

# Network Monitoring- Lab 4

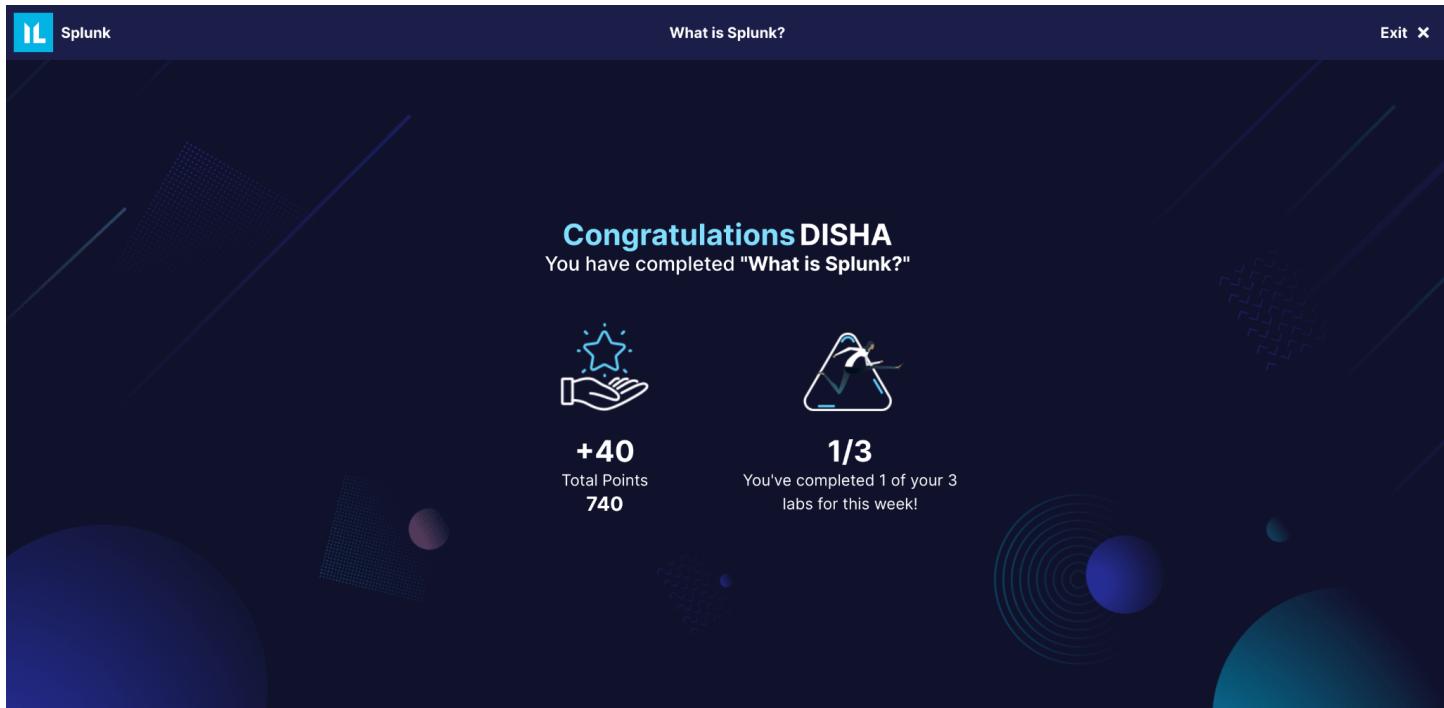
Name: Disha Sheshappa

Net ID: ds7615

Task 1: What is Splunk ?

Learnings:

- Data Source Variety: Understanding that Splunk can collect data from diverse sources such as files, network traffic, script outputs, Windows event logs, and more highlights the versatility of Splunk in handling data generated across an organization.
- Significance of Source Types: Recognizing the importance of source types in Splunk is crucial for efficient data handling. Source types determine how data is formatted and indexed, impacting the effectiveness of search queries and data analysis.
- Operational Insights: Learning about sources and source types in Splunk provides insights into efficient administration, filtering, and searching of data. This knowledge contributes to troubleshooting potential issues and identifying and preventing threats more quickly through a better understanding of data sources.

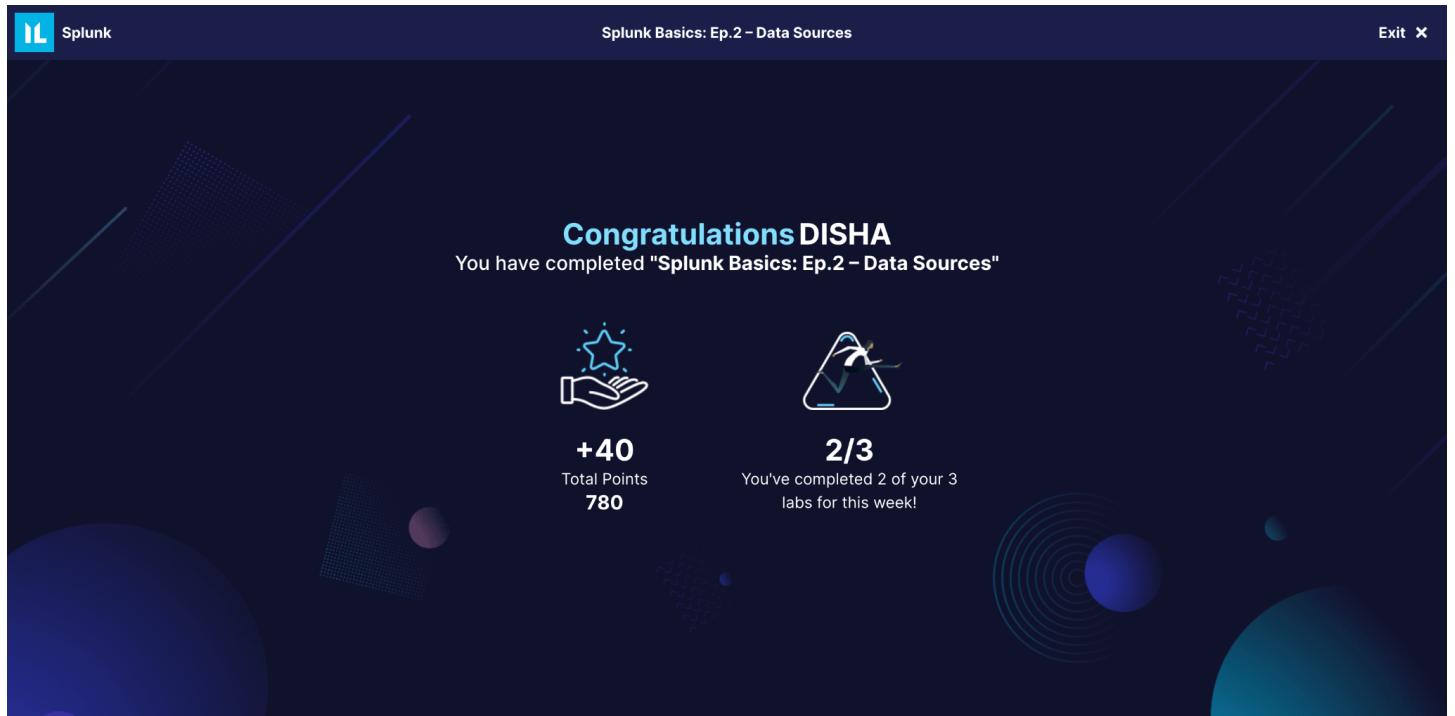


## Splunk Basics: Ep.2 – Data Sources

Learnings:

- Data Source Variety: Understanding that Splunk can collect data from diverse sources such as files, network traffic, script outputs, Windows event logs, and more highlights the versatility of Splunk in handling data generated across an organization.
- Significance of Source Types: Recognizing the importance of source types in Splunk is crucial for efficient data handling. Source types determine how data is formatted and indexed, impacting the effectiveness of search queries and data analysis.

- Operational Insights Learning about sources and source types in Splunk provides insights into efficient administration, filtering, and searching of data. This knowledge contributes to troubleshooting potential issues and identifying and preventing threats more quickly through a better understanding of data sources.



## Splunk Basics: Ep.3 – Search

Q1 : Perform a search for the domain “imreallynotbatman.com”. How many events are returned?

Answer: The query returned 78,683 entries. When we directly give the domain name in the search bar it searches for the string in all the possible fields instead of limiting itself to one single field.

The screenshot shows the Splunk interface for "Splunk Basics: Ep.3 – Search". The search bar at the top contains the query "imreallynotbatman.com". Below the search bar, it says "78,683 events (before 11/30/23 10:33:10.000 PM) No Event Sampling". The main area displays a timeline visualization of the events. A table below the timeline shows event details, with the first few rows being:

Time	Event
8/10/16 10:23:09.473 PM	<pre> app_proto: http dest_ip: 40.80.148.42 dest_port: 49501 event_type: fileinfo fileinfo: f+1 </pre>

Q2: Perform a search for the domain “imreallynotbatman.com”, this time including the field “http\_method=POST”. How many events are returned?

Answer: the query returned 14,238 events. The search in the previous question only searched for the domain name. We added further refinement to it by mentioning http\_method as POST. Hence the number of events filtered are less compared to previous one.

The screenshot shows a Splunk search interface titled "Splunk Basics: Ep.3 – Search". The search bar contains the query "imreallynotbatman.com http\_method=POST". The results summary indicates 14,238 events found between Nov 30, 2023, and Nov 30, 2023, at 10:36:21.000 PM. The "Events (14,238)" tab is selected. The timeline visualization shows a dense series of green bars representing event times. Below the timeline is a table view of the first few events, showing fields like host, source, accept, and bytes. The table has columns for Time, Event, and a header row with icons for List, Format, and 20 Per Page.

Q3: 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?

Answer: 988.

The search query explicitly mentions the status to be of value 500. All the other statuses are ignored. This kind of query can be used when we need to focus on only outcome and ignore rest of the noise.

The screenshot shows a Splunk search interface titled "Splunk Basics: Ep.3 – Search". The search bar contains the query "imreallynotbatman.com http\_method=POST status=500". The results summary indicates 988 events found between Nov 30, 2023, and Nov 30, 2023, at 10:55:45.000 PM. The "Events (988)" tab is selected. The timeline visualization shows a series of green bars. Below the timeline is a table view of the first few events, showing fields like host, source, accept, and bytes. The table has columns for Time, Event, and a header row with icons for List, Format, and 20 Per Page.

Q4: Expand the search query from the previous question to also include all "status=4\*" results. How many events are returned?

Answer: the number of entries returned is 1,171.

The search query used is [imreallynotbatman.com](http://imreallynotbatman.com) http\_method=POST (status=4\* OR status=500). We are making use of OR operator here to filter entries which either have status 500 or any status starting with 4.

The screenshot shows the Splunk search interface with the following details:

- Header:** Tools (Defensive) | Desktop, Splunk Basics: Ep.3 – Search, Thu 30 Nov, 22:47 forensics
- Search Bar:** Applications, Search | Splunk 8.2.1 - C..., Search | Splunk 8.2.1, Help - Splunk
- Search Query:** imreallynotbatman.com http\_method=POST (status=4\* OR status=500)
- Results Summary:** 1,171 events (before 11/30/23 10:46:53.000 PM), No Event Sampling
- Event List:** Shows a timeline from 8/10/16 to 10/22/25 297 PM. The results show a series of green bars representing event counts across different time intervals.
- Selected Fields:** host 1, source 1, sourcetype 1
- Interesting Fields:** accept 1, \_bytes\_in\_ 5, \_bytes\_out\_ 4

Q5: Perform a search for the filepath "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp". How many events does it appear in?

Answer: 189

In this case if we directly search the string in the search bar we will not get any result. The key here is to enclose the string within double quotes. This is a necessary step for file paths containing spaces. As space is considered as start of new keyword in splunk.

The screenshot shows the Splunk search interface with the following details:

- Header:** Tools (Defensive) | Desktop | Splunk Basics: Ep.3 – Search | Thu 30 Nov, 22:49 forensic
- Search Bar:** Applications | Search | Splunk 8.2.1 - C... | Search | Splunk 8.2.1 | Help - Splunk
- Toolbar:** Apps, Debian.org, Latest News, Help
- Navigation:** Search, Analytics, Datasets, Reports, Alerts, Dashboards
- Search Results:** New Search | 1 "C:\\Users\\bob.smith.WAYNECORPINC\\AppData\\Roaming\\121214.tmp"
- Event List:** 189 events (before 11/30/23 10:49:28.000 PM) | No Event Sampling | All time | Smart Mode
- Event Types:** Events (189), Patterns, Statistics, Visualization
- Timeline:** Format Timeline | Zoom Out | +Zoom to Selection | Deselect | 1 second per column
- Event Preview:** List View | Format View | 20 Per Page | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... | Next >
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** Channel, CurrentDirectory, LogonGUID, LogonID, IntegrityLevel, Hashes
- Event Data Preview:** XML snippet showing event details like provider name, timestamp, and logon information.

## Learnings:

- Basic Search Structure: Understood the core structure of Splunk searches, which consists of a series of instructions separated by the pipe symbol (|), allows for more effective data exploration.
- Search Pipeline: The search pipeline idea allows for step-by-step refining and augmentation of search results by chaining consecutive instructions together using the pipe character.
- Fields and Filtering: Understanding the role of fields in Splunk searches and their use as searchable key/value pairs aids in successful data filtering and refining.
- Boolean Expressions: Learned how to utilize Boolean expressions (AND, OR, NOT) and parenthesis in search queries to combine numerous search phrases for accurate results.
- Wildcard Usage and Escaping Characters: Utilizing wildcards, such as the asterisk (\*) as a placeholder, and understanding the need to escape characters like quotes and backslashes enhances the flexibility and accuracy of search queries, especially in scenarios like searching for Windows file paths.
- Using wildcards as placeholders, such as the asterisk (\*), and understanding the need to escape characters such as quotes and backslashes improves the flexibility and accuracy of search queries, especially when searching for Windows file paths.

The screenshot shows the Splunk Labs search interface. At the top, there's a navigation bar with tabs for 'Tasks' and 'Clipboard'. Below that is a 'Briefing' tab and a 'Desktop' tab. The main area is titled 'Briefing' and contains several search tasks:

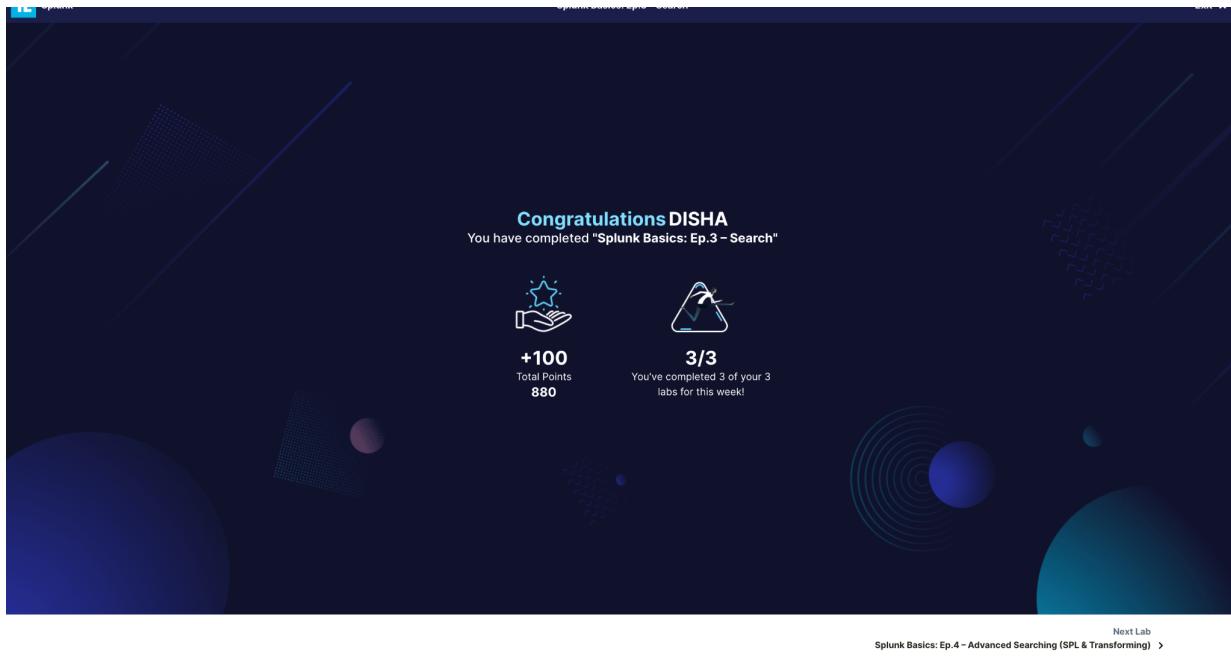
- Task 4: Perform a search for the domain "imreallynotbatman.com". How many events are returned? Result: 78,683. Status: Correct.
- Task 5: Perform a search for the domain "imreallynotbatman.com", this time including the field "http.method=POST". How many events are returned? Result: 14,238. Status: Correct.
- Task 6: 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? Result: 988. Status: Correct.
- Task 7: Expand the search query from the previous question to also include all "status=4\*" results. How many events are returned? Result: 1171. Status: Correct.
- Task 8: Perform a search for the filepath "C:\Users\bob.smith\WAYNECORPINC\AppData\Roaming\1121214.tmp". How many events does it appear in? Result: 189. Status: Check.

In the center, there's a code editor window showing a search command:

```
3 | web_error
4 | "web_error"
5 | index="webmain"
```

A tooltip explains Boolean operators: AND, OR, and NOT. It also discusses the use of parentheses and the AND operator being implied between terms. The asterisk (\*) is used as a wildcard placeholder. A search assistant feature is mentioned, showing autocomplete suggestions for "myhost".

On the right side, there's a sidebar titled "ON THIS PAGE" with links to various Splunk search concepts: Note, About Search, Anatomy of a search, Search visualisation, Search pipeline, Fields, Quotes and escaping characters, Basic Search usage, Using fields to search, Interpreting the results, and In this lab.



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

Q1: 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?

Answer: 68

This task gives us an overview of how to make sense of the statistics tab in the splunk to get an aggregated view.

http_method	count	percent
POST	14248	68.087547

Q2: Perform a search that lists only the least common (rare) “status” field value from the index “botsv1”. What is the status code given?

Answer: 206

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

Thu 30 Nov, 23:41 | forensics

Search | Splunk 8.2.1 - C...

Not secure | 10.102.104.77:8000/en-US/app/search/search?q=search%20index%3D"botsv1"%20%0A%7C%20rare%20status%20limit%3D1&display.page=search.m...

Apps Debian.org Latest News Help

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Messages Settings Activity Help Find

New Search

```
1 index="botsv1"
2 | rare status limit=1
```

955,807 events (before 11/30/23 11:37:31.000 PM) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

status	count	percent
206	1	0.000549

Q3: 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?

Answer: 3

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

Thu 30 Nov, 23:49 | forensics

Search | Splunk 8.2.1 - C...

Not secure | 10.102.104.77:8000/en-US/app/search/search?q=search%20index%3D"botsv1"%20source%3D"WinEventLog%3AMicrosoft-Windows-Sysmon%2FOpera...

Apps Debian.org Latest News Help

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Messages Settings Activity Help Find

New Search

```
1 index="botsv1" source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
2 | stats count by EventID
3 | sort -count
```

87,500 of 87,500 events matched No Event Sampling

Events Patterns Statistics (5) Visualization

20 Per Page Format Preview

EventID	count
7	57569
3	17248
1	89
5	89
2	5

Q4: 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').

Answer: 40.80.148.42

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

Thu 30 Nov, 23:59 | forensics

Search | Splunk 8.2.1 - C... | Applications

Not secure | 10.102.104.77:8000/en-US/app/search/search?q=search%20imreallynotbatman.com%20%0A%7C%20top%20src\_ip&display.page=search.mode=smart...

Apps Debian.org Latest News Help

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 | imreallynotbatman.com  
2 | top src\_ip

78,683 events (before 11/30/23 11:58:49.000 PM) No Event Sampling

Events Patterns Statistics (3) Visualization

20 Per Page Format Preview

src_ip	count	percent
40.80.148.42	34967	70.865168
192.168.250.70	11493	23.292058
23.22.63.114	2883	5.842774

Q5: Perform a search using the domain and IP address from the previous question. What is the top 'alert.signature' field value reference?

Answer: ET WEB\_SERVER Script tag in URI, Possible Cross Site Scripting Attempt

In this case our speculation from the previous answer that there might be an attack on the concerned IP is conformed.

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

Fri 01 Dec, 00:10 | forensics

Search | Splunk 8.2.1 - C... | Applications

Not secure | 10.102.52.125:8000/en-US/app/search/search?q=search%20imreallynotbatman.com%20src\_ip%20%3D%2040.80.148.42%0A%7C%20top%20alert.sig...

Apps Debian.org Latest News Help

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 | imreallynotbatman.com src\_ip = 40.80.148.42  
2 | top alert.signature

34,967 events (before 12/1/23 12:10:17.000 AM) No Event Sampling

Events Patterns Statistics (10) Visualization

20 Per Page Format Preview

alert.signature	count	percent
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	103	21.775899
ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	48	10.147992
ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	41	8.668076
SURICATA HTTP Host header invalid	35	7.399577
ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	33	6.976744
ET WEB_SERVER SQL Injection Select Sleep Time Delay	32	6.765328
ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	18	3.885497

Q6: Using the previously discovered ‘attacker IP’, determine the IP address of the web server being targeted by incoming attacker activity.

Answer: 192.168.250.70

In this case we are able to find the source where attack is coming from. This can be further used to get more information of the attacker. Also to block the attacker.

The screenshot shows the Splunk search interface with the following details:

- Search Query:** 1 imreallynotbatman.com src\_ip = 40.88.148.42  
2 | top dest\_ip
- Results Summary:** ✓ 34,967 events (before 12/1/23 12:04:27000 AM) No Event Sampling ▾
- Statistics View:** Statistics (2) selected. Shows a table with one row:

dest_ip	count	percent
192.168.250.70	34965	99.994280
192.168.250.40	2	0.005720
- Toolbar:** Includes icons for Home, Search, File, and others.

## Learnings:

- Understanding Search Processing Language (SPL), Splunk's query language, is critical for dealing with event data, allowing for a wide variety of activities such as searching, filtering, and altering data.
- SPL Components: Understanding essential components like search words, commands, functions, arguments, and clauses lays the groundwork for creating successful and exact search queries in Splunk.
- Learning converting commands such as Chart, Timechart, Stats, Top, and Rare enables the construction of visualizations and reports, assisting in the understanding of patterns and statistical summaries within the data.
- Subsearches: Recognizing subsearches as a strategy for narrowing down events by utilizing the results of one search as evidence for another improves the capacity to mix and evaluate diverse sets of data.
- Practical Application: The lab activities show how to use SPL commands and techniques in real-world situations, such as recognizing common and unusual field values, counting events based on certain criteria, and tracking probable attack scenarios using real-world data.

**Tasks**

**Machines**

Double click the **Splunk** icon on the **Desktop** to launch the application.

Click on the **'Search & Reporting'** app in the sidebar.

Apply filters in search to transform certain pieces of data within the dataset.

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

68.087547

Correct

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

206

Correct

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?

3

Correct

Perform a search for the domain `"microsoftbadman.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 web_ip`).

40.80148.42

Correct

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

ET WEB\_SERVER Script tag in URI, Possible Cross Site Scripting Attempt

Correct

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

192.168.250.74

Check

**Briefing**

**Commands**

Commands indicate certain actions that you want to perform on the results of a given search. This can include formatting, filtering, sorting, altering, counting, renaming, or generating commands. For example, the `stats` command can be used to generate statistics for the data contained within specific fields:

`stats ...`

All the available commands, along with a description of each one, can be found in Splunk's [command quick reference](#).

**Functions**

Functions are used to specify what sort of computation is performed on certain fields. They're often used alongside statistical commands, such as `stats`. Some common statistical functions are `avg`, `sum`, `min`, `max`, `count`, `where`, `format`, `sort`, and `order`.

`stats max(...)`

See the Splunk documentation for details of available [statistical functions](#), [evaluation functions](#), [comparison and conditional](#), [mathematical functions](#), and more.

**Arguments**

SPL commands can take arguments that are either optional or required. In the latter case, Splunk will throw an error if an argument is not supplied. Arguments require either a field name, value, or boolean operators `AND`, `OR`, `NOT`.

`stats max((field))`

See the Splunk documentation for details of available [arguments](#) and their uses.

**Classes**

Classes are used to group or re-name fields included in a search to format the results in a specific way. Common examples include the `(A)` clause, which sorts results by a certain field, the `(B)` clause, used for sorting and filtering, and the `(C)` clause, which renames fields in your results.

Both the `(A)` and `(B)` clauses are generally used alongside search terms to specify what will be included in a search. The `(B)` clause is implied by search terms unless specified otherwise.

`stats max((field)) AS (fields)`

See the Splunk documentation for details of available [classes in SPL](#) and their uses.

The diagram illustrates the execution flow of the SPL command. It starts with the command `stats max((field)) AS (fields)` at the top. Arrows point down to four boxes: `The first part indicates the initial data to be processed`, `PIPE: The data is then separated by the pipe (|) character`, `FUNCTION: The stats command is run to calculate the number of times the given data appears`, and `COMMAND: The data is grouped with the (B) command -> sort`. An arrow points from the `FUNCTION` box to the `PIPE` box. Another arrow points from the `COMMAND` box to the `PIPE` box. A large bracket at the bottom groups the `PIPE`, `FUNCTION`, and `COMMAND` boxes, with an arrow pointing to it from the `AS (fields)` part of the original command. Below this bracketed group, an arrow points to the `(A)` and `(B)` clauses of the command. Finally, an arrow points from the `(A)` and `(B)` clauses to the `(C)` clause, which is labeled `CLAUSE: The total count of the data to then return -> field`.

**Basic transforming commands and searches**

Transforming commands are used to order the results of a search into statistical data tables. As the name implies, these commands "transform" specific event data cell values into numerical values/data structures

**ON THIS PAGE**

Advanced search  
Splunk's SPL (Search Processing Language)  
Search terms

**Commands**  
**Functions**  
**Arguments**  
**Clauses**

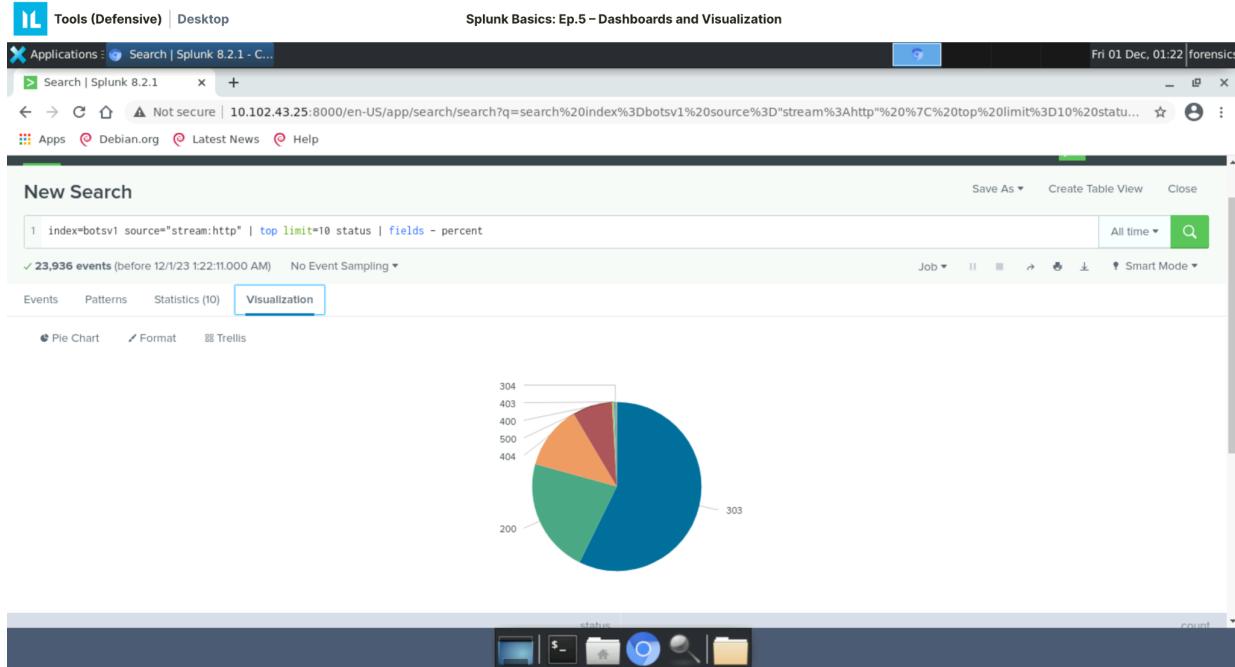
**Basic transforming commands and searches**

Chart  
Timechart  
Stats  
Top  
Rare  
Subsearches  
In this lab

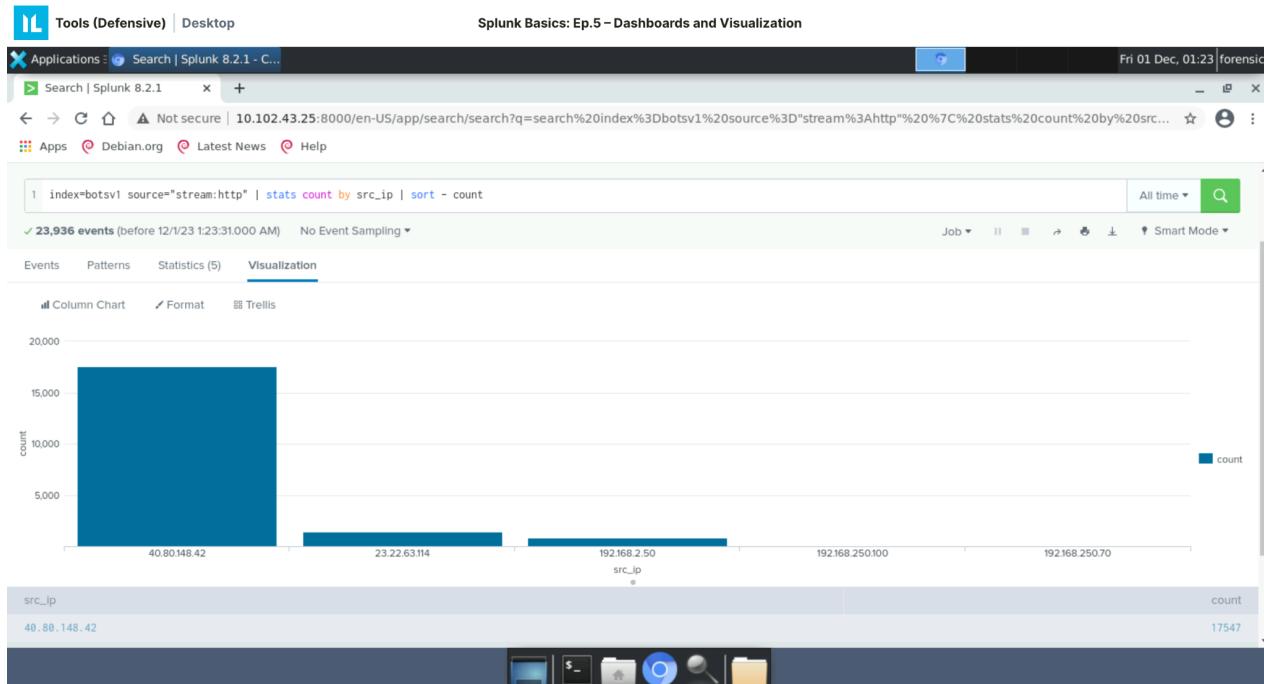
The image shows a completion screen for a Splunk Basics course. At the top left is the Splunk logo. The top center displays the title "Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)". On the top right is an "Exit" button with a close icon. The main message in the center says "Congratulations DISHA" and "You have completed 'Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)'". Below this are two achievement icons: one showing a hand holding three stars with the text "+200 Total Points 1080", and another showing a triangle with a checkmark inside with the text "4/3 You've completed 4 of your 3 labs for this week!". The background features abstract geometric shapes like triangles and circles in shades of blue and white.

# Splunk Basics: Ep.5 - Dashboards and Visualization

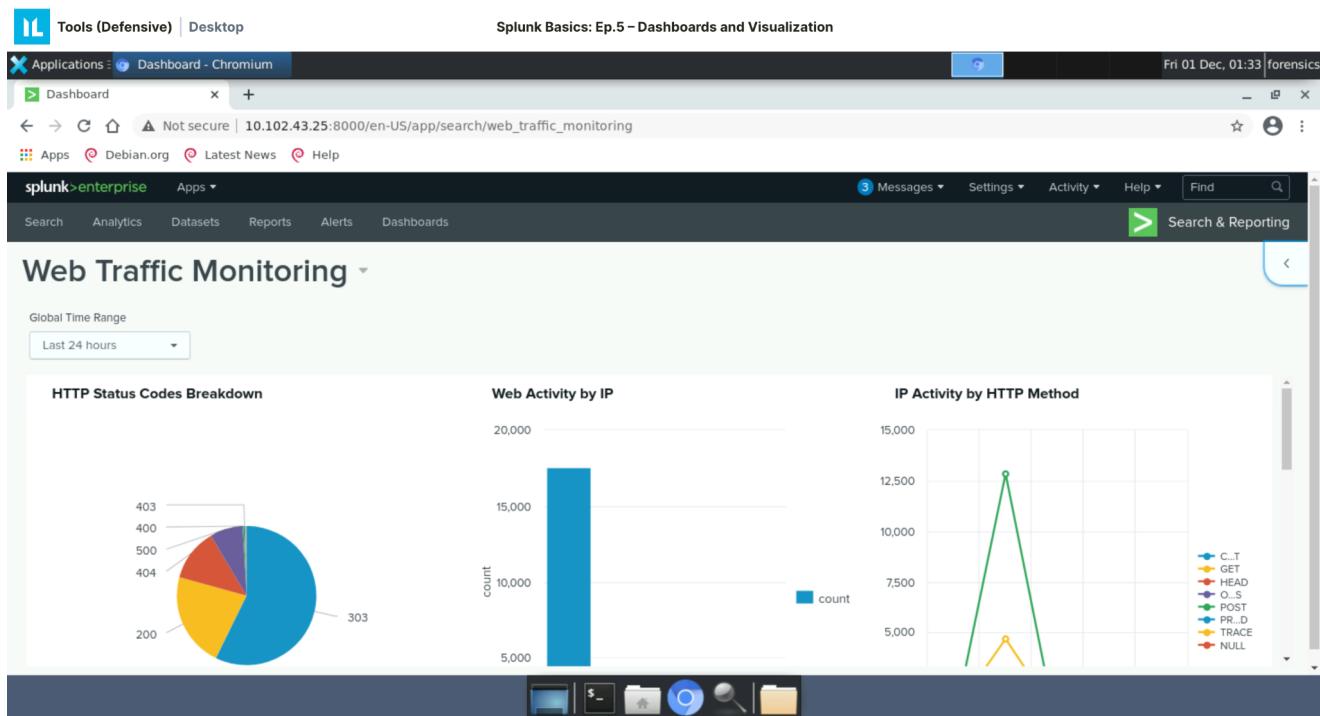
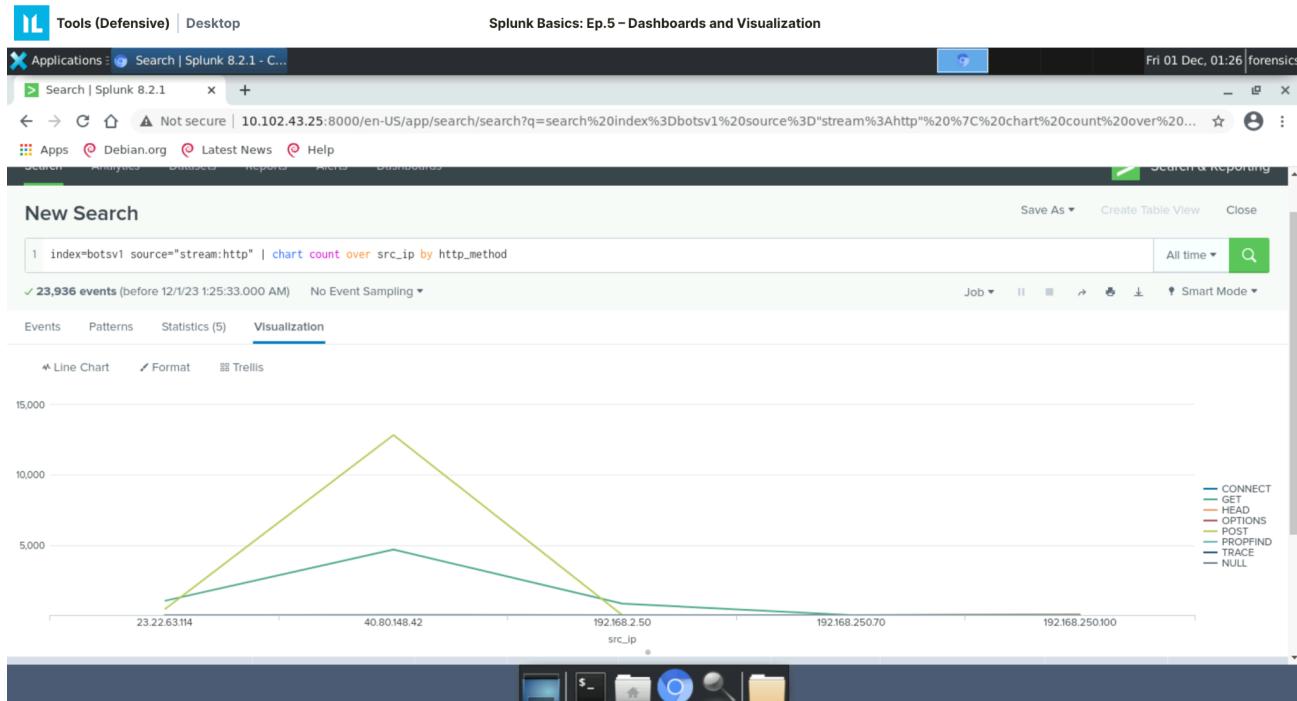
## First chart



## Second chart



### Third Chart:



### Learnings:

- **Dashboard Creation:** The lab gave hands-on experience in developing a dashboard in Splunk, highlighting the necessity of structuring and visualizing summary data.
- **Visualization Types:** Understanding how to translate search results into multiple visualization forms, such as Pie Charts, Bar Charts, and Line Charts, improves the capacity to effectively present data insights.

- Dashboard Customization: The process of adding, naming, and organizing visualizations inside a dashboard was explained, demonstrating how to modify dashboards to specific monitoring and data presentation needs.

Final Token:

Splunk Basics: Ep.5 – Dashboards and Visualization

EN Exit X

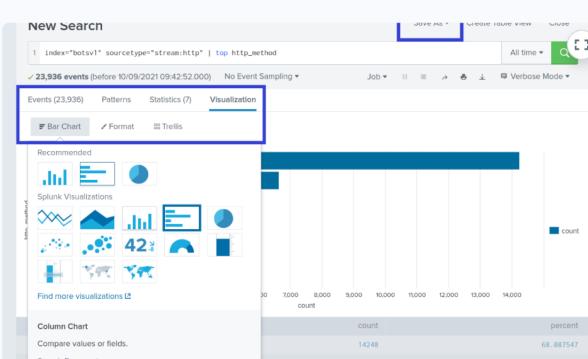
Tasks Clipboard Briefing Desktop Popout

### Tasks

- ② Navigate to the “Search & Reporting” app in the sidebar.
- ③ Search for the provided data.
- ④ Save your searches as visualizations and add them to a dashboard.
- ⑤ After you’ve added all three visualizations, navigate to the dashboard page and select your Web Traffic Monitoring dashboard. Click on ‘Edit’ at the top right and adjust your visualizations, by resizing and dragging them to match the background template.
- ⑥ Once you’re finished, click on “Save” to save your dashboard. If done correctly, you’ll receive a token.txt file on the desktop.
- ⑦ What is the token you receive for completing the game?  
 Check

### Briefing

This can be achieved by selecting “Create” at the top right corner of the search page.



**ON THIS PAGE**

- What is data visualization?
- What are dashboards?
- Why use dashboards?
- Adding visualizations to a dashboard
- In this lab

**In this lab**

In this lab, you need to create a new dashboard that displays a summary of the web traffic. A dashboard template has been created for you in advance, which, during the course of completing the lab tasks, you will add visualizations to. This is found within the Dashboards app under the name “Web Traffic Monitoring”.

Splunk Basics: Ep.5 – Dashboards and Visualization

Exit X

**Congratulations DISHA**  
You have completed "Splunk Basics: Ep.5 – Dashboards and Visualization"

 +100 Total Points 1180

 5/3 You've completed 5 of your 3 labs for this week!

Next Lab Demonstrate Your Skills: Splunk Basics >

## Demonstrate Your Skills: Splunk Basics

Q1: Select the Data Summary on the Search and Reporting App home page. How many hosts are there?

Answer: 7

The screenshot shows the Splunk 8.2.1 interface. The title bar reads "Demonstrate Your Skills: Splunk Basics". The main search bar at the top has the URL "10.102.122.102:8000/en-US/app/search/search". The left sidebar is titled "Search" and includes sections for "Search", "Analytics", "Datasets", and "Reports". The "Search" section has a search bar with placeholder text "enter search here...". Below it is a "How to Search" section with a link to documentation. The central area displays a "Data Summary" table. The table has three tabs: "Hosts (7)", "Sources (24)", and "Sourcetypes (22)". The "Hosts (7)" tab is selected. The table lists the following hosts:

Host	Count	Last Update
192.168.2.50	65	8/24/16 4:34:37.000 PM
192.168.2501	80,922	8/24/16 6:27:44.000 PM
splunk-02	293,579	8/24/16 6:27:43.000 PM
suricata-ids.waynecorpinc.local	125,584	8/24/16 6:27:43.000 PM
we1149srv	121,348	8/24/16 6:27:31.000 PM
we8105desk	244,009	8/24/16 6:27:42.000 PM
we9041srv	90,300	8/24/16 6:27:37.000 PM

Q2: Looking at the data summary, which source has the highest count?

Answer: WinEventLog:Microsoft-Windows-Sysmon/Operational

The screenshot shows the Splunk 8.2.1 interface, identical to the previous one but with a different table selection. The title bar reads "Demonstrate Your Skills: Splunk Basics". The main search bar at the top has the URL "10.102.122.102:8000/en-US/app/search/search". The left sidebar is titled "Search" and includes sections for "Search", "Analytics", "Datasets", and "Reports". The "Search" section has a search bar with placeholder text "enter search here...". Below it is a "How to Search" section with a link to documentation. The central area displays a "Data Summary" table. The table has three tabs: "Hosts (7)", "Sources (24)", and "Sourcetypes (22)". The "Sources (24)" tab is selected. The table lists the following sources:

Source	Count	Last Update
WinEventLog:Microsoft-Windows-Sysmon/Operational	270,597	8/24/16 6:27:40.000 PM
stream:smb	151,568	8/24/16 6:27:38.000 PM
/var/log/suricata/eve.json	125,584	8/24/16 6:27:43.000 PM
WinEventLog:Security	87,430	8/24/16 6:27:41.000 PM
udp:514	80,922	8/24/16 6:27:44.000 PM
WinRegistry	74,720	8/24/16 6:27:42.000 PM
stream:ip	62,083	8/24/16 6:27:43.000 PM
stream:tcp	28,291	8/24/16 6:27:43.000 PM
stream:http	23,936	8/24/16 6:11:45.000 PM
C:\inetpub\logs\LogFiles\W3SVC1\_\ex160810.log	22,401	8/10/16 10:22:48.000 PM

Q3: Looking at the data summary, provide one of the two sourcetypes with the lowest count.

Answer: stream:snmp

Splunk Basics

Demonstrate Your Skills: Splunk Basics

Applications Search | Splunk 8.2.1 - C... Search | Splunk 8.2.1 Fri 01 Dec, 02:16 forensics

Not secure | 10.102.122.102:8000/en-US/app/search/search

Apps Debian.org Latest News Help

splunk>enterprise Apps

Search Analytics Datasets Reports

Search

1 enter search here...

No Event Sampling > Search History

How to Search

If you are not familiar with the search features, click the following resources:

Documentation Tutorial Data

Data Summary

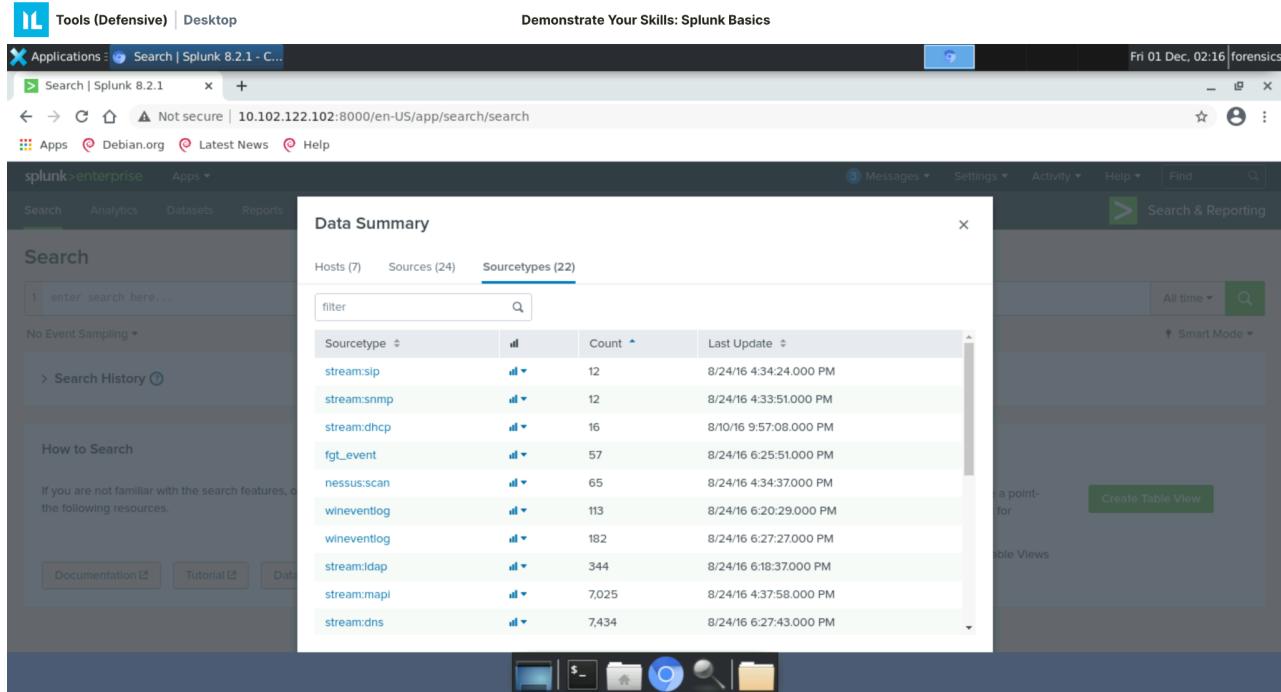
Hosts (7) Sources (24) Sourcetypes (22)

filter

Sourcetype	Count	Last Update
stream:sip	12	8/24/16 4:34:24.000 PM
stream:snmp	12	8/24/16 4:33:51.000 PM
stream:dhcp	16	8/10/16 9:57:08.000 PM
fgt_event	57	8/24/16 6:25:51.000 PM
nessus:scan	65	8/24/16 4:34:37.000 PM
wineventlog	113	8/24/16 6:20:29.000 PM
wineventlog	182	8/24/16 6:27:27.000 PM
stream:ldap	344	8/24/16 6:18:37.000 PM
stream:mapi	7,025	8/24/16 4:37:58.000 PM
stream:dns	7,434	8/24/16 6:27:43.000 PM

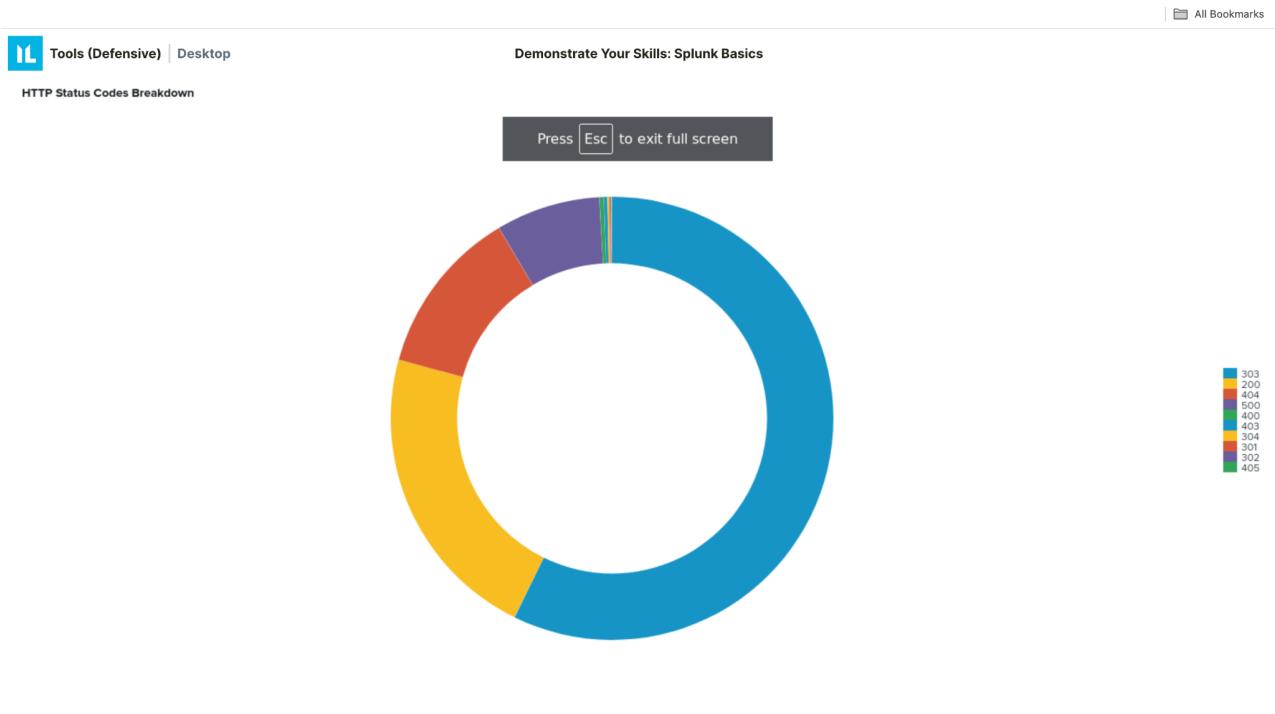
All time Smart Mode

Create Table View



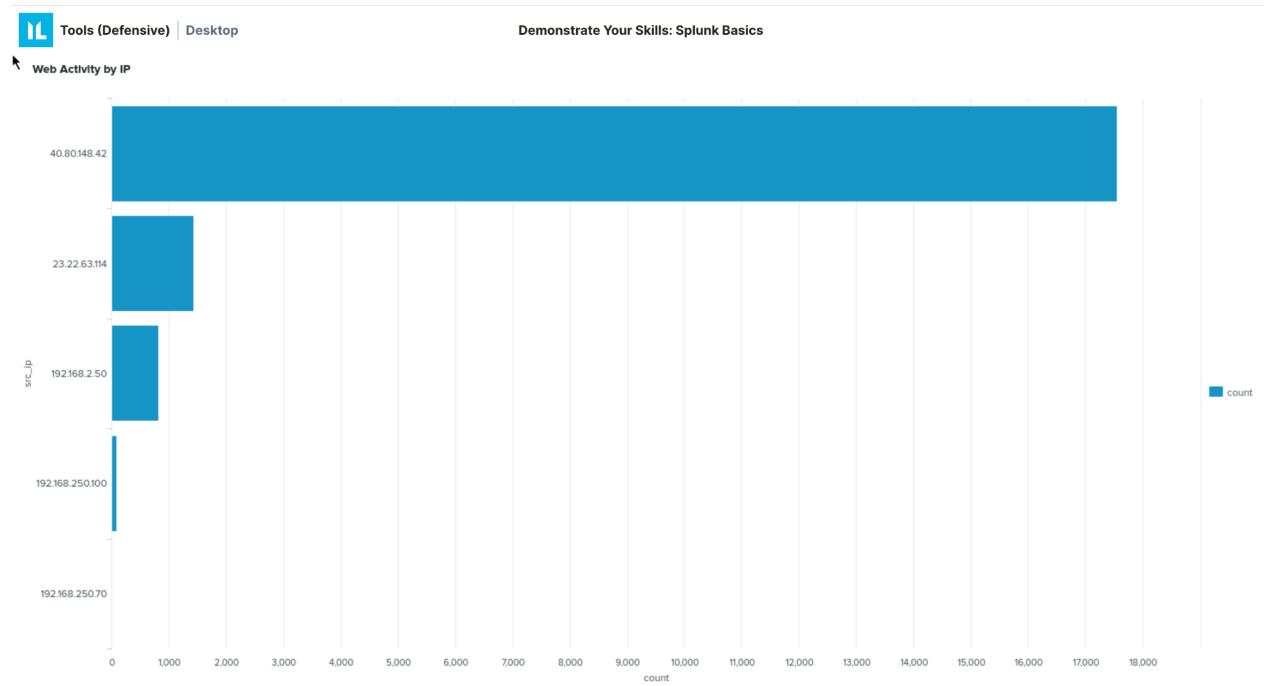
Q4: Navigate to the dashboard called Web Traffic Monitoring. Which status code appears the most?

Answer: 303



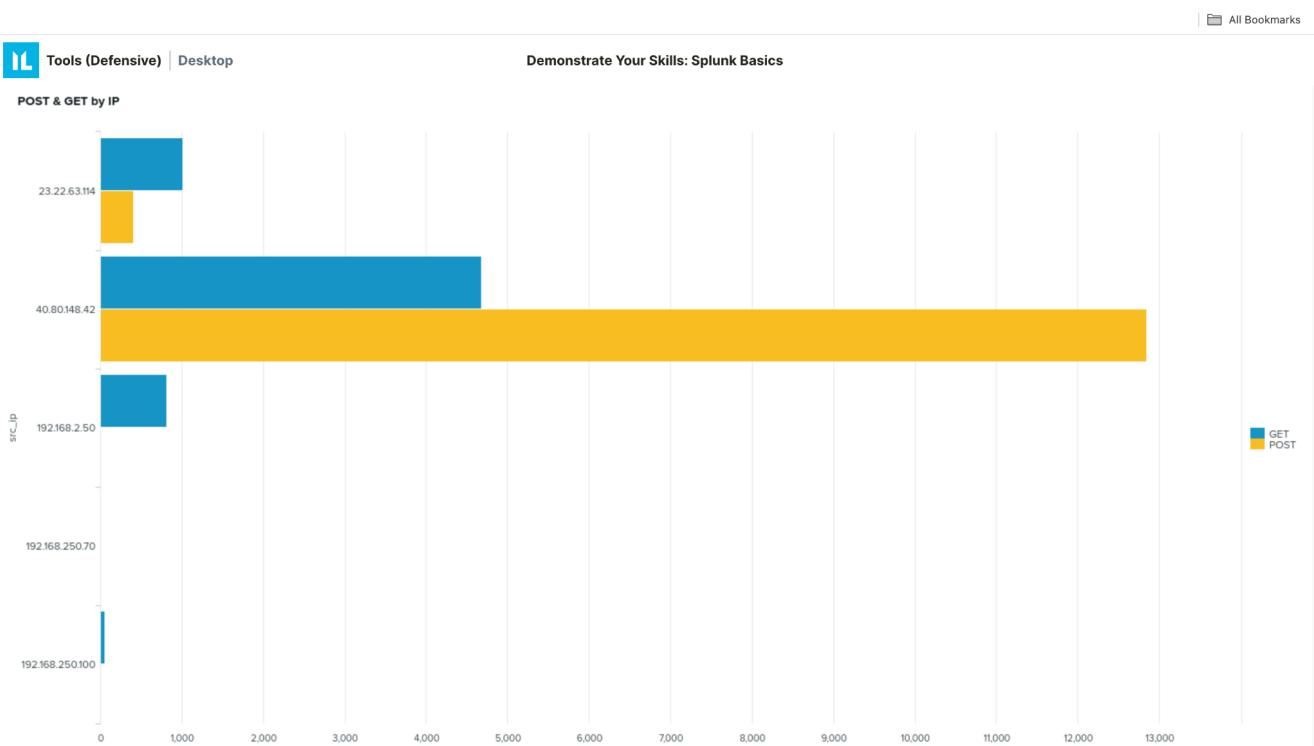
Q5: Which of the active IP addresses has the lowest number of requests?

Answer: 192.168.250.70



Q6: Which IP has the highest number of POST requests?

Answer: 40.80.148.42



Q7: Search for the host we8105desk, source WinEventLog:Microsoft-Windows-Sysmon/Operational, and the 192.168.250.20 DestinationIp. How many events are returned?

Answer: 1608

This answer arrived when the search query Query = host=we8105desk source="WinEventLog:Microsoft-Windows-Sysmon/Operational" DestinationIp=192.168.250.20 was used.

The screenshot shows the Splunk interface with a search bar containing the query "host='we8105desk' source='WinEventLog:Microsoft-Windows-Sysmon/Operational' DestinationIp=192.168.250.20". The results section displays 1,608 events found before 12/1/23 2:27:10.000 AM. The event details show XML event data, including the timestamp (8/24/16 6:23:44.000 PM) and event ID (5770385F-C22A-3E0-BF4C-06F5698FB09). The interface includes a sidebar for selected fields like host, source, and sourcetype, and a bottom toolbar with various icons.

Q8: Looking at the results from the previous question, find the host name of the remote server. What is the DestinationHostname?

Answer: we9041srv

The screenshot shows the Splunk interface with a search bar containing the query "host='we8105desk' source='WinEventLog:Microsoft-Windows-Sysmon/Operational' DestinationIp=192.168.250.20" followed by "| table DestinationHostname". The results section displays 1,608 events found before 12/1/23 2:31:36.000 AM. The statistics section shows that there is 1 occurrence of the DestinationHostname field. The results table lists the value "we9041srv" repeated multiple times. The interface includes a sidebar for selected fields like host, source, and sourcetype, and a bottom toolbar with various icons.

Q9: 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?

Answer: 2816763

To get this answer we had to construct search query as below.

Query= sourcetype=suricata cerber | stats count by alert.signature, alert.signature\_id | sort count

The screenshot shows the Splunk Enterprise interface with the title "Demonstrate Your Skills: Splunk Basics". The search bar contains the command: "cerber sourcetype=suricata" followed by a pipeline operator "|", then "stats count by alert.signature,alert.signature\_id", and finally another pipeline operator "|", then "sort count". The search results table has three columns: "alert.signature" (with values ETPRO TROJAN Ransomware/Cerber Checkin 2, ETPRO TROJAN Ransomware/Cerber Checkin Error ICMP Response, and ETPRO TROJAN Ransomware/Cerber Onion Domain Lookup), "alert.signature\_id" (with values 2816763, 2816764, and 2820156), and "count" (with values 1, 2, and 2 respectively). The table also includes sorting and filtering icons.

Learnings:

- Log Enumeration: Understanding the sources of logs, such as Windows Sysmon, Suricata, Windows Event Logs, Windows Registry, Stream, and fgt, provides insight into the diverse data available for monitoring and analysis within the Splunk environment.
- Metadata Exploration: The use of metadata commands, like `| metadata type=sourcetypes index=botsv1`, facilitates the enumeration of logs, helping identify the types and sources of data available for analysis.
- Dashboard Navigation: Navigating and exploring dashboards, such as "Web Traffic Monitoring," allows for a more visual representation of data, aiding in quickly identifying patterns, anomalies, and critical information.
- Search Queries Performing targeted searches, such as searching for specific hosts, source types, and keywords like "cerber," enhances the ability to extract relevant information from the vast dataset and focus on specific security-related events.
- Data Analysis: Extracting meaningful insights from search results, including identifying the most common status codes, the IP with the lowest requests, and the host name of a remote server, demonstrates the practical application of data analysis skills for a SOC analyst.

**Tools (Defensive)**

**Demonstrate Your Skills: Splunk Basics**

**Briefing**

**Tasks**

1 Use SPL queries to look through the dataset and answer the questions.

2 Select the Data Summary on the Search and Reporting App home page. How many hosts are there?  
7  
Correct

3 Looking at the data summary, which source has the highest count?  
WinEventLog.Microsoft-Windows-Sysmon/Operational  
Correct

4 Looking at the data summary, provide one of the two sourcetypes with the lowest count.  
stream:slp  
Correct

5 Navigate to the dashboard called Web Traffic Monitoring. Which status code appears the most?  
303  
Correct

6 Which of the active IP addresses has the lowest number of requests?  
192.168.250.70  
Correct

7 Which IP has the highest number of POST requests?  
40.80.148.42  
Correct

8 Search for the host web04tsvsl, source WinEventLog.Microsoft-Windows-Sysmon/Operational, and the 192.168.250.20 DestinationIP. How many events are returned?  
160  
Correct

9 Looking at the results from the previous question, find the host name of the remote server. What is the DestinationHostname?  
web04tsv  
Correct

10 Search for the keyword "curl" 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?  
2816763  
Check

**Note**  
If the message "Connection refused" appears after clicking on the Splunk shortcut, you can simply refresh the in-lab browser, which will then connect to the Splunk instance needed to complete this lab.

**Scenario**  
You're a junior SOC analyst and have just completed your first few weeks of training. Now you're expected to start independently monitoring and searching data. You'll need to familiarize yourself with your company's data, explore the dashboard, identify HTTP traffic, and conduct your first searches on specific hosts.

**ON THIS PAGE**

Note  
Scenario  
Log enumeration



**Splunk**

**Demonstrate Your Skills: Splunk Basics**

**Congratulations DISHA**  
You have completed "Demonstrate Your Skills: Splunk Basics"

**+0**  
Total Points  
**1380**

**6/3**  
You've completed 6 of your 3 labs for this week!

## **Writeup on Overall Learning:**

The six Splunk lab activities provided a thorough grasp of the platform's capabilities and practical applications in network monitoring. The tour began with an introduction of Splunk fundamentals, stressing the tool's ability to collect different data from several sources inside an organization. The importance of source types became clear, emphasizing their function in data structuring and indexing, which is required for effective search queries and data analysis.

A detailed look into the search functionality evolved as the labs continued. Each phase gave insights into improving and supplementing search results, from simple searches to sophisticated queries utilizing the Search Processing Language (SPL). The ability to use Boolean expressions, wildcards, and escape characters improved the versatility and precision of search queries, which is critical for circumstances such as researching Windows file paths.

SPL components and transformational commands like Chart, Timechart, Stats, Top, and Rare were added during the research of sophisticated searching. This information was put to use in real-world scenarios such as finding common and uncommon field values, counting events, and tracking probable attack scenarios using actual data.

The laboratories then moved on to visualization, focusing the design and customisation of dashboards. This hands-on training emphasized the significance of arranging and presenting summary data, resulting in a significant skill set for efficient data presentation.

The last set of activities demonstrated the use of newly acquired abilities in the Splunk environment. The ability to navigate the Search and Reporting App, evaluate data summaries, and extract useful information from dashboards indicated a comprehensive awareness of Splunk's capabilities. The capacity to conduct focused searches and evaluate results for specific scenarios, such as identifying hosts, evaluating web traffic, and tracking security-related events, demonstrated the practical application of information gained.

In essence, the six lab exercises not only provided a thorough overview of Splunk's features, but also equipped participants with practical skills required for network monitoring, data analysis, and security incident response. The exploration of Splunk's capabilities has provided me with a versatile skill set applicable to real-world scenarios in the dynamic landscape of network and security operations.