Windows Server 2012 Standard Evaluation
File Used: Domain controller disk image - DC01 → E01
Tool Used: Autopsy
Method: After mounting disk image on Autopsy, it showed the domain controller name as CITADEL-DC01 and showed the operating system as Windows Server 2012 Standard Evaluation.

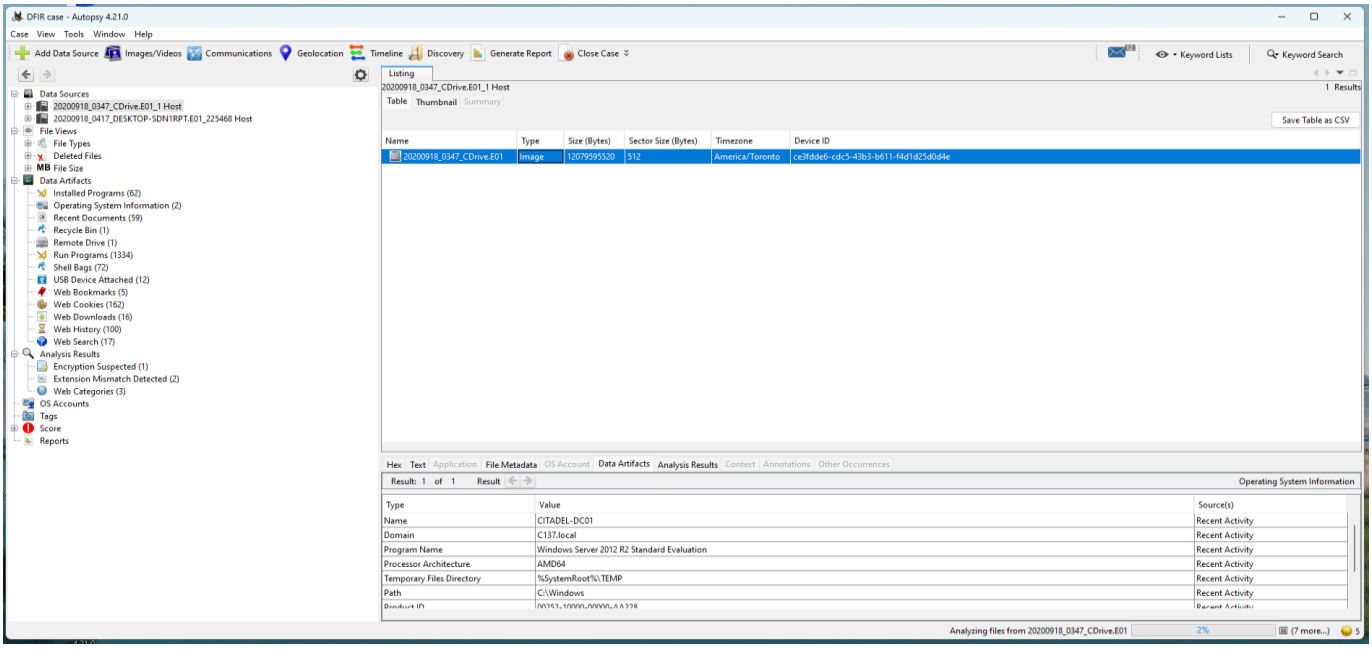

Figure 1: Server Operating System in Autopsy

2). What's the Operating System of the Desktop?

Answers: Windows10 enterprise evaluation

Files used: Desktop disk image- Desktop-01
Tools used : Autopsy
Method: After mounting disk image Desktop-E01 on Autopsy, it showed the desktop name as DESKTOP-SDN1RPT and showed the operating system as Windows10 enterprise evaluation.

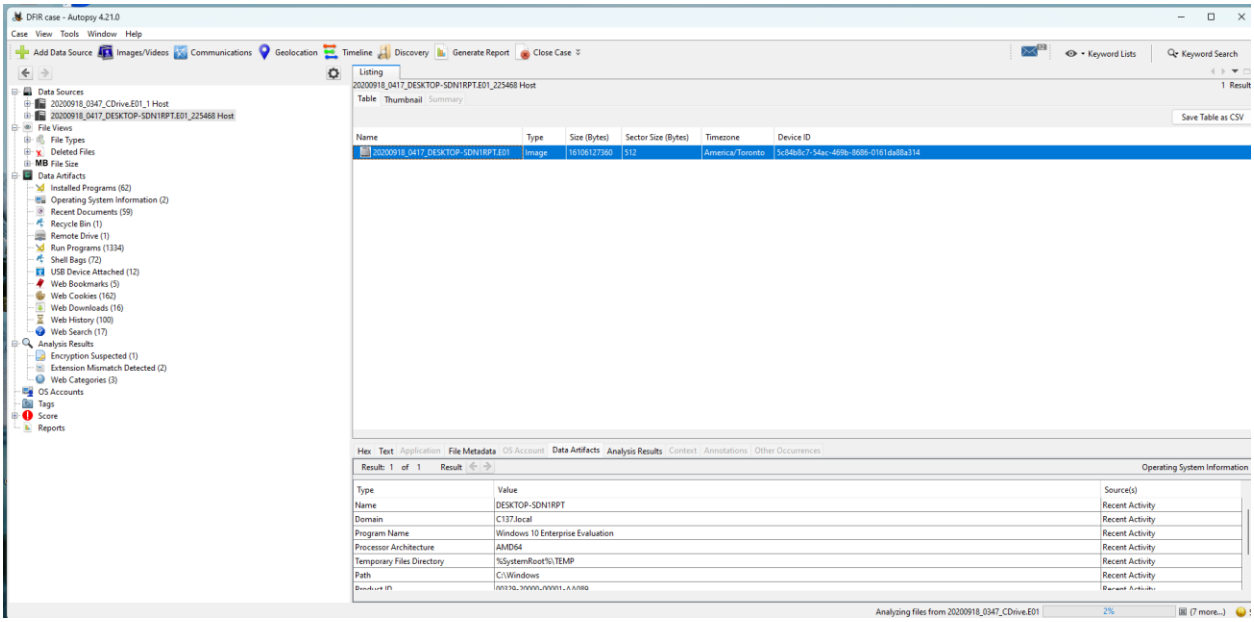

Figure 2: workstation operating system in Autopsy

3). What was the local time of the Server?

Answer: Pacific Standard Time

Tool Used: Autopsy and Registry Explorer

Method: Time Zone Information can be found on registry system hive. To access the required information registry system file was exported from DC01-E01 using Autopsy. The registry location for windows is Windows-> system 32->Config-> System. The extracted “System” registry file was saved on computer and the file was opened with windows registry explorer. Using Registry Explorer the information was located in the following path

System hive -> ControlSet001 -> Control -> TimeZoneInformation

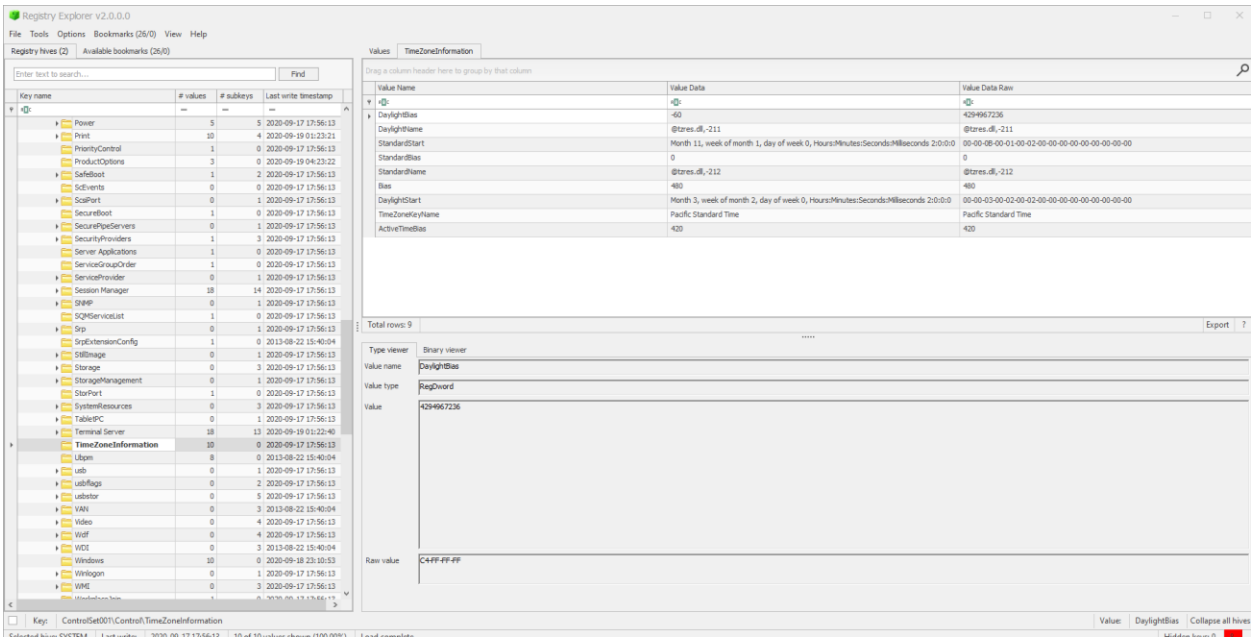

Figure 3: Timezone information of System hive on Registry explorer

4). Was there a breach?

Answer: Yes

File Analyzed: DC01-E01 and PCAP

At first I looked at network packets using Wireshark Packet Analyzer of the DC01-pcap file. I loaded the PCAP file in Wireshark and applied two display filters to look for suspicious activities. I was specifically looking if any suspicious IP address trying to sniff packet or scan the network. For this purpose I used the following command

tcp.flags.syn == 1 and tcp.flags.ack == 0

this command should return all the IP address trying to ping the above system.

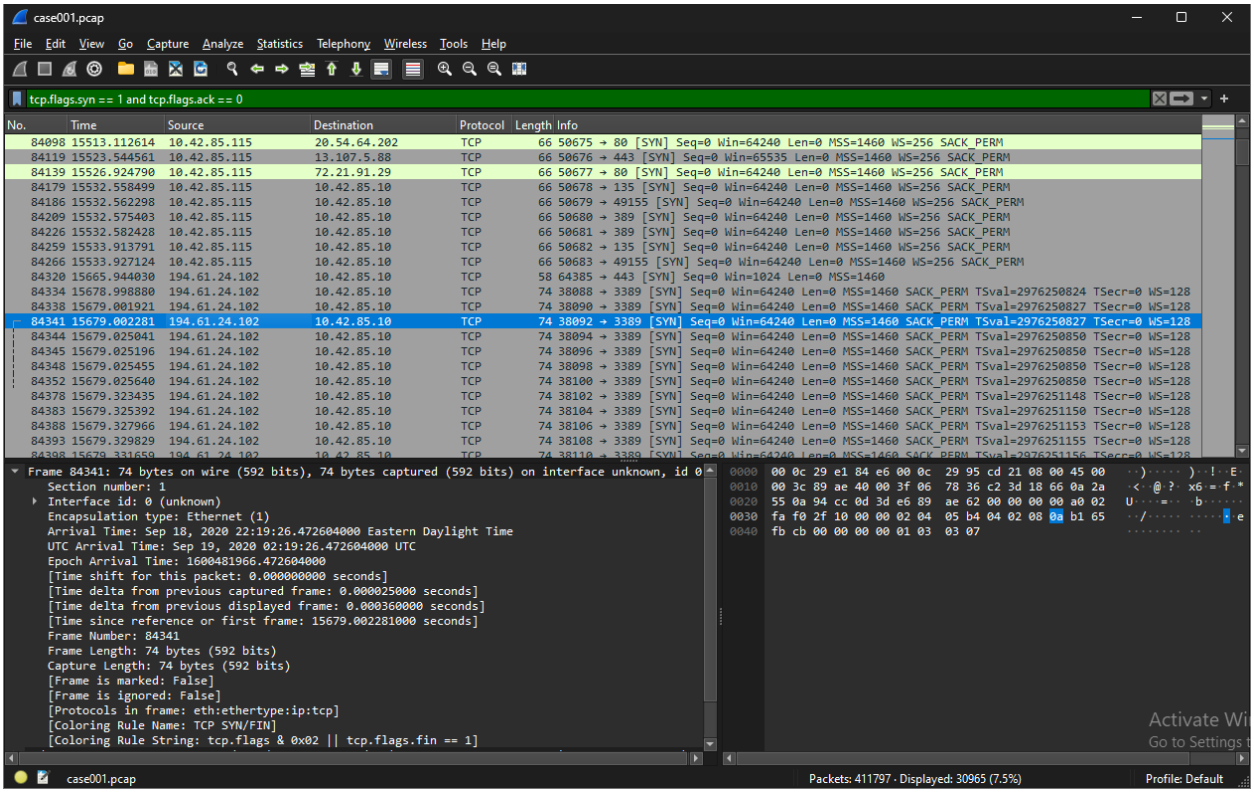

Figure 4: Wireshark packet-capture analysis

Here we can see the IP address 194.61.24.102 is making unusually large number of request. Checking the time we can see it was between Saturday night and Sunday early morning. For this reason, I investigated it further to see if they were able to access the system using the following the command

tcp.flags.syn == 1 and tcp.flags.ack == 1

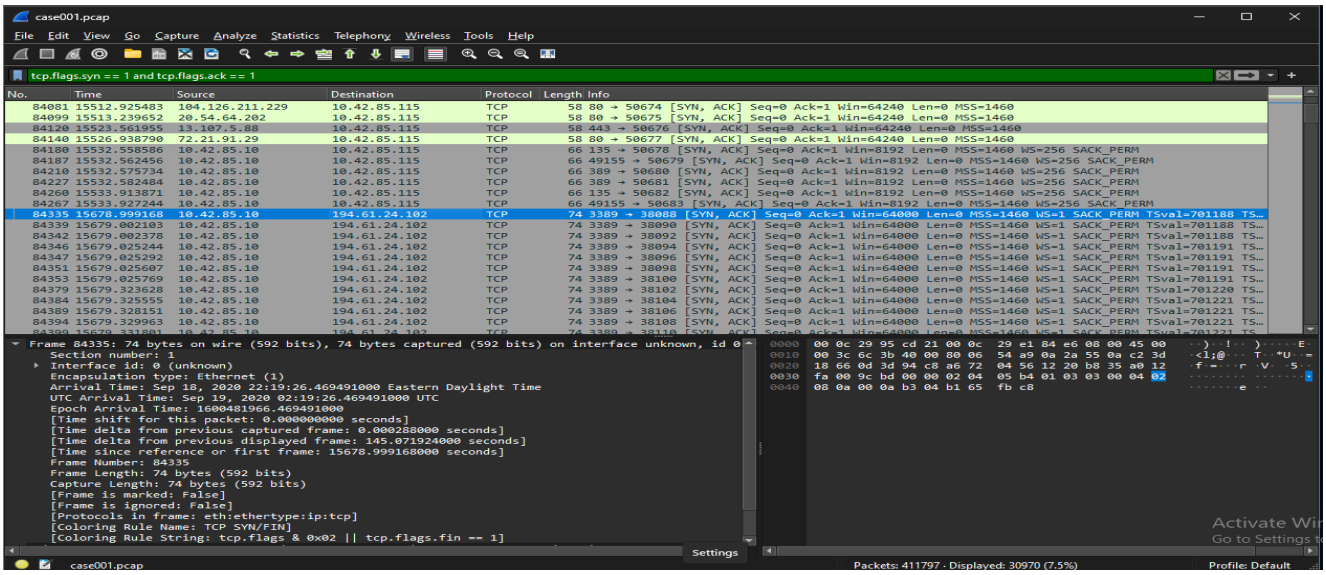

Figure 5: Wireshark packet-capture analysis

Further analysis shows multiple requests are made from the IP address 194.61.24.102 to the domain controller IP address 10.42.85.10 on port 3389. Further research shows port 3389 is used for Windows computers' Remote Desktop Protocol (RDP). This suspicious activity started 22:19:26,on the weekend suggesting more than likely it's a brute-force login attempt on the domain controller server (*Brute force, technique T1110, n.d.)* (*Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®*, n.d.).

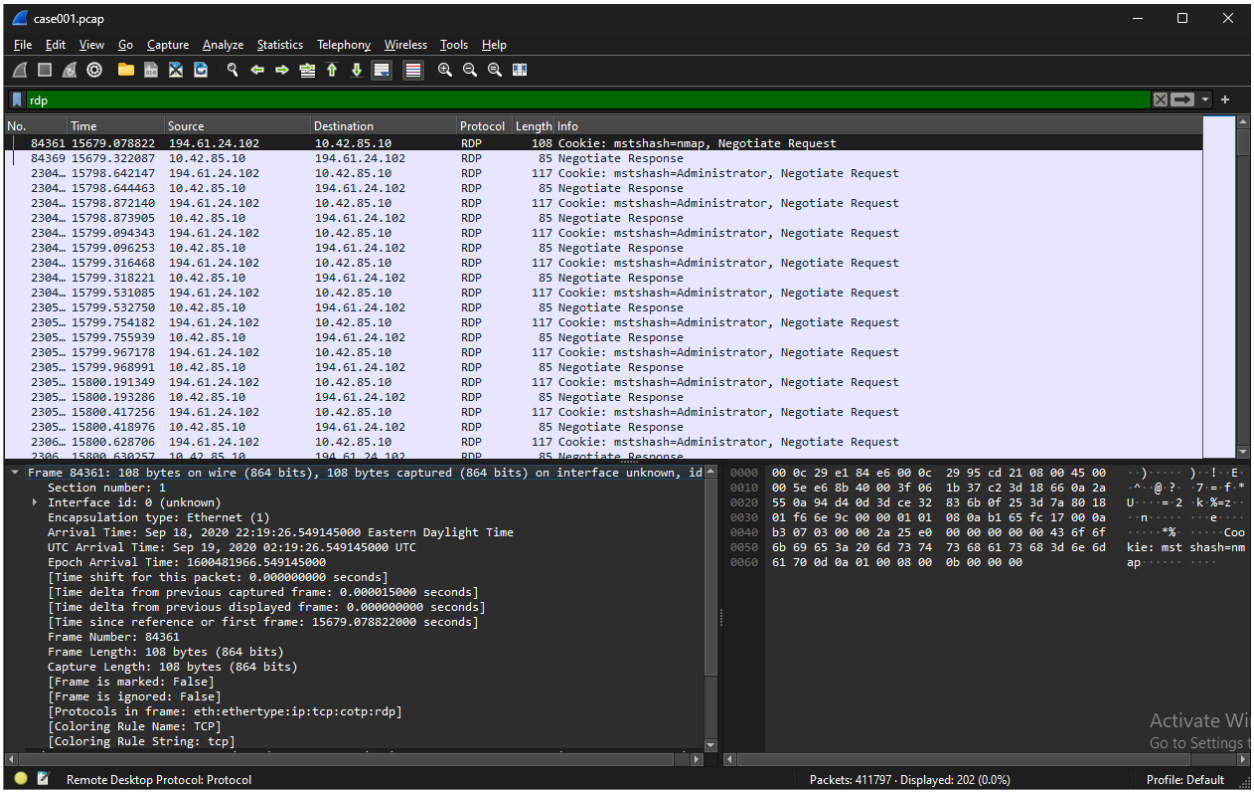

Figure 6: Wireshark RDP request Analysis

The above diagram shows multiple RDP request from single IP address. For further analysis, we are going to look into IP address in Virus Total website.

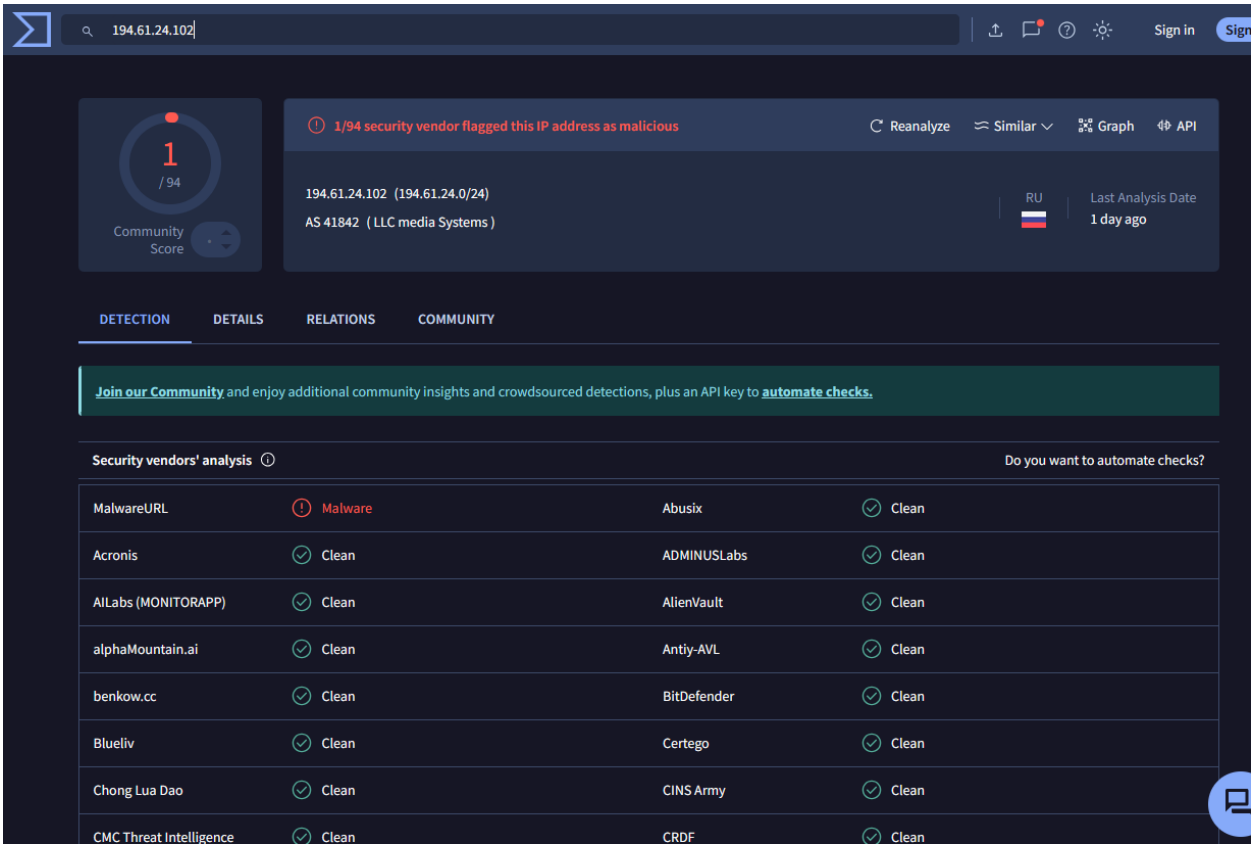

Figure 7: Virus total analysis

Virus total website shows the IP address generated from Russia. This further solidifies our theory that this is a malware attack.

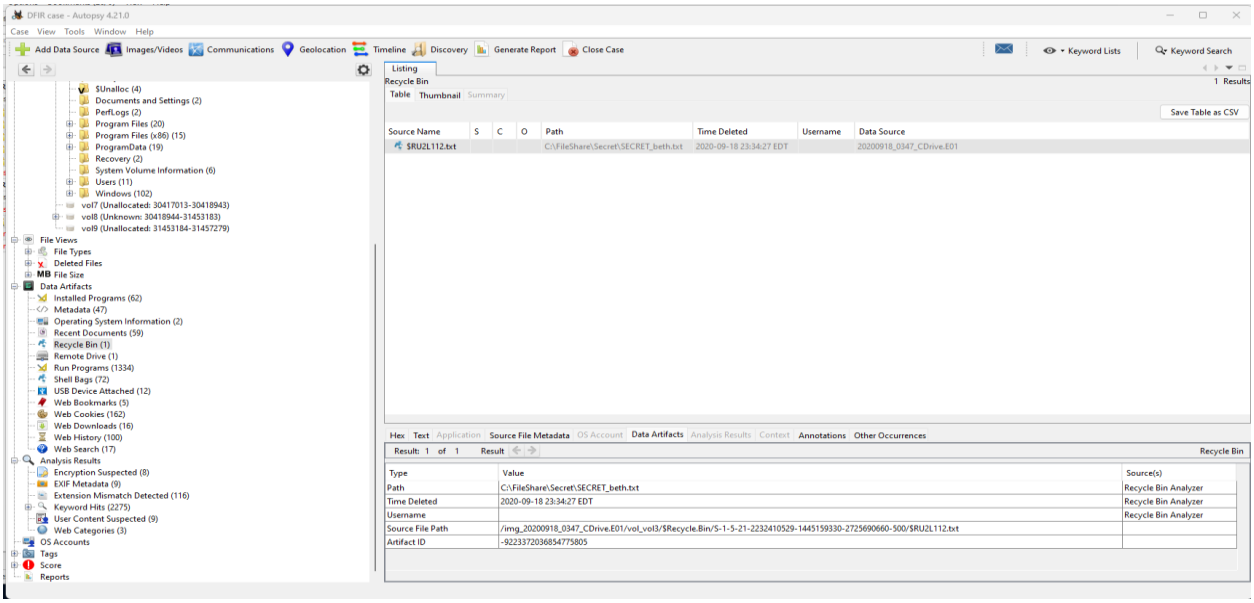

Figure 8: Recycle bin analysis

The recycle bin file, shows the file “C:\FileShare\Secret\SECRET_beth.txt," which is a target location of a possible breach. The actual Szechuan sauce recipe can be found in "C:\FileShare\Secret\Szechuan Sauce.txt."

In addition to that, a network drive was found on the desktop of CITADEL-DC01 implying possible breach of personal Data.

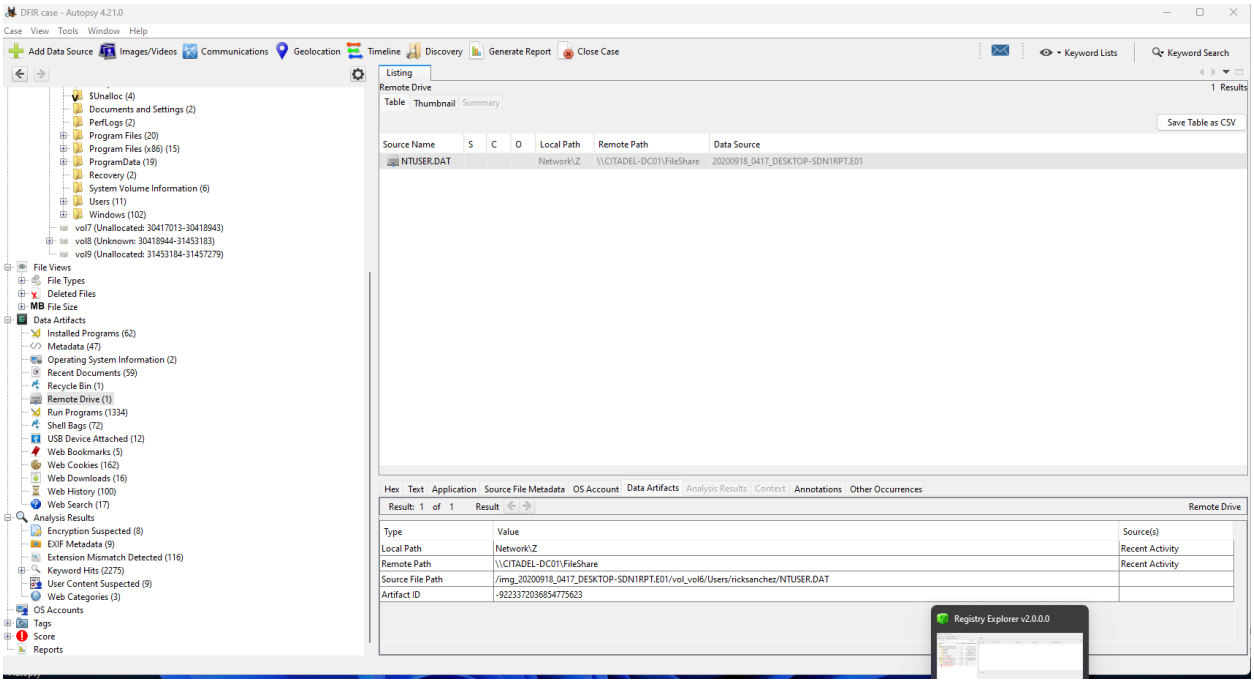

Figure 9: remote network drive found in Autopsy

A successful HTTP connection can be seen made from malicious IP 194.61.24.102 to the DC01 server with IP 10.42.85.10 further confirming the brute-force RDP connection attack.

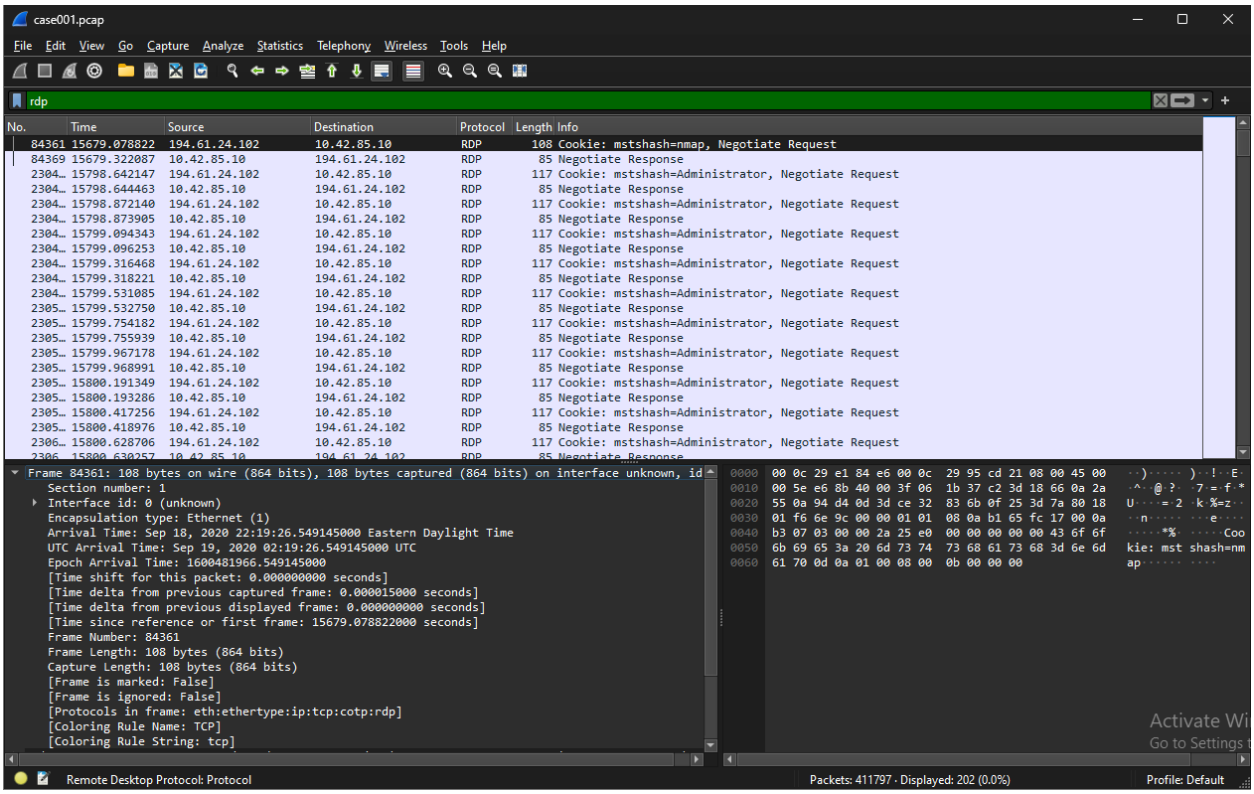

Figure 10: RDP protocol Analysis in wireshark

5). What was the initial entry vector (how did they get in)?

Method: From the above Wireshark analysis above it can be proved that that the initially the attacker gained access with remote Protocol using brute force connection from a malicious IP to the DC01 server, after a successful HTTP connection.

6). Was malware used? If so, what was it?

File Analyzed: DC01-E01, PCAP, DC01-autoruns

Tools used: Autopsy, Wireshark and Timeline Explorer

Procedure: Based on the above information, an HTTP connection was established, so further searched for all communication between DC01 and malicious IP with display search in Wireshark as

http and ip.addr== 194.61.24.102

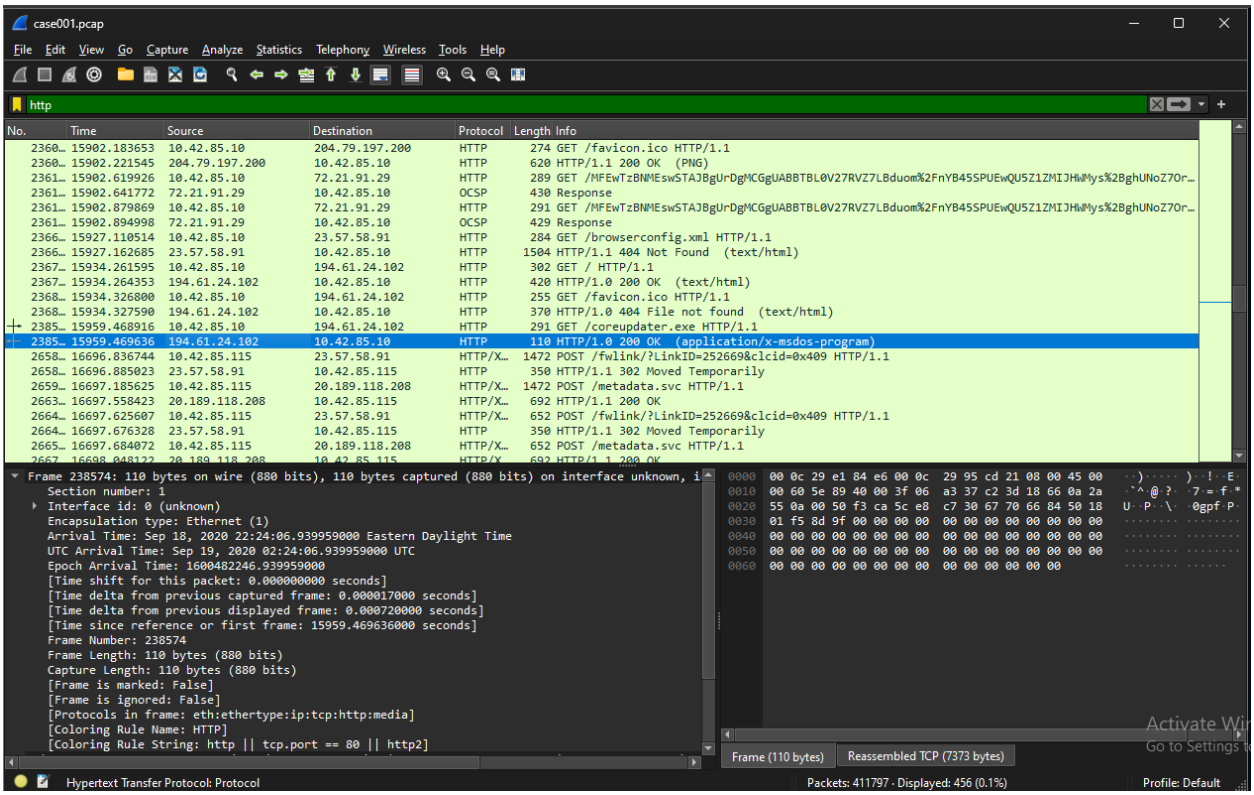

Figure 11: HTTP analysis

Analysis revealed that the coreupdater.exe file is downloaded on the DC server from a malicious IP 194.61.24.102 using the HTTP protocol from the victim RDP session. The session was carried out on September 19th 2020 at 02.24 GMT

Below is the script used for the Coreupdater.exe

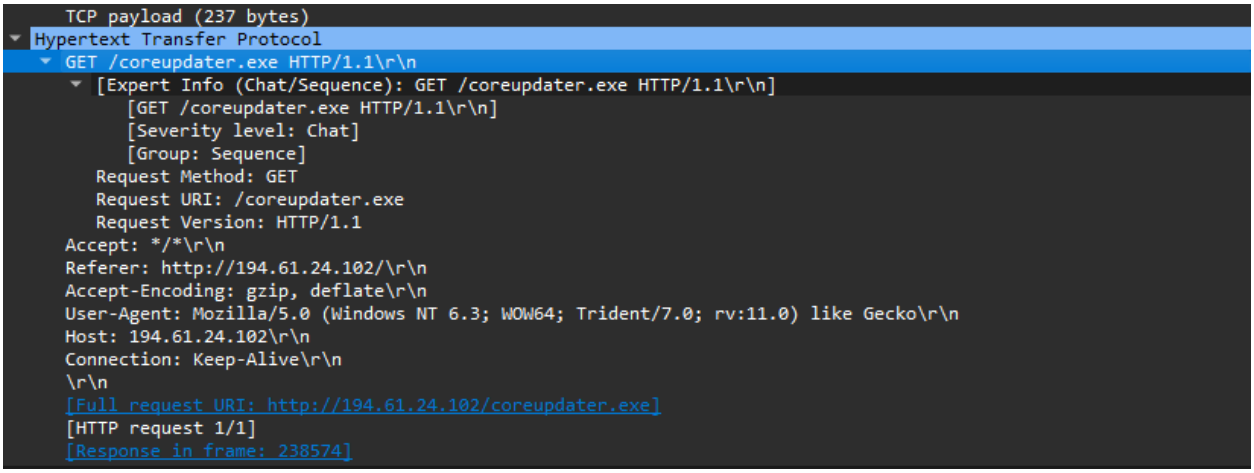

Figure 12: coreupdater.exe script

Using the SHA256 Hash of coreupdater.exe from the autorun csv file **10F3B92002BB98467334161CF85D0B1730851F9256F83C27DB125E9A0C1CFDA6 .** In The Virus Total website confirmed that the file is a known malicious file used to communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic

(VirusTotal, n.d.).

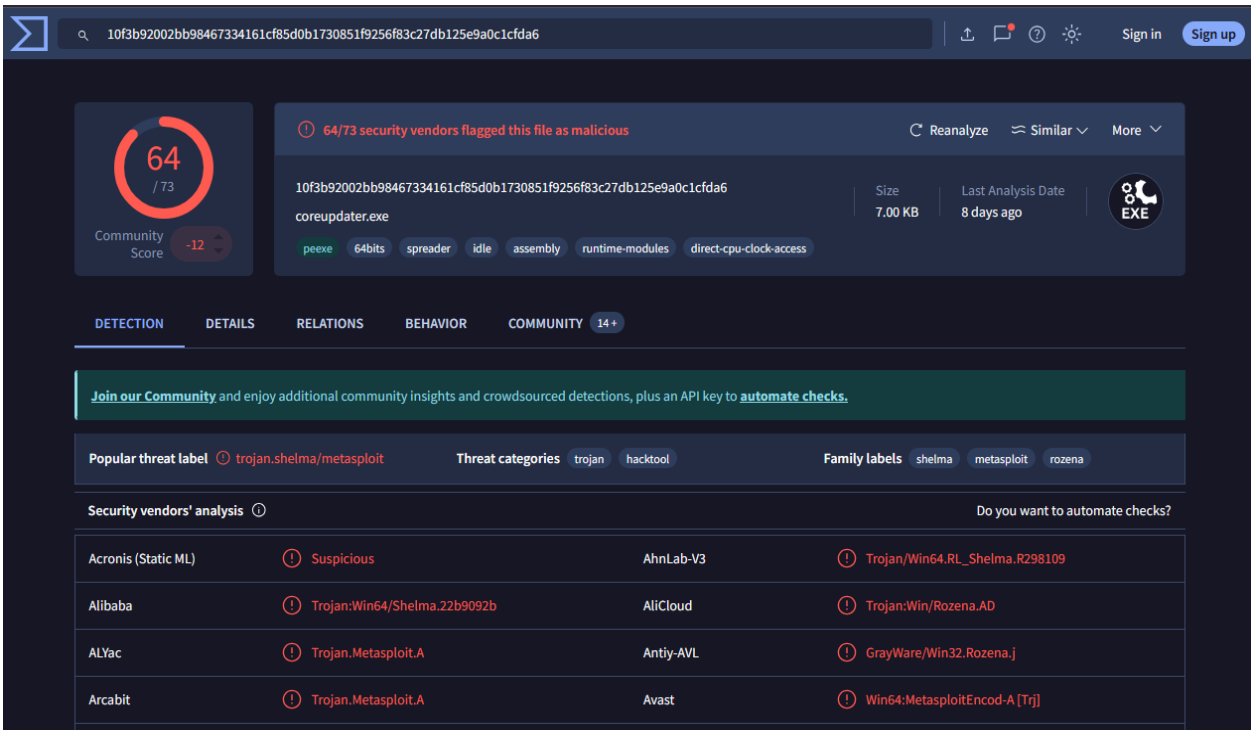

Figure 13: Coreupdater.exe hash matching for malware

I further looked for the file location in registry and found its location in windows->system32/

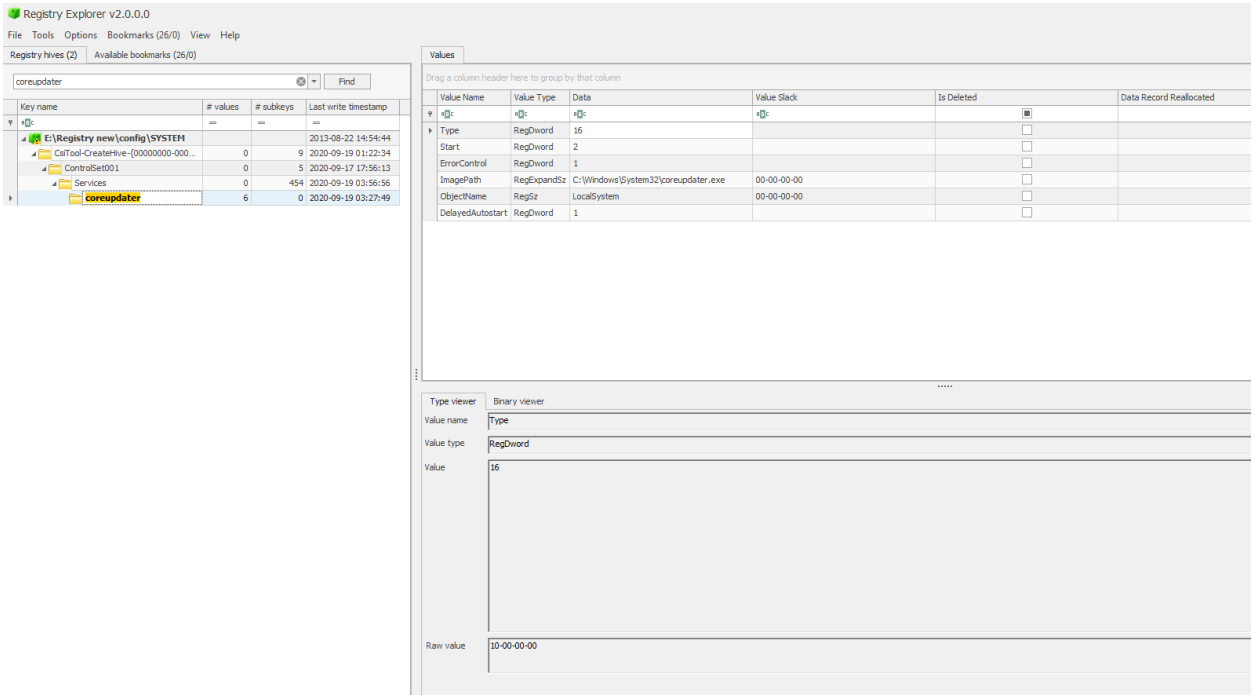

Figure14: locating coreupdater.exe in registry hive.

Further analysis showed the malware to be active in both DC01 and Desktop installed in the registry and as a service.

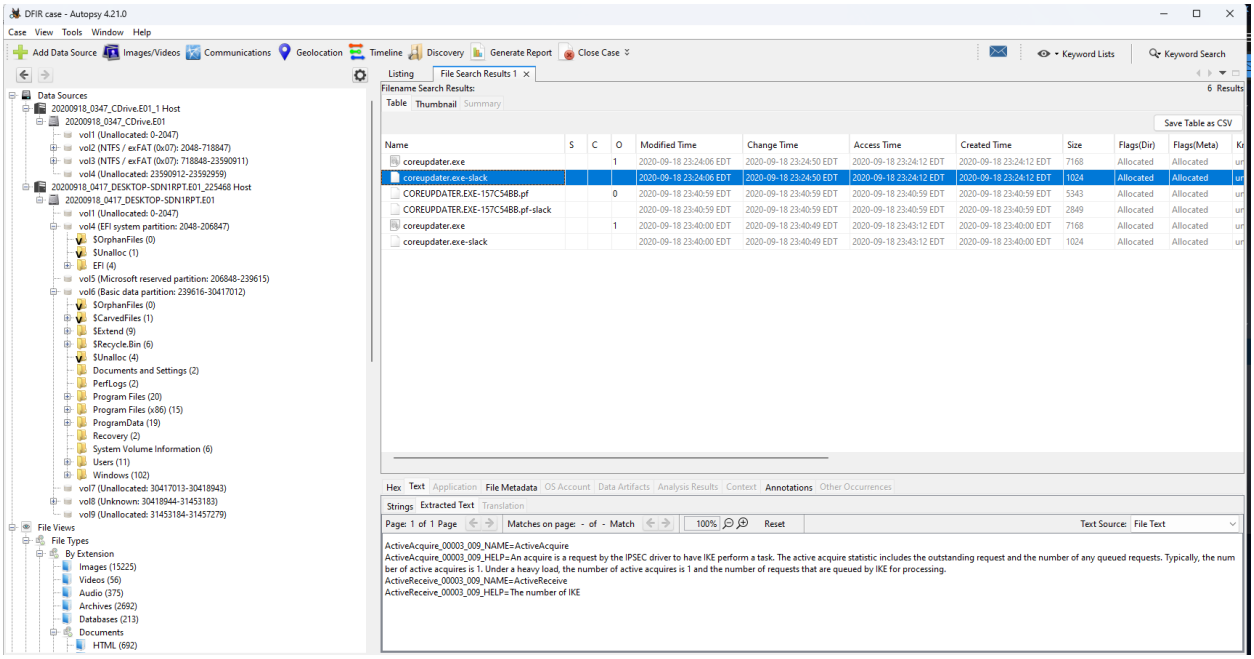

Figure 15: coreupdater.exe present in both registry hive and as a service.

We can see the file manipulation in USN journal, extracts the $UsnJrnl:$Max file from the image, and inputs it in the Timeline Explorer tool.

MFTECmd.exe -f "Jfile" --csv "c:\temp\output" --csvf “JournalfileMyOutputFile.csv

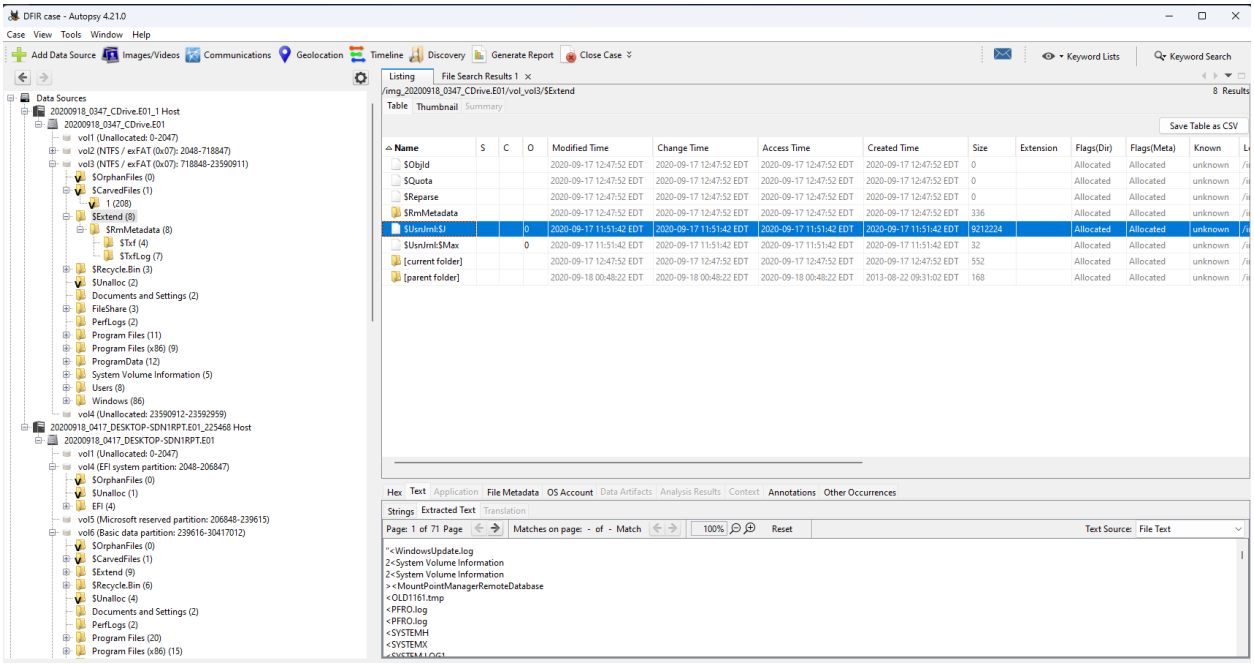

Figure 16: file manipulation

Below we can see the changes of coreupdater.exe file with timestamps, updates and file information.

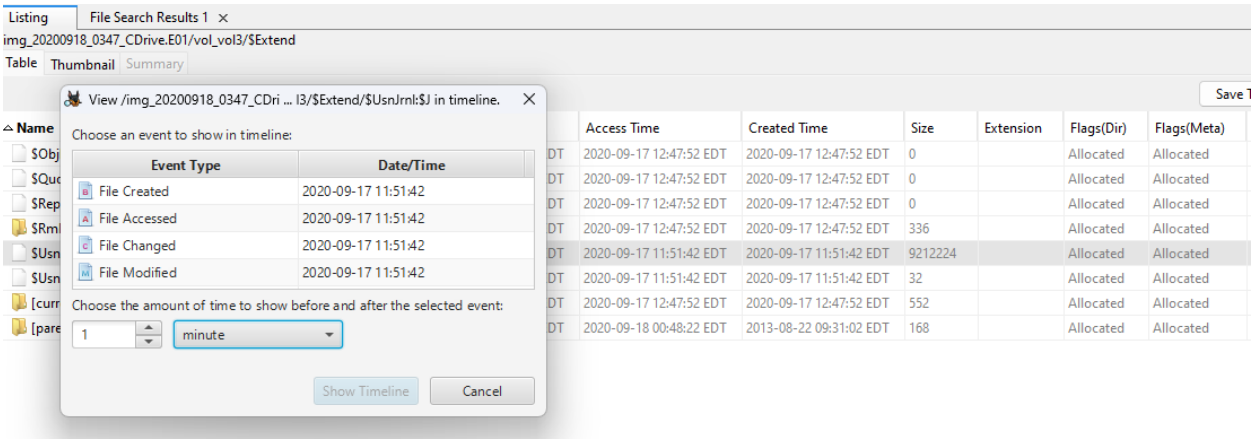

Figure 17: time stamp changed in the file

7). What malicious IP Addresses were involved?

From previous analysis IP address 194.61.24.102 has been found to have used RDP protocol to carry out brute force attack to gain access (*VirusTotal*, n.d.).

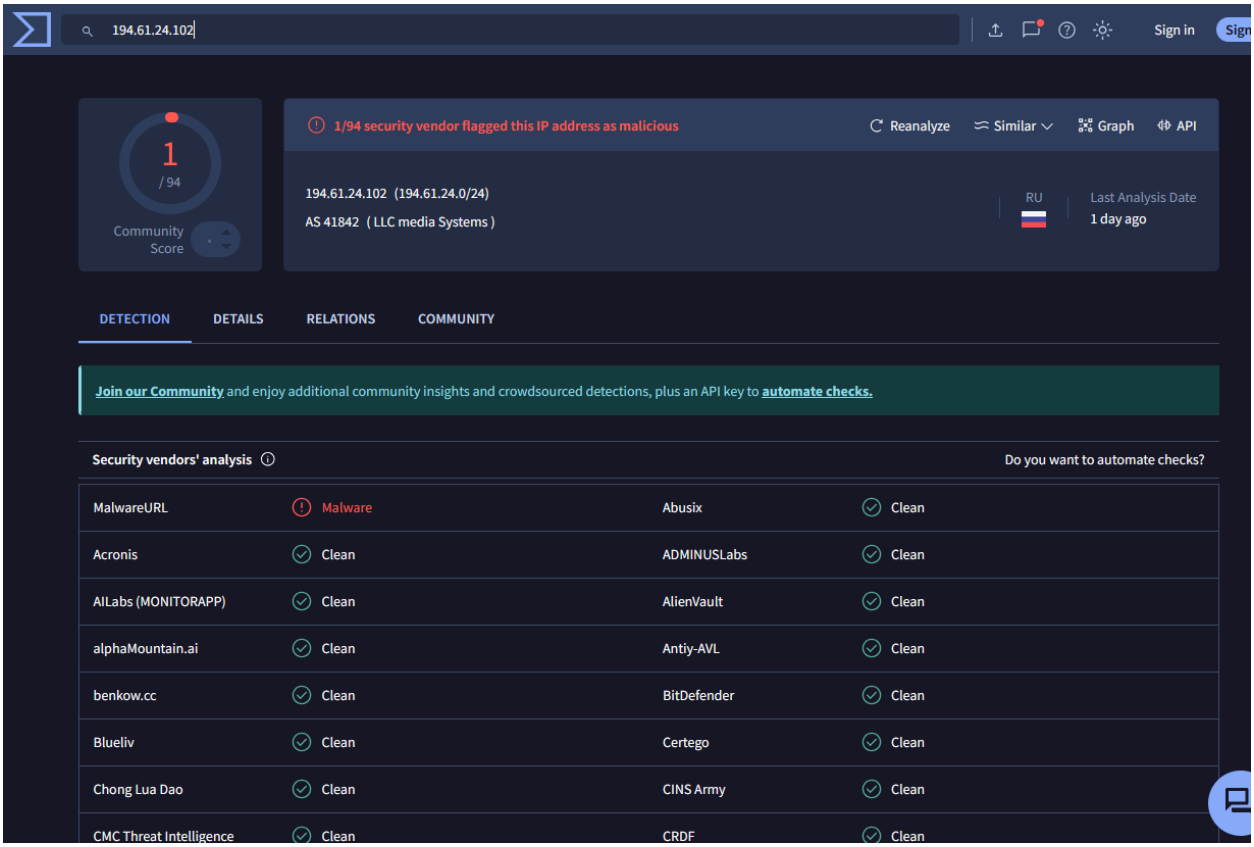

Figure 18: IP address analysis

8) Did the attacker access any other systems?

From the above analysis we are able to confirm that the attacker was able to access the desktop system by utilizing the vulnerability of remote desktop protocol (RDP) from the Domain controller. Through autopsy, it is clear the files have been compromised and modified with administrative privileges.

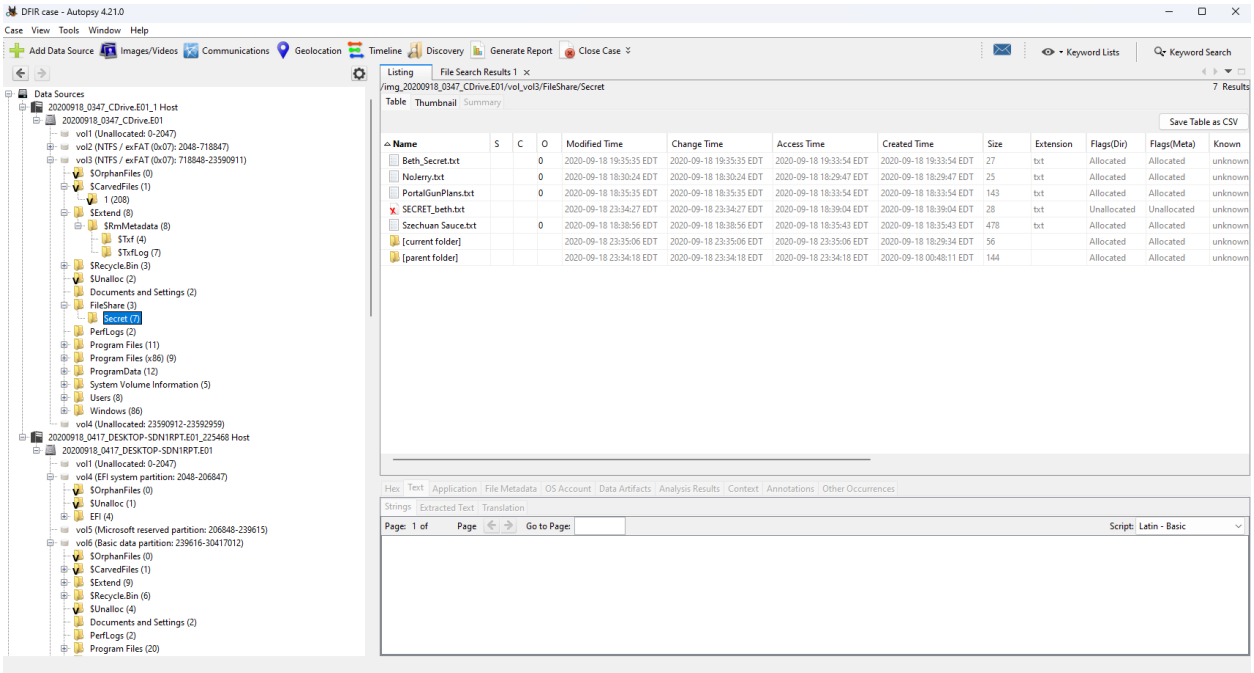

Figure 18- Access to Secret Folder

9)What was the network layout of the victim network ?

Through network traffic we can say that Desktop IP was 10.42.85.115 and Domain Control IP address was 10.42.85.10.

References

Obfuscated files or information, technique T1027 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1027/

Obfuscated files or information, technique T1027 - Enterprise | MITRE ATT&CK®. (n.d.-b). https://attack.mitre.org/techniques/T1027/

VirusTotal. (n.d.). VirusTotal. https://www.virustotal.com/gui/ip-address/194.61.24.102

VirusTotal. (n.d.). VirusTotal. https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

James. (2021b, March 25). Case 001 – The stolen Szechuan Sauce. DFIR Madness. https://dfirmadness.com/the-stolen-szechuan-sauce/

Brute force, technique T1110 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1110/