13.2 Getting your bearings

**Sprint 13** Incident Investigation

40.80.148.42

← Use the **Document tabs** to locate the notes for each task in this investigation.

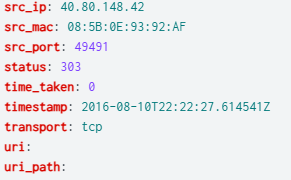
13.2.1 Device

13.2.1 Finding the attacking device

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/ed170c7e-c684-404d-a05c-9ec26701f34e)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

10:22:27.614 PM



index=client1 imreallynotbatman.com

What is the most probable IP address associated with the unusually high number of requests reported by the junior sysadmin in the original alert?

40.80.148.42

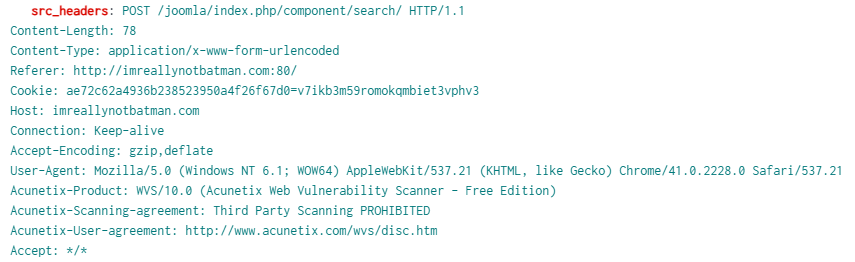
13.2.2 Tool

13.2.2 Determining the tool

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/7e44a0f2-431e-4133-9e5c-3b5c2605388f)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

10:22:27.612 PM



index=client1 imreallynotbatman.com sourcetype="stream:http" src\_ip="40.80.148.42" http\_method=POST

Question: Which organization developed the web vulnerability scanning tool used by the threat actor? (*Type in the company’s name.*)

Acunetix

13.2.3 Exploited CMS

13.2.3 Identifying the exploited CMS

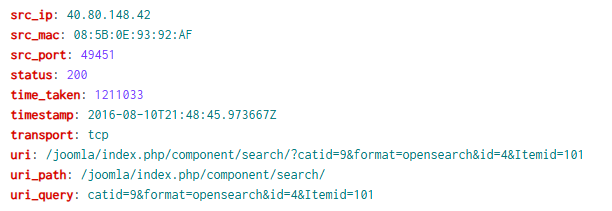
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/85c86d89-67fa-49cc-92f0-ce2db494bda8)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client1 imreallynotbatman.com sourcetype="stream:http" src\_ip="40.80.148.42" dest\_ip="192.168.250.70"http\_method="GET" status="200" | top limit=20 uri

8/10/16

9:48:47.184 PM



index=client1 imreallynotbatman.com sourcetype="stream:http" src\_ip="40.80.148.42" dest\_ip="192.168.250.70"http\_method="GET" status="200" uri="/joomla/index.php/component/search/?catid=9&format=opensearch&id=4&Itemid=101"

Which content management system (CMS) is imreallynotbatman.com most likely using?

Joomla

13.2.4 Defacement image’s filename

13.2.4 Establishing the defacement image’s filename

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/9baef6e2-8541-4b81-af6e-d5760ad40a5d)**.** Use this worksheet to keep notes as you complete it. |
| --- |

2016-08-10 22:19:11.351



index=client1 sourcetype=suricata src\_ip="192.168.250.70" http.http\_content\_type="image/\*" | table \_time, http.url, fileinfo.filename

What is the filename associated with the file used to deface the imreallynotbatman.com website?

poisonivy-is-coming-for-you-batman.jpeg

13.2.5 FQDN

13.2.5 Associating the malicious FQDN

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/60050616-d243-43e7-a37e-fe2cfa7a8878)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

10:19:11.351 PM



index=client1 sourcetype=suricata OR sourcetype="stream:http" "poisonivy-is-coming-for-you-batman.jpeg"

Which fully qualified domain name (FQDN) was used in this attack to resolve to the malicious IP address via dynamic DNS?

prankglassinebracket.jumpingcrab.com

13.2.6 Pre-staging IP

13.2.6 Discovering the pre-staging IP address

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/1272b1a3-97ff-4fc7-a642-d3bbe366f477)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

10:19:11.351 PM



index=client1 sourcetype=suricata OR sourcetype="stream:http" "poisonivy-is-coming-for-you-batman.jpeg"

Which IP address did the threat actor link to domains that were preconfigured (“pre-staged”) for an attack on Wayne Enterprises?

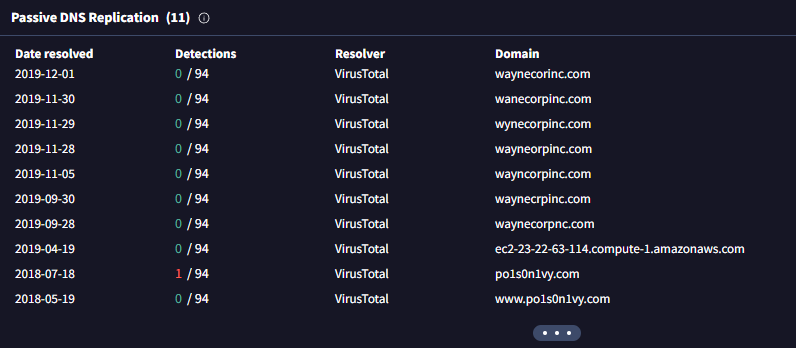
[23.22.63.114](https://soc.0x2asec.com/en-US/app/search/search?earliest=1470862800&latest=1470870000&q=search%20index%3Dclient1%20sourcetype%3Dsuricata%20OR%20sourcetype%3D%22stream%3Ahttp%22%20%22poisonivy-is-coming-for-you-batman.jpeg%22&display.page.search.mode=verbose&dispatch.sample_ratio=1&display.events.fields=%5B%22host%22%2C%22source%22%2C%22sourcetype%22%2C%22index%22%2C%22remote_host%22%2C%22request_url%22%2C%22status_code%22%2C%22user_agent%22%2C%22client_ip%22%2C%22src_ip%22%2C%22dest_ip%22%2C%22uri%22%2C%22status%22%5D&display.page.search.tab=events&display.general.type=events&sid=1754356406.18227#)

13.2.7 APT email

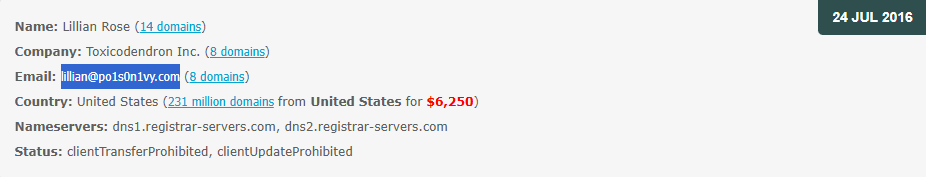
13.2.7 Using OSINT to confirm the APT group’s email address

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/047c98c0-2065-4eb2-8c24-2666175eb56e)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/4/2025



[VirusTotal - IP address - 23.22.63.114](https://www.virustotal.com/gui/ip-address/23.22.63.114/relations)



[Po1s0n1vy.com [Whois Lookup & Whois History]](https://www.whoxy.com/po1s0n1vy.com)

Which email address is most likely linked to the threat actor? *(Using information collected from this attack and typical open source intelligence related to domain names.)*

lillian@po1s0n1vy.com

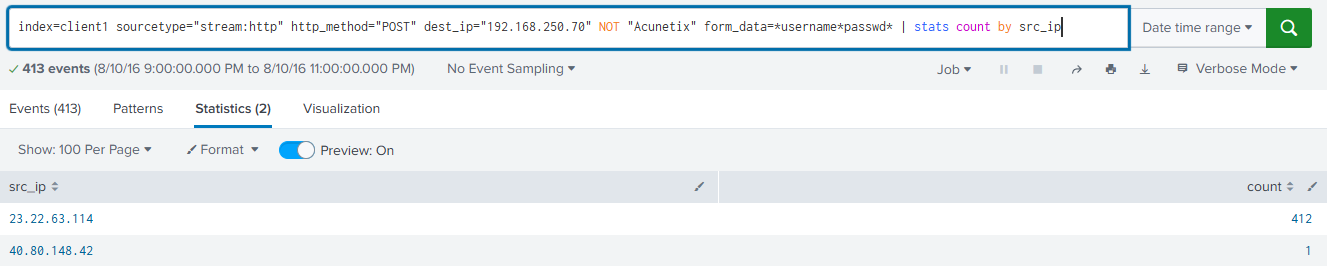
13.2.8 Brute-force IP

13.2.8 Assessing the brute-forcing IP address

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/9ddec3b8-5813-4597-8273-e5a49cd47c68)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

9:46:51.154 PM







index=client1 sourcetype="stream:http" http\_method="POST" dest\_ip="192.168.250.70" NOT "Acunetix" form\_data=\*username\*passwd\* src\_ip="23.22.63.114"

Which IP address is most likely conducting a brute force password attack targeting [imreallynotbatman.com](http://imreallynotbatman.com)?

23.22.63.114

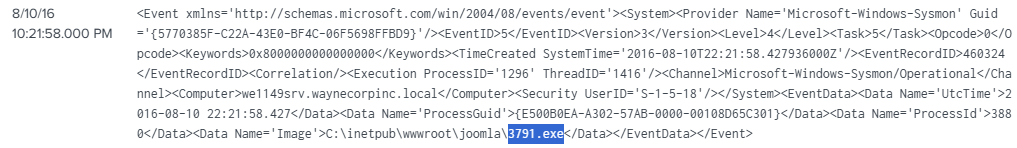
13.2.9 Malware filename

13.2.9 Figuring out the malicious executable’s filename

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/c756e3c2-59a9-4e15-9213-8933f481740f)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

10:21:58.000 PM



index=client1 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" 3791.exe

What is the filename of the malicious executable uploaded by the threat actor? *(Include the full filename, including the extension.)*

*3791.exe*

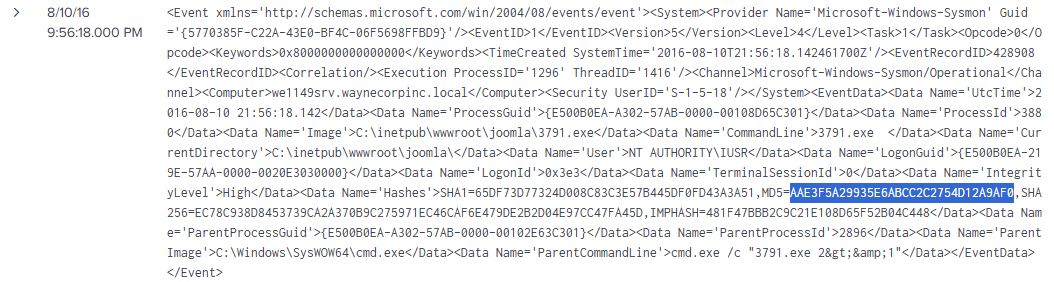
13.2.10 MD5 hash

13.2.10 Locating the MD5 hash of that executable

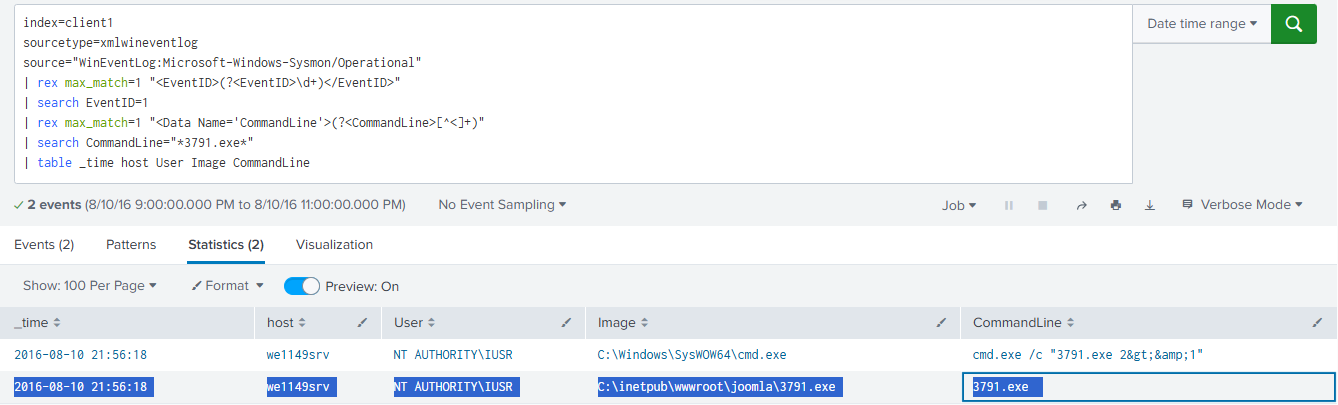
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/0e031cb7-1fbf-420a-91f5-ec9c83556472)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

9:56:18.000 PM



index=client1 sourcetype=xmlwineventlog source="WinEventLog:Microsoft-Windows-Sysmon/Operational" | rex max\_match=1 "<EventID>(?<EventID>\d+)</EventID>" | search EventID=1 | rex max\_match=1 "<Data Name='CommandLine'>(?<CommandLine>[^<]+)" | search CommandLine="\*3791.exe\*" host=we1149srv User="NT AUTHORITY\\IUSR" Image="C:\\inetpub\\wwwroot\\joomla\\3791.exe" CommandLine="3791.exe "



index=client1

sourcetype=xmlwineventlog

source="WinEventLog:Microsoft-Windows-Sysmon/Operational"

| rex max\_match=1 "<EventID>(?<EventID>\d+)</EventID>"

| search EventID=1

| rex max\_match=1 "<Data Name='CommandLine'>(?<CommandLine>[^<]+)"

| search CommandLine="\*3791.exe\*"

| table \_time host User Image CommandLine

What is the MD5 hash value of that executable file uploaded by the threat actor?

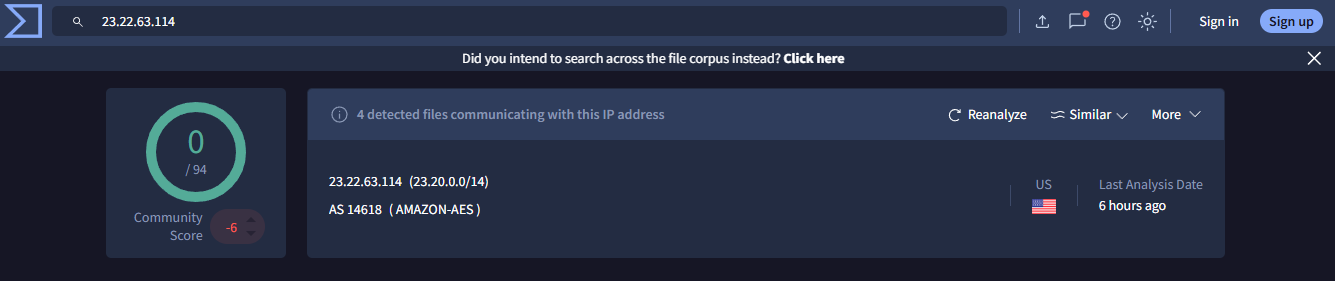
AAE3F5A29935E6ABCC2C2754D12A9AF0

13.2.11 SHA256 hash

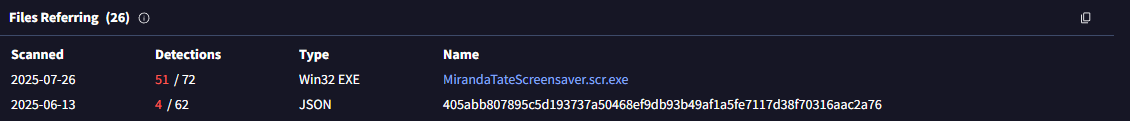
13.2.11 Using OSINT to find the SHA256 of an APT group’s custom malware

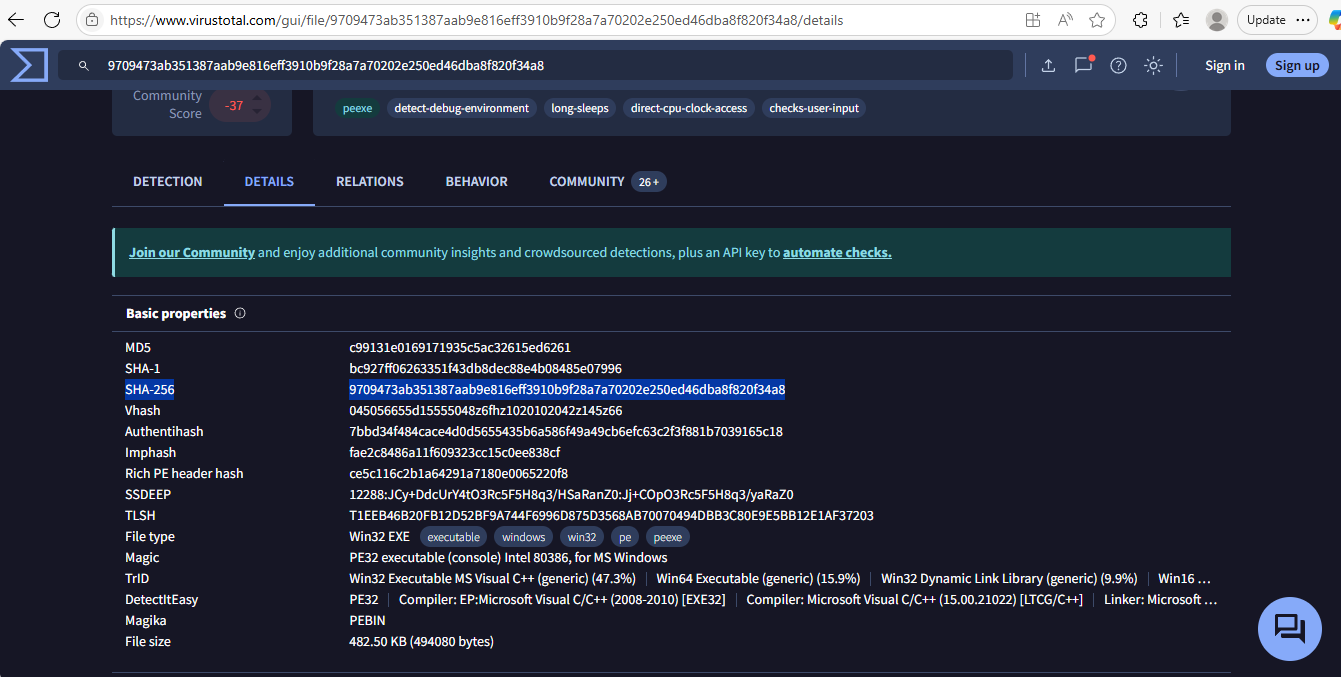
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/1f2bb62e-653b-4df7-8d80-16d8fa16c83f)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/5/2025



[VirusTotal - IP address - 23.22.63.114](https://www.virustotal.com/gui/ip-address/23.22.63.114/relations)





[VirusTotal - File - 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8](https://www.virustotal.com/gui/file/9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8/details)

According to GCPD, when this threat actor’s initial compromise attempts are unsuccessful, they typically follow up by sending a spear phishing email containing custom malware to their target. This malware is generally linked to the group’s original attack infrastructure.

What is the SHA256 hash of this malware sample?

9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

13.2.12 Custom hex

13.2.12 Figuring out the malware’s custom hex

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/cb7db699-700e-4e83-879b-e45434acfc4e)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/5/2025



[VirusTotal - File - 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8](https://www.virustotal.com/gui/file/9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8/community)

What is the unique hexadecimal code linked to the custom malware used by the threat actor *(identified in the* [*previous lesson*](https://tripleten.com/trainer/csa/lesson/1f2bb62e-653b-4df7-8d80-16d8fa16c83f)*)?*

* We are looking for the hex blob that decodes to a literary reference.

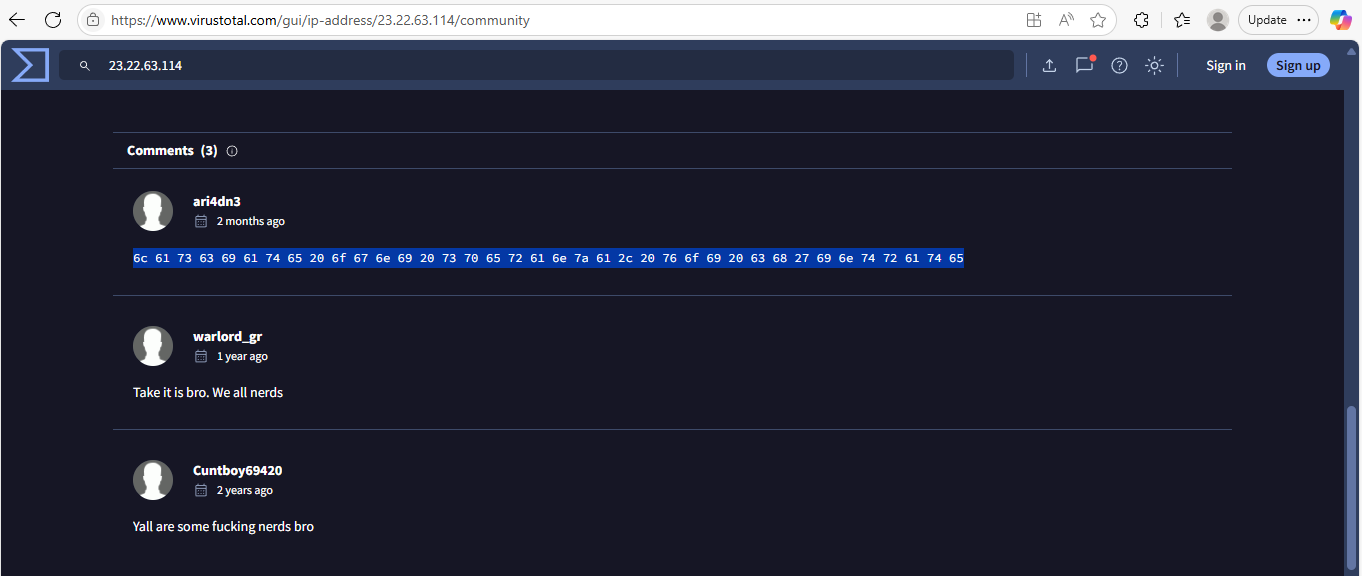
4e 65 6c 20 6d 65 7a 7a 6f 20 64 65 6c 20 63 61 6d 6d 69 6e 6f 20 64 69 20 6e 6f 73 74 72 61 20 76 69 74 61 20 6d 69 20 72 69 74 72 6f 76 61 69 20 70 65 72 20 75 6e 61 20 73 65 6c 76 61 20 6f 73 63 75 72 61

13.2.13 WHOIS info

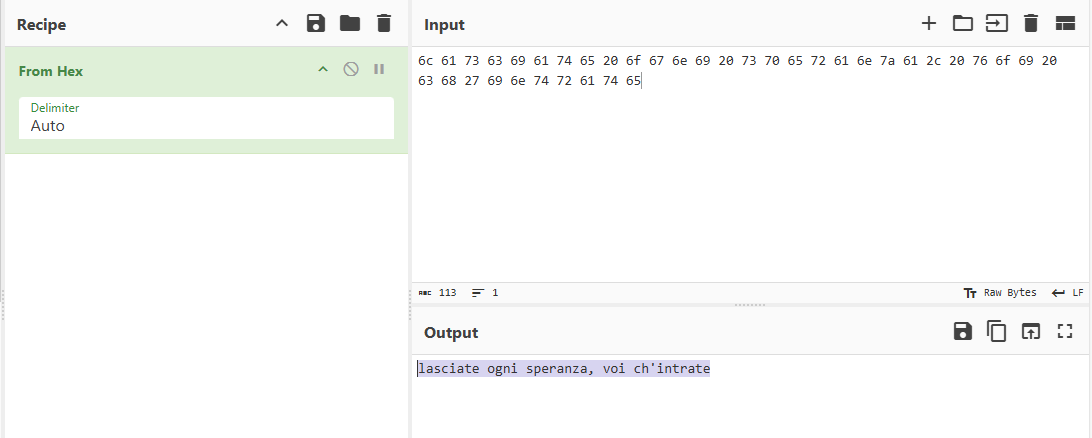
13.2.13 Using OSINT to discover interesting WHOIS information

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/f233bda9-8628-4ac0-8bf4-a2d0680dab2f)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/5/2025



https://www.virustotal.com/gui/ip-address/23.22.63.114/community



https://gchq.github.io/CyberChef/#recipe=From\_Hex('Auto')&input=NmMgNjEgNzMgNjMgNjkgNjEgNzQgNjUgMjAgNmYgNjcgNmUgNjkgMjAgNzMgNzAgNjUgNzIgNjEgNmUgN2EgNjEgMmMgMjAgNzYgNmYgNjkgMjAgNjMgNjggMjcgNjkgNmUgNzQgNzIgNjEgNzQgNjU

What is the *decoded* interesting WHOIS data associated with the threat actor’s staged domain? *(Do NOT provide the hex code! Provide the message you decoded with CyberChef!)*

*lasciate ogni speranza, voi ch'intrate*

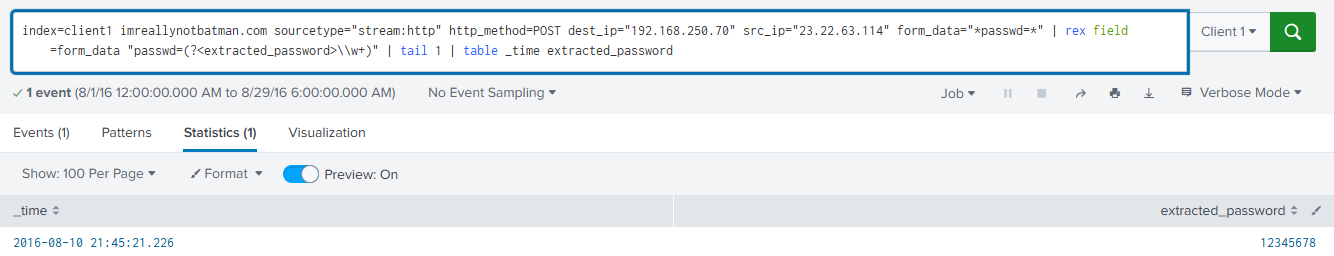
13.3 Analyzing the brute force attack

8/10/16

9:45:21.226 PM



index=client1 imreallynotbatman.com sourcetype="stream:http" http\_method=POST dest\_ip="192.168.250.70" src\_ip="23.22.63.114" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<extracted\_password>\\w+)" | tail 1



index=client1 imreallynotbatman.com sourcetype="stream:http" http\_method=POST dest\_ip="192.168.250.70" src\_ip="23.22.63.114" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<extracted\_password>\\w+)" | tail 1 | table \_time extracted\_password

What is the very first password used during the brute force attack?

12345678

13.3.1 Passwords used

13.3.1 Identifying passwords used

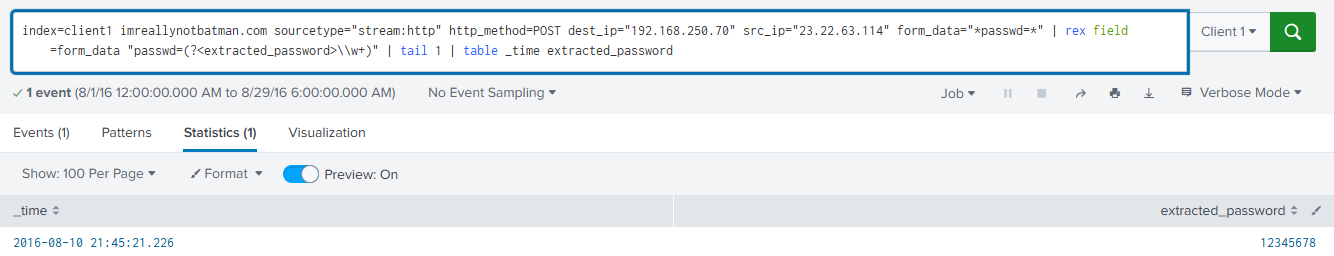
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/3ffad5dd-3947-4425-b426-bdc691f8d2b1)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/10/16

9:45:21.226 PM



index=client1 imreallynotbatman.com sourcetype="stream:http" http\_method=POST dest\_ip="192.168.250.70" src\_ip="23.22.63.114" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<extracted\_password>\\w+)" | tail 1



index=client1 imreallynotbatman.com sourcetype="stream:http" http\_method=POST dest\_ip="192.168.250.70" src\_ip="23.22.63.114" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<extracted\_password>\\w+)" | tail 1 | table \_time extracted\_password

What is the very first password used during the brute force attack?

12345678

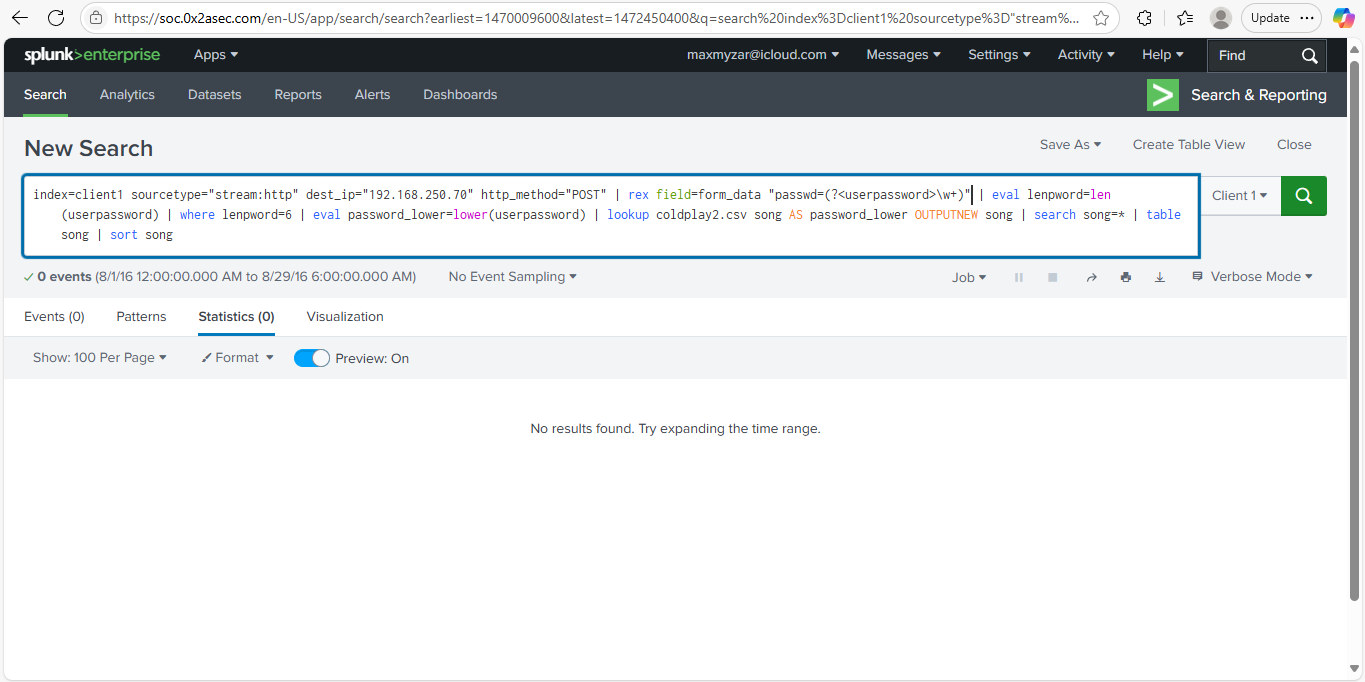
13.3.2 6-char passwords

13.3.2 Figuring out 6-character passwords

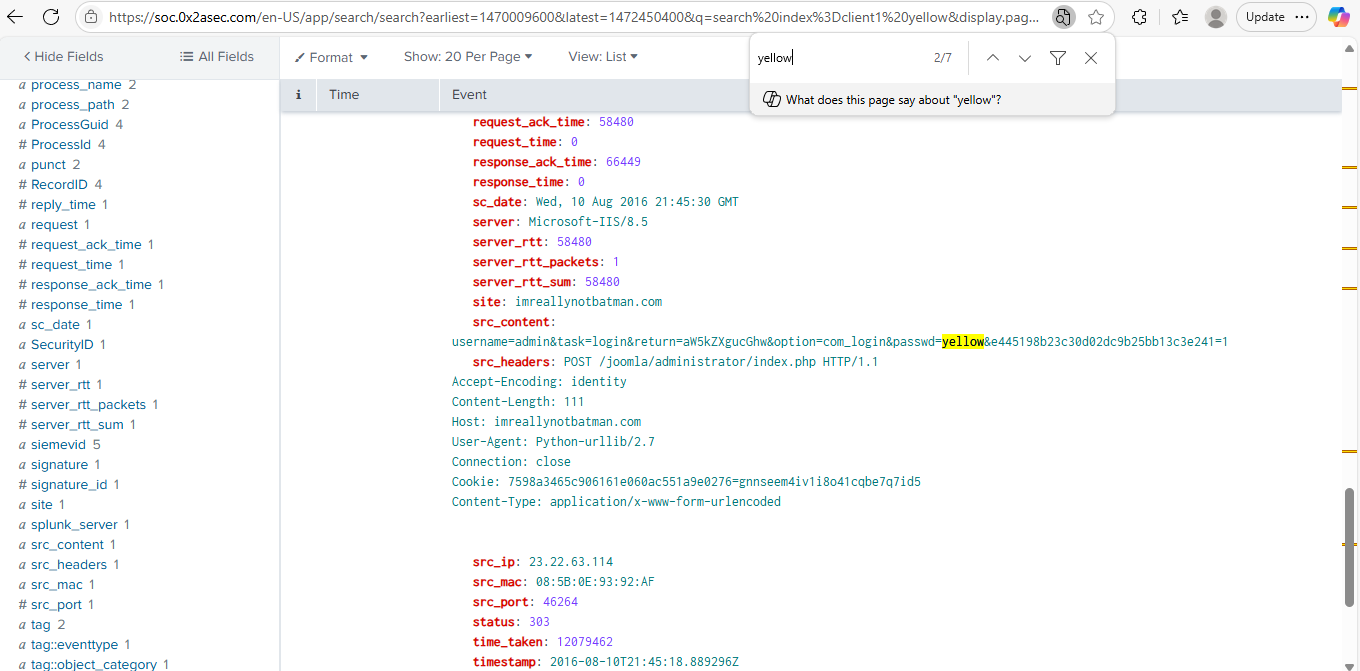
8/10/16

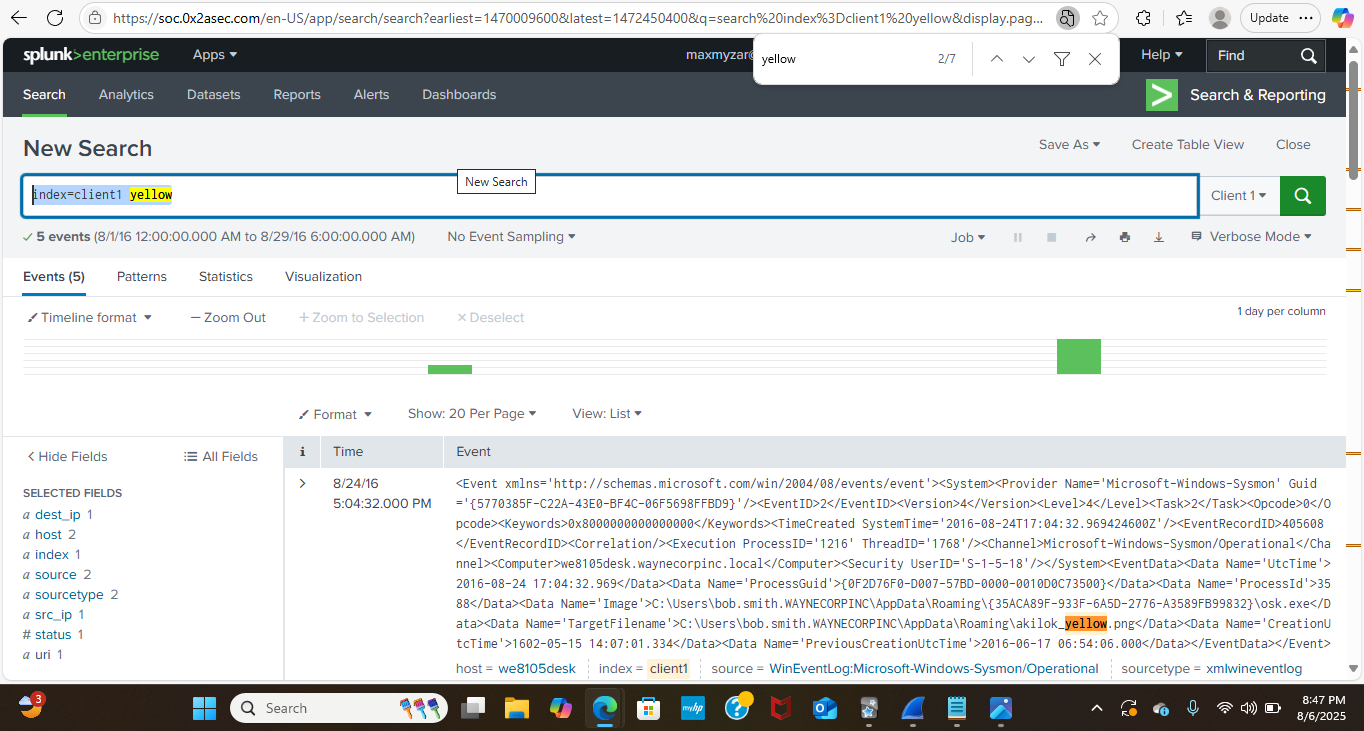
9:45:30.867 PM

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/6d42fbb5-085a-4b86-9019-1c1550c13c7f)**.** Use this worksheet to keep notes as you complete it. |
| --- |









index=client1 yellow

Threat intelligence tells us this threat actor is a fan of the band Coldplay — and that their favorite song is 6-characters long.

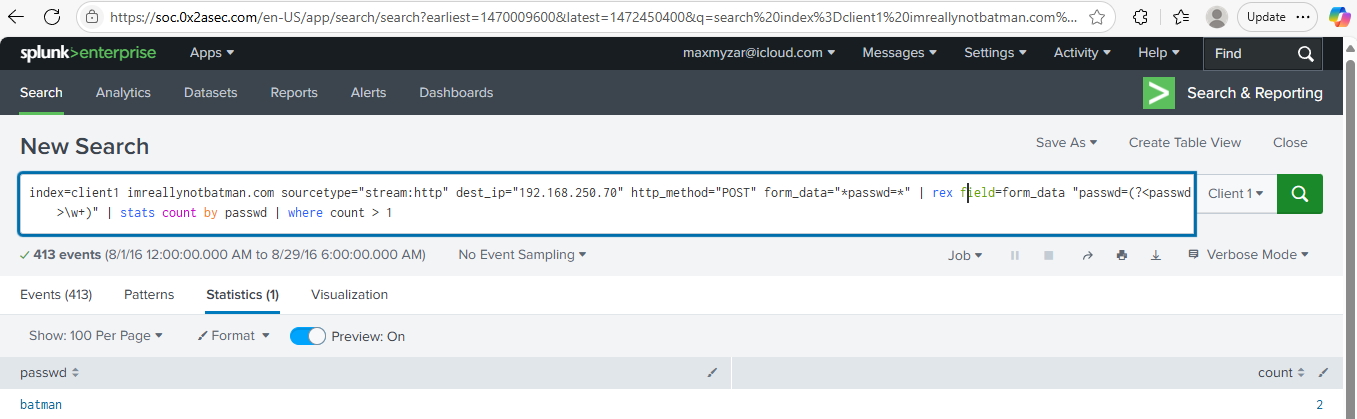
* Which of the passwords matches a 6-character long Coldplay song?

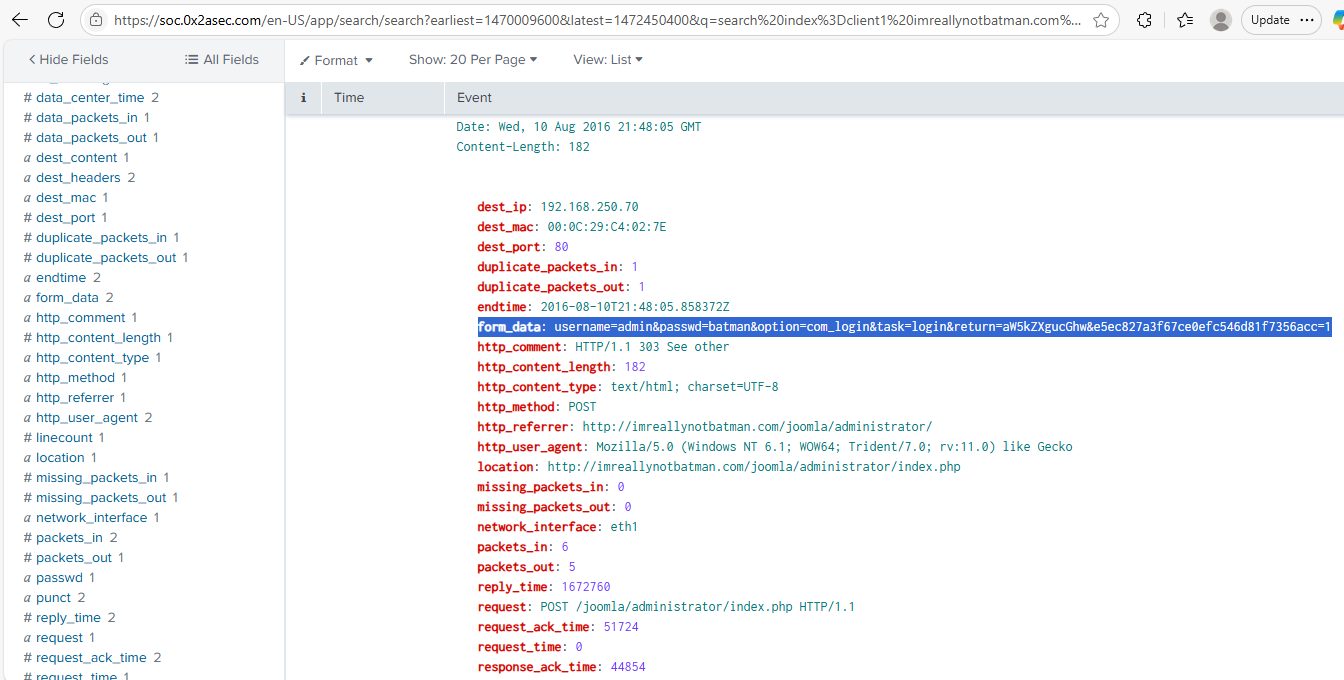
Yellow

13.3.3 Admin password

13.3.3 Establishing the correct admin password

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/810d00c2-4850-4868-90d1-dde32bda34a4)**.** Use this worksheet to keep notes as you complete it. |
| --- |





index=client1 imreallynotbatman.com sourcetype="stream:http" dest\_ip="192.168.250.70" http\_method="POST" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<passwd>\w+)" | stats count by passwd | where count > 1

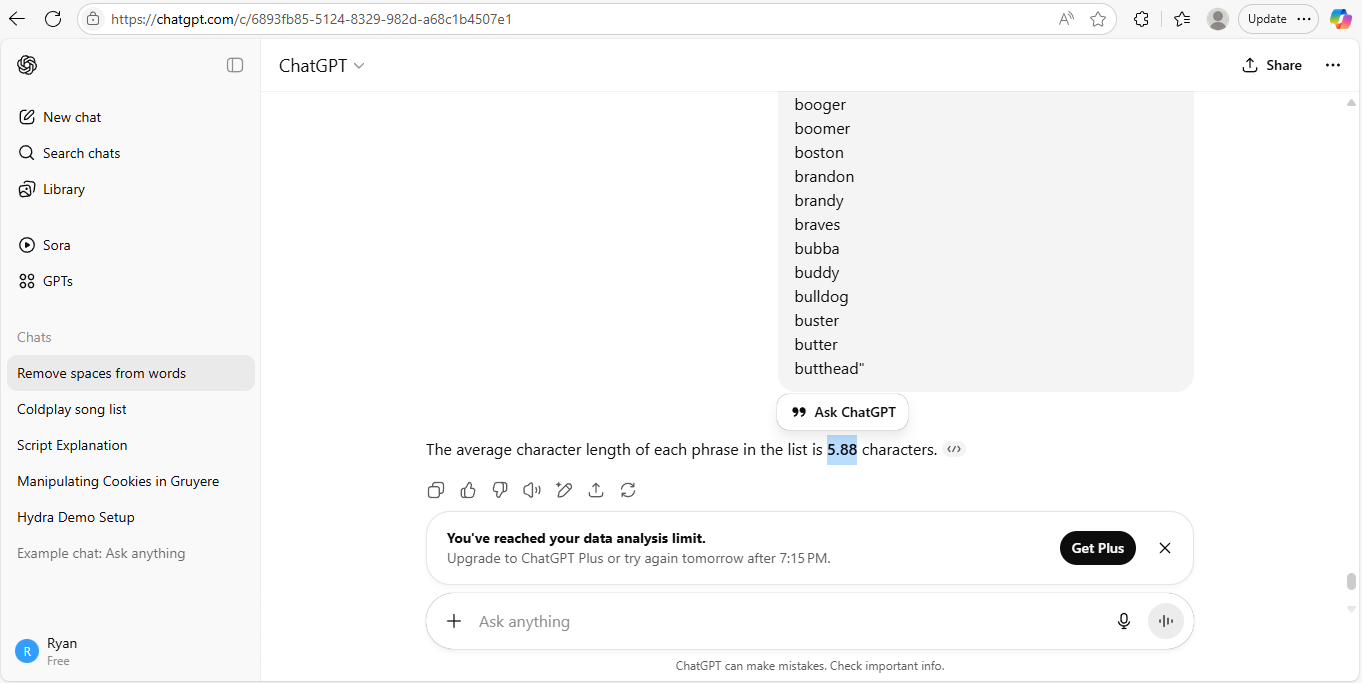
batman

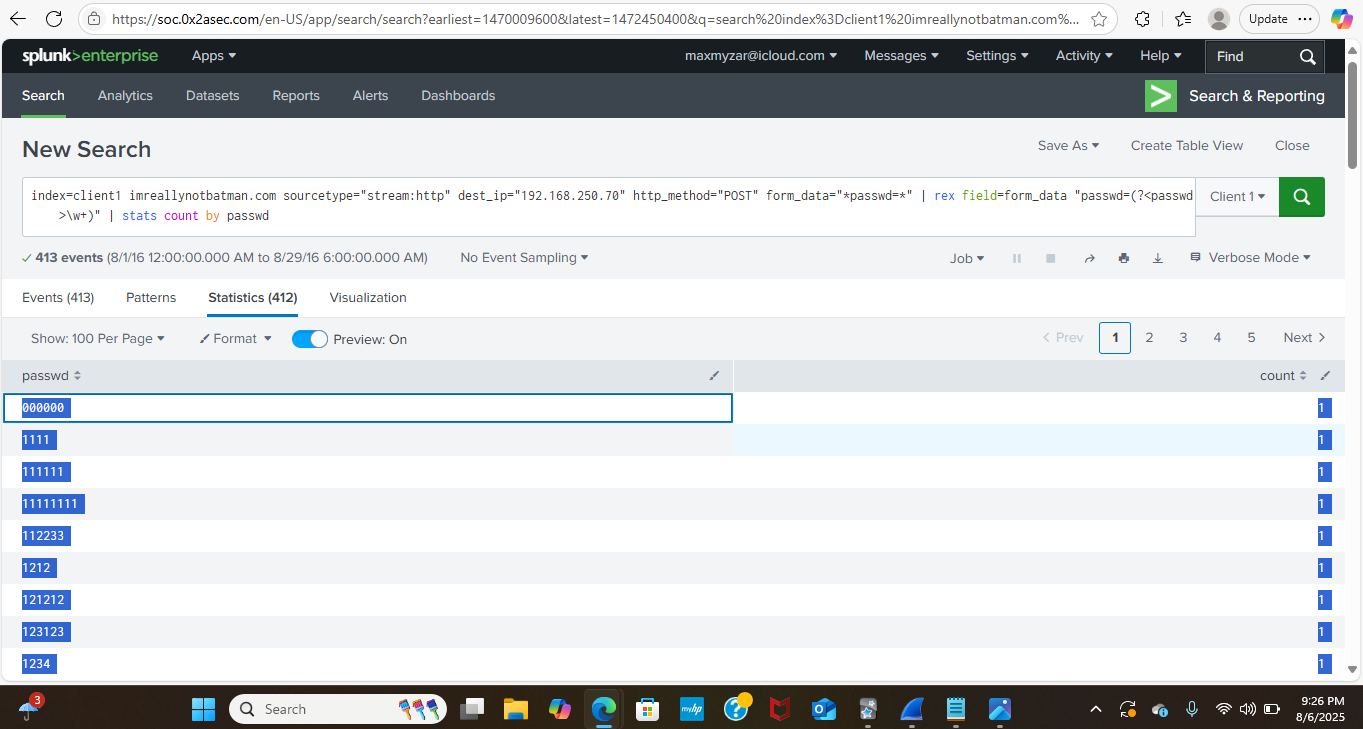
13.3.4 Average password length

13.3.4 Determining the average password length

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/7d60c6cc-bf00-4906-be26-aa97f14111e3)**.** Use this worksheet to keep notes as you complete it. |
| --- |

5/8/2025





index=client1 imreallynotbatman.com sourcetype="stream:http" dest\_ip="192.168.250.70" http\_method="POST" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<passwd>\w+)" | stats count by passwd

We want to figure out the average length of the passwords used during the brute force attempt. (Round up to the closest whole integer — for example, submit 11 if your result is 10.97598 or 11.4.)

6

13.3.5 Seconds between events

13.3.5 Calculating seconds elapsed between two events

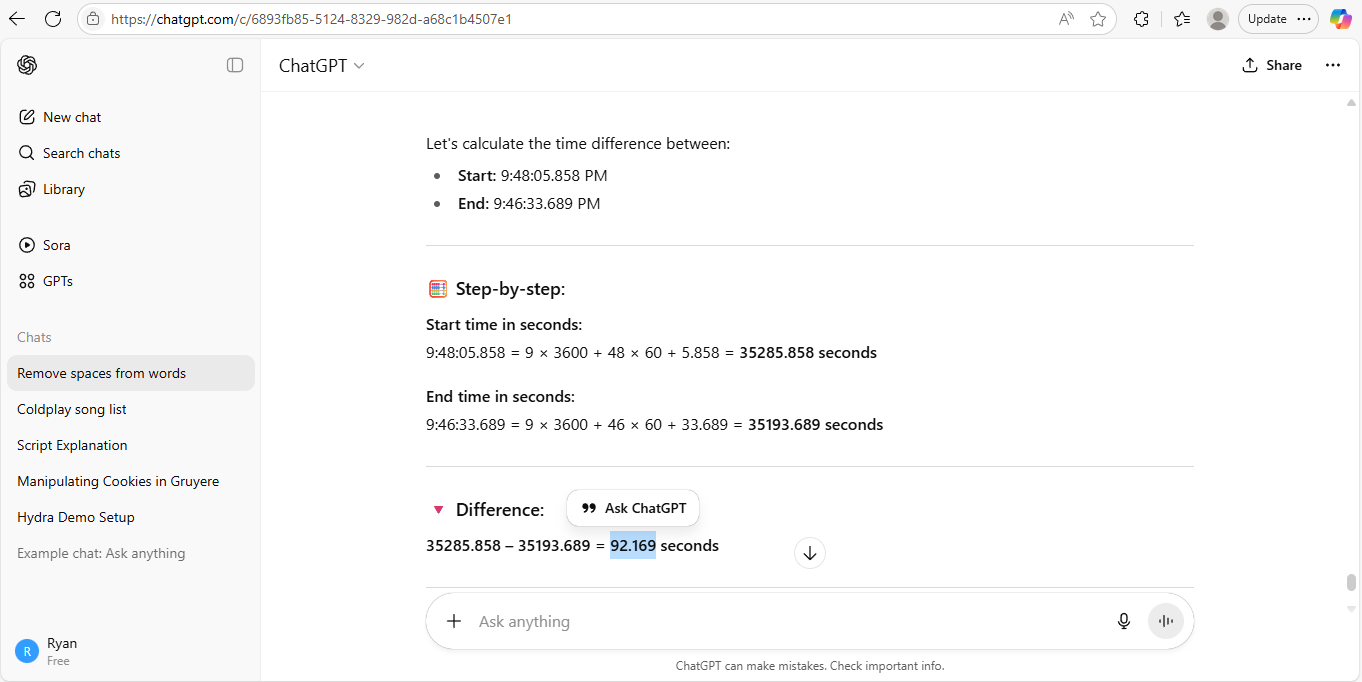
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/2a2a607e-0464-409c-a196-cc3b742b6c02)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/5/2025





index=client1 imreallynotbatman.com sourcetype="stream:http" dest\_ip="192.168.250.70" http\_method="POST" form\_data="\*passwd=\*" | rex field=form\_data "passwd=(?<passwd>\w+)" | search passwd=batman



We want to figure out what was the time interval *(in seconds)* between the moment the brute force scan discovered the correct password and when the compromised login occurred. *Include up to two decimal places for this duration (e.g.,* 48.03*).*

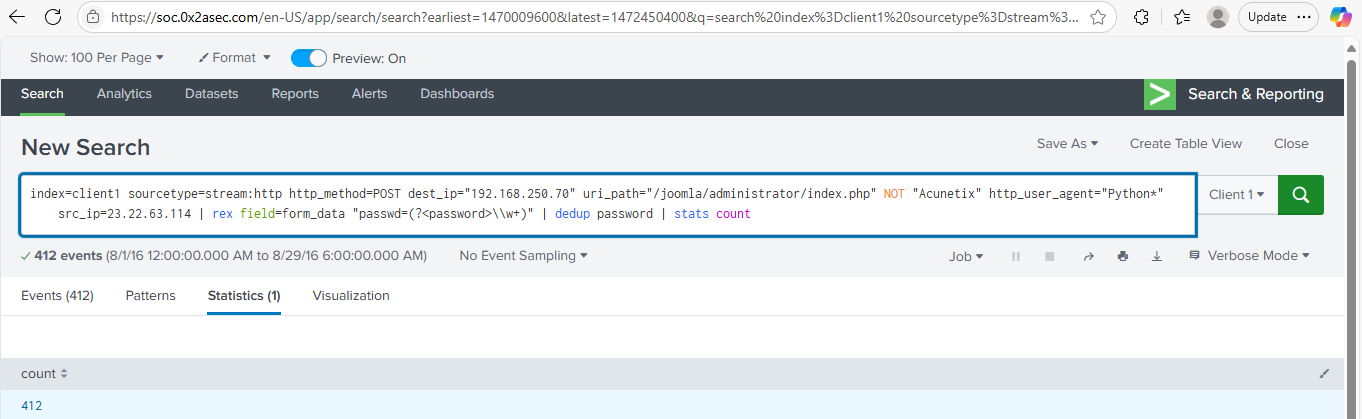
92.17

13.3.6 Unique password count

13.3.6 Reckoning the unique password count

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/c0eb81b2-c485-43dc-a82b-37da3e913479)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/6/2025



index=client1 sourcetype=stream:http http\_method=POST dest\_ip="192.168.250.70" uri\_path="/joomla/administrator/index.php" NOT "Acunetix" http\_user\_agent="Python\*" src\_ip=23.22.63.114 | rex field=form\_data "passwd=(?<password>\\w+)" | dedup password | stats count

We want to figure out the total number of distinct passwords tried during the brute force attack.

412

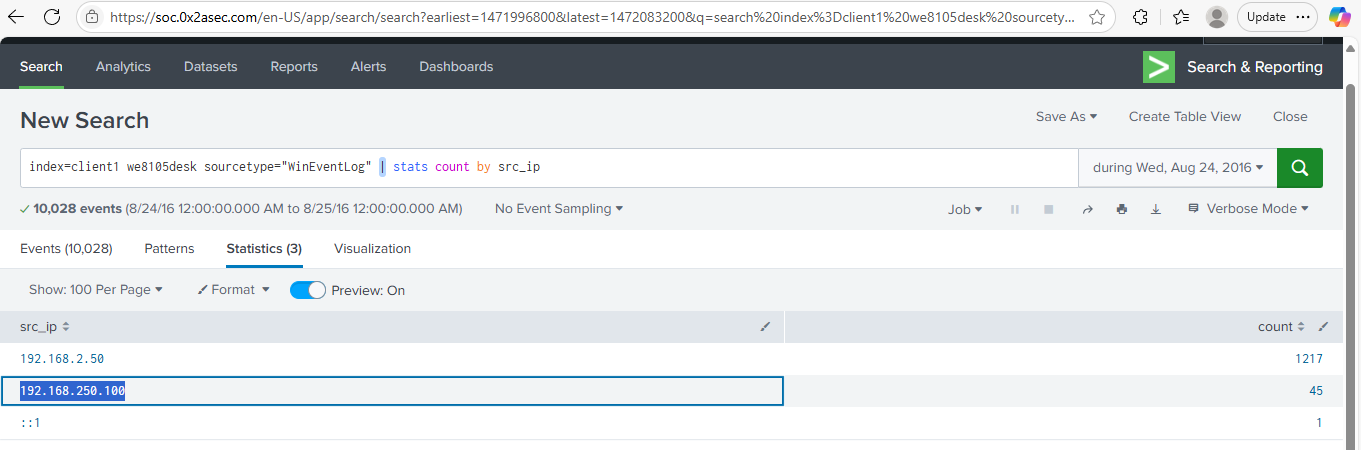
13.4 Digging in deeper

13.4.1 Host IP

13.4.1 Determining a host’s IP address

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/21570146-46b6-4e06-aa30-b7f446de5b95)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/7/2025



index=client1 we8105desk sourcetype="WinEventLog" | stats count by src\_ip

Which IP address was we8105desk most likely using on 2016-08-24?

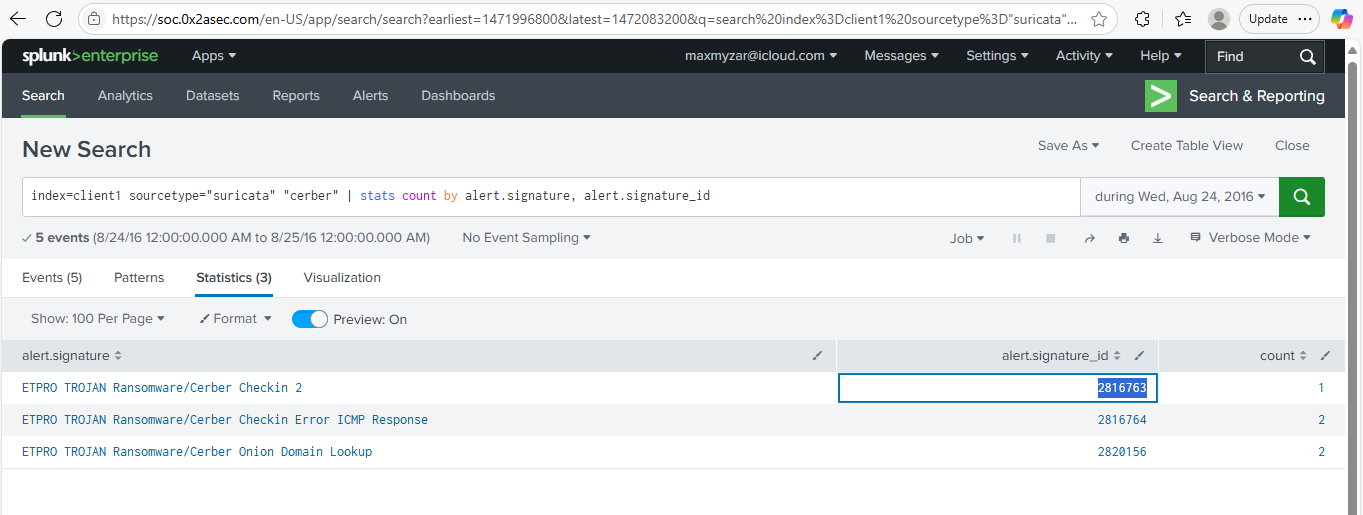
192.168.250.100

13.4.2 Least frequent alert

13.4.2 Calculating the least frequent alert

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/47488eff-f26c-415b-a472-9e6b977cffc9)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/7/2025

index=client1 sourcetype="suricata" "cerber" | stats count by alert.signature, alert.signature\_id

Which Suricata signature *(associated with the detection of Cerber malware)* generated the lowest number of alerts?

*(This should be a 7-integer number.)*

2816763

13.4.3 Ransomware FQDN

13.4.3 Working out which FQDN the ransomware redirects to

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/25edd786-1280-4c24-baab-8fa3b3e17ba3)**.** Use this worksheet to keep notes as you complete it. |
| --- |

2016-08-24 17:15:12.668



index=client1 sourcetype="stream:dns" src\_ip="192.168.250.100" query\_type=A NOT \*.microsoft NOT \*.google.com NOT \*.waynecorpinc.local | table \_time, query{}

Which FQDN does the Cerber ransomware try to redirect the user to post-encryption?

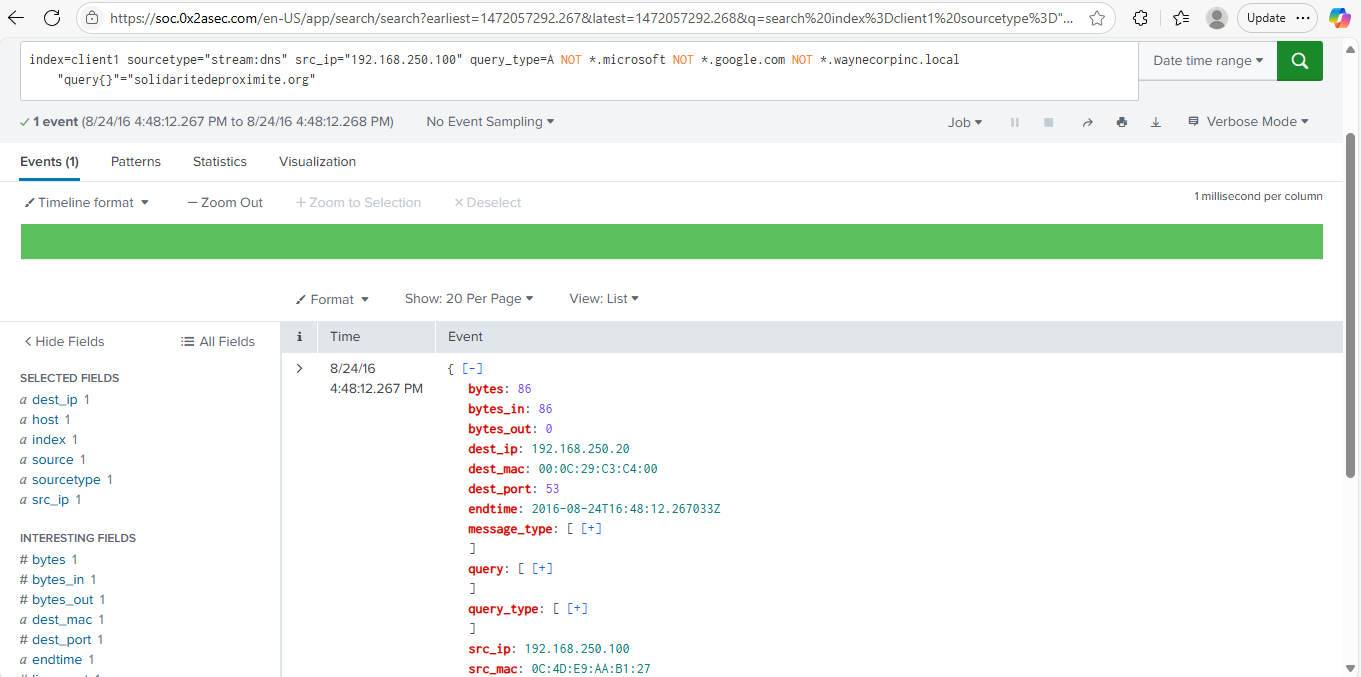
cerberhhyed5frqa.xmfir0.win

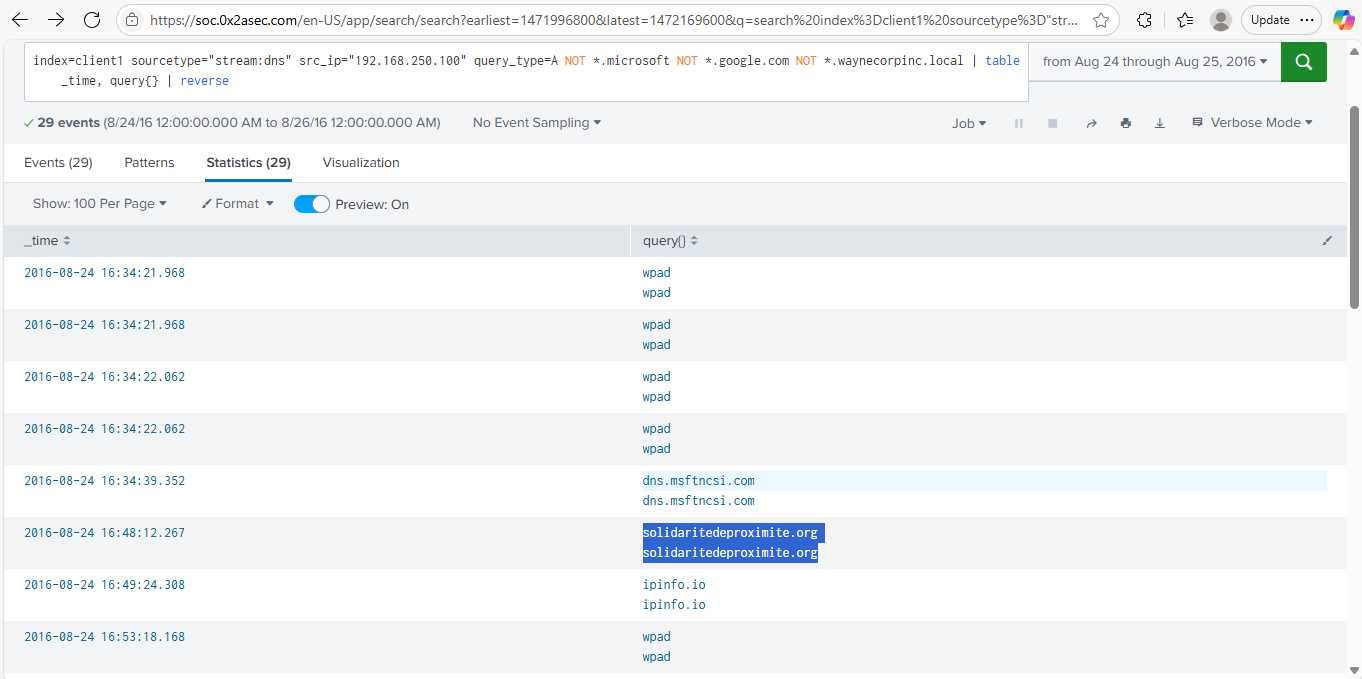
13.4.4 Malicious URL by host

13.4.4 Discovering the first malicious URL visited by a host

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/bdb7ba25-4b5b-46e6-b3ef-069543f85686)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/24/16  4:48:12.267 PM | { [[-]](https://soc.0x2asec.com/en-US/app/search/search?earliest=1472057292.267&latest=1472057292.268&q=search%20index%3Dclient1%20sourcetype%3D%22stream%3Adns%22%20src_ip%3D%22192.168.250.100%22%20query_type%3DA%20NOT%20*.microsoft%20NOT%20*.google.com%20NOT%20*.waynecorpinc.local%20%20%22query%7B%7D%22%3D%22solidaritedeproximite.org%22&display.page.search.mode=verbose&dispatch.sample_ratio=1&display.page.search.tab=events&display.general.type=events&sid=1754623307.26838#) |
| --- | --- |

index=client1 sourcetype="stream:dns" src\_ip="192.168.250.100" query\_type=A NOT \*.microsoft NOT \*.google.com NOT \*.waynecorpinc.local "query{}"="[solidaritedeproximite.org](http://solidaritedeproximite.org)"



index=client1 sourcetype="stream:dns" src\_ip="192.168.250.100" query\_type=A NOT \*.microsoft NOT \*.google.com NOT \*.waynecorpinc.local | table \_time, query{} | reverse

What is the initial suspicious domain accessed by we8105desk on 2016-08-24?

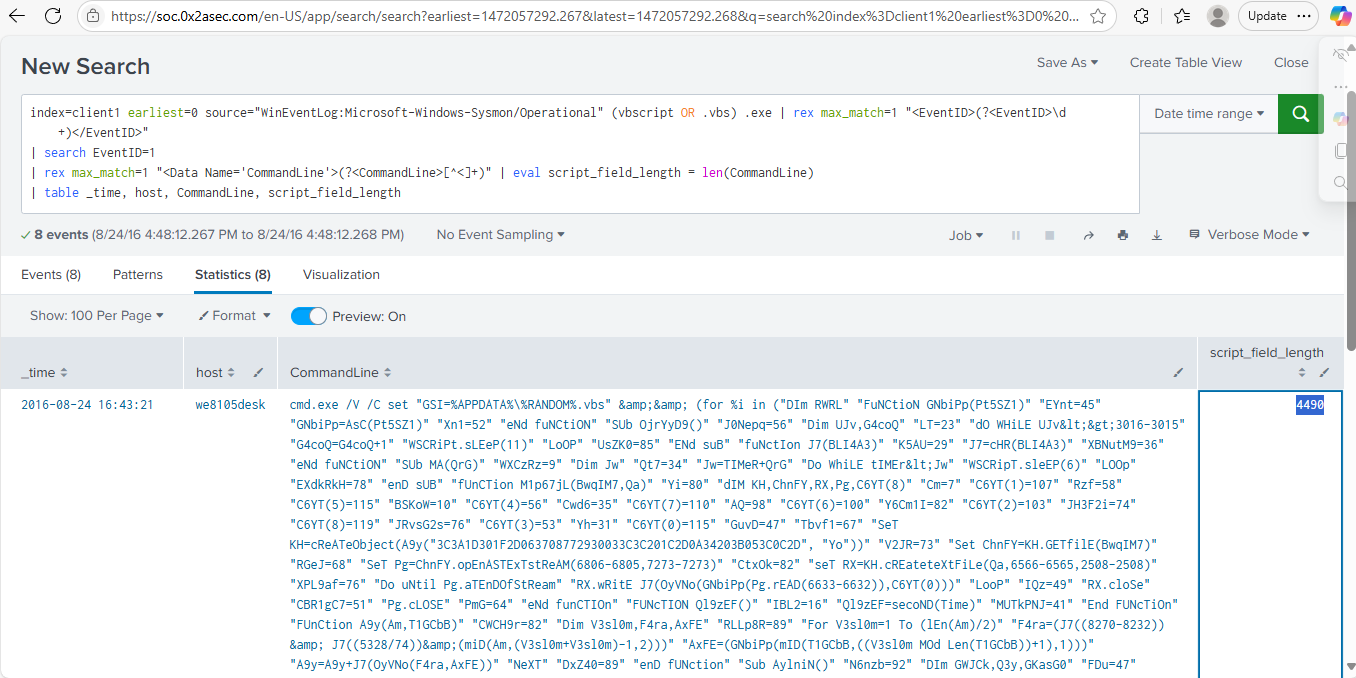
solidaritedeproximite.org

13.4.5 VB script run during infection

13.4.5 Locating the VB script run during infection

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/00c65cec-b82e-40db-be7f-ac383db1b4da)**.** Use this worksheet to keep notes as you complete it. |
| --- |

2016-08-24 16:43:21



index=client1 earliest=0 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" (vbscript OR .vbs) .exe | rex max\_match=1 "<EventID>(?<EventID>\d+)</EventID>"

| search EventID=1

| rex max\_match=1 "<Data Name='CommandLine'>(?<CommandLine>[^<]+)" | eval script\_field\_length = len(CommandLine)

| table \_time, host, CommandLine, script\_field\_length

As part of the initial Cerber infection, a VB script is executed. The full script content, preceded by the name of the executable that launched it, is stored in script\_field\_length.

What is the character count of that particular field’s value?

4490

13.4.6 USBs

13.4.6 Digging up evidence of USBs connected to a device

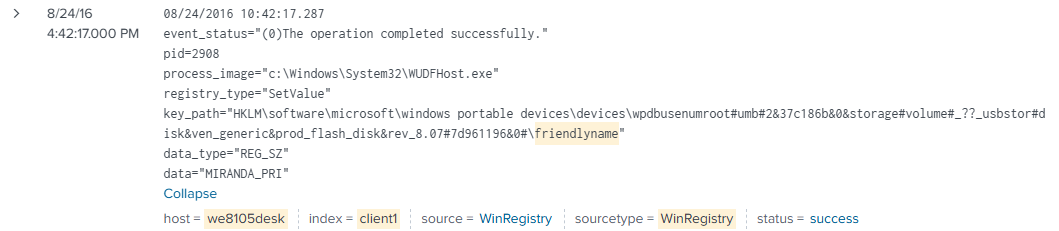
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/453ff782-05c0-46ce-8b7f-11185cfbf0d7)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/24/16

4:42:17.000 PM



index=client1 host=we8105desk sourcetype="WinRegistry" friendlyname | top limit=1 data



index=client1 host=we8105desk sourcetype="WinRegistry" friendlyname data=MIRANDA\_PRI

What is the label or name of the USB device that Bob Smith inserted?

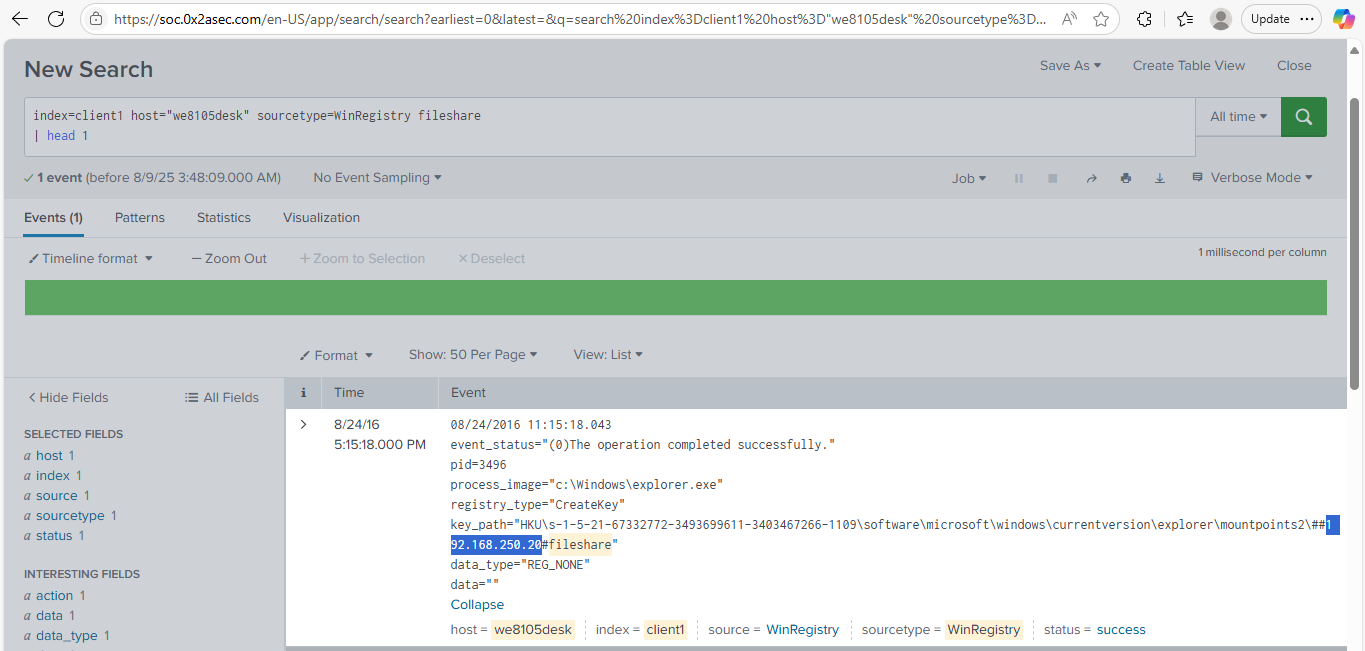
MIRANDA\_PRI

13.4.7 File server

13.4.7 Identifying the file server

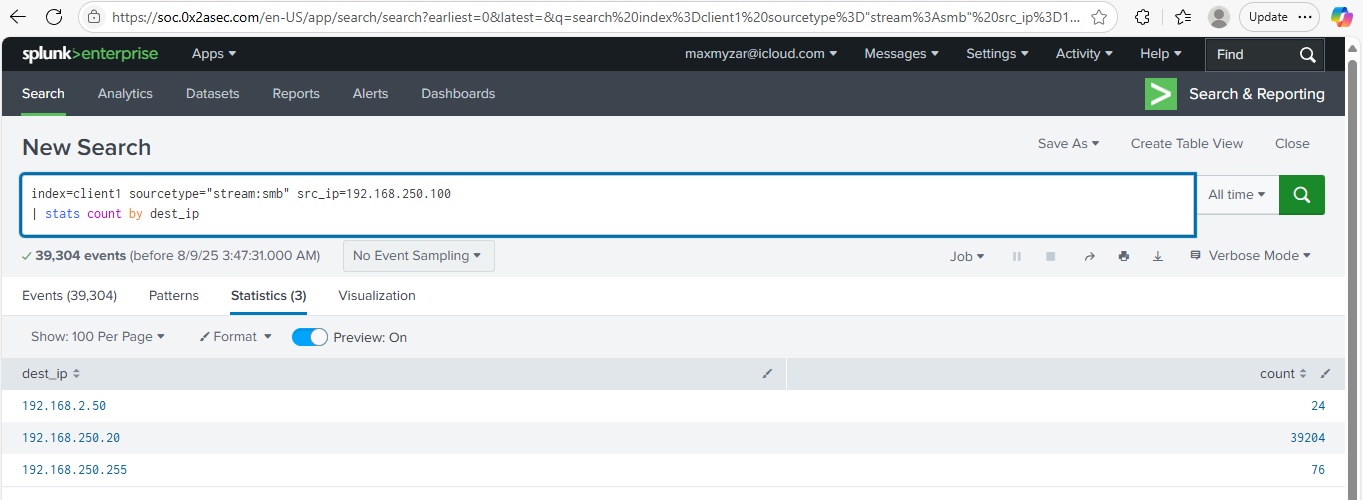
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/09899568-dfea-4ea8-918c-bec17c773303)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/24/16  5:15:18.000 PM |
| --- |



index=client1 host="we8105desk" sourcetype=WinRegistry fileshare

| head 1



index=client1 sourcetype="stream:smb" src\_ip=192.168.250.100

| stats count by dest\_ip

During the ransomware outbreak, Bob Smith’s workstation (we8105desk) was linked to a file server.

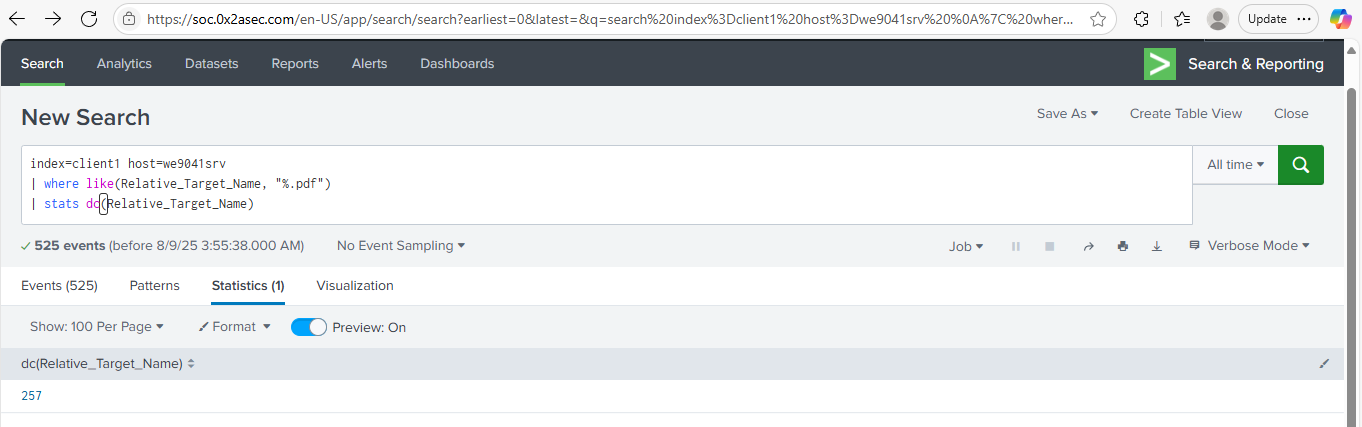
192.168.250.20

13.4.8 Unique files

13.4.8 Computing unique files encrypted by the ransomware

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/25bdd803-b991-4c18-b6a8-ae38d3b7523b)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/8/2025



index=client1 host=we9041srv

| where like(Relative\_Target\_Name, "%.pdf")

| stats dc(Relative\_Target\_Name)

We want to figure out the total number of unique PDF files encrypted by the ransomware on the remote file server.

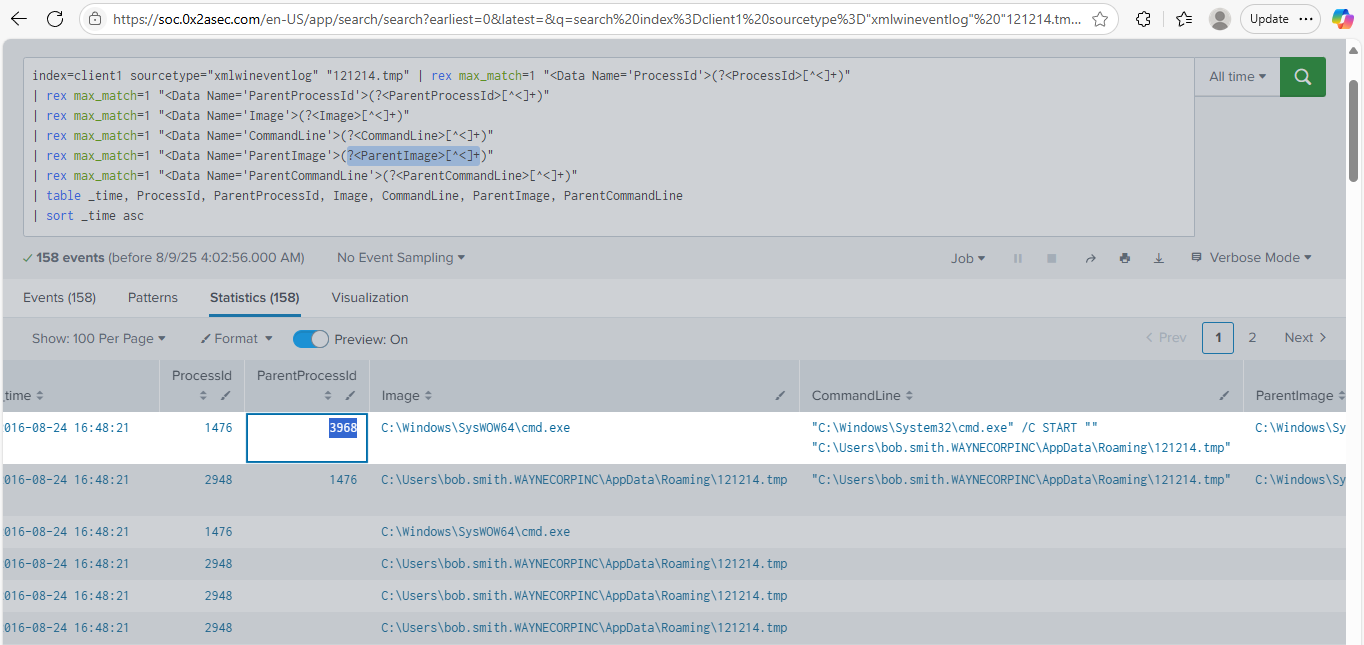
257

13.4.9 Process

13.4.9 Tracking down the responsible process

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/d3c700b4-52bf-4001-8754-77d744a926dc)**.** Use this worksheet to keep notes as you complete it. |
| --- |

2016-08-24 16:48:21



index=client1 sourcetype="xmlwineventlog" "121214.tmp" | rex max\_match=1 "<Data Name='ProcessId'>(?<ProcessId>[^<]+)"

| rex max\_match=1 "<Data Name='ParentProcessId'>(?<ParentProcessId>[^<]+)"

| rex max\_match=1 "<Data Name='Image'>(?<Image>[^<]+)"

| rex max\_match=1 "<Data Name='CommandLine'>(?<CommandLine>[^<]+)"

| rex max\_match=1 "<Data Name='ParentImage'>(?<ParentImage>[^<]+)"

| rex max\_match=1 "<Data Name='ParentCommandLine'>(?<ParentCommandLine>[^<]+)"

| table \_time, ProcessId, ParentProcessId, Image, CommandLine, ParentImage, ParentCommandLine

| sort \_time asc

The VBscript found in [Locating the VB script run during infection](https://tripleten.com/trainer/csa/lesson/00c65cec-b82e-40db-be7f-ac383db1b4da) launches 121214.tmp. What is the ParentProcessId of this initial launch?

3968

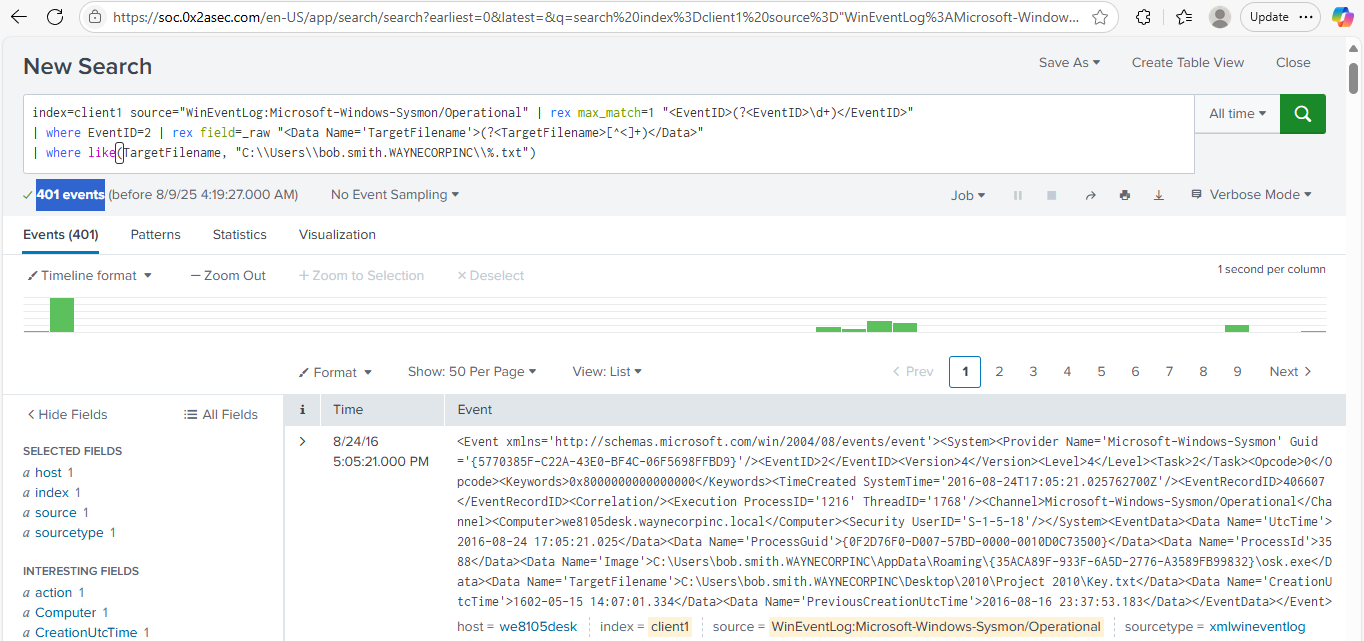
13.4.10 Counting files

13.4.10 Calculating the number of encrypted files of a specific format

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/c4aafd33-78bc-4514-9076-676c88cad704)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/24/16

5:05:21.000 PM



index=client1 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" | rex max\_match=1 "<EventID>(?<EventID>\d+)</EventID>"

| where EventID=2 | rex field=\_raw "<Data Name='TargetFilename'>(?<TargetFilename>[^<]+)</Data>"

| where like(TargetFilename, "C:\\Users\\bob.smith.WAYNECORPINC\\%.txt")

We want to figure out how many .txt files within Bob Smith’s Windows user profile were encrypted by the Cerber ransomware.

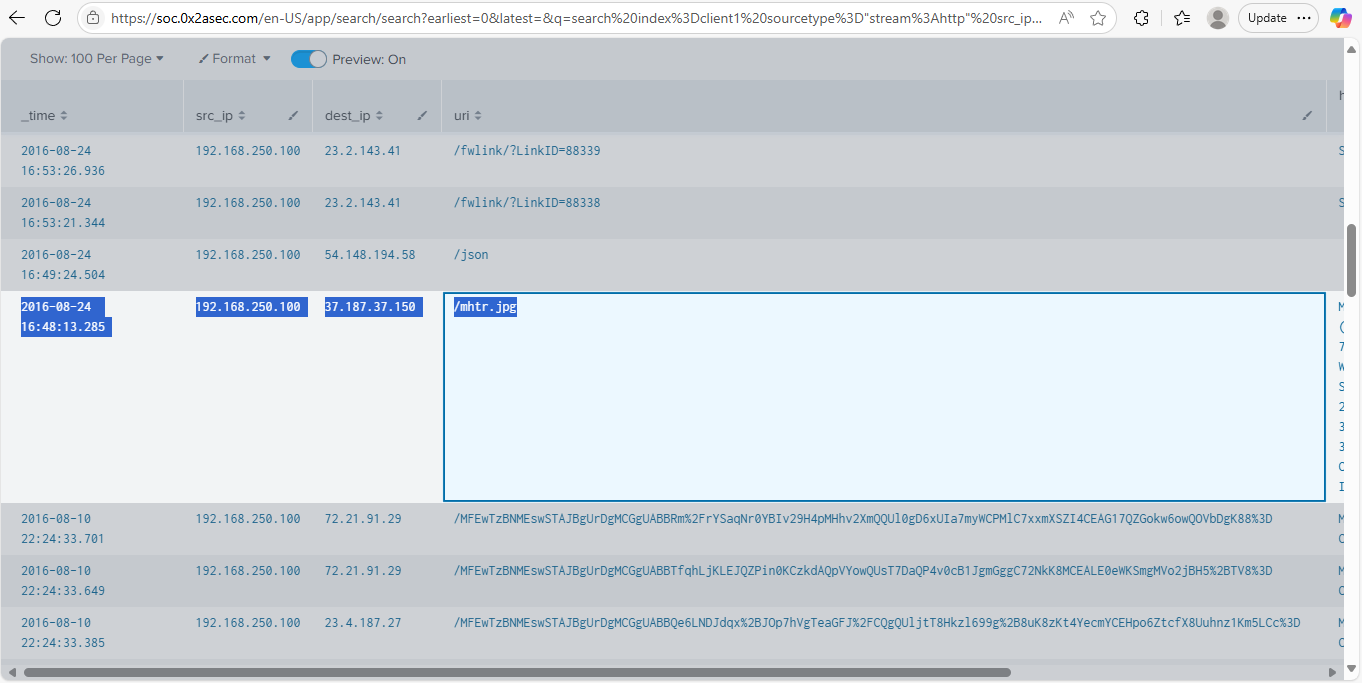
401

13.4.11 Cryptor's filename

13.4.11 Locating the cryptor’s filename

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/12b83726-f1a2-47eb-85a0-c2618a2d40cd)**.** Use this worksheet to keep notes as you complete it. |
| --- |

2016-08-24 16:48:13.285



index=client1 sourcetype="stream:http" src\_ip="192.168.250.100" uri!="\*/\*.crl" uri!="/favicon.ico"

| table \_time, src\_ip, dest\_ip, uri, http\_user\_agent, http\_method, bytes\_in, bytes\_out

What is the name of the downloaded file that contains the Cerber ransomware’s cryptor code?

mhtr.jpg

13.4.12 Obfuscation

13.4.12 Using OSINT to determine the ransomware’s obfuscation technique

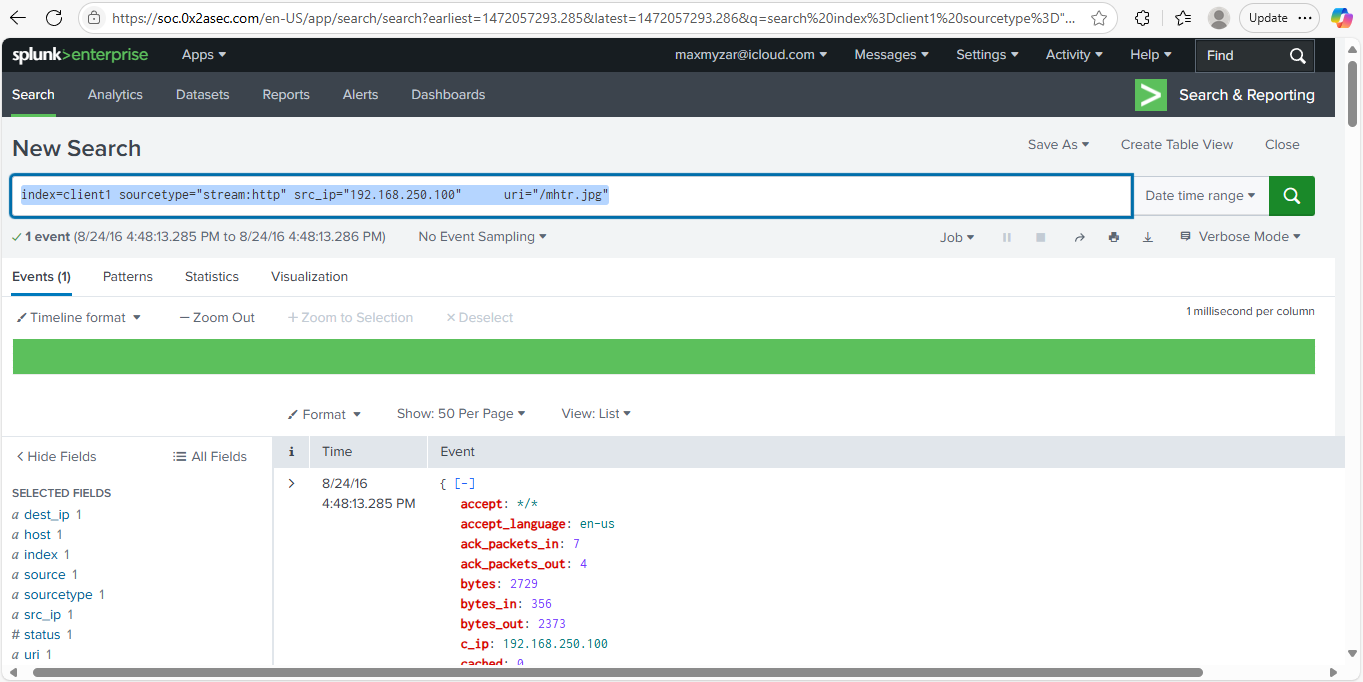
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/18811d0b-06f5-486e-9970-cf088f8af3c0)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/9/2025



index=client1 sourcetype="wineventlog" \*wscript.exe

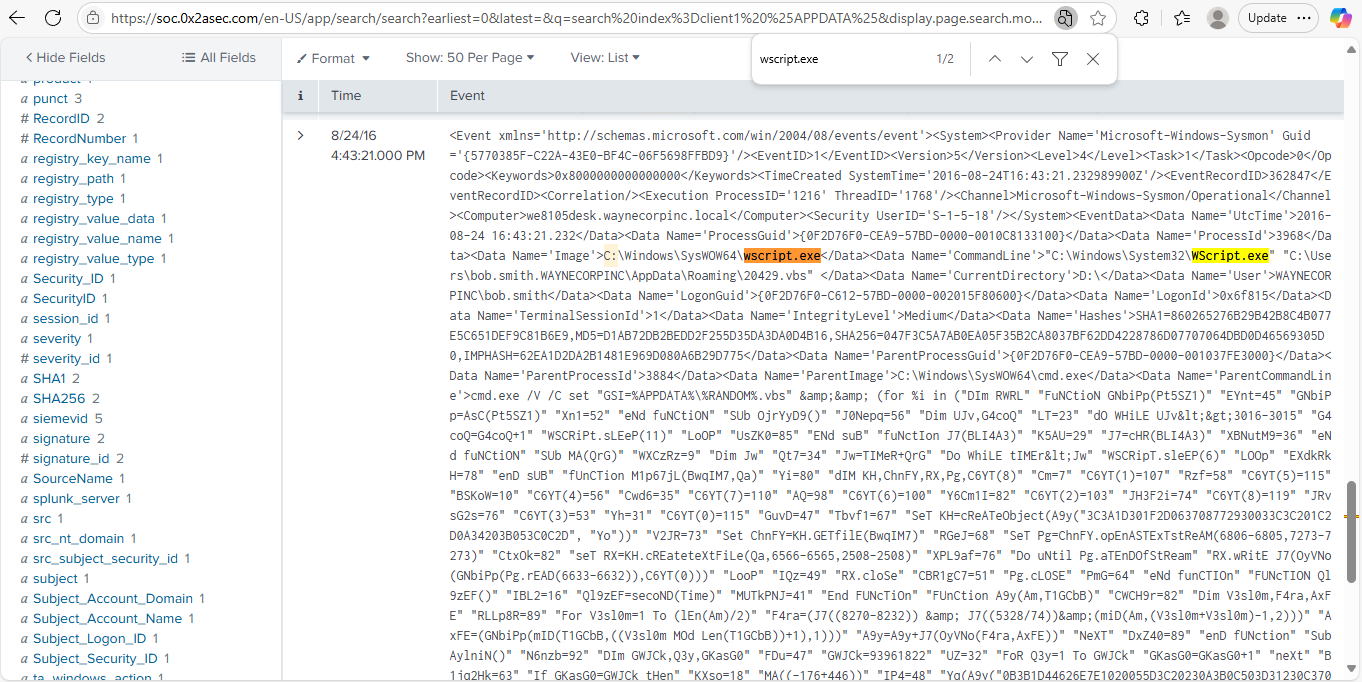
8/24/16

4:48:13.285 PM

index=client1 sourcetype="stream:http" src\_ip="192.168.250.100" uri="/mhtr.jpg"

8/24/16

4:43:21.000 PM



index=client1 %APPDATA%

Now that we know the ransomware’s encryptor filename, which obfuscation method it is most likely employing?

steganography