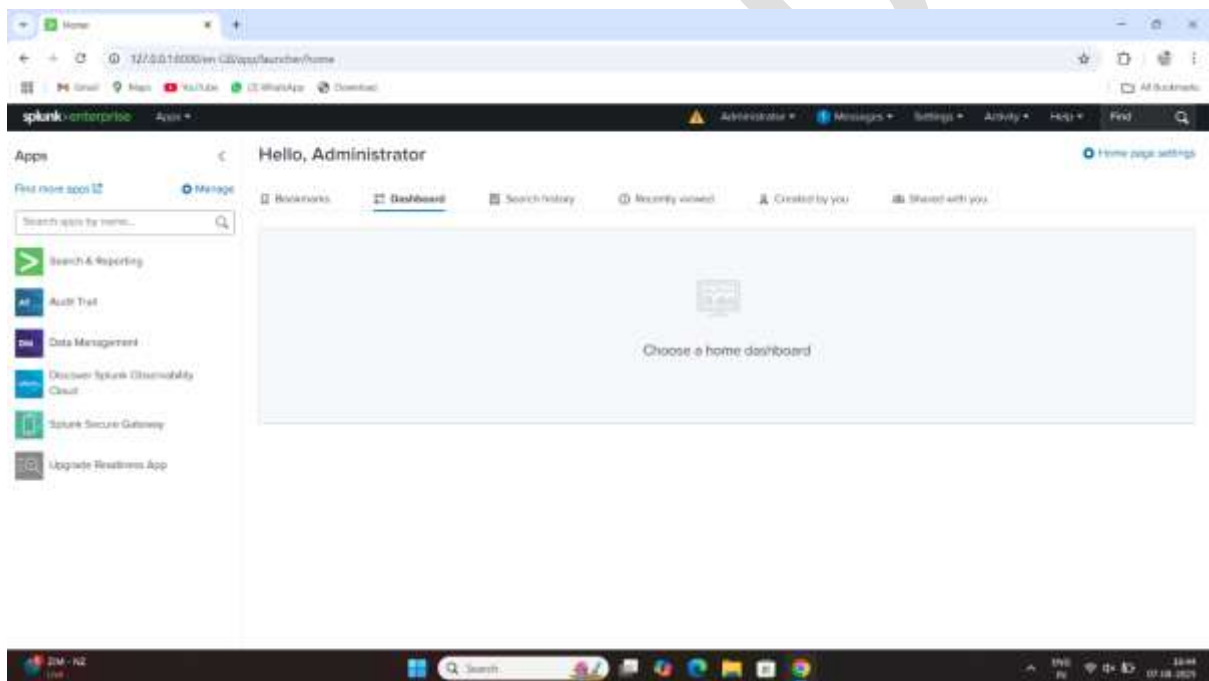


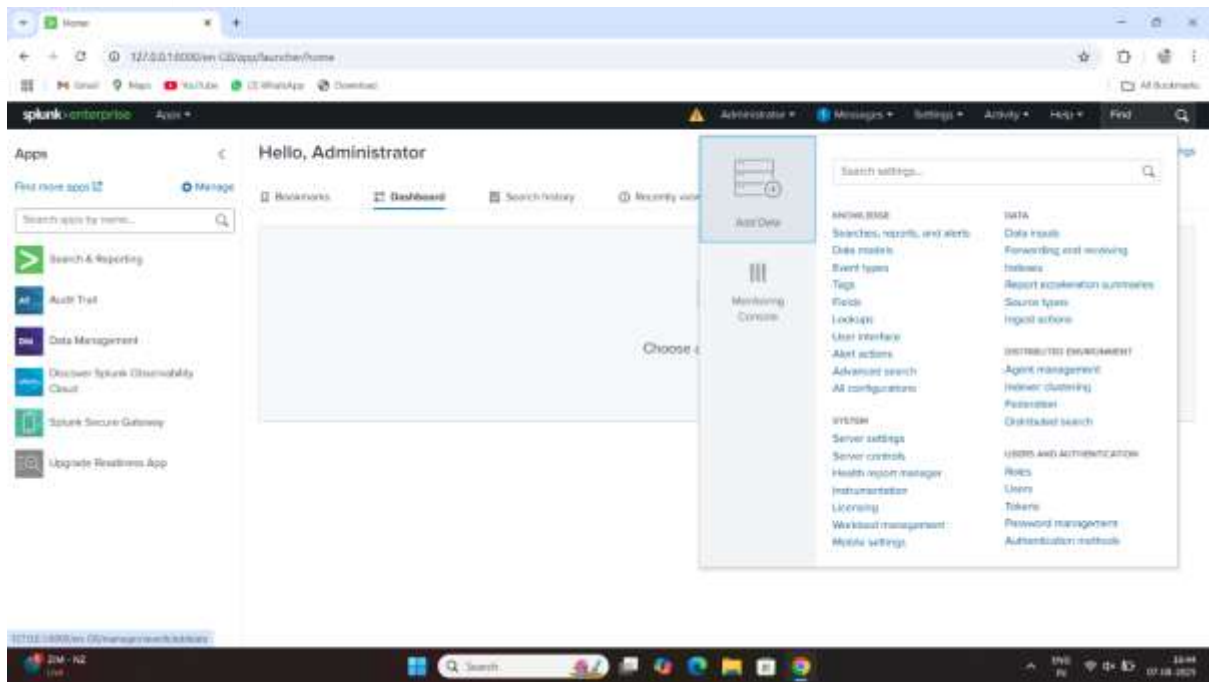
## Module 8 network forensic

### Lab 1 identify and investigate on ftp brute force attack using splunk

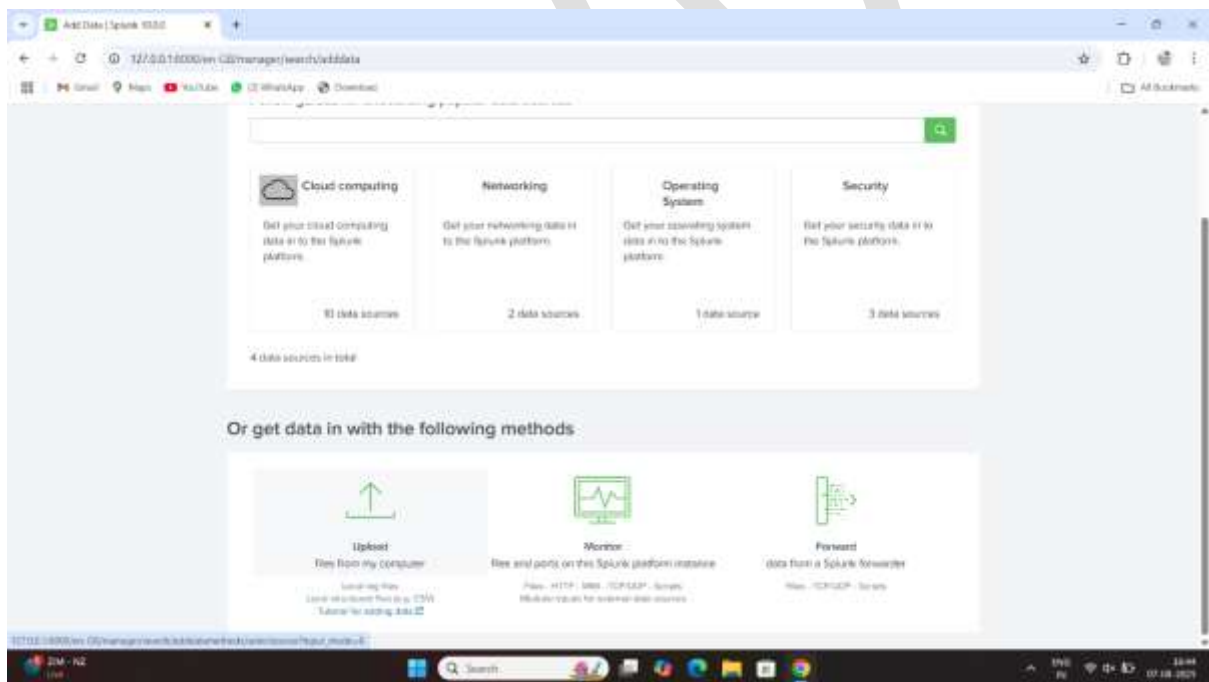
Step1 start the splunk



Step2 go to setting option

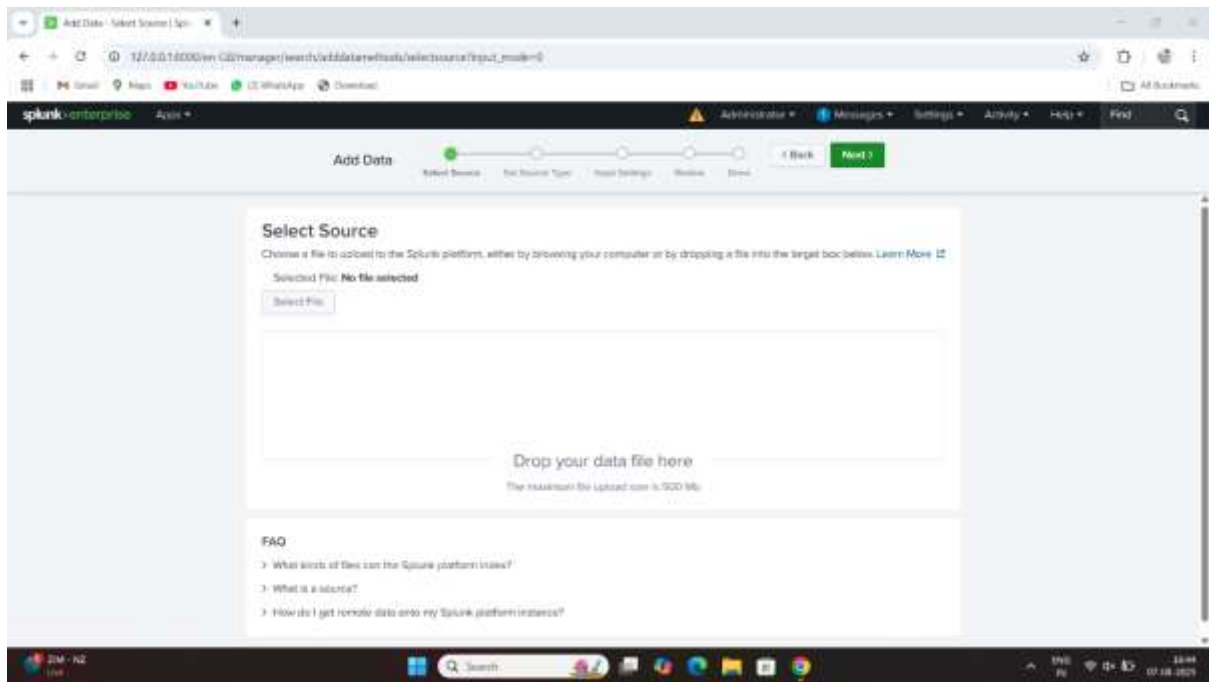


Step3 click on add data option

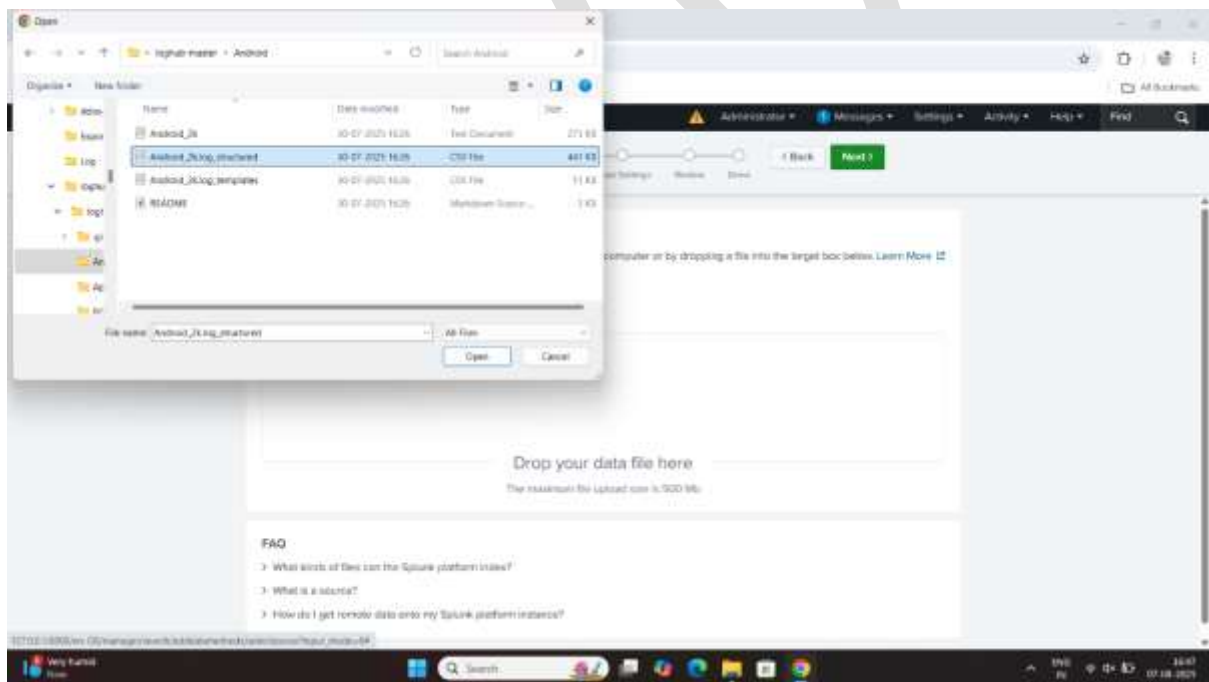


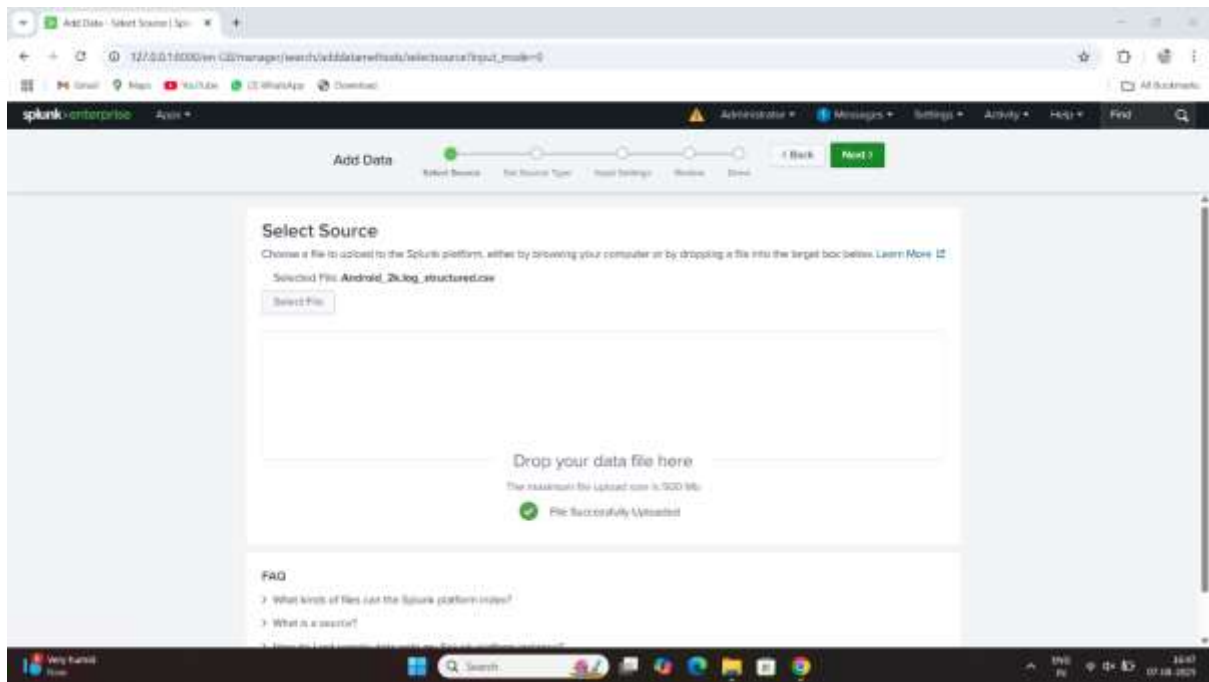
Step4 click on upload option

Step5 select source file

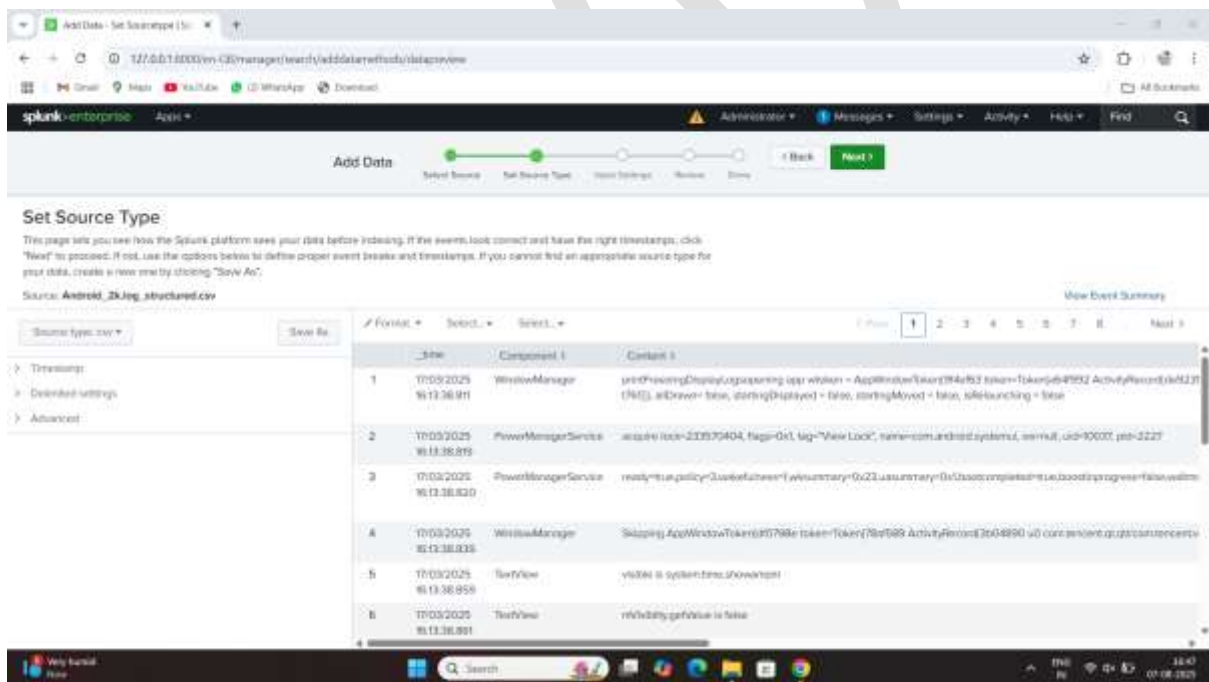


Step6 click on the source option and select the log file





## Step7 set source type



Click on next

## Step8 select the input setting

**Add Data** | Select Source | Set Source Type | **Input Settings** | Review | Done

### Input Settings

Optionally set additional input parameters for this data input as follows:

**Host**  
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Host field value:

**Index**  
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index:  [Choose a new index](#)

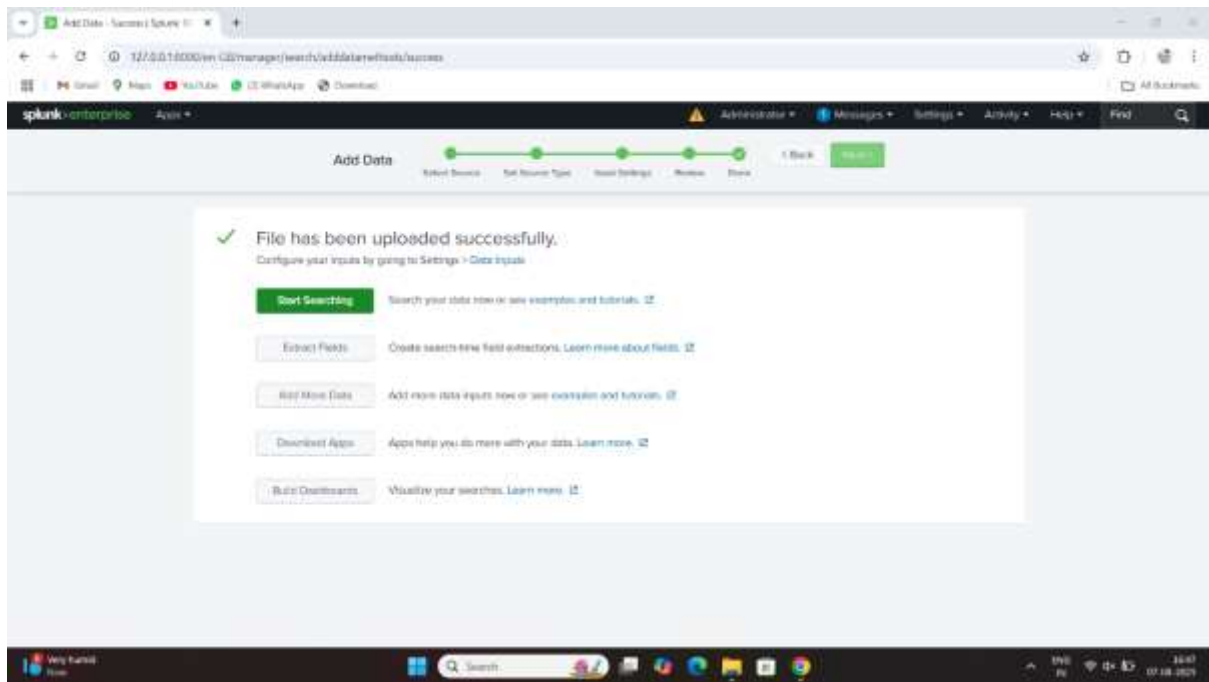
**FAQ**  
[How do indexes work?](#)

Click on next  
Step9 review

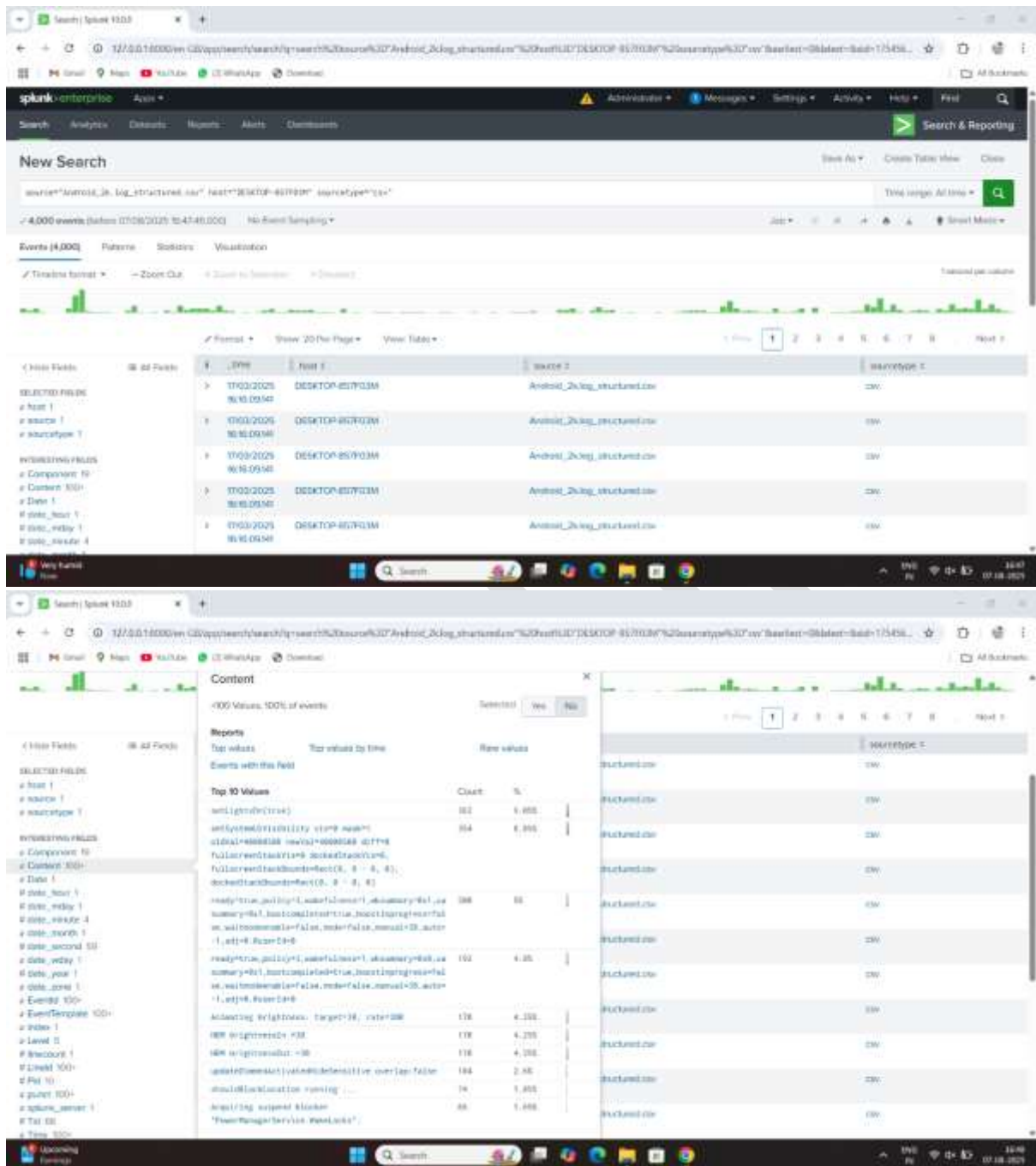
**Add Data** | Select Source | Set Source Type | Input Settings | **Review** | Done

### Review

Input Type:   
 File Name:   
 Source Type:   
 Host:   
 Index:



Step 10 click on start searching

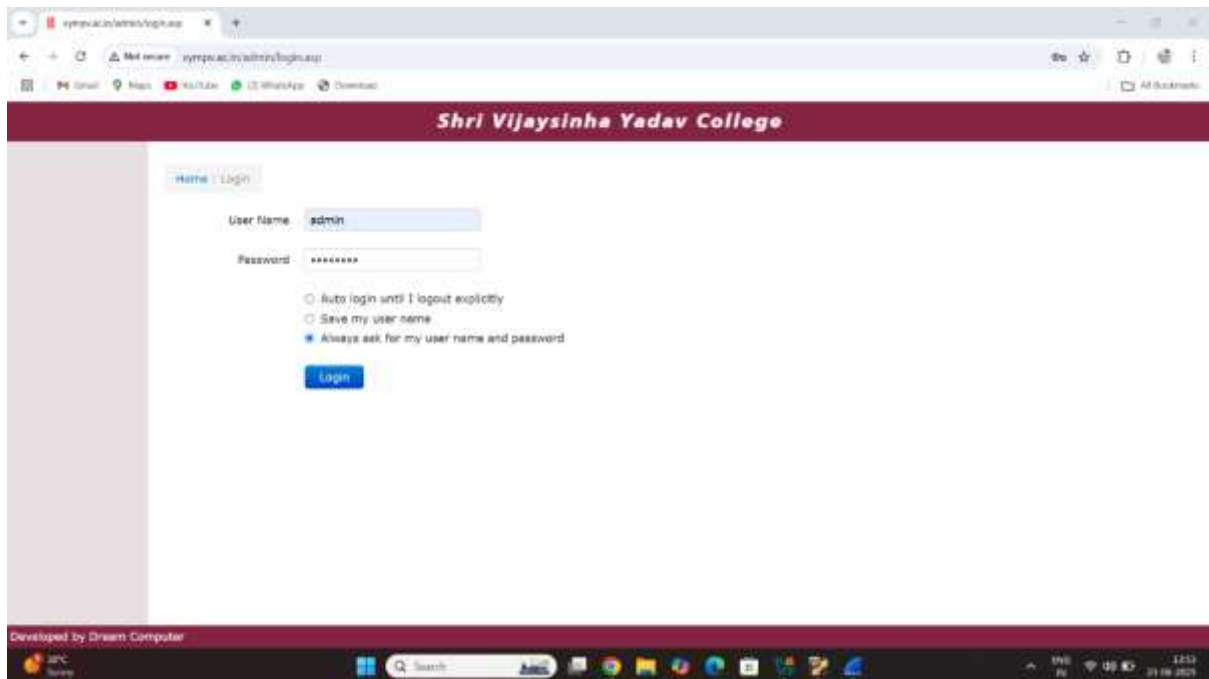


## Lab2 identify and investigate various network attack using wireshark

Step1: select the url target I am select the web site

<http://www.vympv.ac.in>

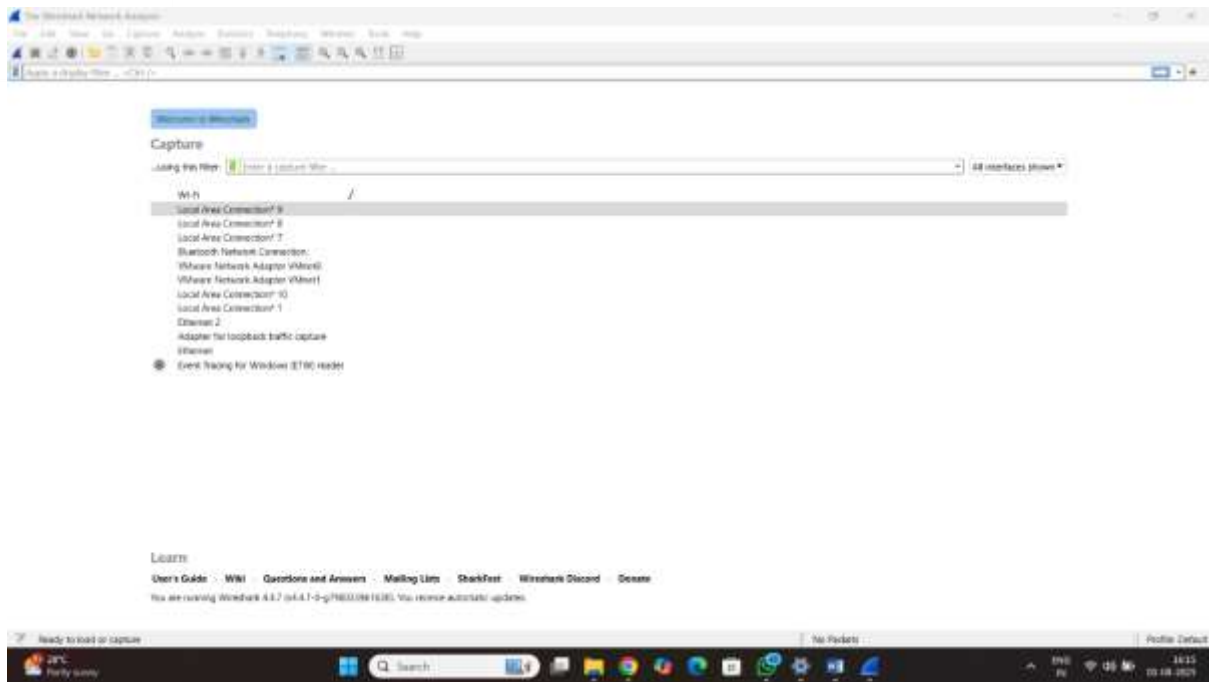
Step2: open the web site and login the user id and password



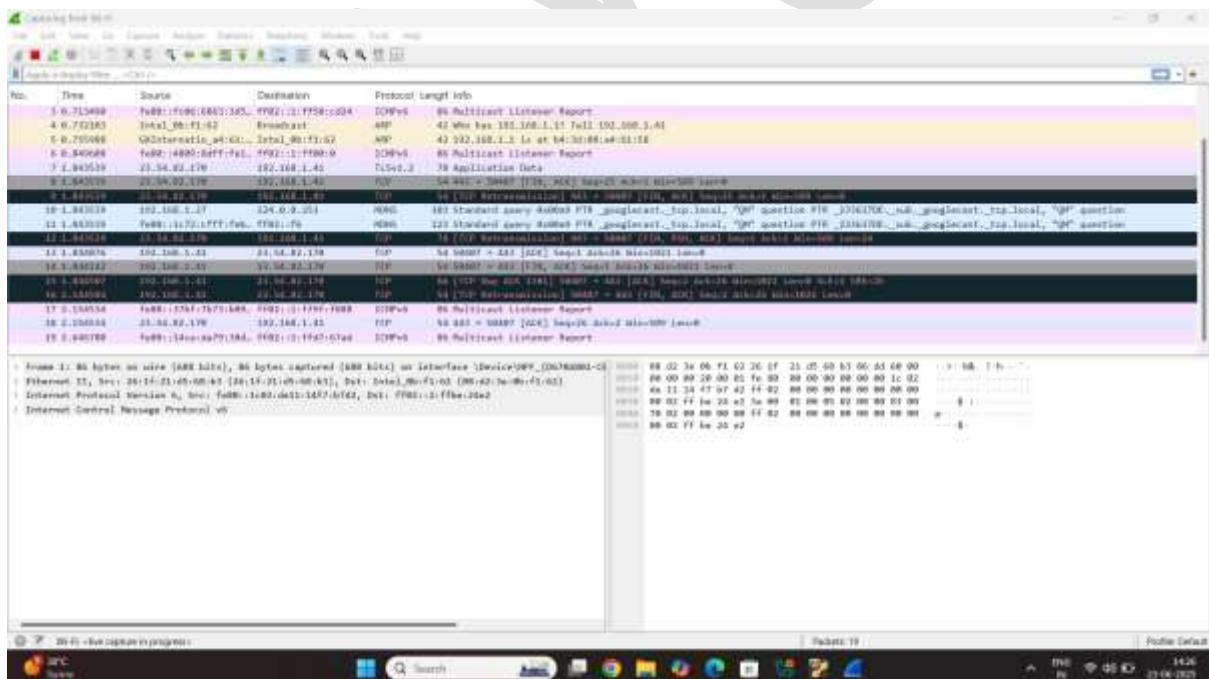
Step3: start the wire shark on network select the Lan

Step4 start the wireshark

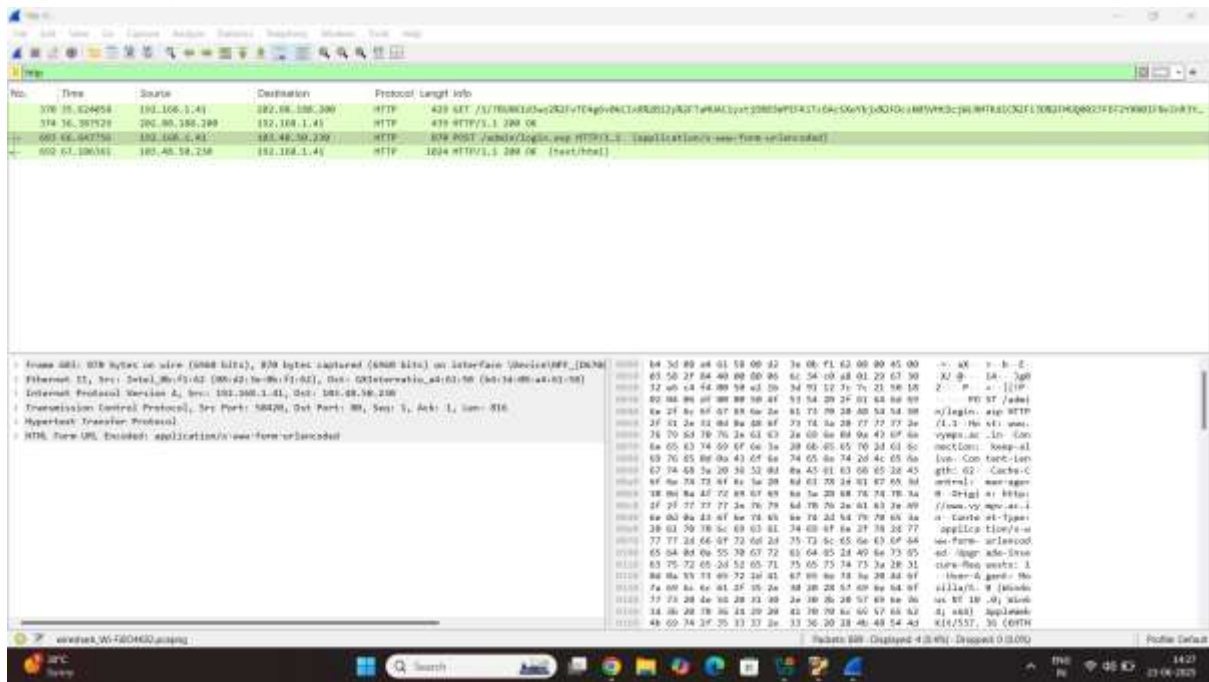




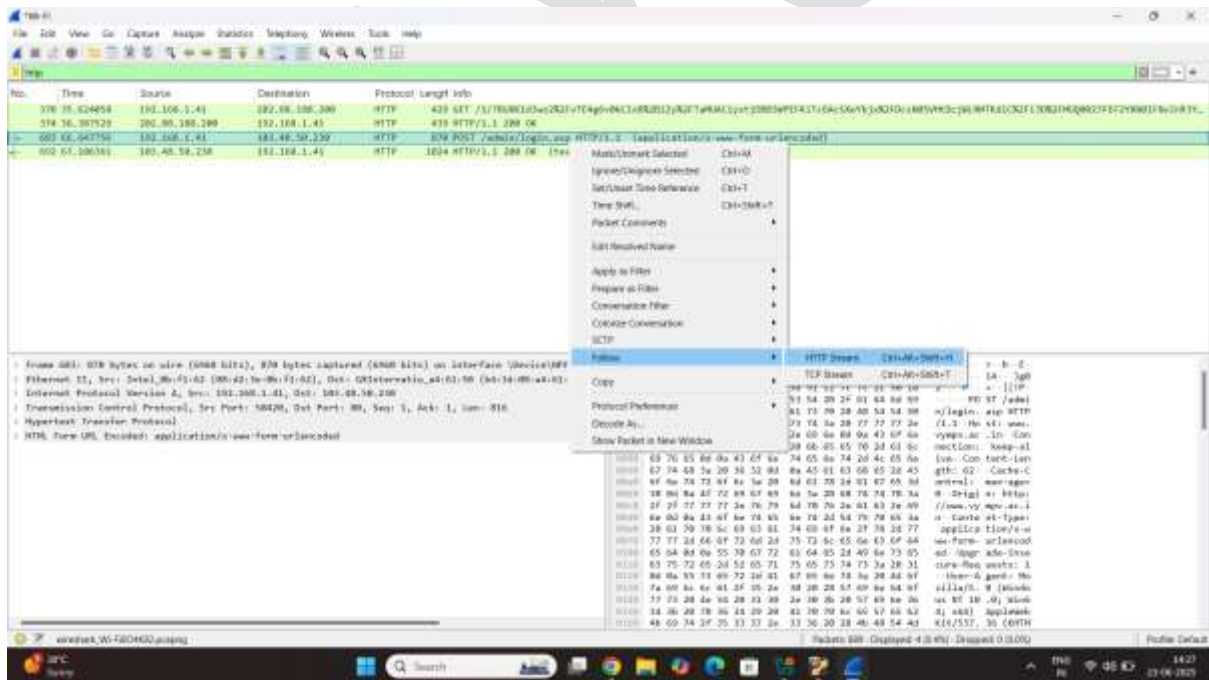
Step5 capture the request of wireshark



Step6: and apply the filter in wire shark i am apply the filter is http because is try this method is http web site



Step7: apply this filter and click on write in your keyboard select the follow option



## Result:

