Lab computers (on-campus)

Use the following credentials to login as admin in Splunk:

Username: **SplunkUsr**

Password: **U0Msplunk**

For installing Splunk on your personal PC, follow the installation instructions.

Install Splunk Enterprise License

Download Splunk Enterprise that suits your OS:

- Download link: Splunk
- Login credentials:
  - Username: sanalytics
  - Password: Comp@90073

Assignment Project Exam Help

Go to Splunk installation Manual and follow the related instructions to install Splunk Enterprise

https://tutorcs.com

Start, Stop, Restart Splunk

WeChat: cstutorcs

After installing the license or any application, you should restart the Splunk process.

Splunk Enterprise License

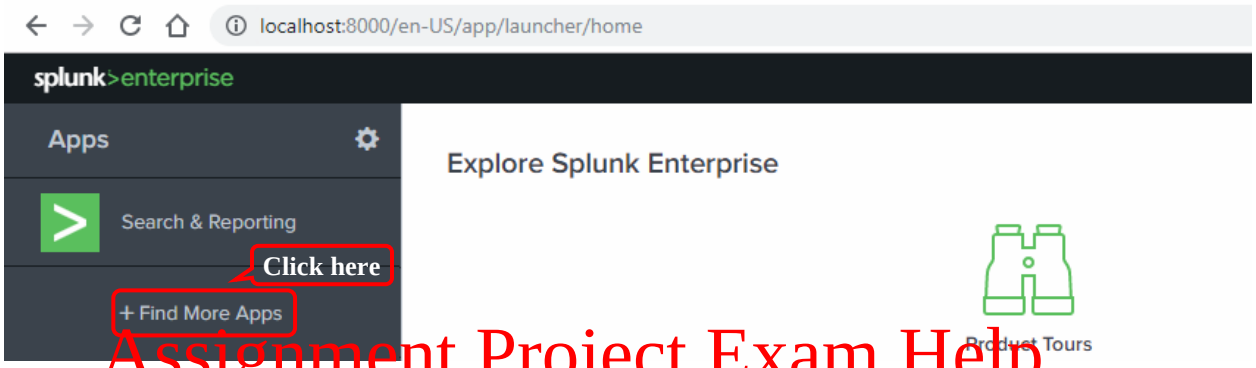
Download Splunk Enterprise license from the content of Week 3 Tutorial.

1. **(Preferred)** Adding a license using the GUI:
   a. Use the “admin” username and the password you have chosen to login to Splunk in your browser by going to http://localhost:8000.
   b. Navigate to Settings > Licensing.
   c. Click Add license.
   d. Click Choose file and navigate to your license file and select it.
   e. Click Install.
   f. Restart the Splunk process.
2. (For advanced user only) Adding a license manually: copy Splunk.License file to your `$SPLUNK_HOME/etc/licenses/enterprise` directory and restart the Splunk process

Install PCAP Analyzer APP

To index packet capture (pcap) files, you can use an application in Splunk called PCAP Analyzer. To install this app:

1. Make sure you have set SPLUNK_HOME variable.
2. Navigate to “Find More APPs” panel.



Assignment Project Exam Help

Figure 1. Finding and installing apps

https://tutorcs.com

3. Search for “PCAP Analyzer for Splunk” and press “Install”. A new folder called SplunkForPCAP will be created for the new app in $SPLUNK_HOME\etc\apps\ directory.
4. Restart Splunk.

WeChat: cstutorcs

5. Make sure you have logged as administrator in your computer, otherwise your user account should have administrative permission to change the PCAP Analyzer folder. To test if this is true, check the user permissions for the directory $SPLUNK_HOME\etc\apps\SplunkForPCAP. For example, in windows, right-click on the folder and navigate to Properties > Security > Edit > (your user-account); give the full control for changing the folder to your user-account.
6. After restarting and logging in, you will see the PCAP Analyzer in the list of your apps.

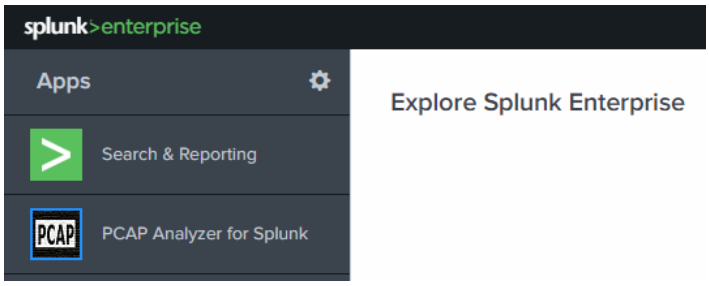


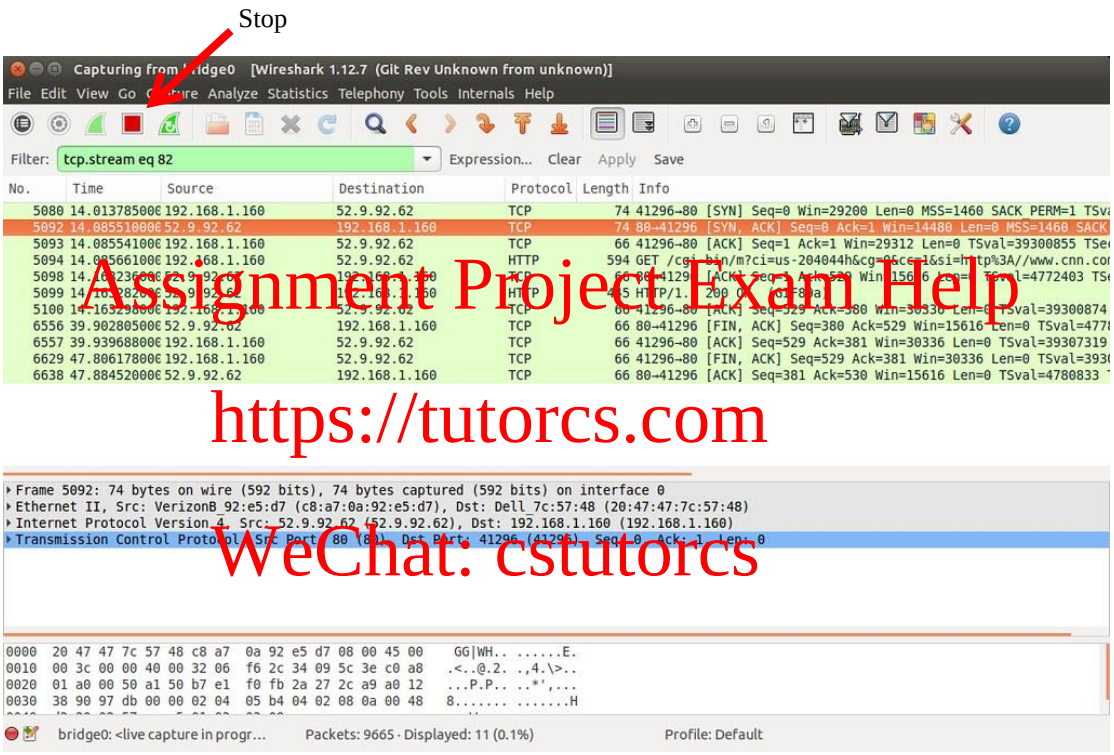
Figure 2. PCAP Analyzer app

Install Wireshark as PCAP Analyzer app uses tshark to generate features.

Make sure Wireshark is located where PCAP Analyzer app expects it to be (e.g., “C:\Program Files\Wireshark” in Windows). Wireshark packet capturing capabilities can be used in combination with Splunk to capture and index network packet traffic in real-time.

To make sure that PCAP Analyzer is working properly, we need a small sample data. Open Wireshark to capture a small pcap file for a couple of seconds. For example, navigate to Capture > Options > Ethernet > Start. Wait for a few seconds, then stop by clicking on the stop sign (or navigating to Capture > Stop).

Create a directory (Desktop\comp90073\) for this tutorial. Save the captured data as a pcap file in this directory and call it “sample.pcap”.



Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

Figure 3. Capturing data using Wireshark

To allow Splunk to collect and index your PCAP Files using the PCAP Analyzer app, you should specify where you have stored your pcap files.

1. Navigate to Settings > Data Inputs > PCAP File Location > New.
2. Choose a name for your new pcap input location.
3. Copy the path to your pcap files and click next.

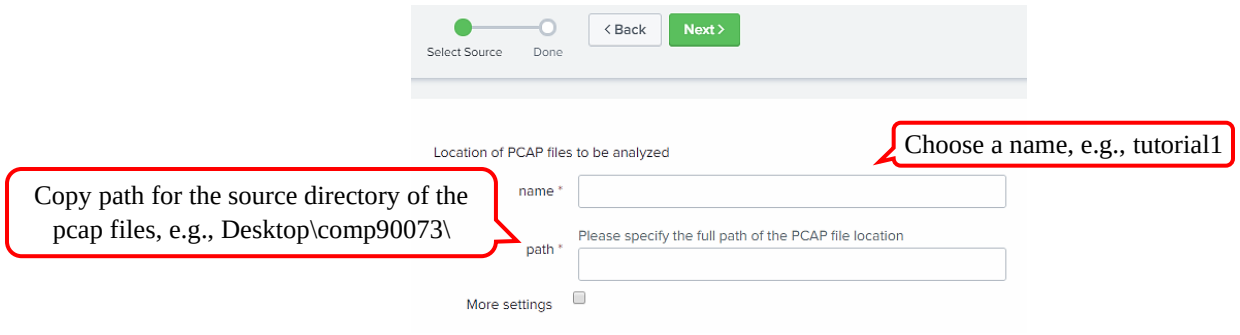


Figure 4. Adding pcap file locations

If these steps are done successfully, a folder named "local" is created[1] contacting a file named inputs.conf. This file has information about the pcap file location you just created. After the data is indexed, the pcap files in your source directory are converted to CSV files[2] and transferred to a new folder called PCAPConverted[3] to avoid duplicating the indexing of the data[4] stored in the pcap files directory. Make sure that this has happened, unless something has gone wrong and your data is not indexed. The PCAP Analyzer app checks every 3 minutes for a new pcap file in your specified pcap directory (e.g., Desktop\comp90073\).

Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

To search the data collected and indexed by this application, you should use the search from inside the application (Figure 3) not the general Search & Reporting in Figure 2.

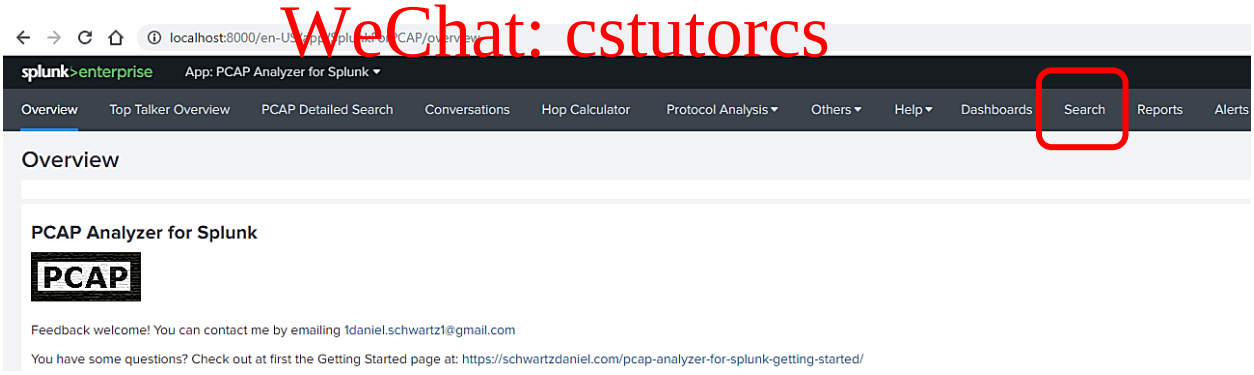


Figure 5. Navigating to search in PCAP Analyzer

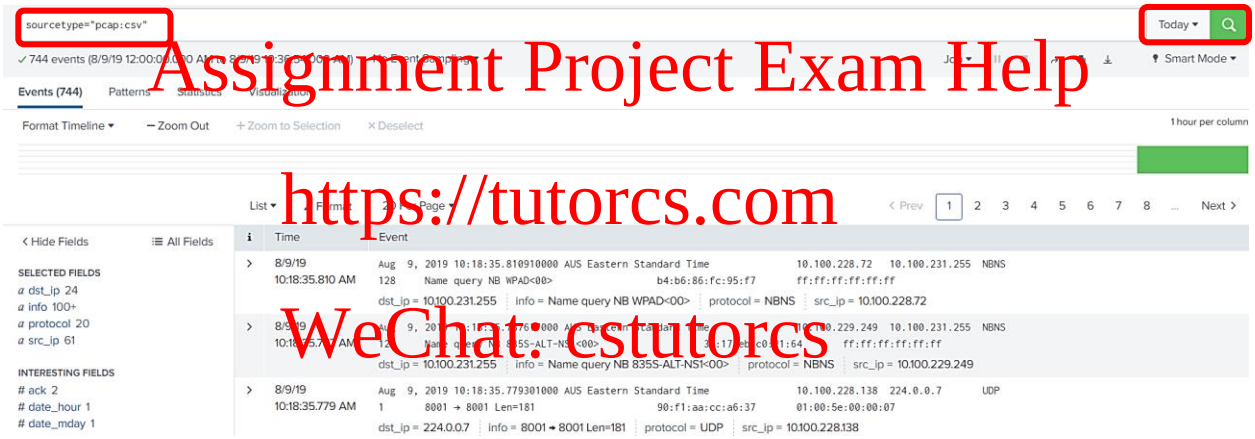
[1] $SPLUNK_HOME\etc\apps\SplunkForPCAP\local
[2] Stored in $SPLUNK_HOME\etc\apps\SplunkForPCAP\PCAPcsv
[3] $SPLUNK_HOME\etc\apps\SplunkForPCAP PCAPConverted
[4] To understand how the batch, shell and python scripts index the data, a good start is to navigate to Settings > Data Inputs > Scripts

By going to search via the app, Splunk will use the scrips, which are written for the app to generate fields. If you use the general Search & Reporting app instead, Splunk automatically generates the fields and it may not be efficient or even correct for the pcap data.

Different dashboards created by PCAP Analyzer make it possible for you to look at your data in different time intervals and detect changes and interesting patterns. We give a demo for “search” and “Top Talker Overview” and you can take similar approach to explore the other dashboards.

Search

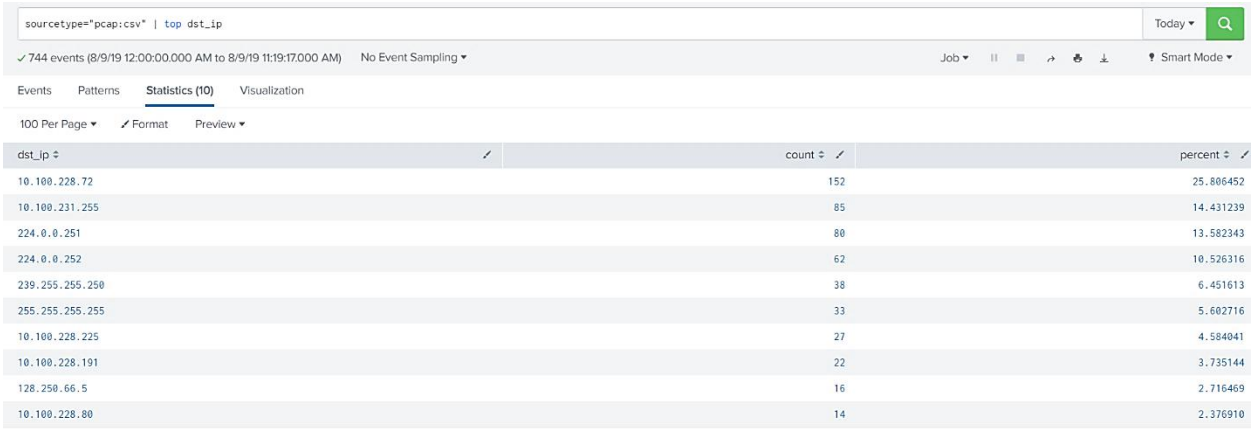
By navigating to PCAP Analyzer > search and running SPL commands, you can see the fields generated for your data. The sourcetype generated by PCAP Analyzer is “pcap:csv”. Use the time range picker to choose the time period (e.g., Today), which you are going to focus on. If you want to see all data of this type, you can choose “All time”.



Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

Figure 6. Search in PCAP Analyzer

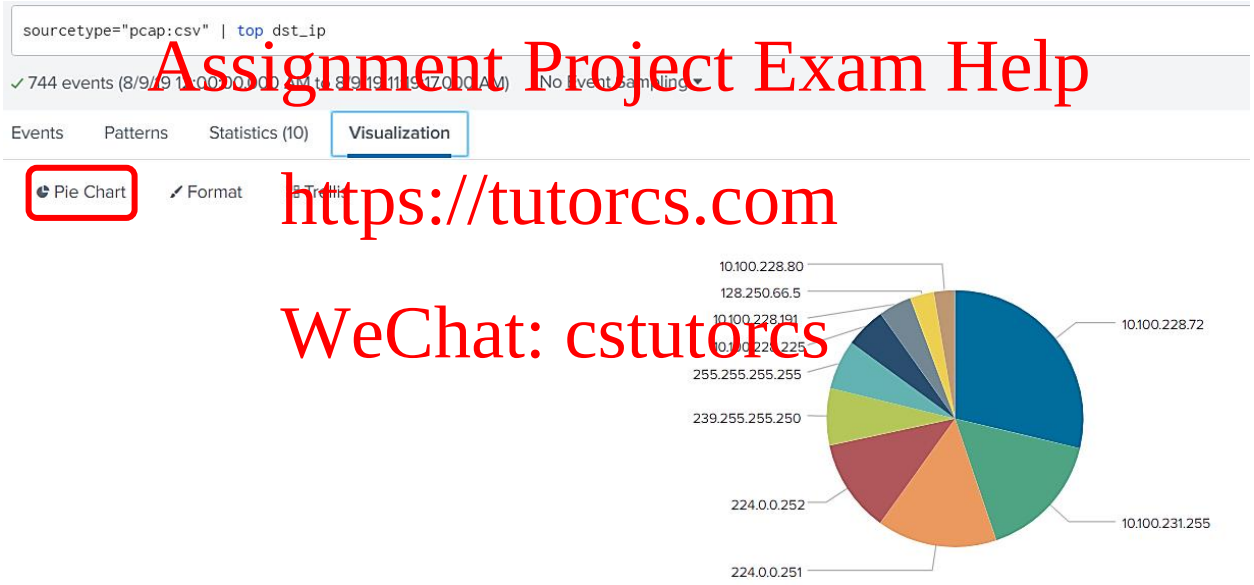
Practice using the SPL commands that you have learned during the lectures and check-out the options that you will have by running them.



dst_ip	count	percent
10.100.228.72	152	25.806452
10.100.231.255	85	14.431239
224.0.0.251	80	13.582343
224.0.0.252	62	10.526316
239.255.255.250	38	6.451613
255.255.255.255	33	5.602716
10.100.228.225	27	4.584041
10.100.228.191	22	3.735144
128.250.66.5	16	2.716469
10.100.228.80	14	2.376910

Figure 7. Running SPL commands on your sample data

You can visualise the results in various ways. e.g.,



Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

Figure 8. Visualising the search results using a pie chart

Top Talker Overview

Let's use a previously captured pcap file, which you can download here, and call it "test.pcap". Save this file in your pcap source directory (in this tutorial Desktop\comp90073\). When data is ingested using the PCAP Analyzer app (i.e., you should see the corresponding CSV file is created in Stored in PCAPcsv folder[1]). Via PCAP Analyzer > Search, you can find the index data by searching **source="*test.pcap.csv*"**

[1] $SPLUNK_HOME\etc\apps\SplunkForPCAP\PCAPcsv

and choosing “All time” for the time range picker. In Top Talker Overview, wait until the tcpdump files are loaded, then choose **test.pcap.csv**. For the timechart Span, you can use the time-units you learned from the lectures (e.g., 1h for 1 hour, which results in aggregating for each hour). Have a look at the different overviews which are provided to see if you can identify any pattern. Aggregated separately based on the number of packets and total number of bytes, you can see:

1. Top Protocols
2. Top Conversation
3. Top Sender
4. Top Receiver
5. Top Ports
6. Top MAC

Discuss how you can use this information to identify suspicions behavior? What if you add more data? How the traffic patterns are changed?

What change will happen in if a certain type of attack occurs? Pick several network attacks from the lecture slides and discuss possible indicators of those attacks in terms of changes in the network traffic data. What can you infer about changes in the network traffic patterns based on the visualised information in the PCAP Analyzer dashboards?

Assignment Project Exam Help
https://tutorcs.com

Customizing the dashboard views in search

WeChat: cstutorcs

To change the properties of the outputs generated in PCAP Analyzer dashboards, such as time range, click on Open in Search:

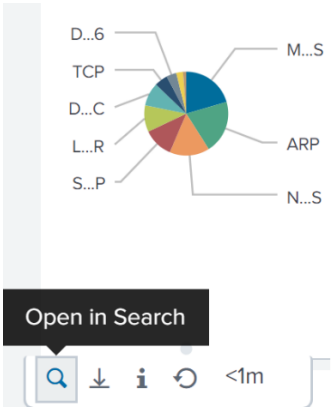


Figure 9. Open a dashboard view in search

You can choose from different visualisation options in search and change the search command as you like.

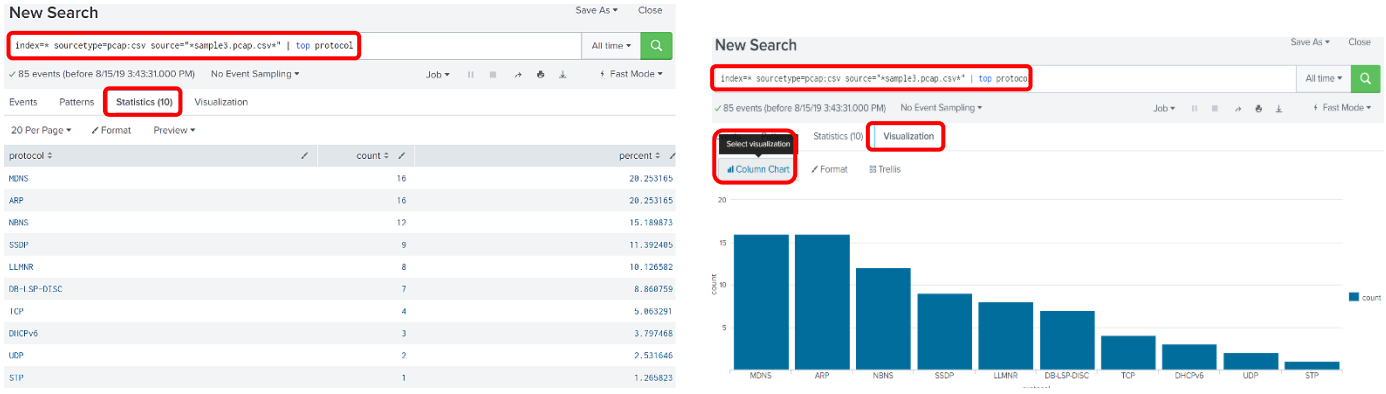


Figure 10. Change the visulisation in search

Replicate these steps on your own data and use the time range picker to change the time period for which you are looking at data.

Assignment Project Exam Help

Add your own CSV files to Splunk

https://tutorcs.com

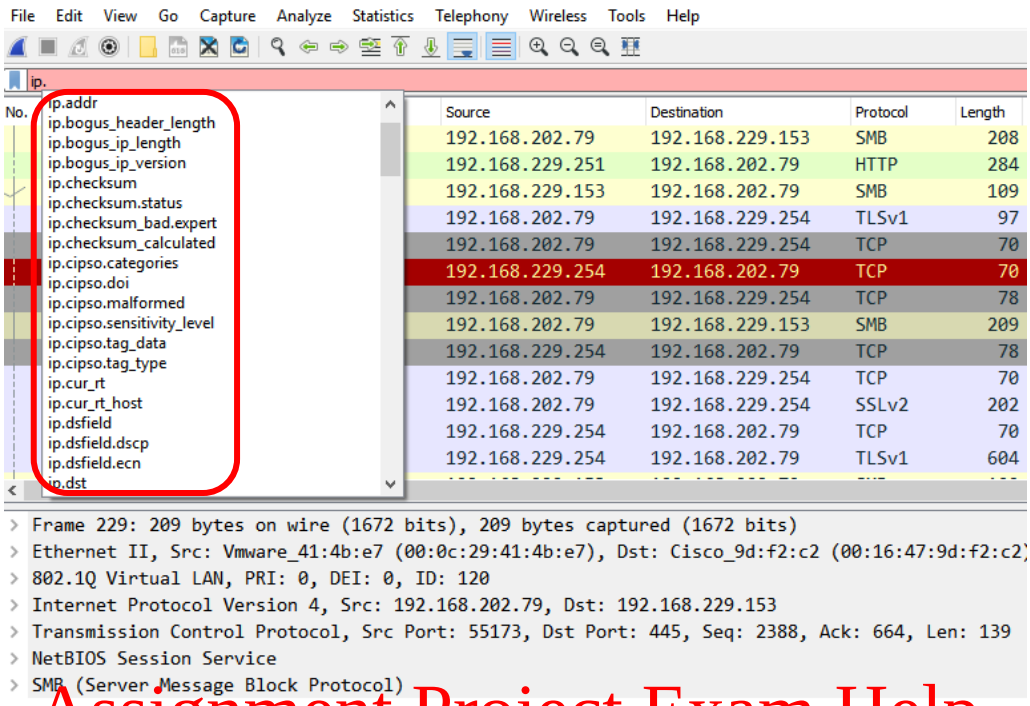
You can create your own CSV files from the pcap files and upload them to Splunk for further analysis. We give you an example in Windows.

WeChat: cstutorcs

Run the command line (cmd) and navigate to the Wireshark directory:

cd C:\Program Files\Wireshark

You can use tshark to generate your own CSV file and import it to Splunk. To check-out the available options for features that you can create using tshark, use Wireshark.



Assignment Project Exam Help

Figure 11. Identifying available fields using Wireshark

https://tutorcs.com

Using cmd, run tshark to generate custom fields:

WeChat: cstutorcs

Figure 12. Extracting fields using tshark

Now import the CSV file into Splunk by navigating to Settings > Add Data > Upload files from my computer. Follow the instructions

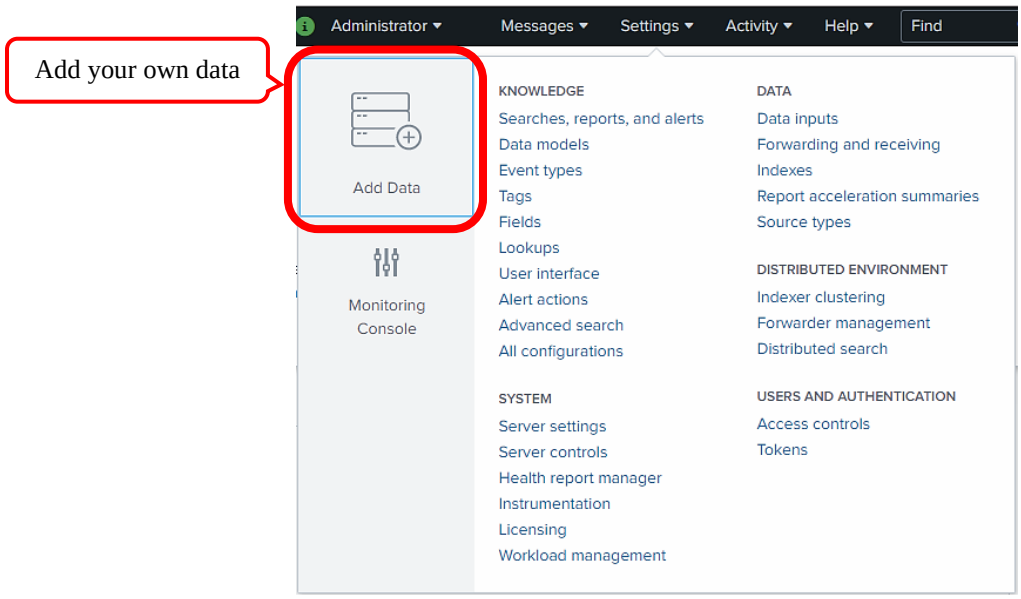


Figure 13. Adding your own data

Assignment Project Exam Help

In Figure 12, you can see that the extracted fields, which are in the header of the sample.csv file, are identified and indexed by Splunk. Note that we have created a new index called “securityanalytics” and have associated the sample.csv file to this index (instead of the default index “main”) while we were uploading it. This means that we should specify the name of the index in search to see these results (Splunk searches the “main” index by default, unless it is told to search another index). To add custom indexes, navigate to Setting > Indexes > New Index.

https://tutorcs.com
WeChat: cstutorcs

In Figure 12, you can see that for the small sample.pcap file that we generated using Wireshark, only TCP streams exist.

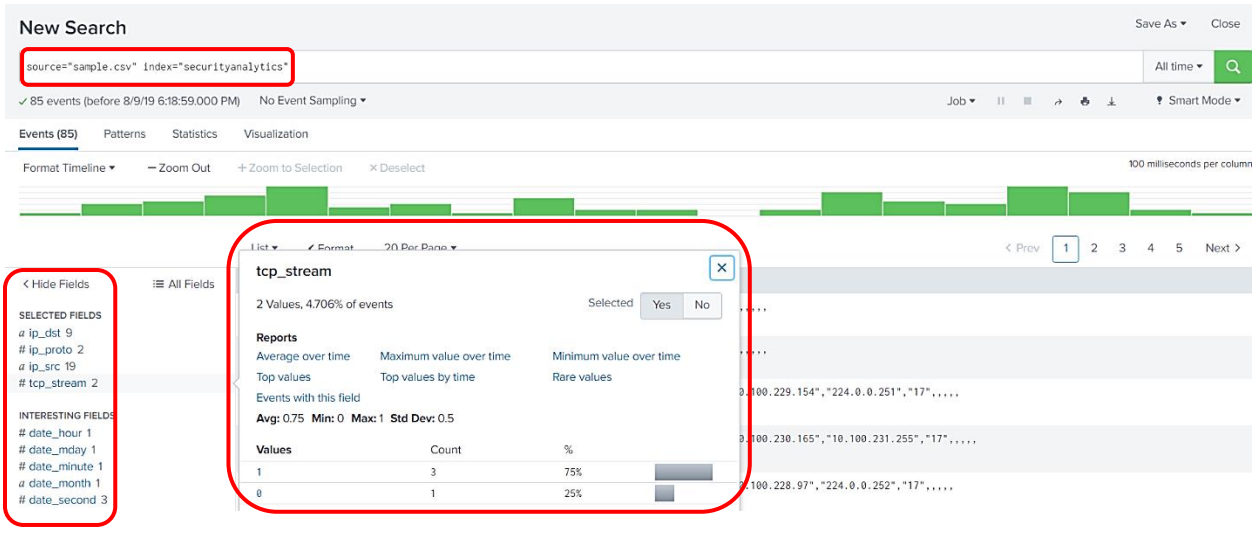


Figure 14. An example of an imported CSV file

Delete an application from Splunk

1. Disable the application by navigating to Manage Apps. Then, restart Splunk
2. Delete the directory corresponding to the application in $SPLUNK_HOME\etc\apps\
3. Delete the application folder in $SPLUNK_HOME\etc\users\YOUR-USERNAME\
    a. YOUR-USERNAME is your username in Splunk
4. Restart Splunk

Installing new applications or updating existing ones, after installing PCAP Analyzer app, may create some issues for PCAP Analyzer due to some dependencies. If you experience issues with PCAP Analyzer app, deleting and reinstalling it may resolve the issues.

Delete the indexed data from Splunk

- You should have can-delete permission to be able to delete data
    - As admin in Splunk GUI, Navigate to Settings > Access control > roles > your-user-name
    - Add can-delete to your permissions
- Syntax: … | delete

Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs