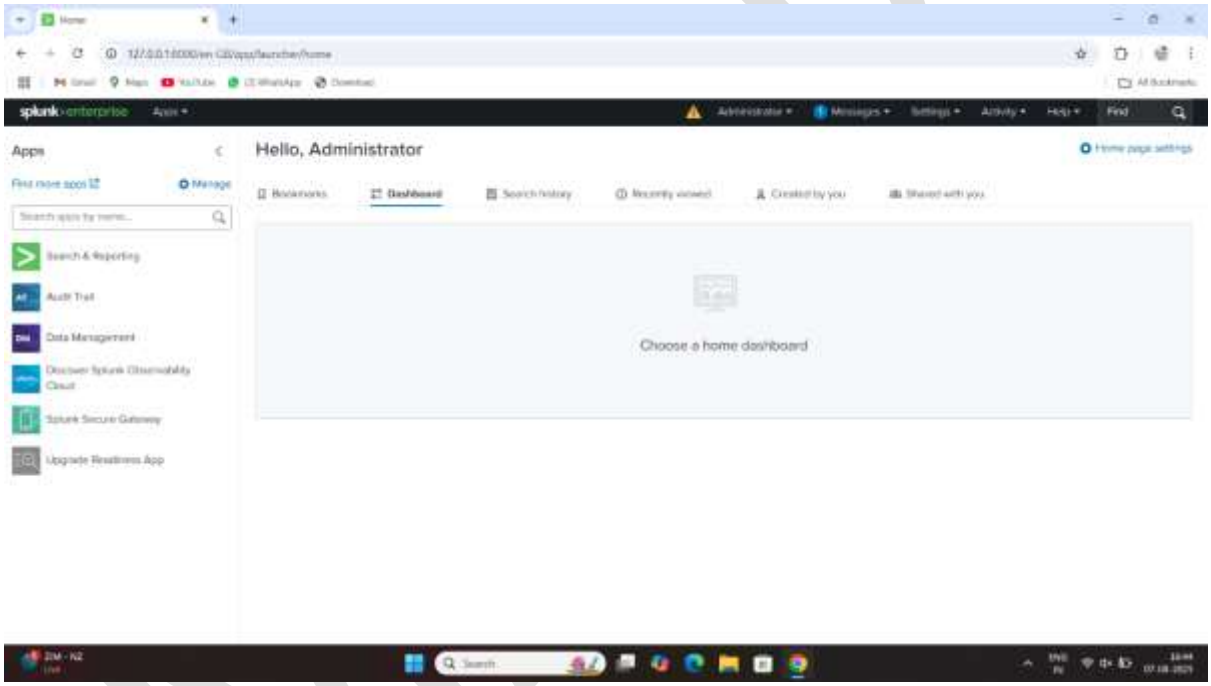
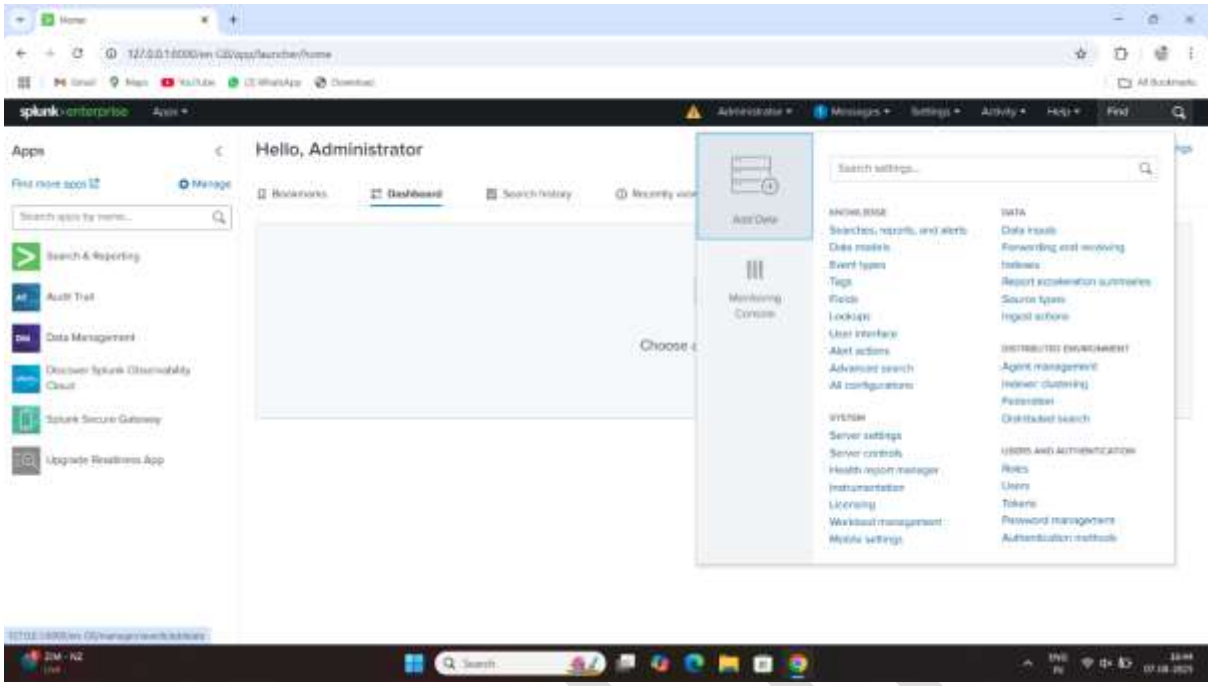
Module 8 network forensic

Lab 1 identifiy and investigate on ftp brute force attack using splunk

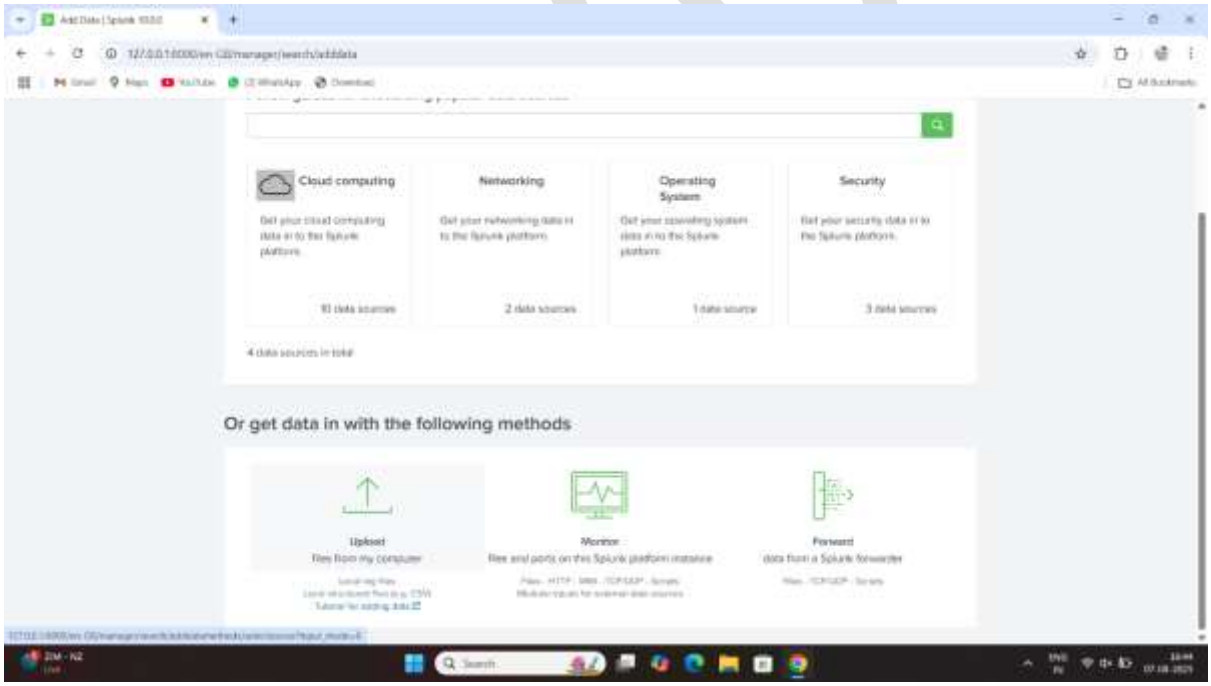
Step1 start the splunk



Step2 go to setting option

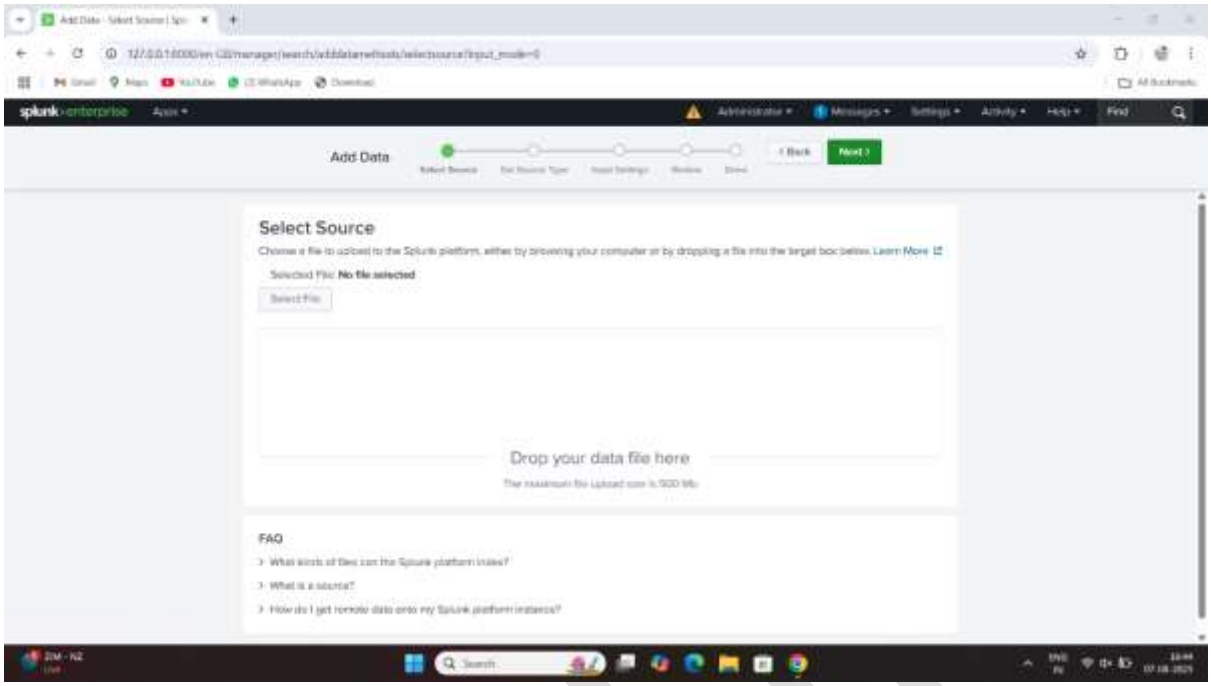


Step3 click on add data option

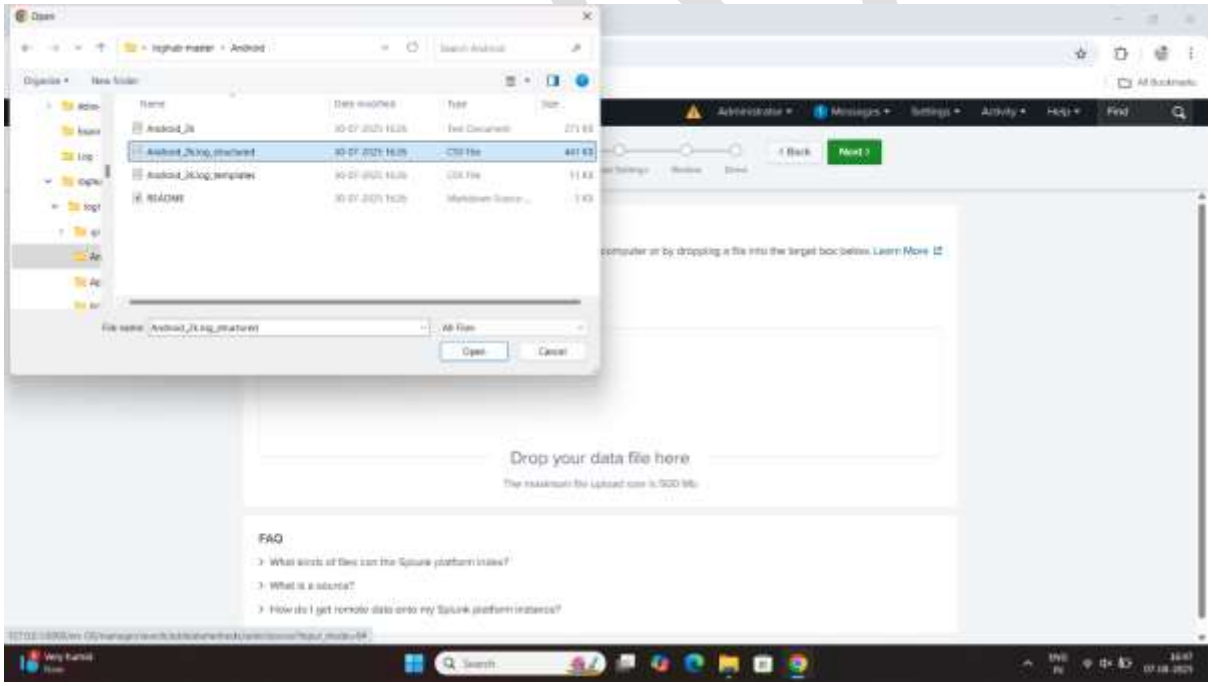


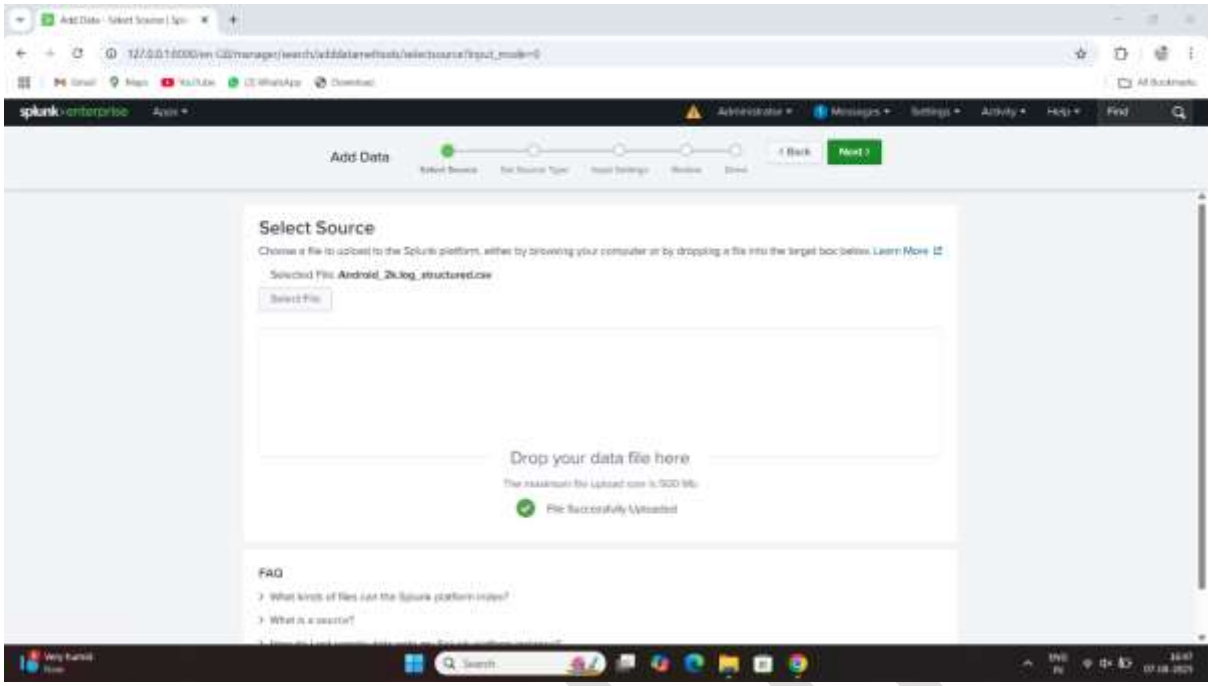
Step4 click on upload option

Step5 select source file

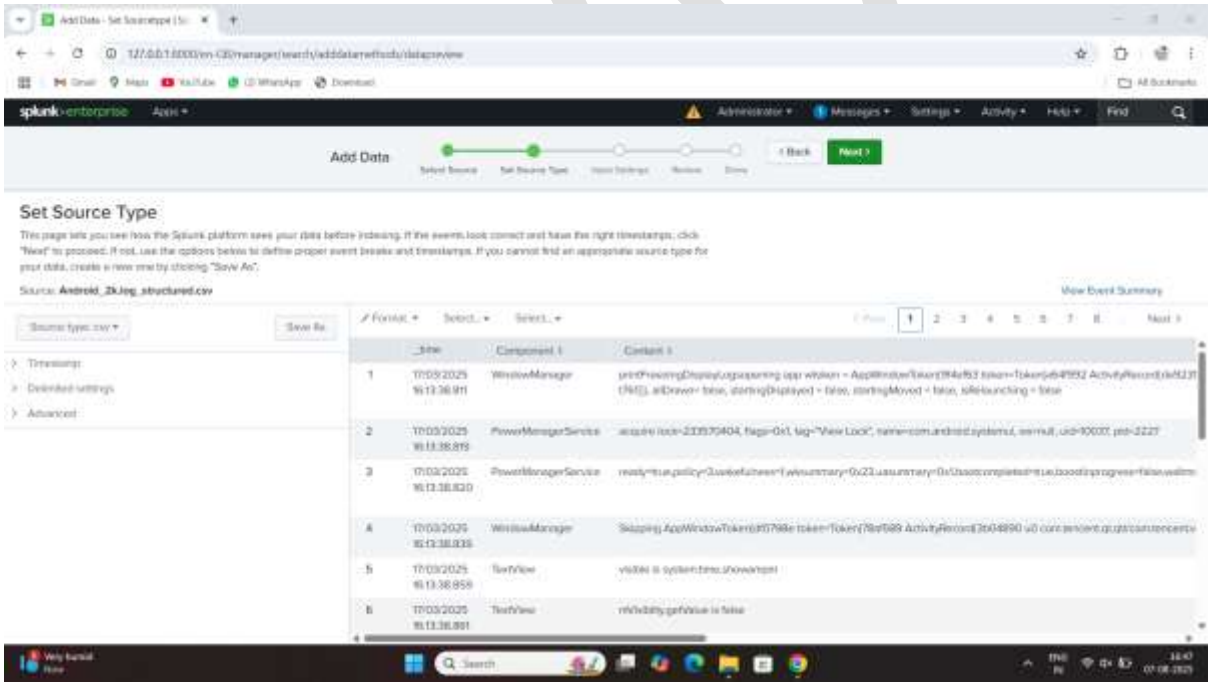


Step6 click on the source option and select the log file



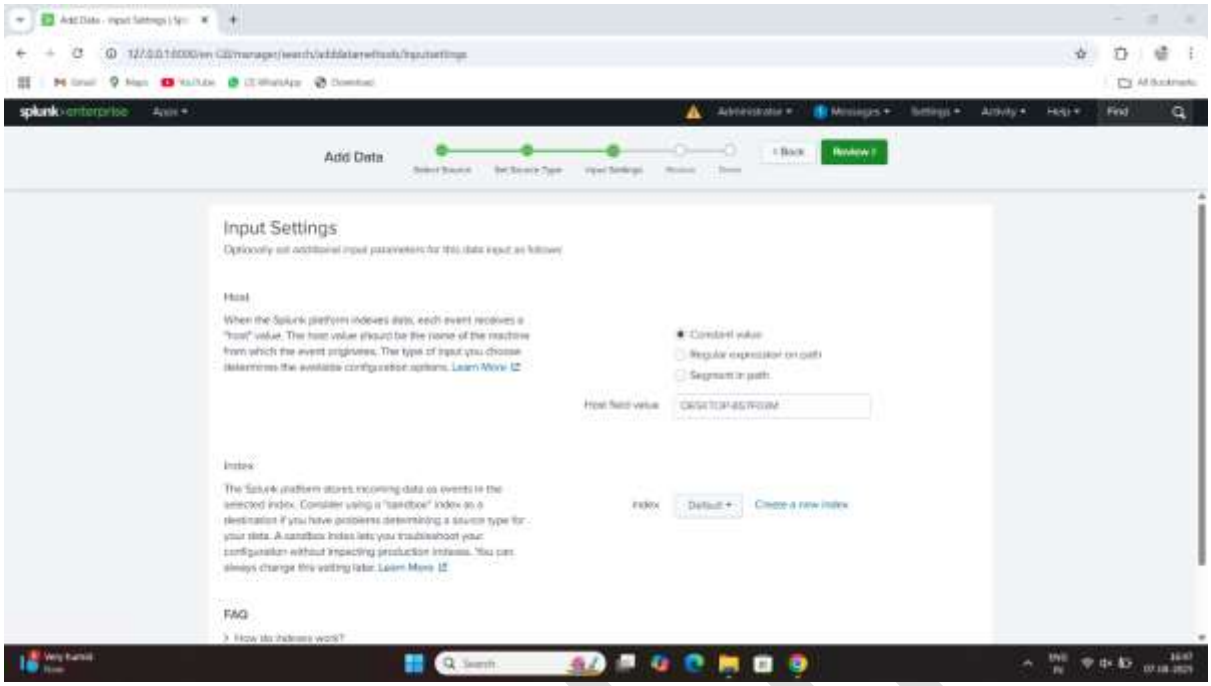


Step7 set source type



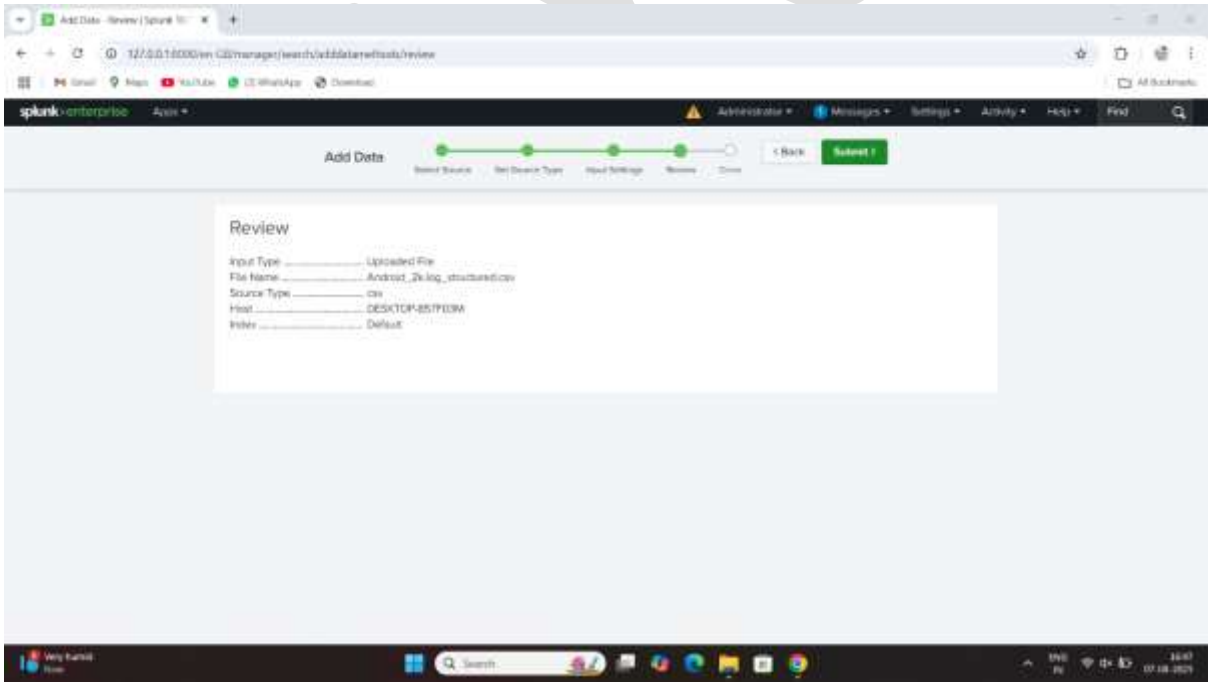
Click on next

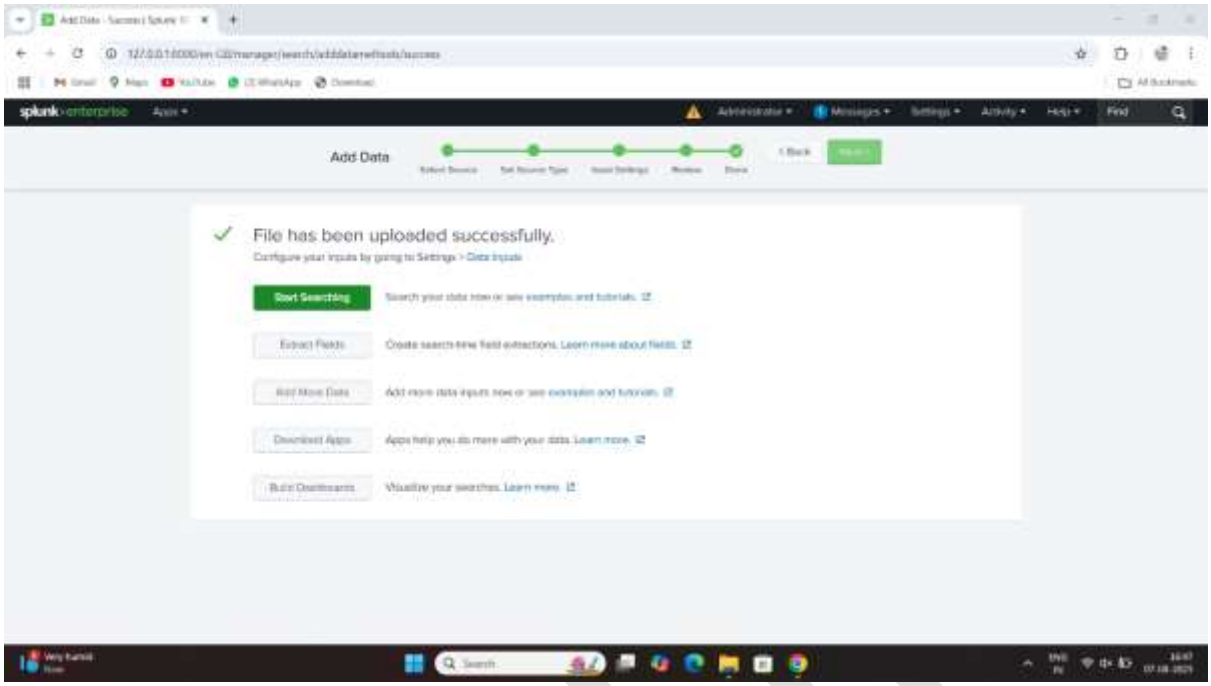
Step8 select the input setting



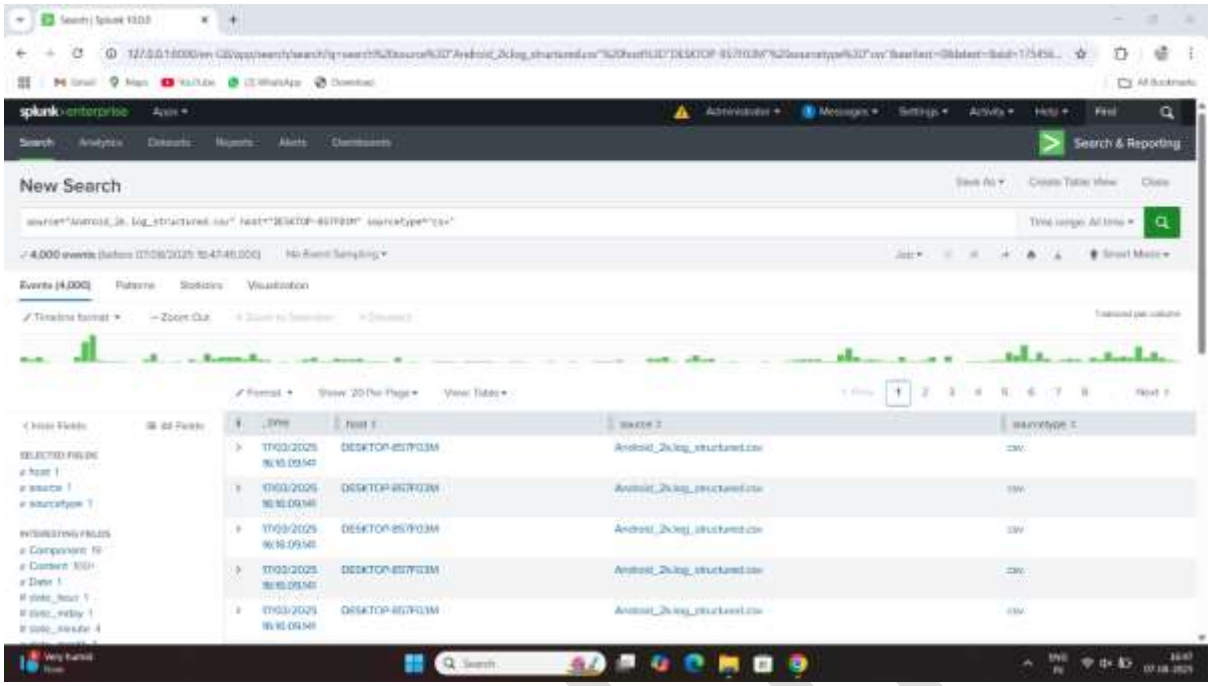
Click on next

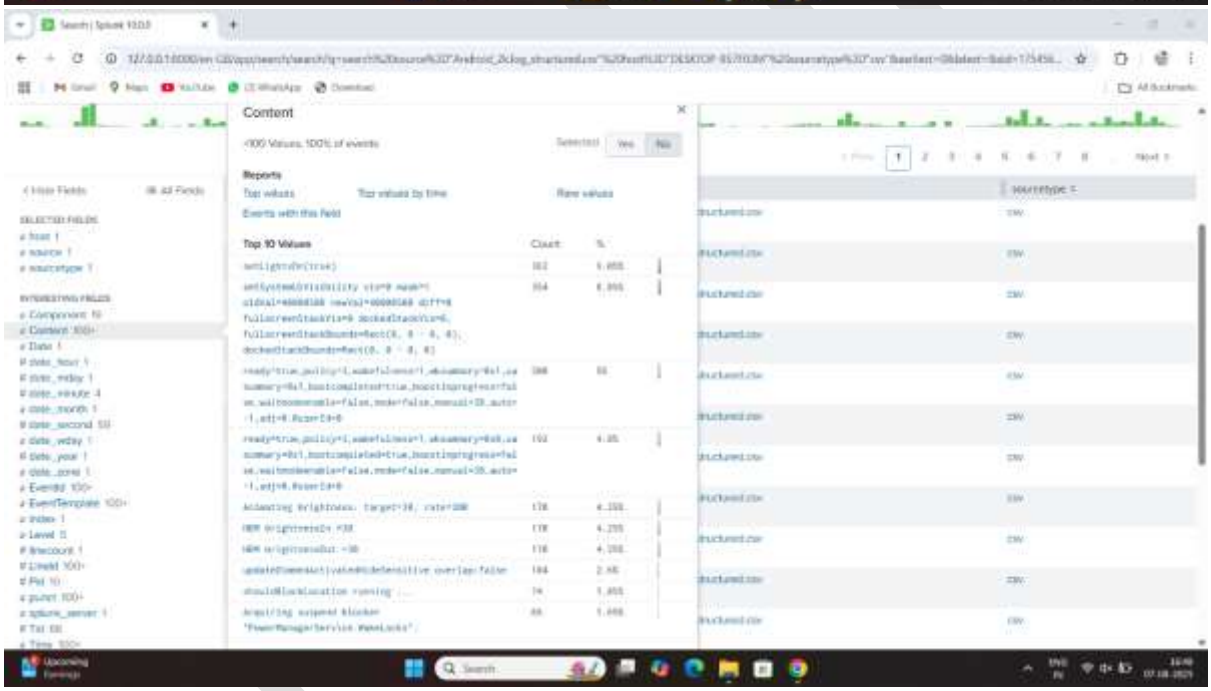
Step9 review





Step 10 click on start searching

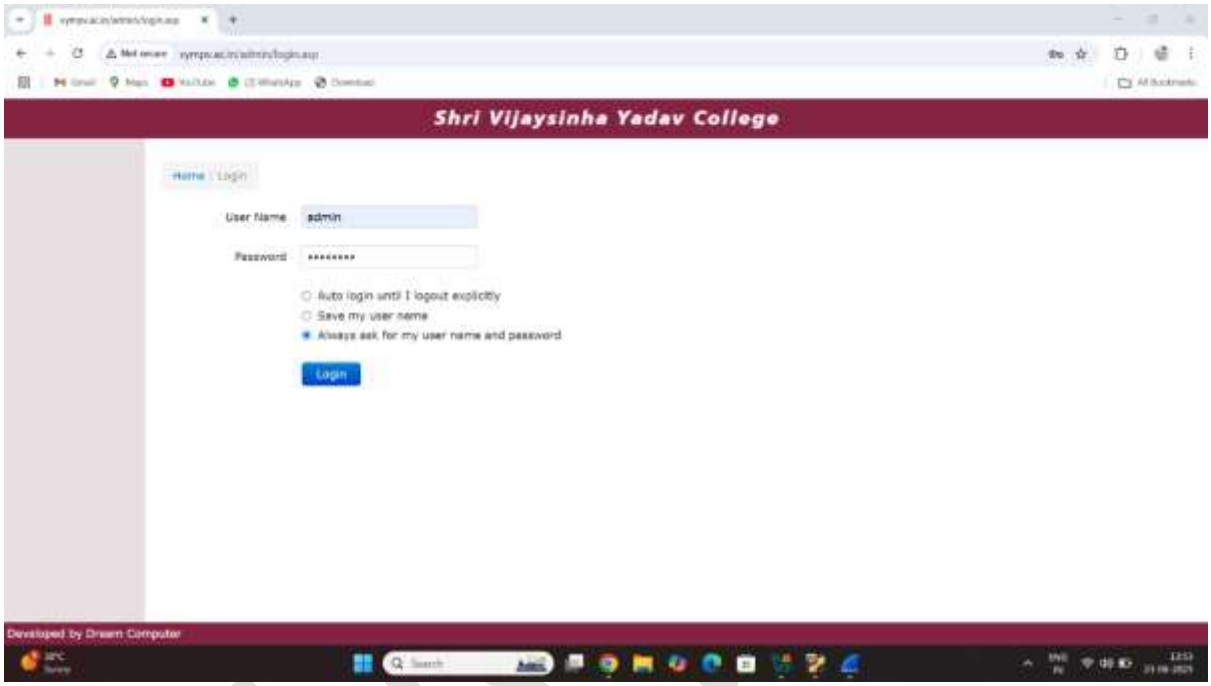




Lab2 identify and investigate various network attack using wireshark

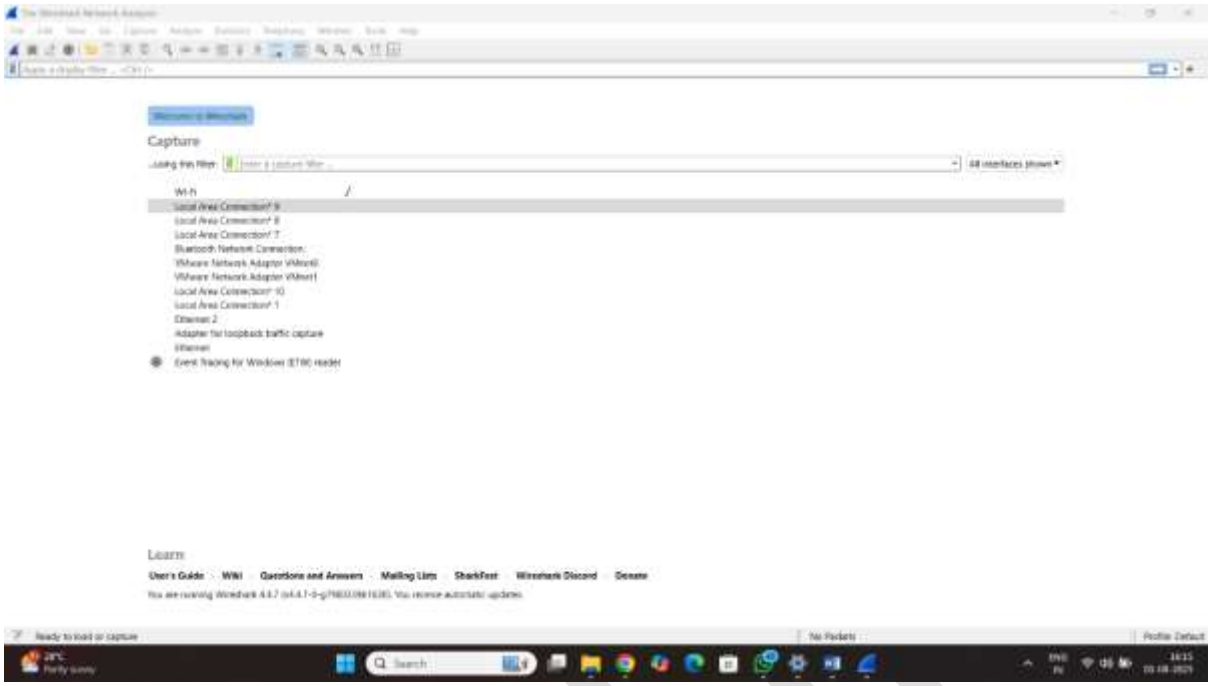
Step1: select the url target I am select the web site http://www.vympv.ac.in

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

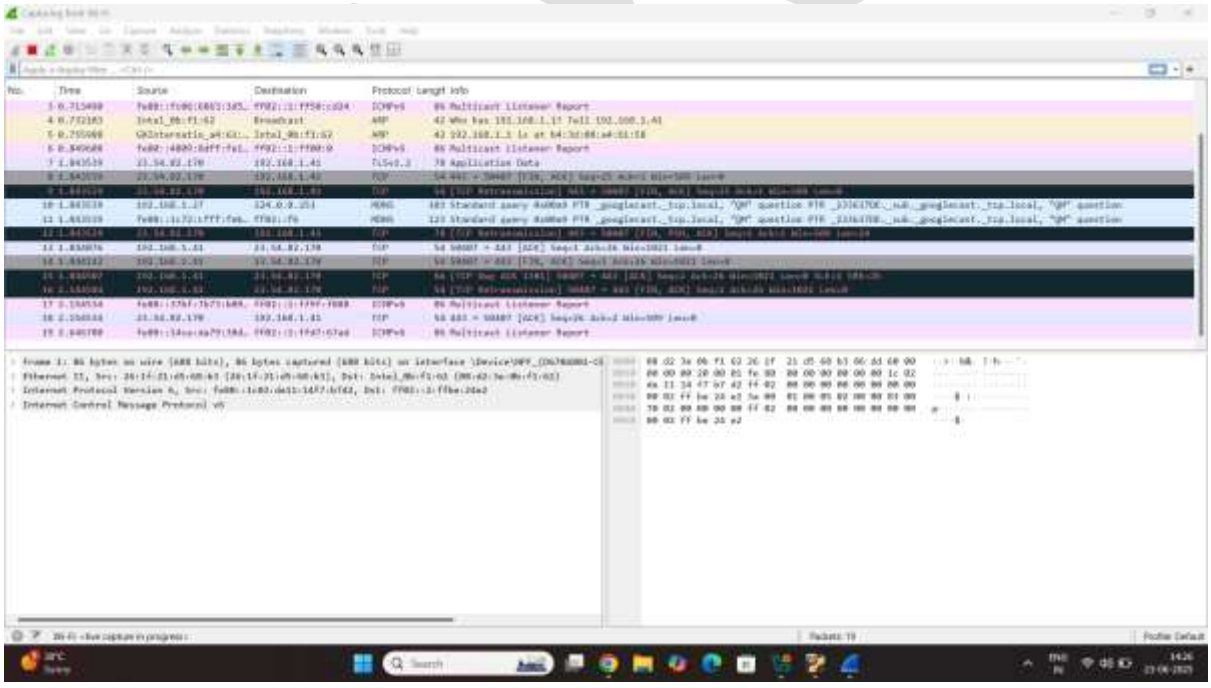


Step3: start the wire shark on network select the Lan

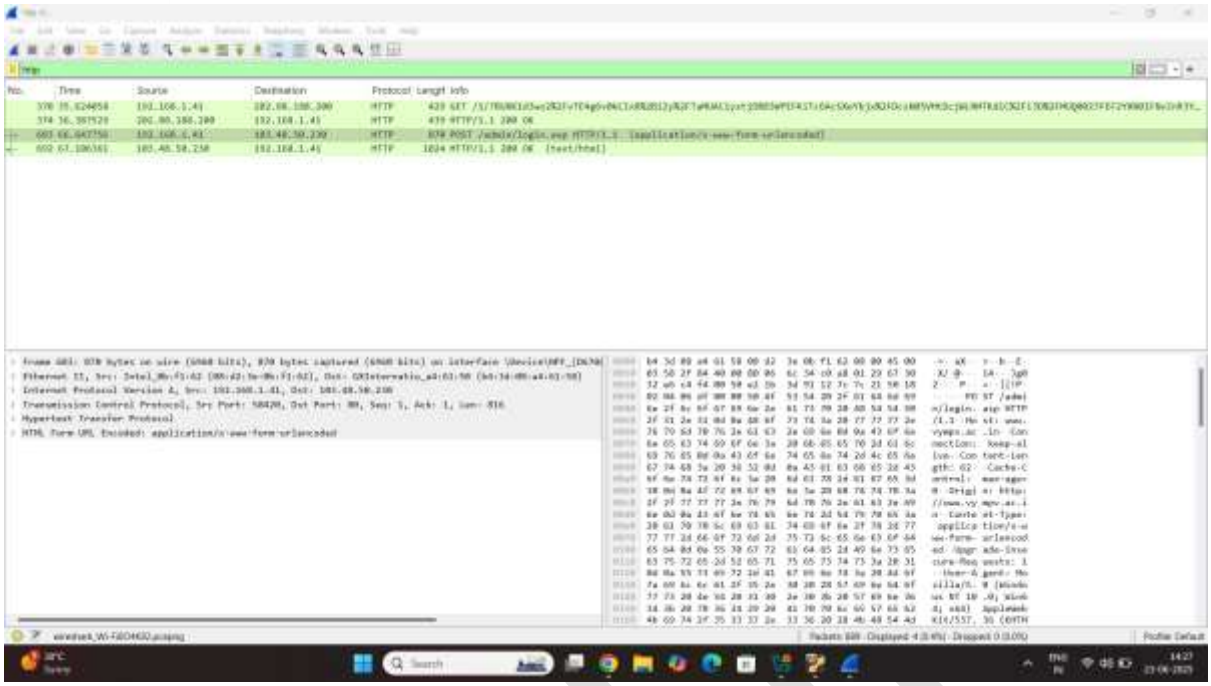
Step4 start the wireshark



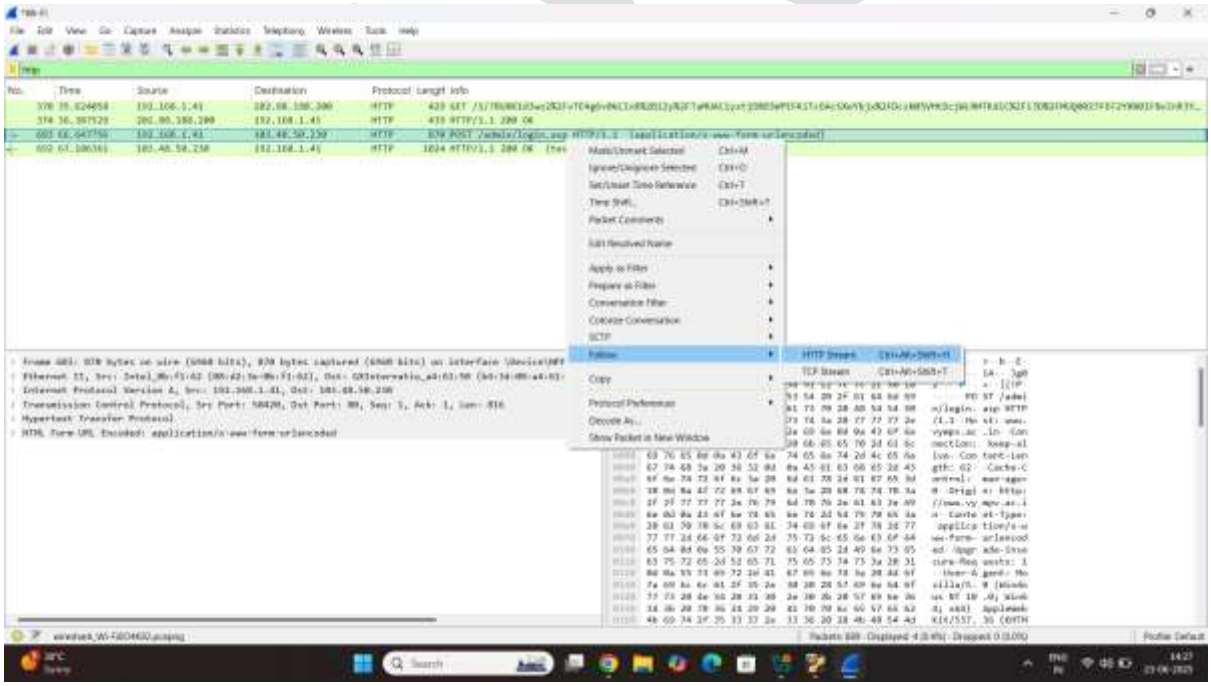
Step5 capture the request of wireshark



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: