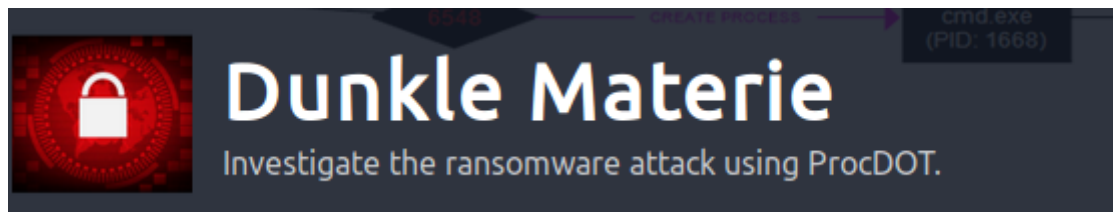




TRY HACK ME: Write-Up Dunkle Materie – Ransomware Investigation using ProcDOT



Task 1 Ransomware Investigation–

The firewall alerted the Security Operations Center that one of the machines at the Sales department, which stores all the customers' data, contacted the malicious domains over the network. When the Security Analysts looked closely, the data sent to the domains contained suspicious base64-encoded strings. The Analysts involved the Incident Response team in pulling the Process Monitor and network traffic data to determine if the host is infected. But once they got on the machine, they knew it was a ransomware attack by looking at the wallpaper and reading the ransomware note.

Can you find more evidence of compromise on the host and what ransomware was involved in the attack?

ProcDOT evaluates result on the basis of Process Monitoring logs and Network Traffic logs.

Answer to the questions of this section-

Provide the two PIDs spawned from the malicious executable. (In the order as they appear in the analysis tool)

Correct Answer

Provide the full path where the ransomware initially got executed? (Include the full path in your answer)

Correct Answer

Hint

This ransomware transfers the information about the compromised system and the encryption results to two domains over HTTP POST. What are the two C2 domains? (no space in the answer)

Correct Answer

What are the IPs of the malicious domains? (no space in the answer)

Correct Answer

Provide the user-agent used to transfer the encrypted data to the C2 channel.

Correct Answer

Hint

cisco umbrella

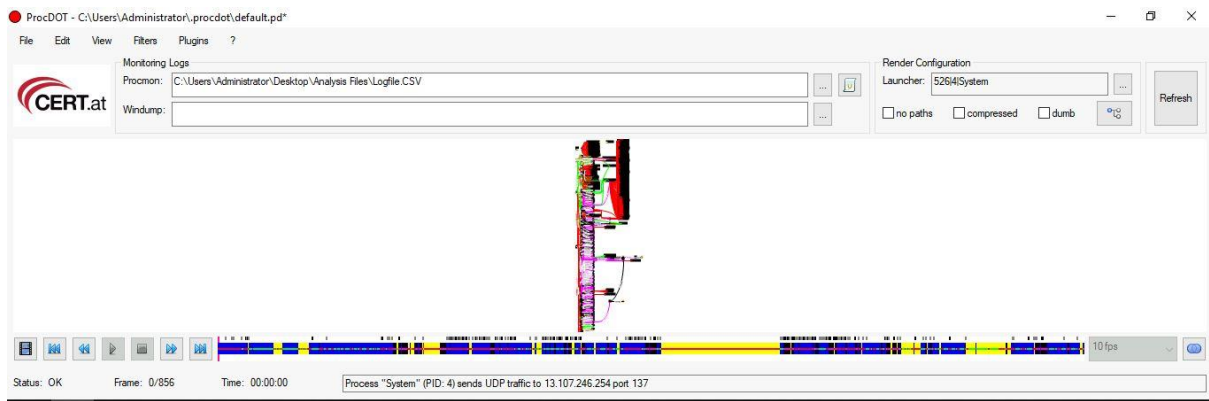
ley9kpi9r.bmp

4892

HKLM\SYSTEM\MountedDevices\\DosDevices\Z:

blackmatter ransomware

We will get something like mentioned below.



Zoom in and look for process itself. [Make use of View tab -> Graph]

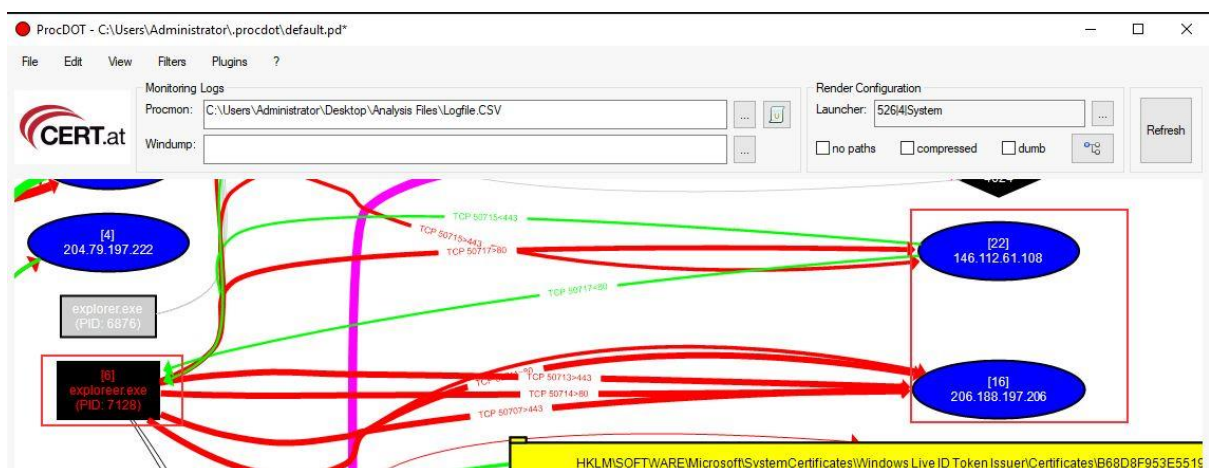
Right click on PID-8644 explorer.exe and select Details to view Full Path.



4) Look at PID-7128 explorer.exe and map mentioned IP addresses related to explorer.exe in Wireshark.

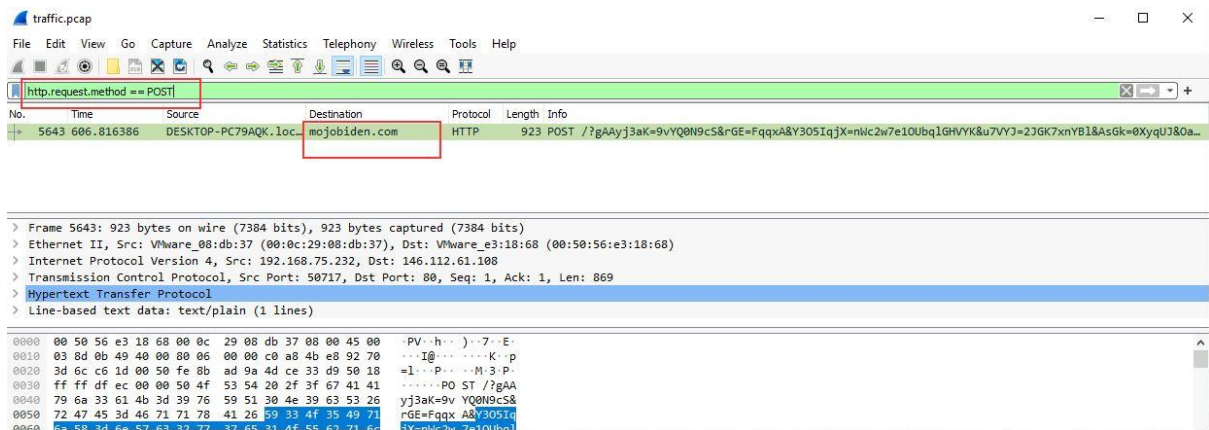
IP address1- 146.112.61.108

IP address 2- 206.188.197.206



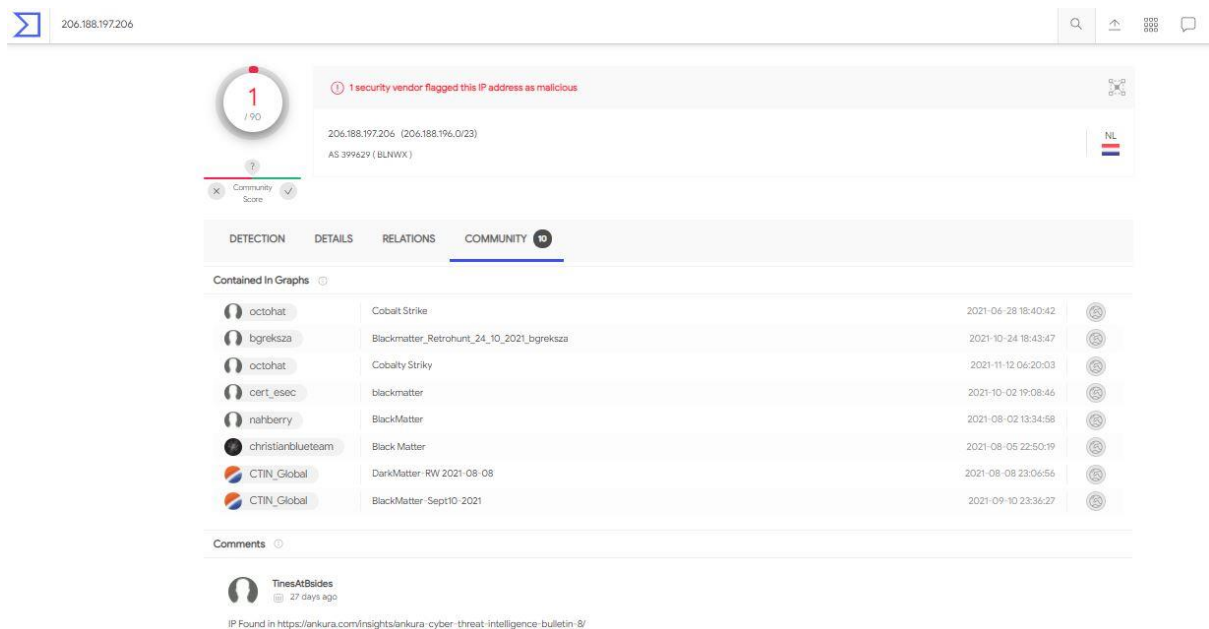
Now type http.request.method == POST as filter in wireshark and navigate to Edit -> preferences -> Name Resolution -> enable resolve network (IP) addresses.

Domain 1- mojobiden.com

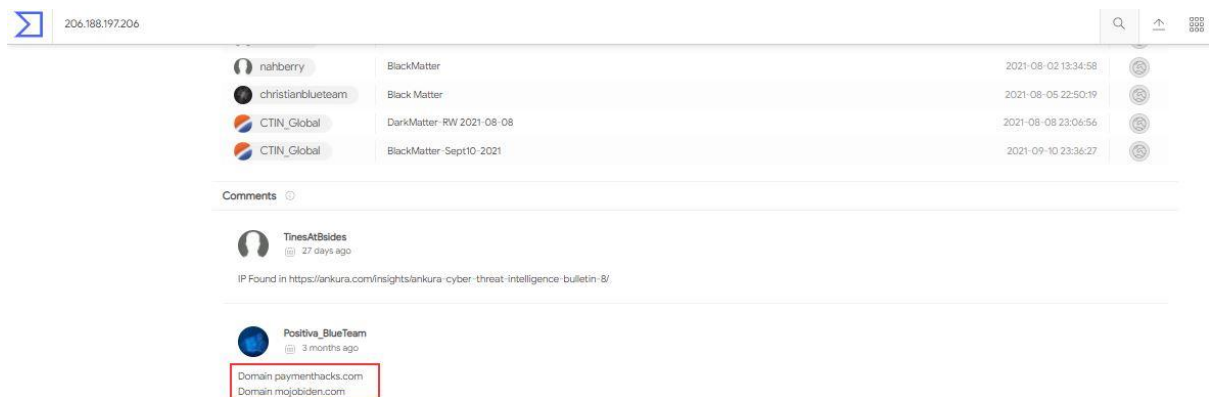


Domain 2- paymenthacks.com

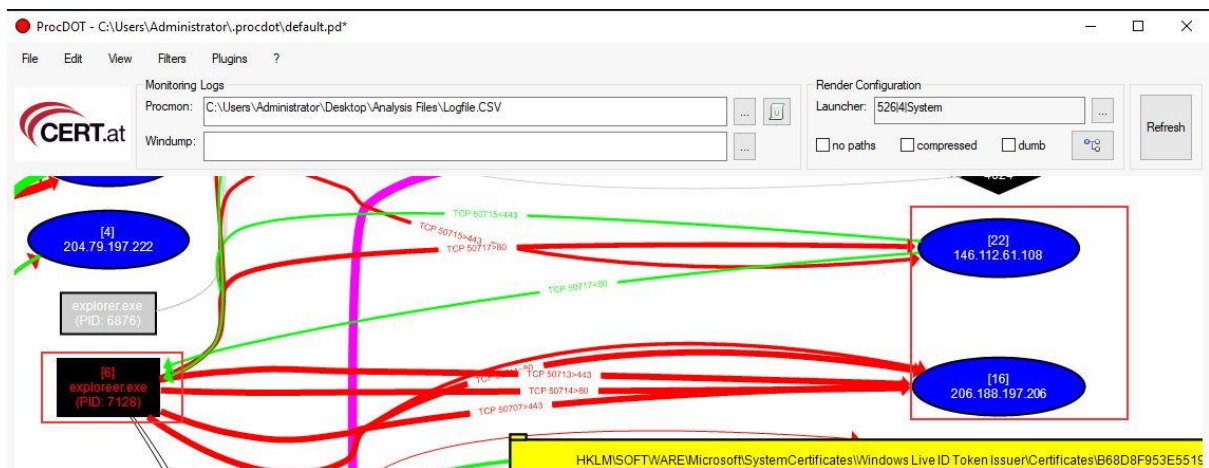
Domain 2 is identified using Threat Hunting Skills by searching information for IP-206.188.197.206 on Virus Total.



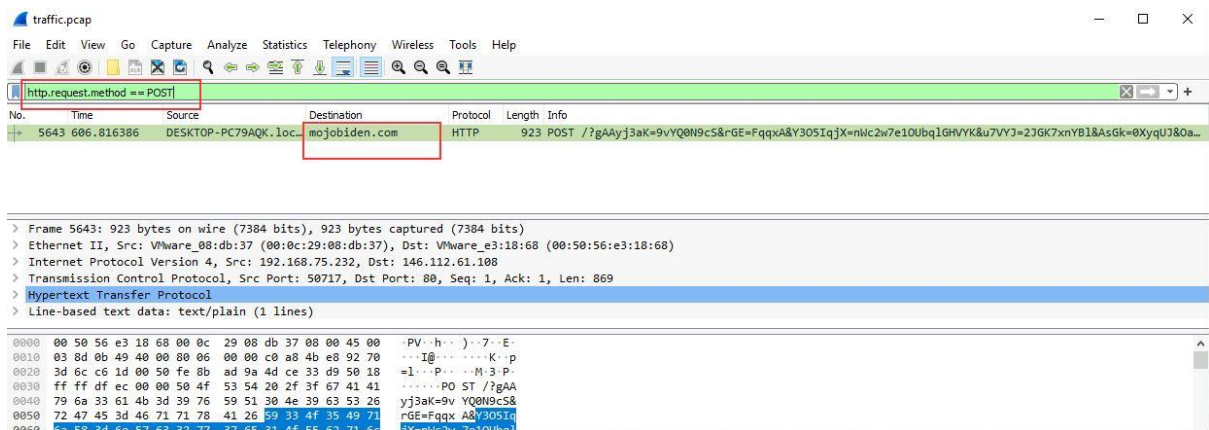
Domain 2 identified.



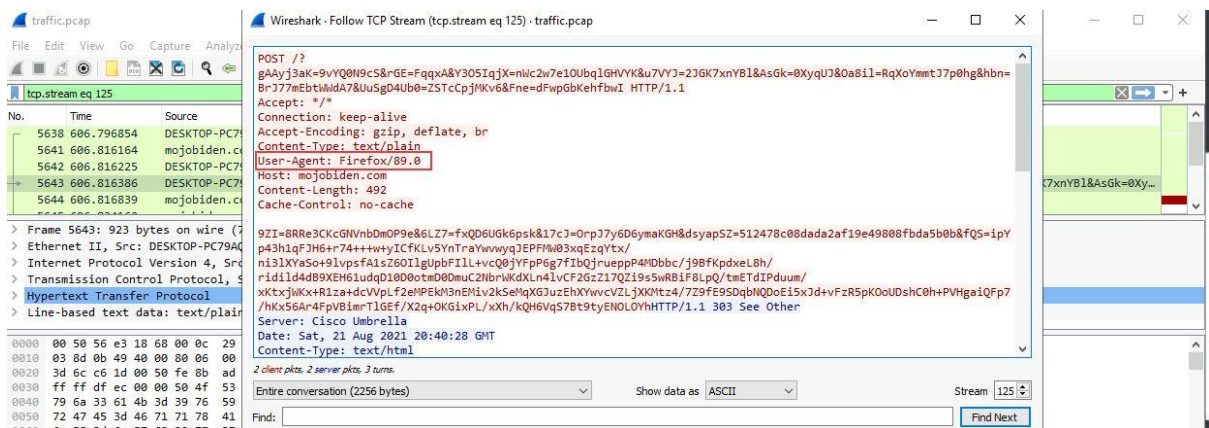
5) Malicious IP address for the identified domains are mentioned below



6) Now type `http.request.method == POST` as filter in Wireshark and navigate to Edit -> preferences -> Name Resolution -> enable resolve network (IP) addresses.



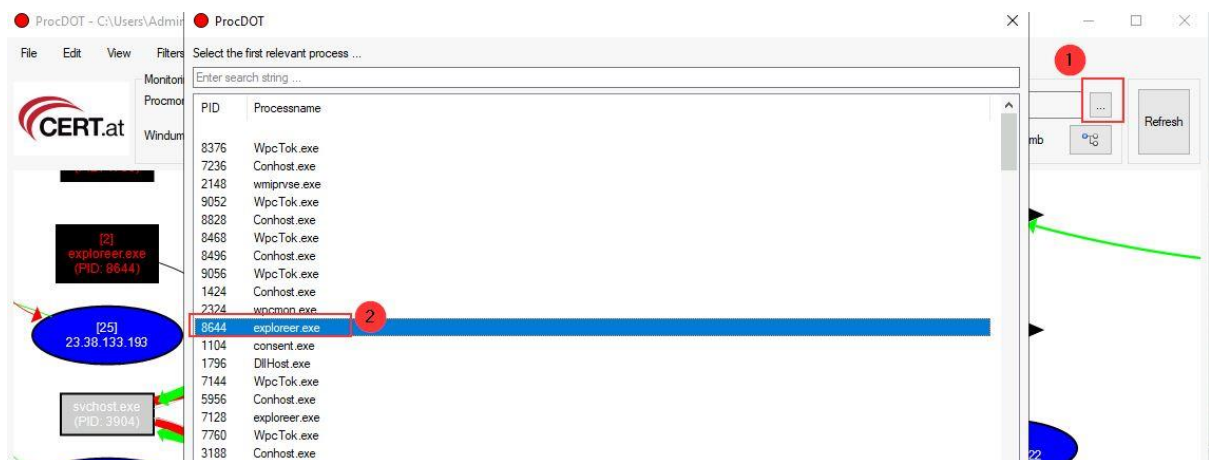
Follow TCP Stream for the traffic mentioned above, we will get User-Agent for the same.



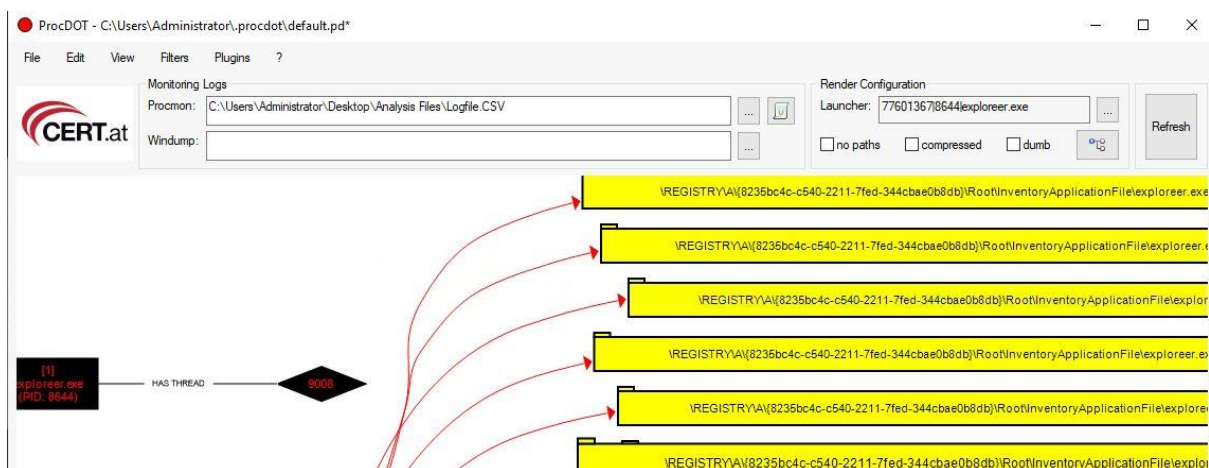
7) Follow TCP Stream for domain -mojobiden.com



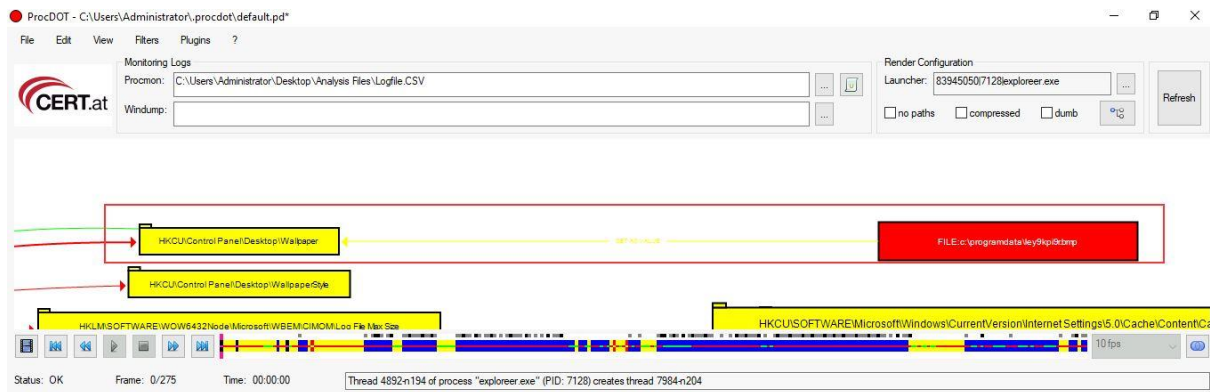
8) Now in ProcDot, click launcher button to view process listing. Select PID-7128 explorer.exe and double click on 7128 explorer.exe



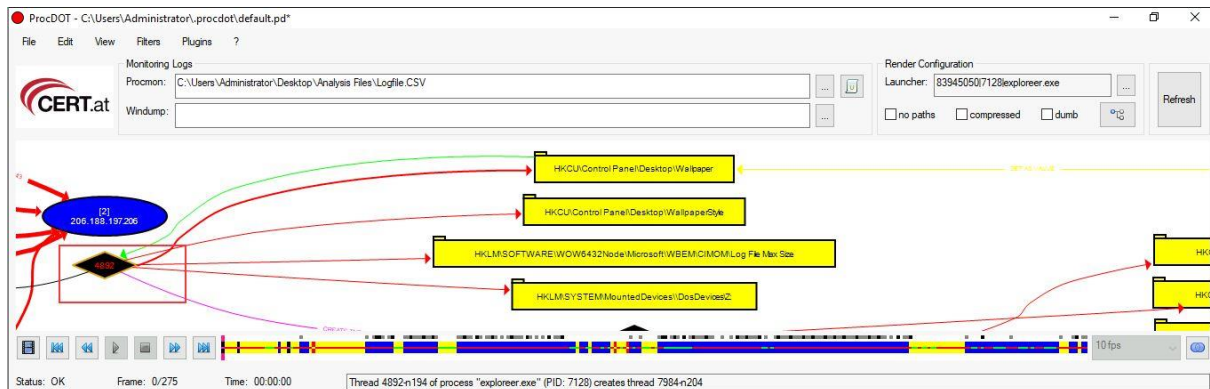
Now visualize PID-7128 explorer.exe



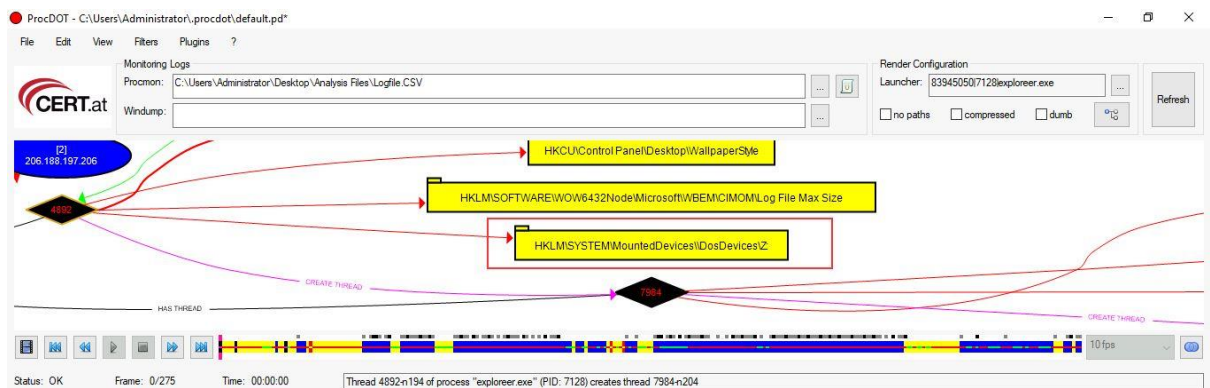
9) Answer 7 – ley9kpi9r.bmp



10) Answer 8- 4892

















11) Answer 10- HKLM\SYSTEM\MountedDevices\DosDevices\Z:



12) Answer 11- blackmatter ransomware

Visit AlienVaultor virus total site with IOCs

DETECTION	DETAILS	RELATIONS	COMMUNITY 10
Contained In Graphs ⓘ			
 octohat	Cobalt Strike		2021-06-28 18:40:42 
 bgreksza	Blackmatter_Retrohunt_24_10_2021_bgreksza		2021-10-24 18:43:47 
 octohat	Cobalt Striky		2021-11-12 06:20:03 
 cert_esec	blackmatter		2021-10-02 19:08:46 
 nahberry	BlackMatter		2021-08-02 13:34:58 
 christianblueteam	Black Matter		2021-08-05 22:50:19 
 CTIN_Global	DarkMatter-RW 2021-08-08		2021-08-08 23:06:56 
 CTIN_Global	BlackMatter-Sept10-2021		2021-09-10 23:36:27 

That is all for this Write-up, hoping this will help you in solving the challenges of Dunkle Materie.
Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai