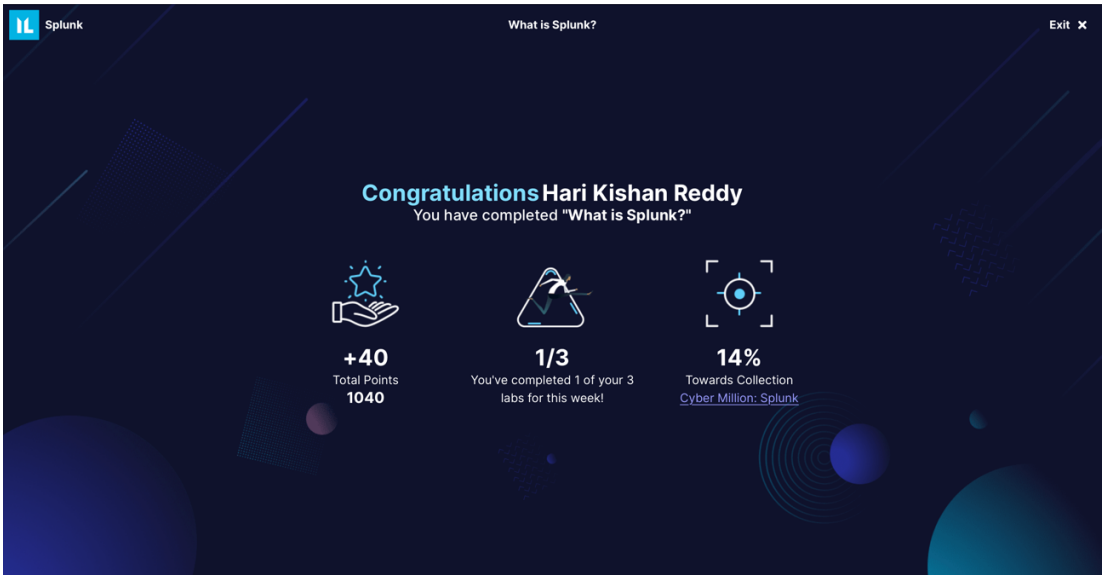
Network Monitoring- Lab 4

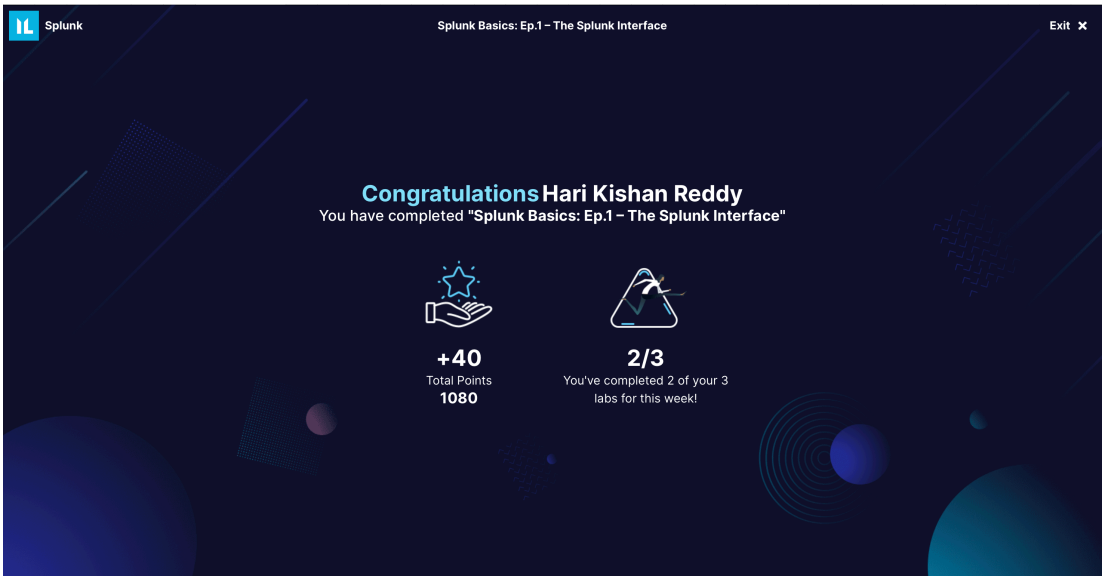
By Hari Kishan Reddy (ha2755)

1. What is Splunk?

Screenshot of lab completion:

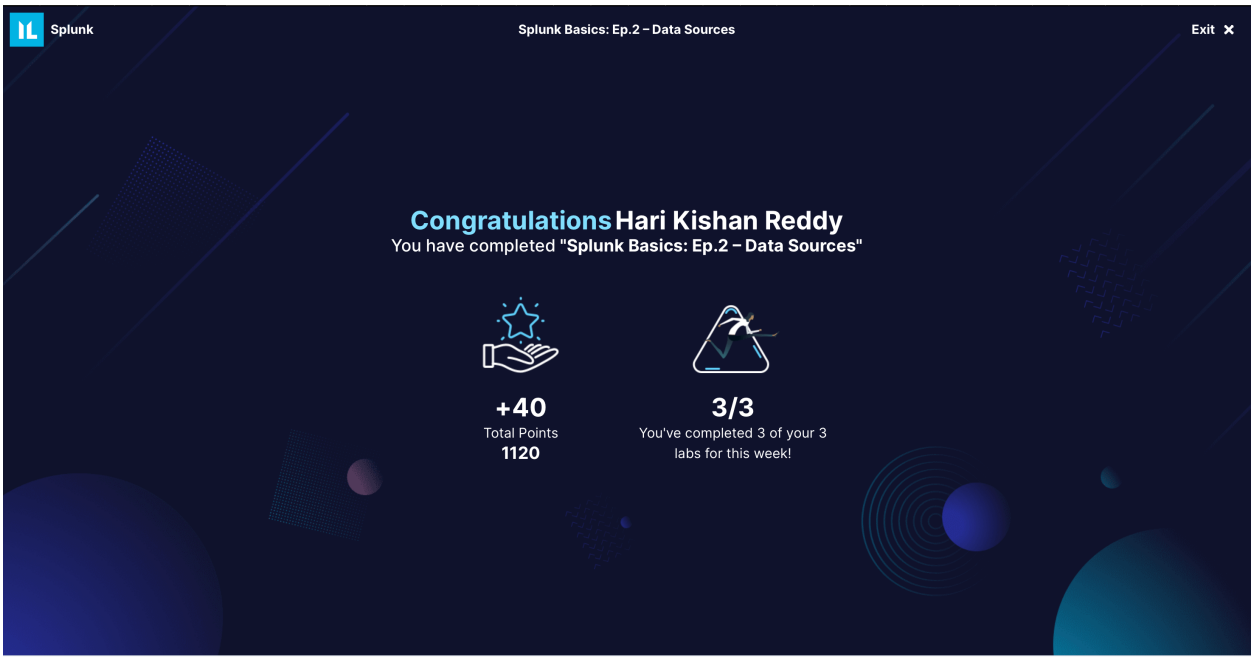


Screenshot of lab completion:

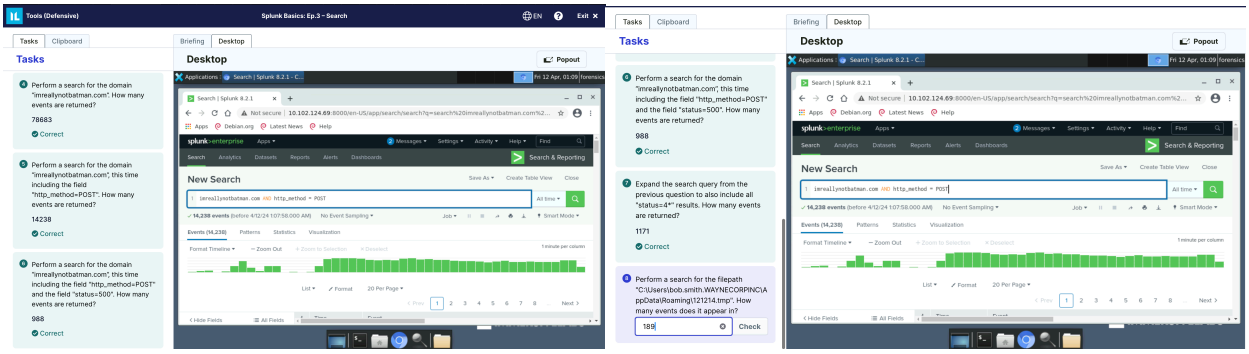


Ep.2 – Data Sources

Screenshot of lab completion:

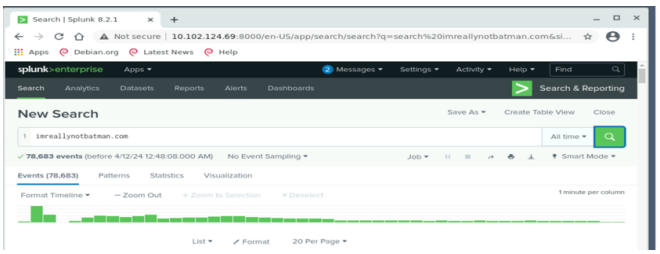


Splunk Basics: Ep.3 – Search



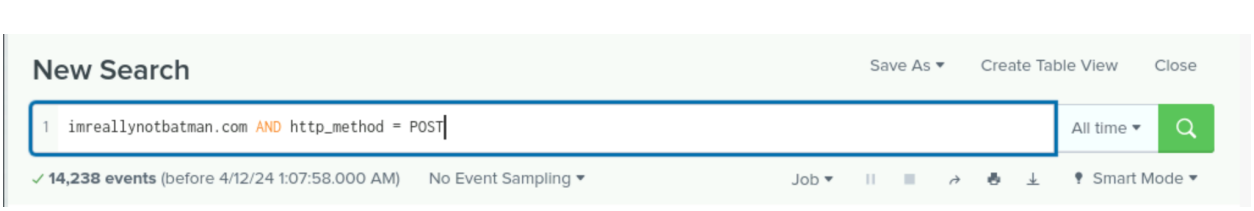
1. Perform a search for the domain "imreallynotbatman.com". How many events are returned?

- ***Command:*** `domain="imreallynotbatman.com"`
- ***Explanation:*** The command filters events based on the specified domain, "imreallynotbatman.com", retrieving a total of 78683 events matching this criterion.



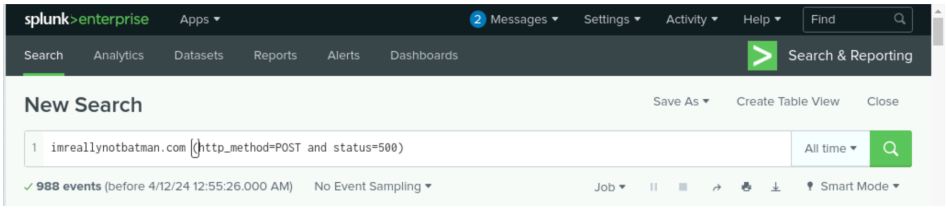
2. Perform a search for the domain "imreallynotbatman.com", this time including the field "http_method=POST". How many events are returned?

- ***Command:*** `domain="imreallynotbatman.com" http_method=POST`
- ***Explanation***: Adding the `http_method=POST` field filters events further to include only those with a POST HTTP method in addition to the specified domain, resulting in 14238 events.



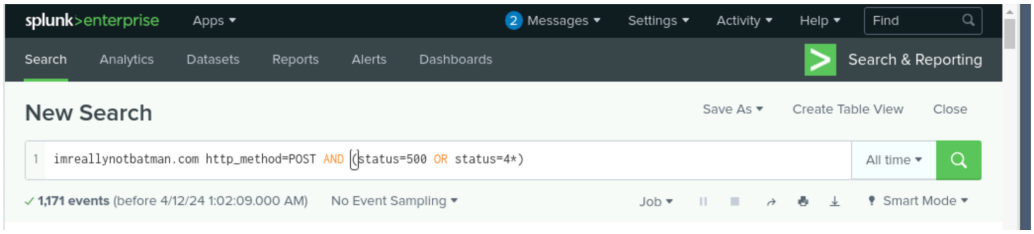
3. Perform a search for the domain "imreallynotbatman.com", this time including the field "http_method=POST" and the field "status=500". How many events are returned?

- ***Command:*** `domain="imreallynotbatman.com" http_method=POST status=500`
- ***Explanation:*** Including both the `http_method=POST` and `status=500` fields narrows down the events to those with a POST method and a status code of 500 for the specified domain, resulting in 988 events.



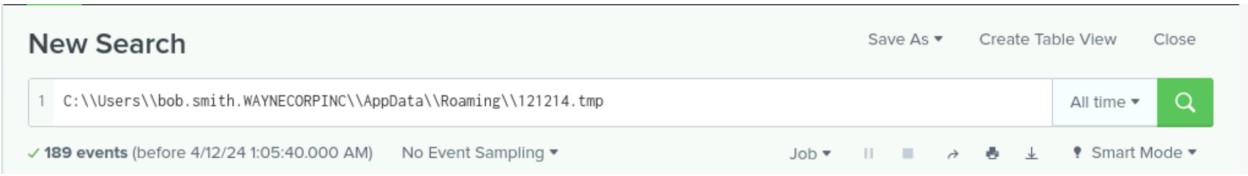
4. Expand the search query from the previous question to also include all "status=4*" results. How many events are returned?

- ***Command:*** `domain="imreallynotbatman.com" http_method=POST (status=500 OR status=4*)`
- ***Explanation:*** By expanding the search to include all status codes starting with "4" in addition to the previous filters, the command retrieves a total of 1171 events.

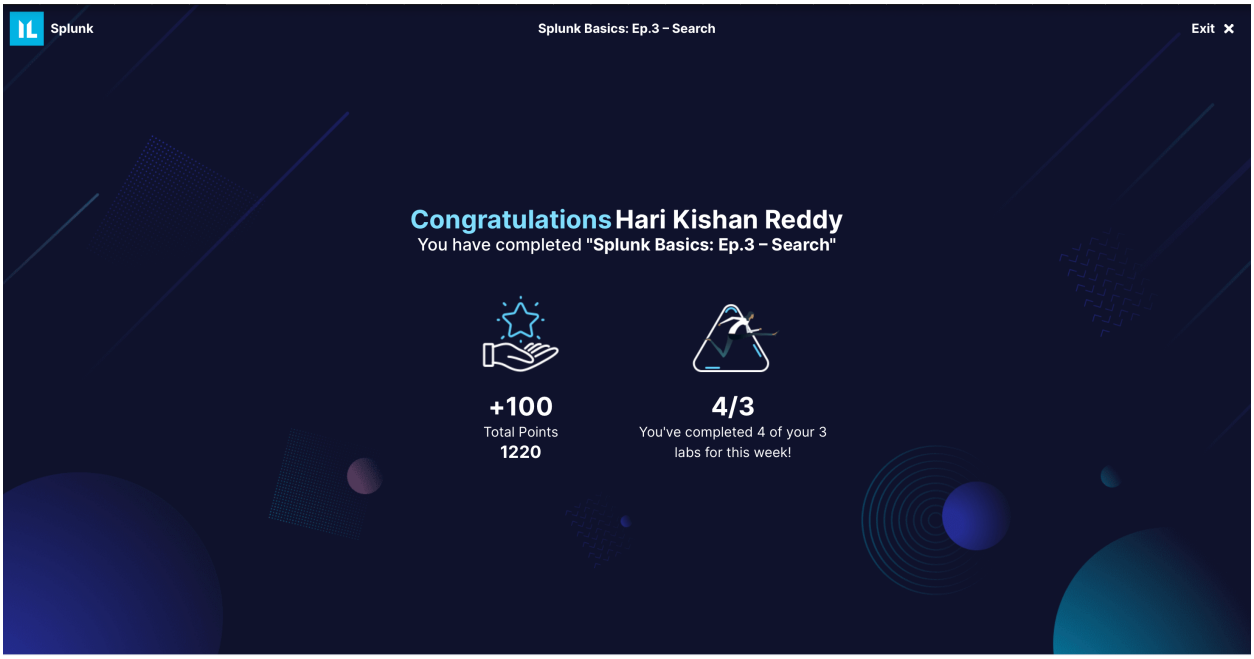


5. Perform a search for the filepath "C:\Users\bob.smith. WAYNECORPINC\AppData\Roaming\121214.tmp". How many events does it appear in?

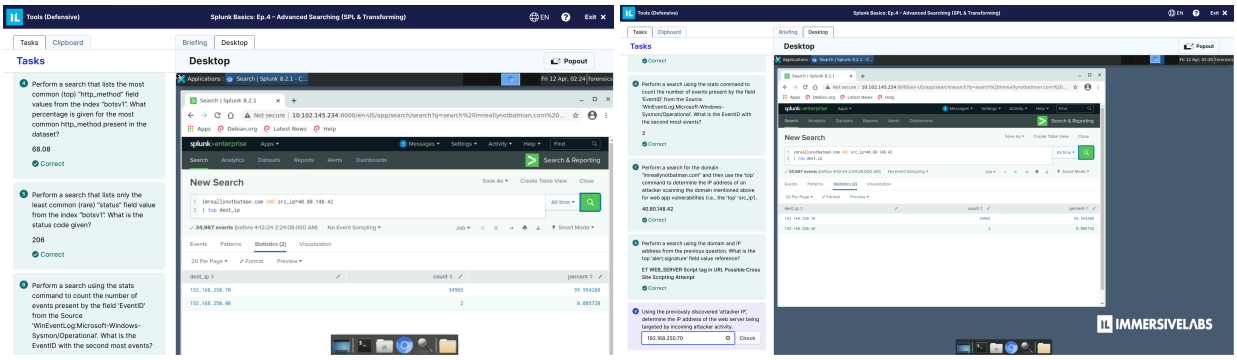
- ***Command:*** `filepath="C:\Users\bob.smith. WAYNECORPINC\AppData\Roaming\121214.tmp"`
- ***Explanation:*** This command searches for events containing the specified filepath, resulting in 189 events that include this filepath.



Screenshot of lab completion:



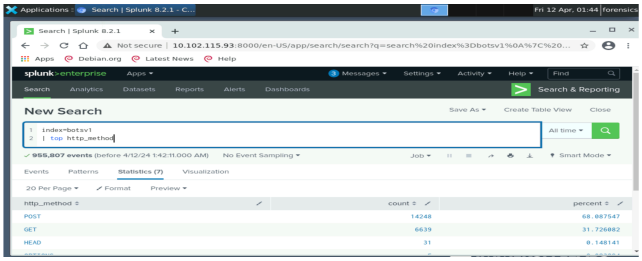
Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)



1. Perform a search that lists the most common (top) "http_method" field values from the index "botsv1". What percentage is given for the most common http_method present in the dataset?

- ***Command:*** index=botsv1 | top http_method

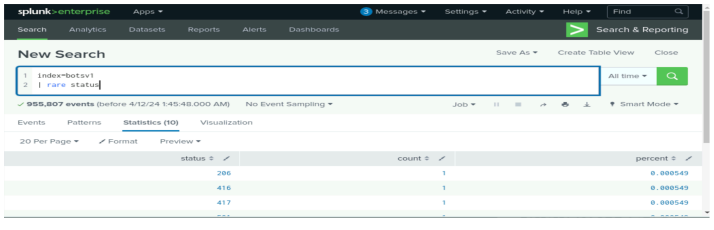
- ***Explanation:*** This command searches the "botsv1" index and uses the stats command to count occurrences of each HTTP method. The top command is then used to identify the most common HTTP method and its percentage 68.08.



2. Perform a search that lists only the least common (rare) "status" field value from the index "botsv1". What is the status code given?

- Command: `index=botsv1 | stats count by status | sort count | head 1`

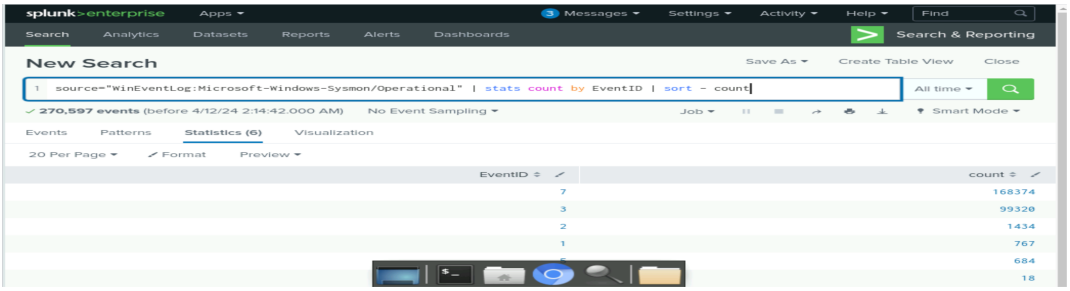
- Explanation: This command searches the "botsv1" index and uses the stats command to count occurrences of each status code. By sorting the results and selecting the least common (head 1), you identified the rarest status code, which is 206.



3. Perform a search using the stats command to count the number of events present by the field 'EventID' from the Source 'WinEventLog:Microsoft-Windows-Sysmon/Operational'. What is the EventID with the second most events?

- ***Command:*** `sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" | stats count by EventID | sort -count

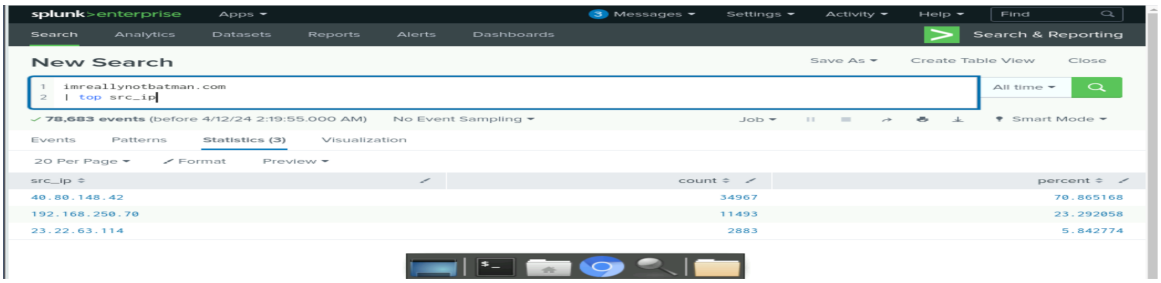
- ***Explanation:*** This command searches events from the specified source and uses the stats command to count events by EventID. By sorting in descending order and selecting the second entry, you identified the EventID with the second-highest number of events, which is 3.



4. Perform a search for the domain "imreallynotbatman.com" and then use the 'top' command to determine the IP address of an attacker scanning the domain mentioned above for web app vulnerabilities (i.e., the 'top' 'src_ip').

- ***Command:*** `domain="imreallynotbatman.com" | top src_ip`

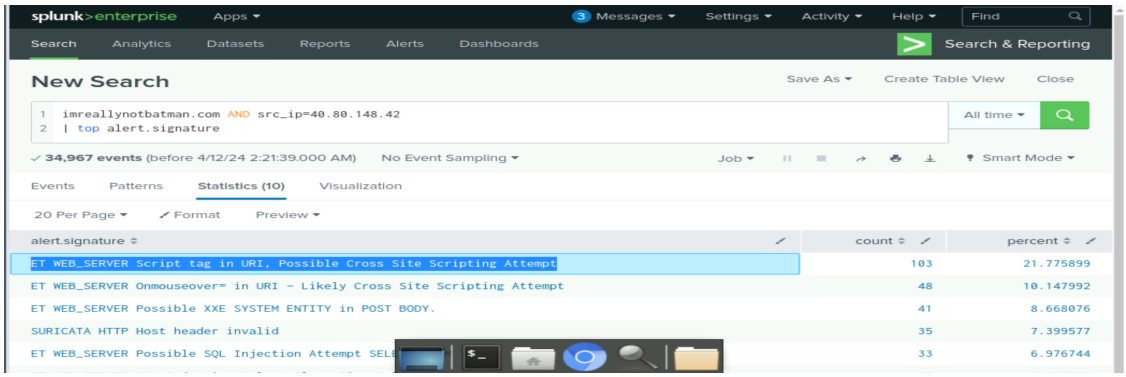
- ***Explanation:*** This command searches for events related to the specified domain and uses the top command to identify the most common source IP address (src_ip) associated with scanning the domain for vulnerabilities.



5. Perform a search using the domain and IP address from the previous question. What is the top 'alert.signature' field value reference?

- ***Command:*** `domain="imreallynotbatman.com" src_ip=40.80.148.42 | top alert.signature`

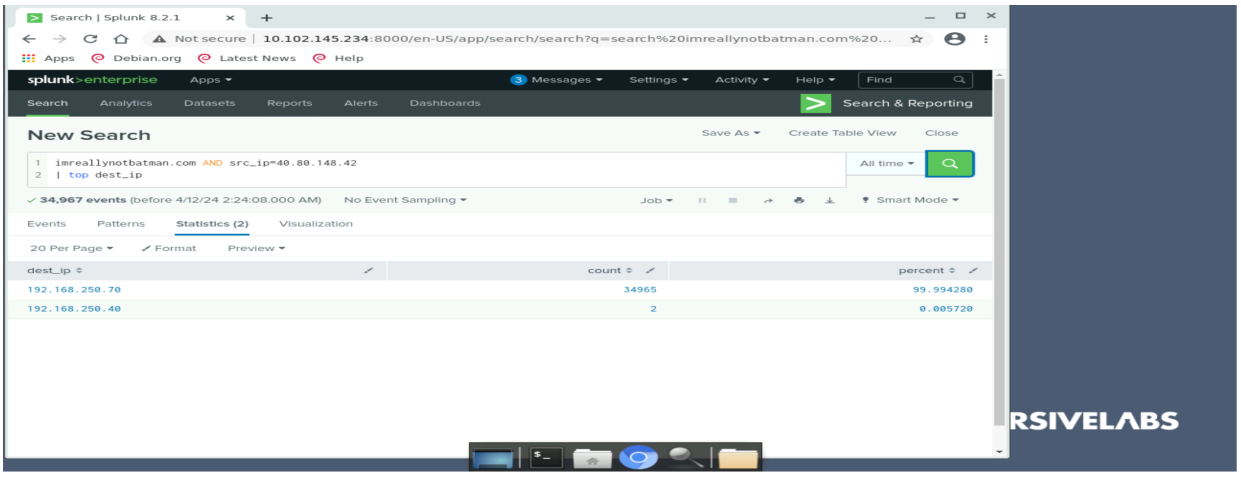
- ***Explanation:*** Building upon the previous search, this command further refines the events by including the specified domain and attacker IP address, then identifies the top 'alert.signature' field value reference related to the attacker's activity.



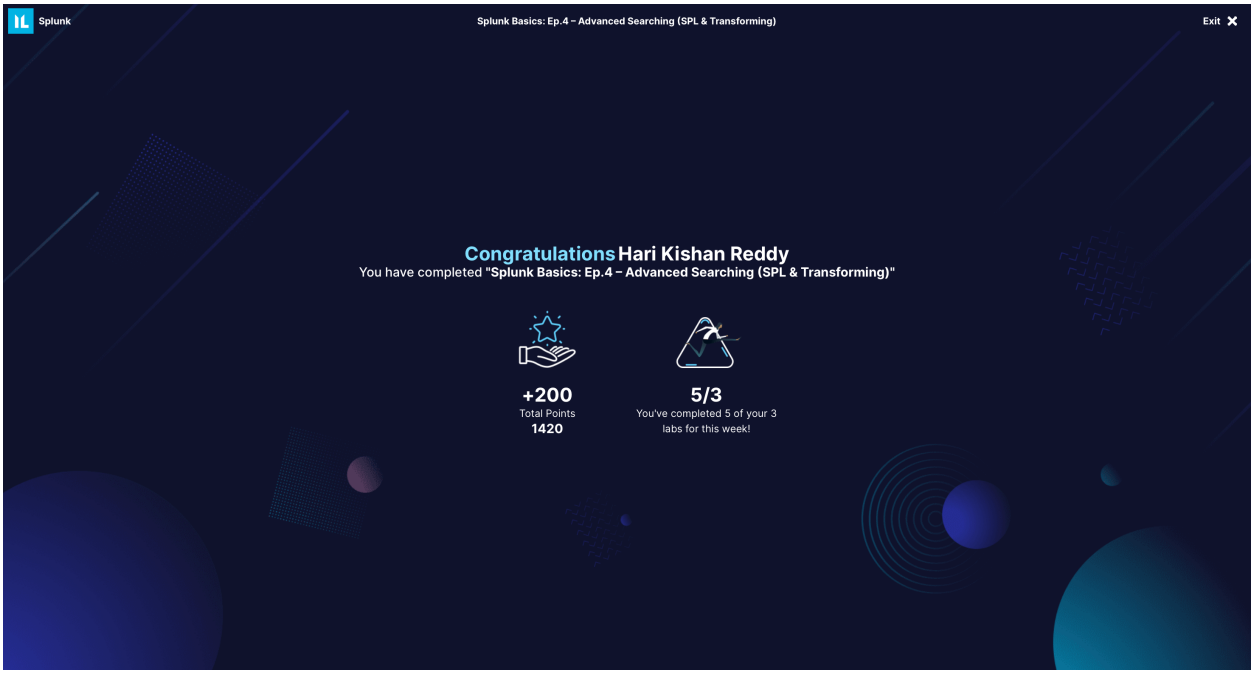
6. Using the previously discovered 'attacker IP', determine the IP address of the web server being targeted by incoming attacker activity.

- ***Command:*** `src_ip=40.80.148.42 | top dest_ip`

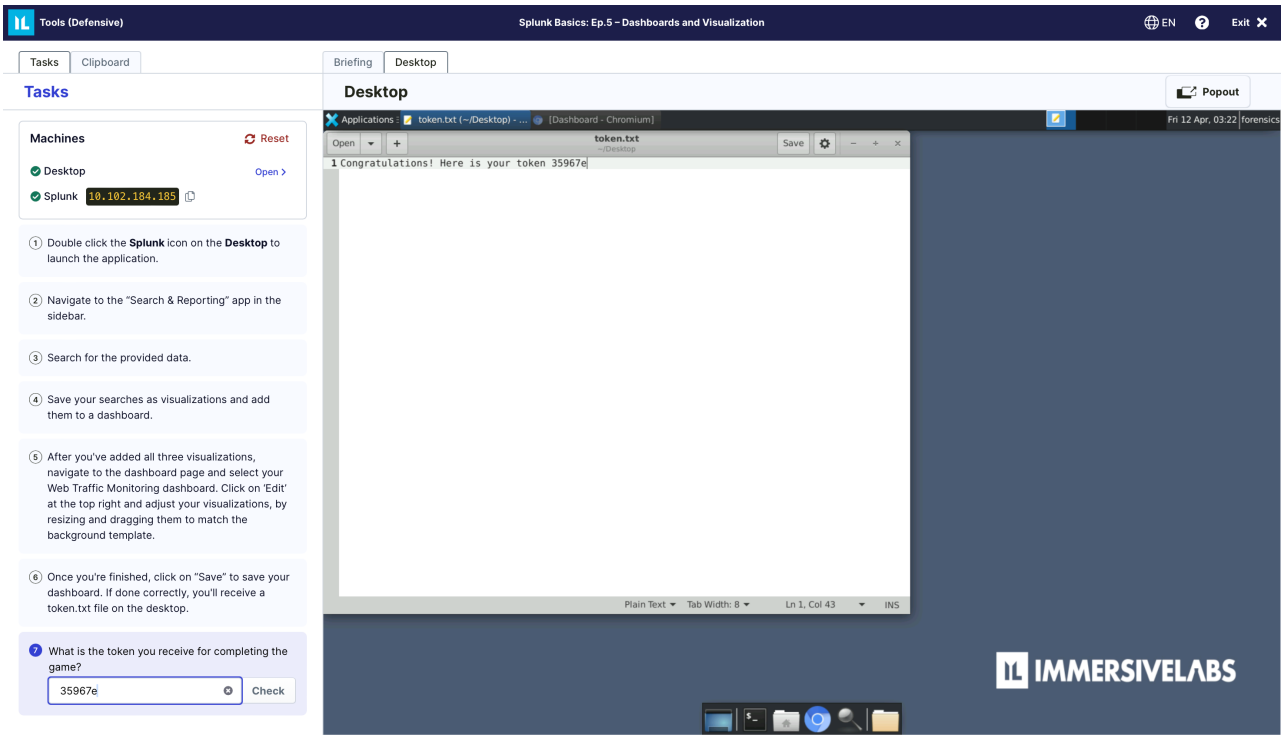
- ***Explanation:*** This command focuses on events from the attacker's IP address and uses the top command to identify the most common destination IP address (dest_ip) targeted by the attacker's activity.



Screenshot of lab completion:



Splunk Basics: Ep.5 - Dashboards and Visualization



What is the token you receive for completing the game?

1. Double-clicked the Splunk icon on the Desktop to launch the application.

2. Navigated to the "Search & Reporting" app in the sidebar.

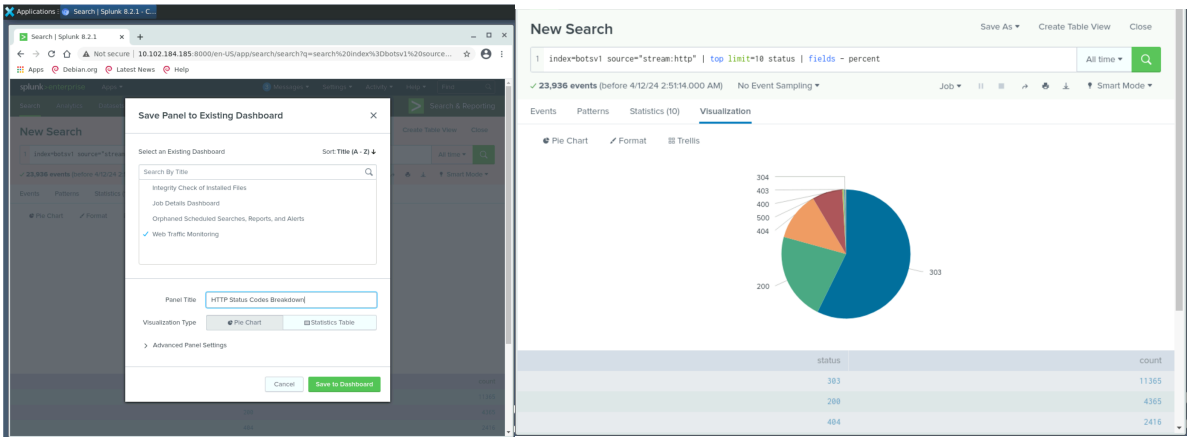
3. Searched for the provided data and saved your searches as visualizations.

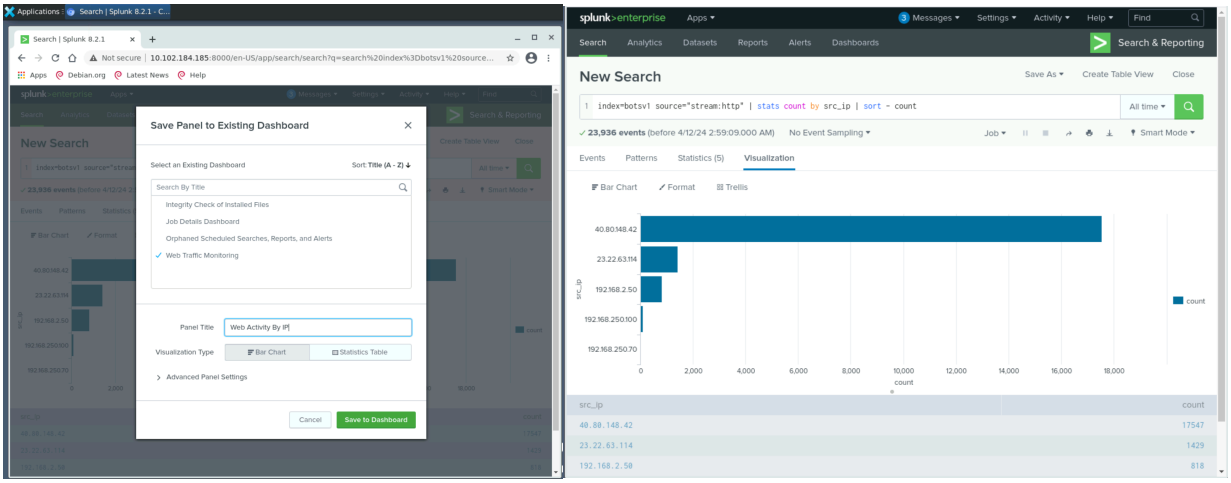
4. Added the visualizations to a dashboard.

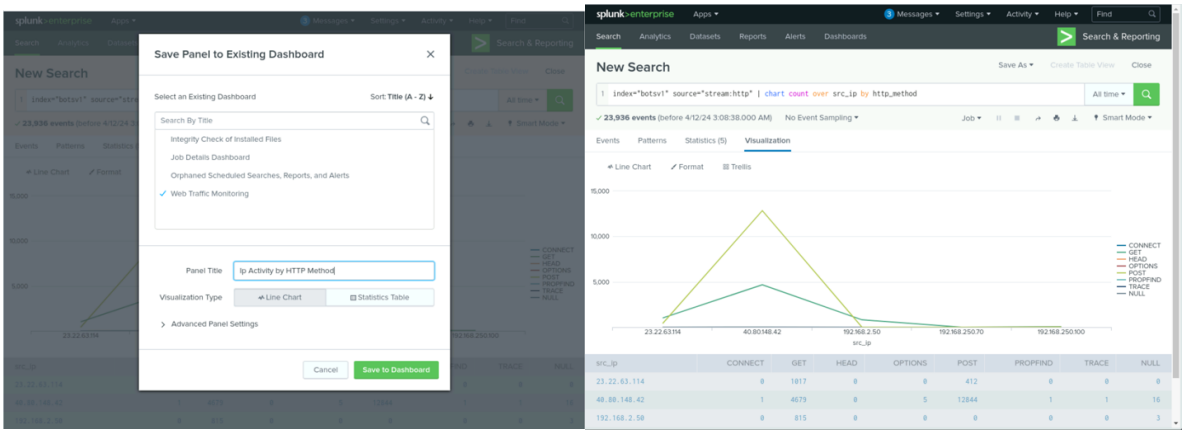
5. Edited the dashboard by resizing and dragging the visualizations to match the background template.

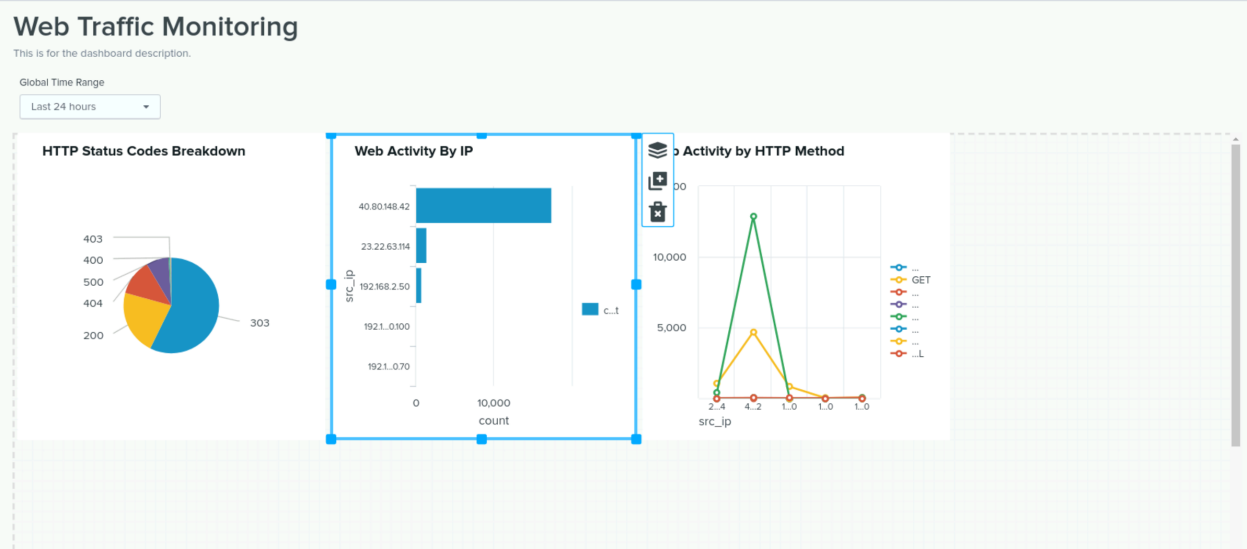
6. Saved the dashboard, resulting in receiving a token.txt file on the desktop with the token "359676."

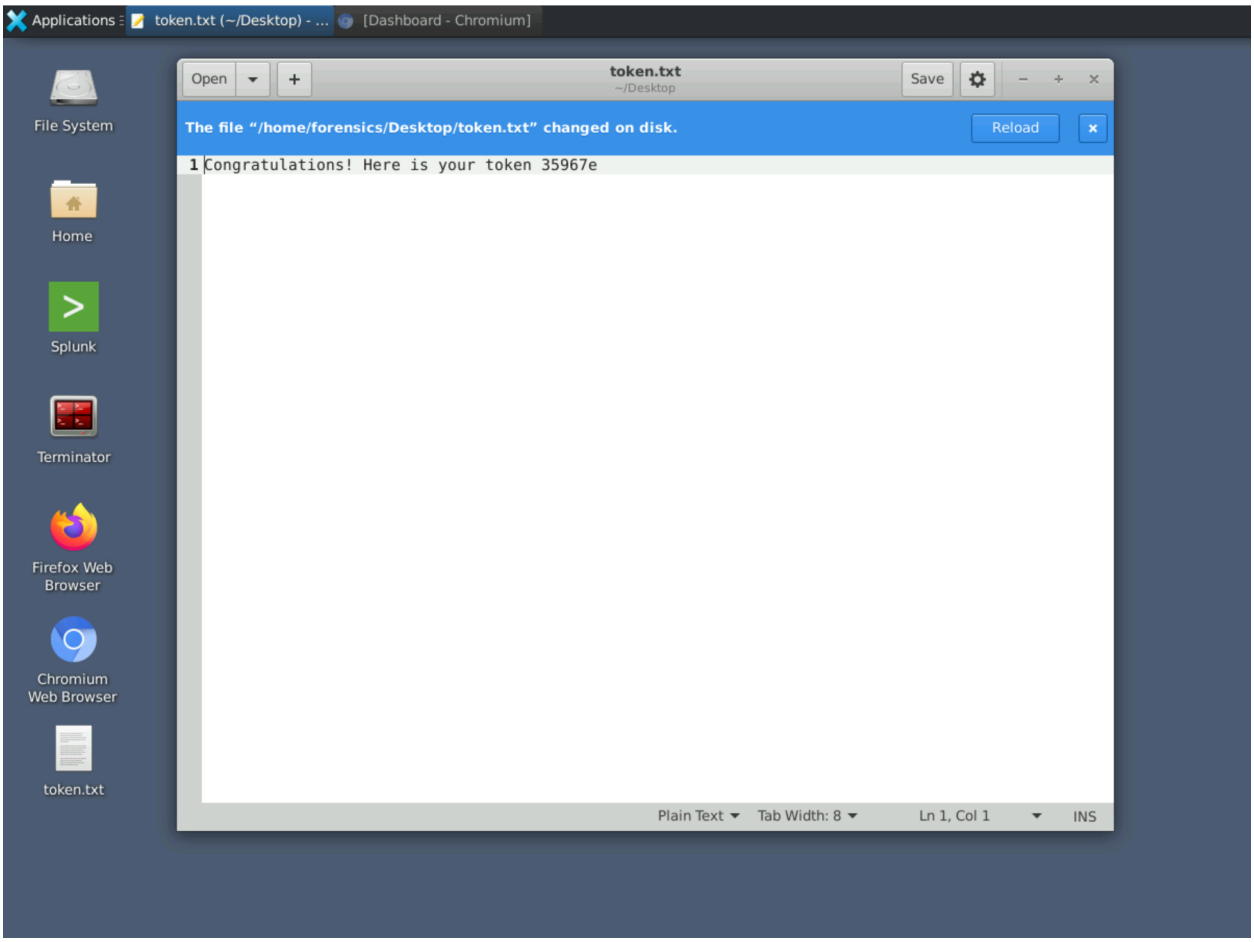
Steps I followed are shown below:



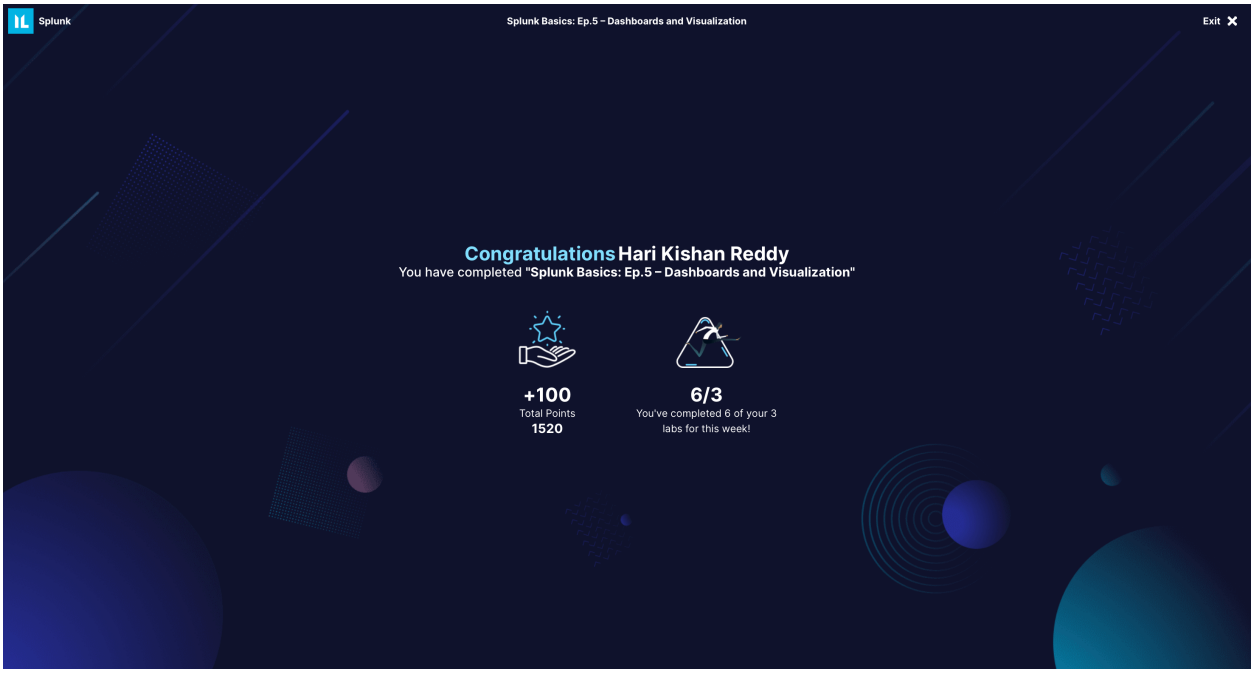




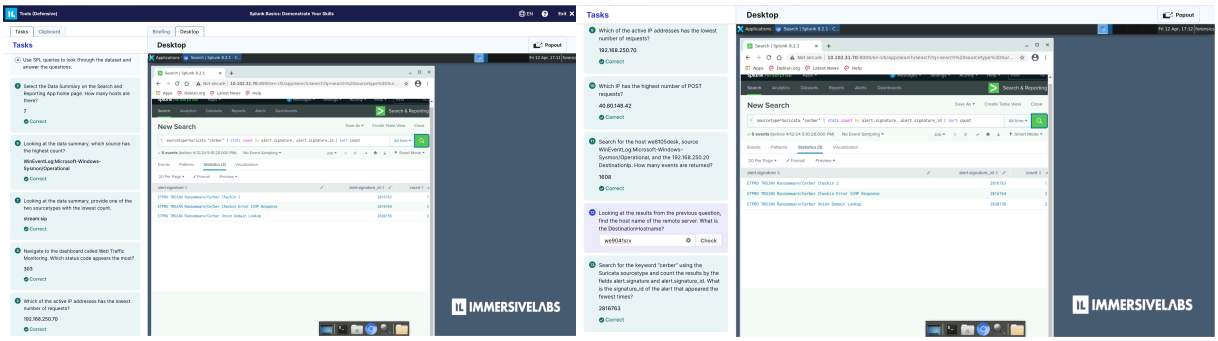

Web Traffic Monitoring
This is for the dashboard description.
Global Time Range
Last 24 hours
HTTP Status Codes Breakdown
403
400
500
404
200
303
Web Activity By IP
40.80.148.42
23.22.63.114
192.168.2.50
192.1...0.100
192.1...0.70
src_ip
0
10,000
count
Activity by HTTP Method
10,000
5,000
GET
src_ip


Applications
token.txt (~/Desktop) - ...
[Dashboard - Chromium]
File System
Home
Splunk
Terminator
Firefox Web Browser
Chromium Web Browser
token.txt
Open
token.txt
~/Desktop
Save
The file "/home/forensics/Desktop/token.txt" changed on disk.
Reload
1 Congratulations! Here is your token 35967e
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

Screenshot of lab completion:



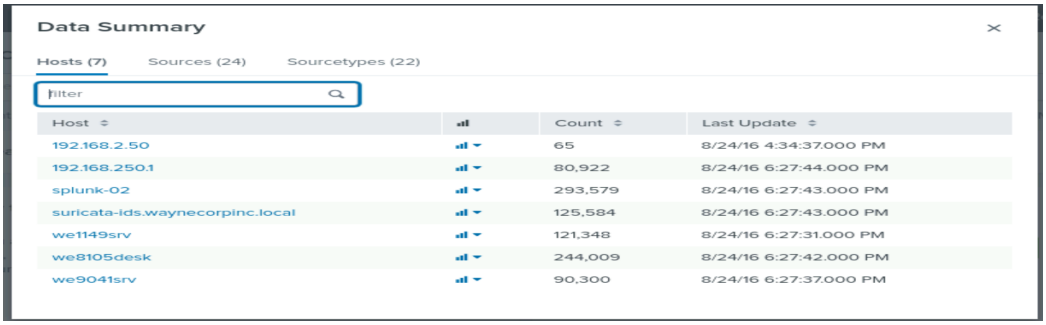
Demonstrate Your Skills: Splunk Basics



1. Select the Data Summary on the Search and Reporting App home page. How many hosts are there?

- ***Action:*** Accessed the Data Summary on the Search and Reporting App home page.

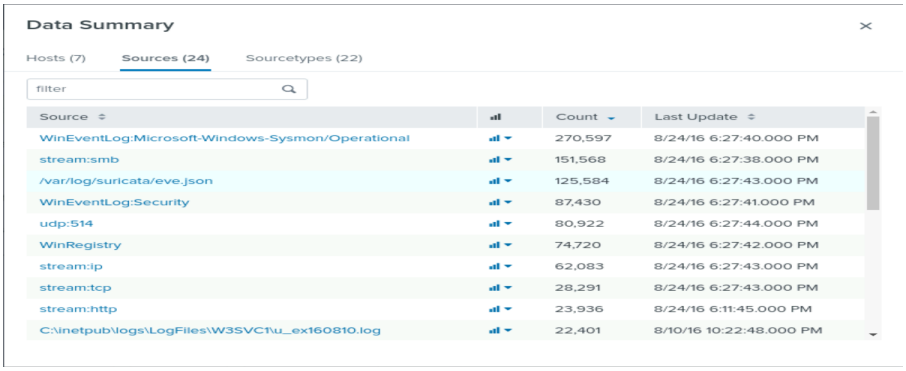
- ***Answer:*** 7



2. Looking at the data summary, which source has the highest count?

- ***Action:*** Examined the data summary to identify the source with the highest count.

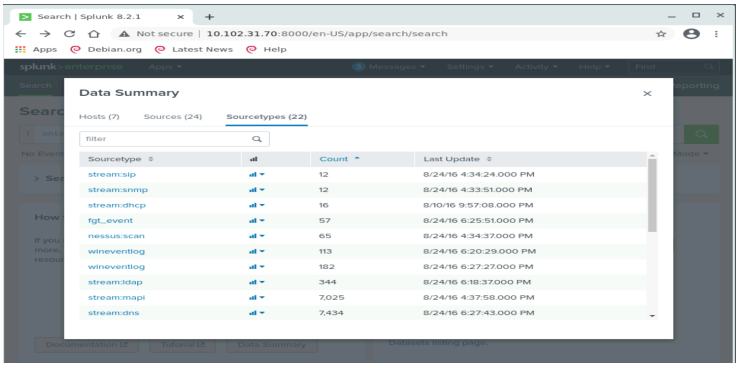
- ***Answer:*** WinEventLog:Microsoft-Windows-Sysmon/Operational



3. Looking at the data summary, provide one of the two sourcetypes with the lowest count.

- ***Action:*** Examined the data summary to identify one of the sourcetypes with the lowest count.

- ***Answer:*** stream:sip



4. Navigate to the dashboard called Web Traffic Monitoring. Which status code appears the most?

- ***Action:*** Accessed the Web Traffic Monitoring dashboard and identified the status code with the highest count.

- ***Answer:*** 303

5. Which of the active IP addresses has the lowest number of requests?

- ***Action:*** Analyzed active IP addresses and determined the one with the lowest request count.

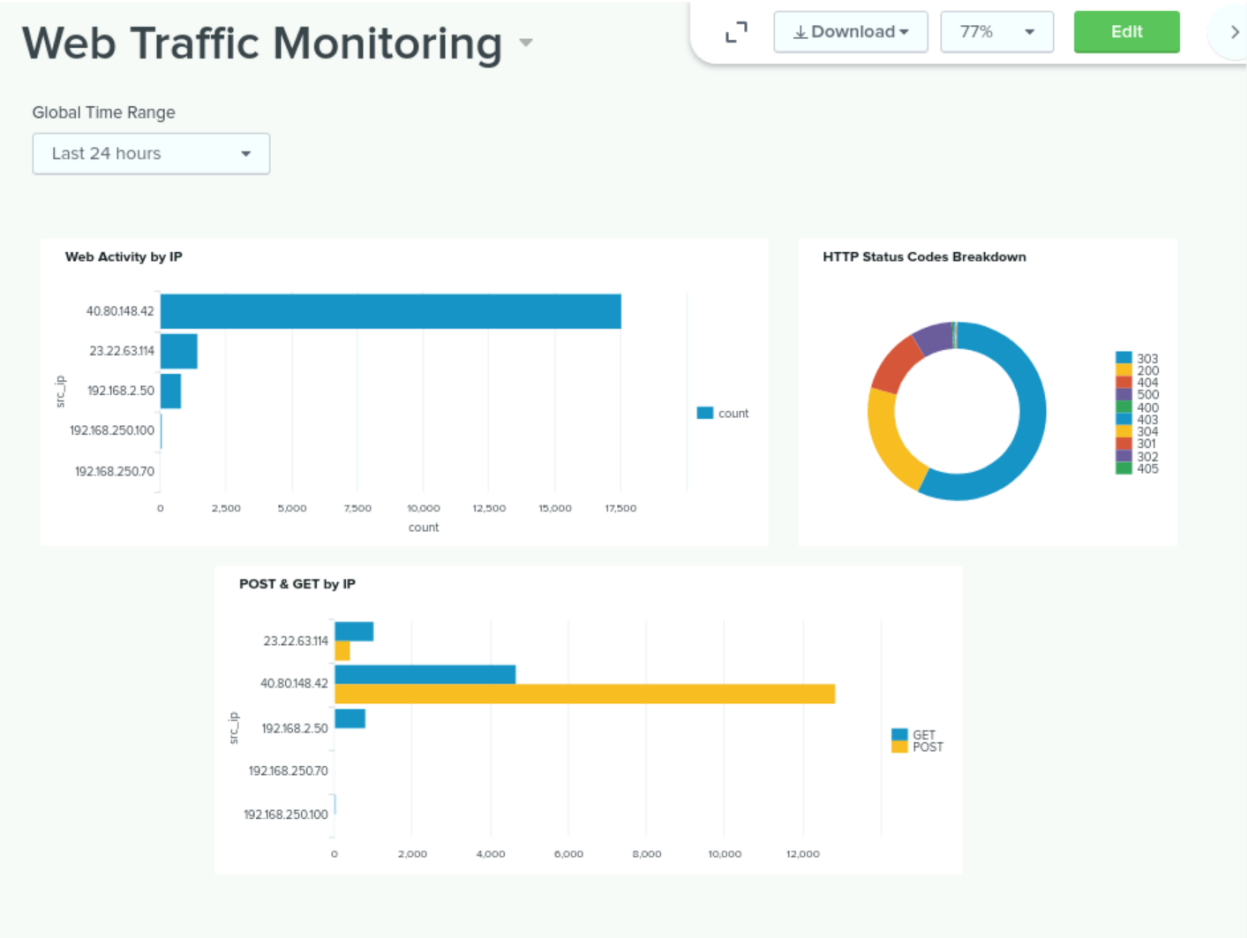
- ***Answer:*** 192.168.250.70

6. Which IP has the highest number of POST requests?

- ***Action:*** Analyzed POST requests and identified the IP with the highest count of POST requests.

- ***Answer:*** 40.80.148.42

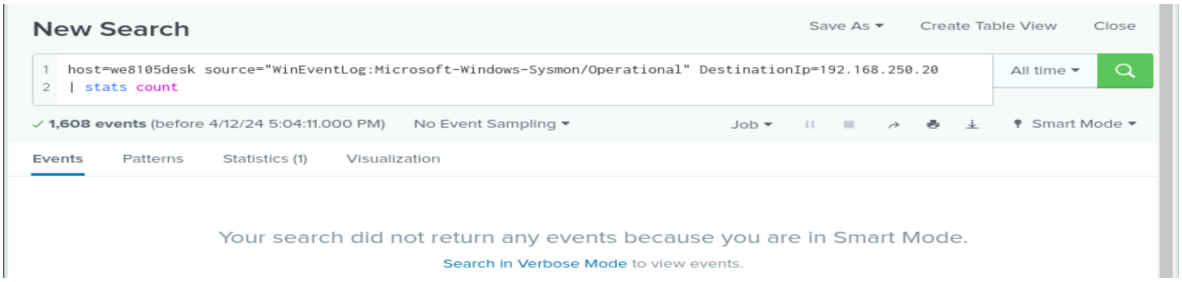
For 4,5,6 questions:



7. Search for the host we8105desk, source WinEventLog:Microsoft-Windows-Sysmon/Operational, and the 192.168.250.20 Destinationlp. How many events are returned?

- ***Command:*** `host=we8105desk sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" dest_ip=192.168.250.20 | stats count`

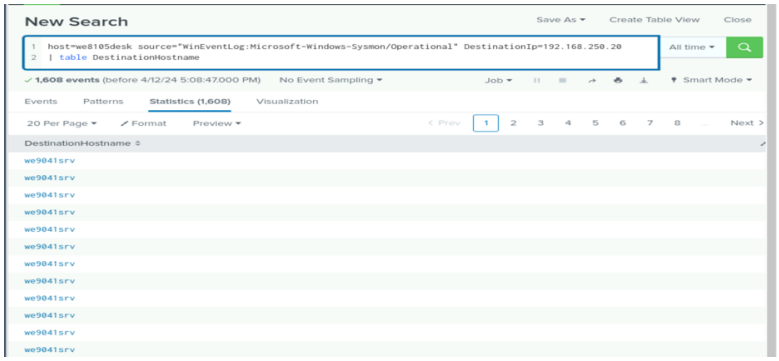
- ***Answer:*** 1608



8. Looking at the results from the previous question, find the host name of the remote server. What is the Destination Hostname?

- ***Action:*** Examined the results of the previous search and added Destination Hostname.

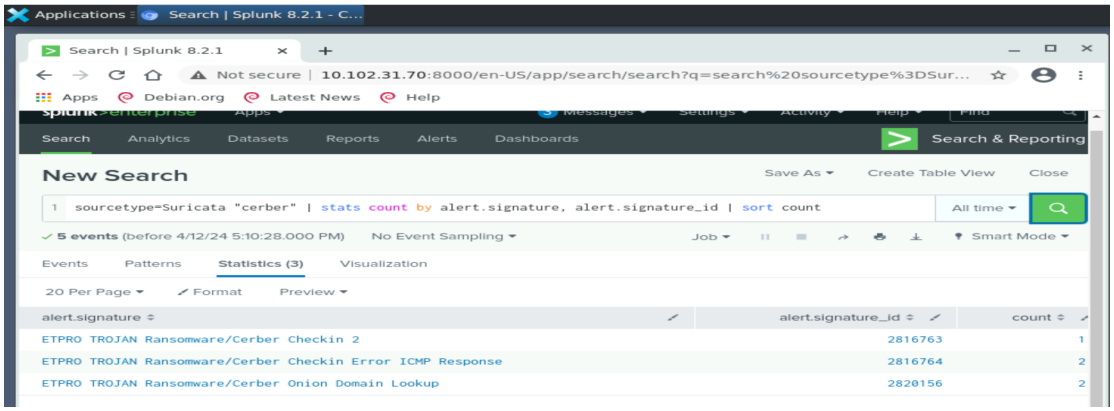
- ***Answer:*** we9041srv



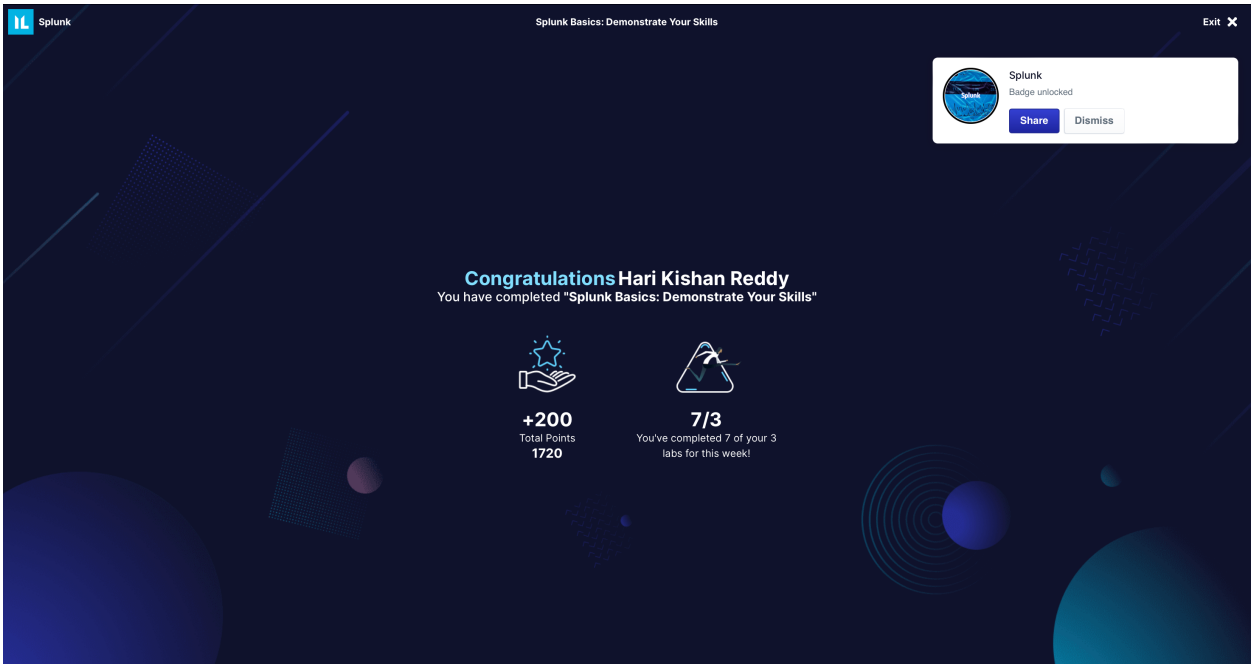
9. Search for the keyword "cerber" using the Suricata sourcetype and count the results by the fields alert.signature and alert.signature_id. What is the signature_id of the alert that appeared the fewest times?

- ***Command:*** `sourcetype=suricata "cerber" | stats count by alert.signature_id | sort count`

- ***Answer:*** 2816763



Screenshot of lab completion:



Write Up

My key learnings and takeaways:

Network Monitoring with Splunk: A Comprehensive Overview

Splunk has proven to be a powerful tool in network monitoring, offering extensive capabilities to gather, analyze, and visualize data from various sources. Through hands-on tasks and modules, I've gained valuable insights into the fundamental aspects of network monitoring using Splunk.

Data Collection and Analysis
One of the core functionalities of Splunk is its ability to collect and index data from diverse sources such as logs, events, and metrics. Using SPL queries, I learned how to search and filter data effectively, allowing me to extract valuable information and perform in-depth analysis.

Visualizations and Dashboards
Splunk's visualization features have been instrumental in creating meaningful representations of data. By creating visualizations such as charts, graphs, and data summaries, I gained a deeper understanding of network trends, anomalies, and performance metrics. Dashboards further enhanced my ability to monitor key indicators in real-time and make informed decisions.

Alerting and Monitoring
Splunk's alerting capabilities proved invaluable in proactive network monitoring. By setting up alerts based on predefined criteria, I was able to detect and respond to potential issues promptly. This proactive approach helped in ensuring network stability and security.

Incident Investigation and Response
In scenarios requiring detailed investigation, Splunk's ability to correlate and analyze vast amounts of data came to the forefront. By conducting searches across multiple data sources and applying statistical analysis, I could identify patterns, anomalies, and potential security threats. This deep dive into incident investigation enhanced my skills in threat detection and response.

Integration and Automation
Splunk's integration capabilities with other tools and systems allowed for seamless data exchange and automation of workflows. Integrating with security tools, for example, enabled me to streamline threat intelligence and incident response processes, enhancing overall network security posture.

Performance Optimization
Through performance monitoring modules, I learned to monitor network traffic, analyze resource utilization, and optimize network performance. This holistic approach to performance management ensures optimal network functioning and user experience.

Conclusion

Overall, my experience with Splunk in network monitoring was good. The platform's robust features, coupled with hands-on exercises and modules, have equipped me with essential skills in data analysis, visualization, alerting, incident response, and performance optimization. Splunk stands out as a versatile and comprehensive solution for effective network monitoring and security.