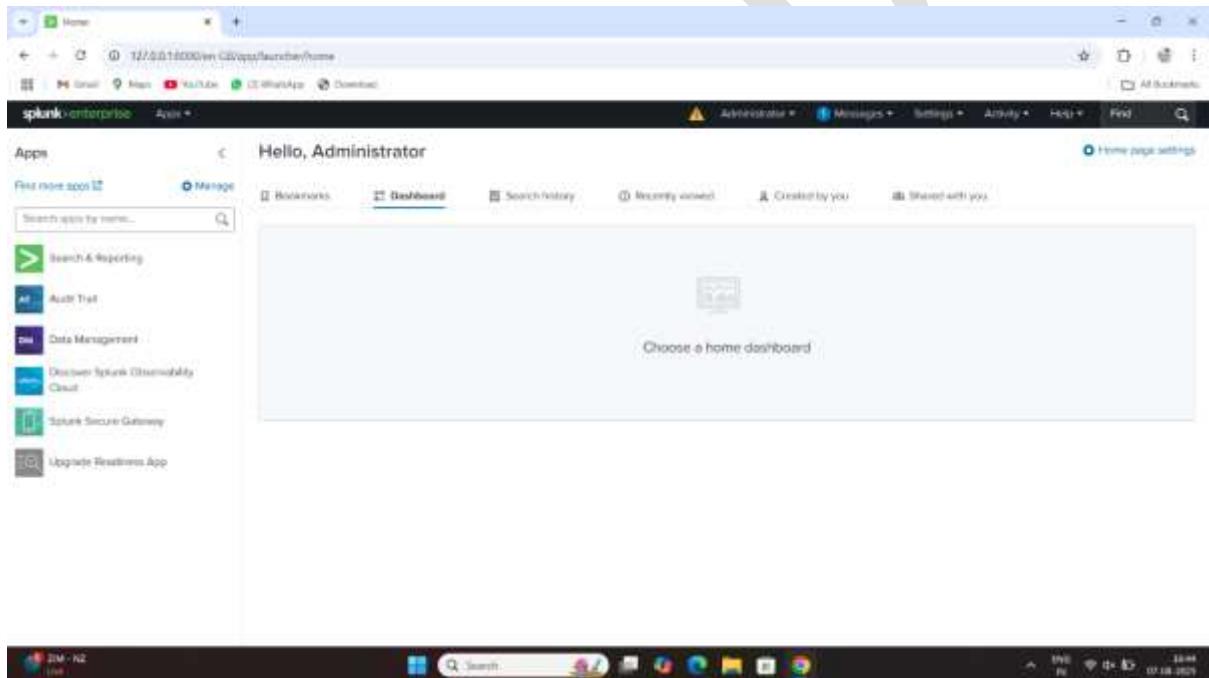


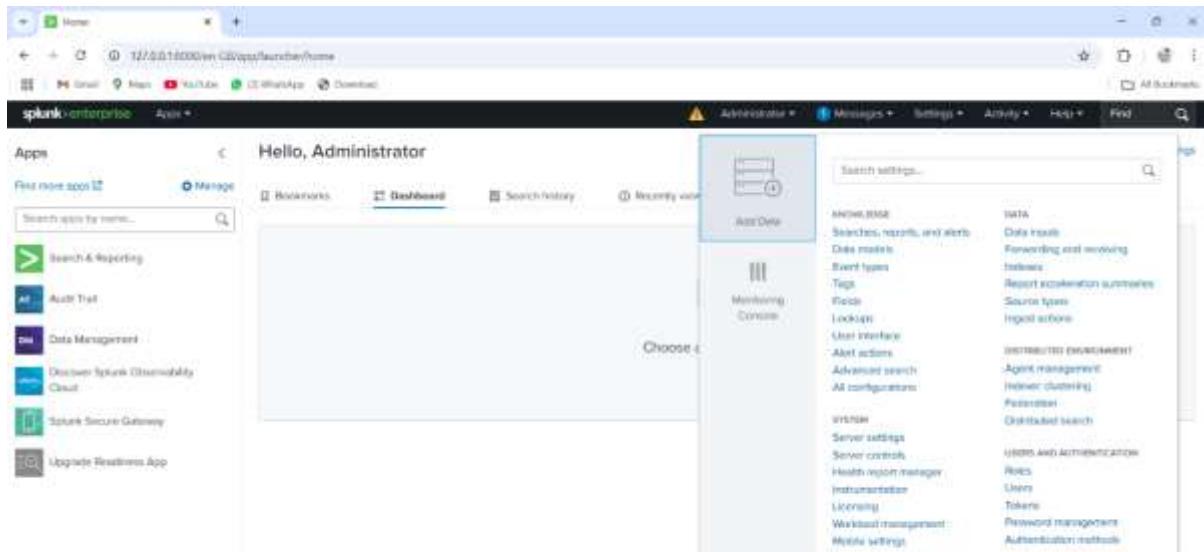
Module 8 network forensic

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

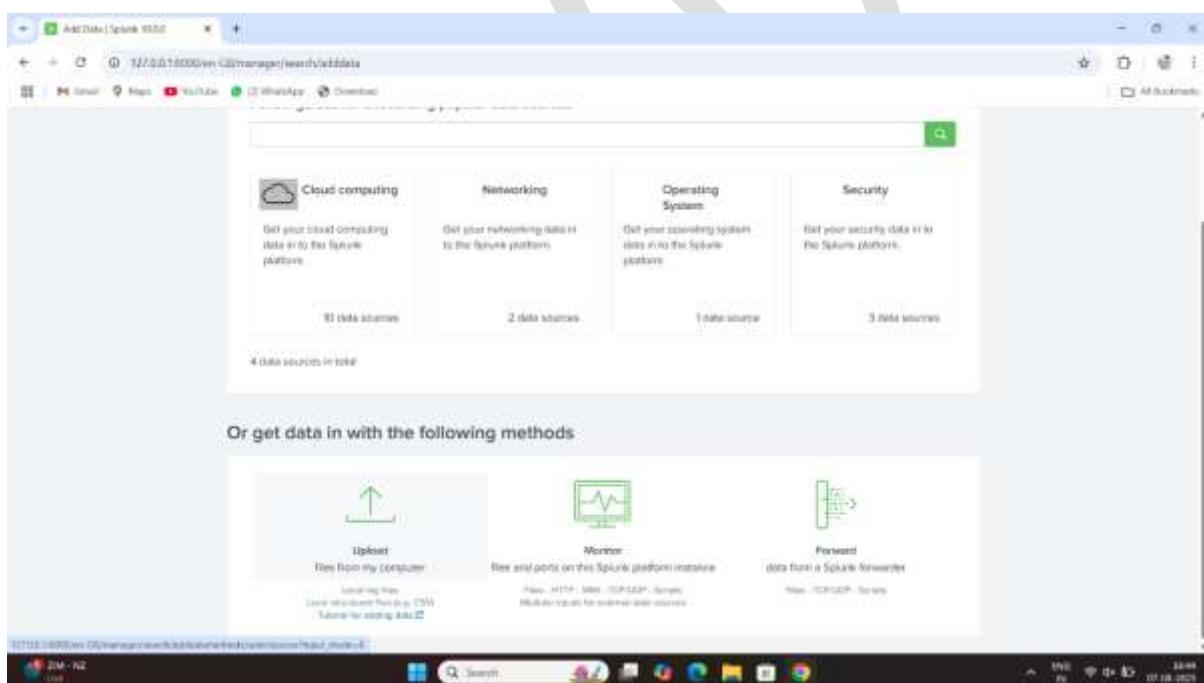
Step1 start the splunk



Step2 go to setting option

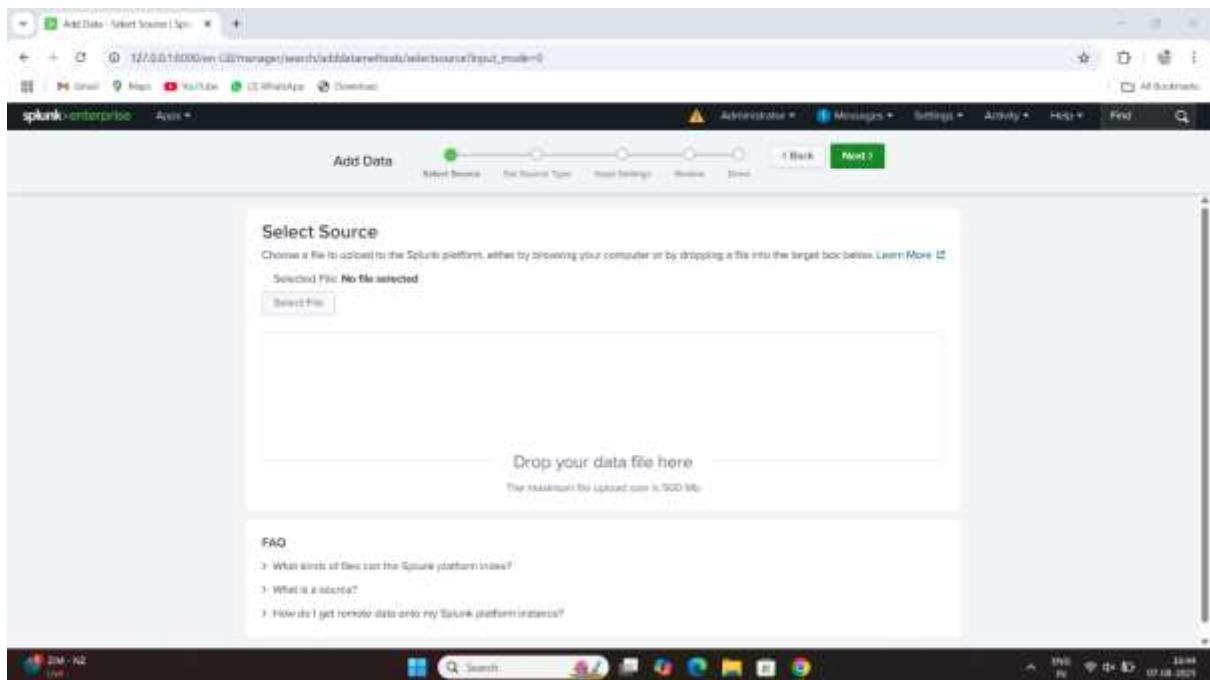


Step3 click on add data option

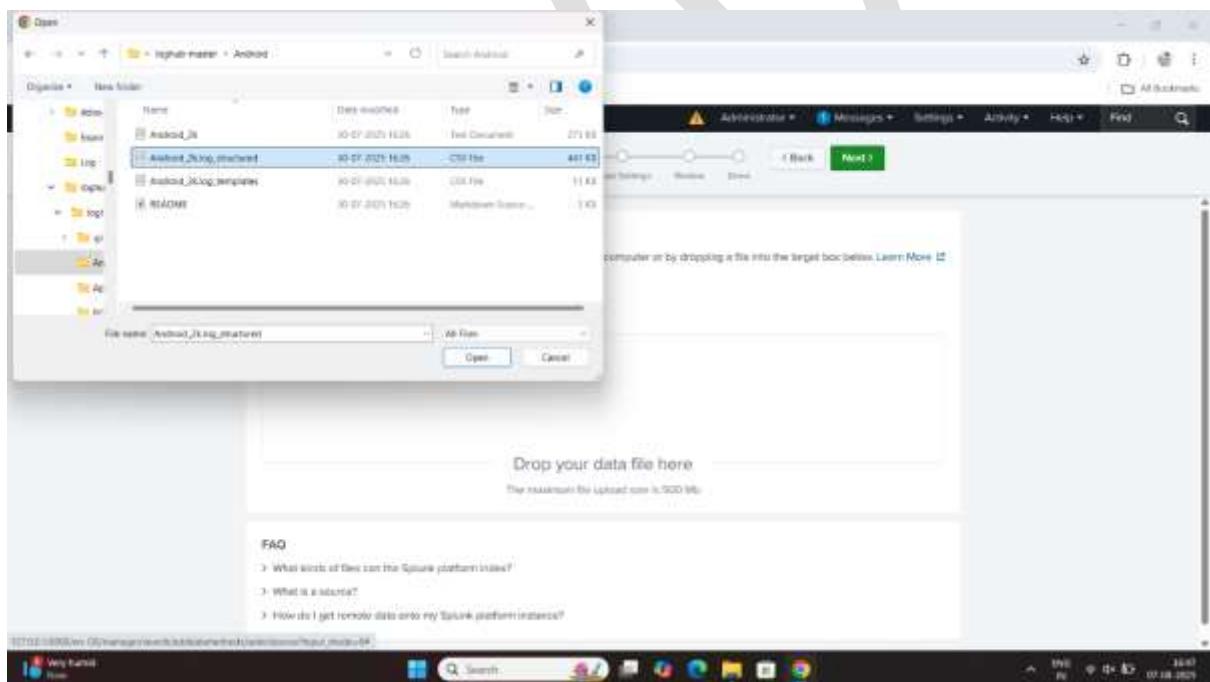


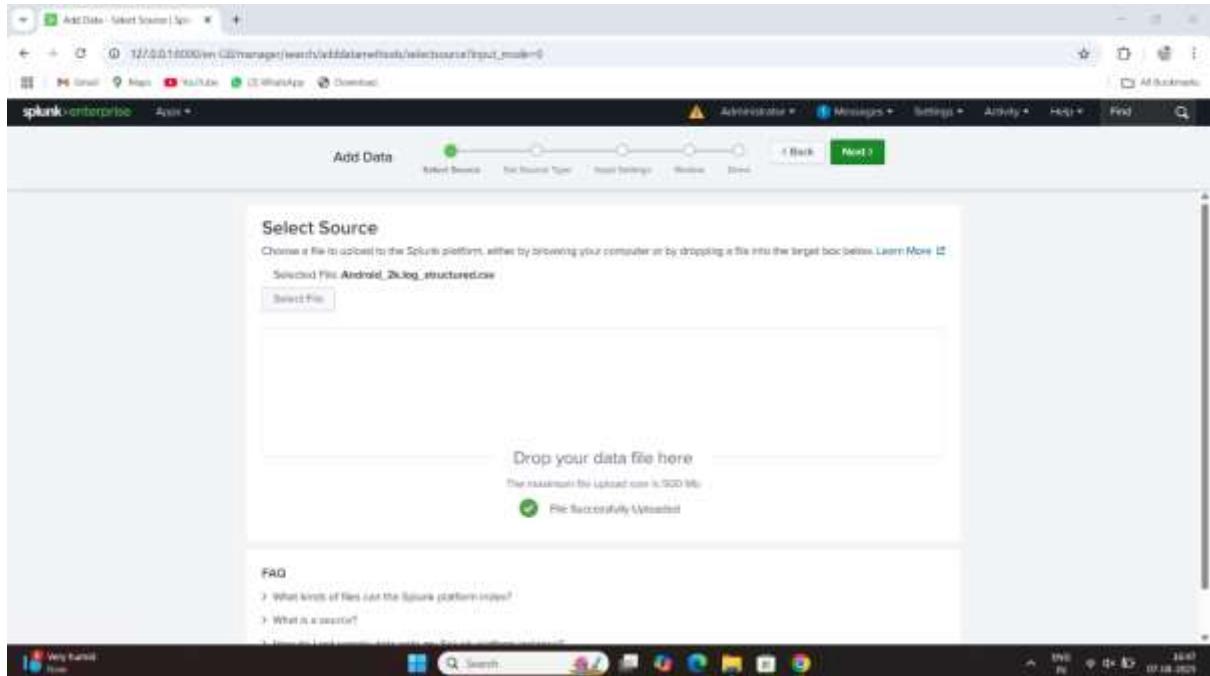
Step4 click on upload option

Step5 select source file



Step6 click on the source option and select the log file





Step7 set source type

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The current step is 'Set Source Type'. The event viewer shows several log entries from the 'Android_2klog_structured.csv' file. The progress bar shows the next steps: Input Settings, Review, and Done.

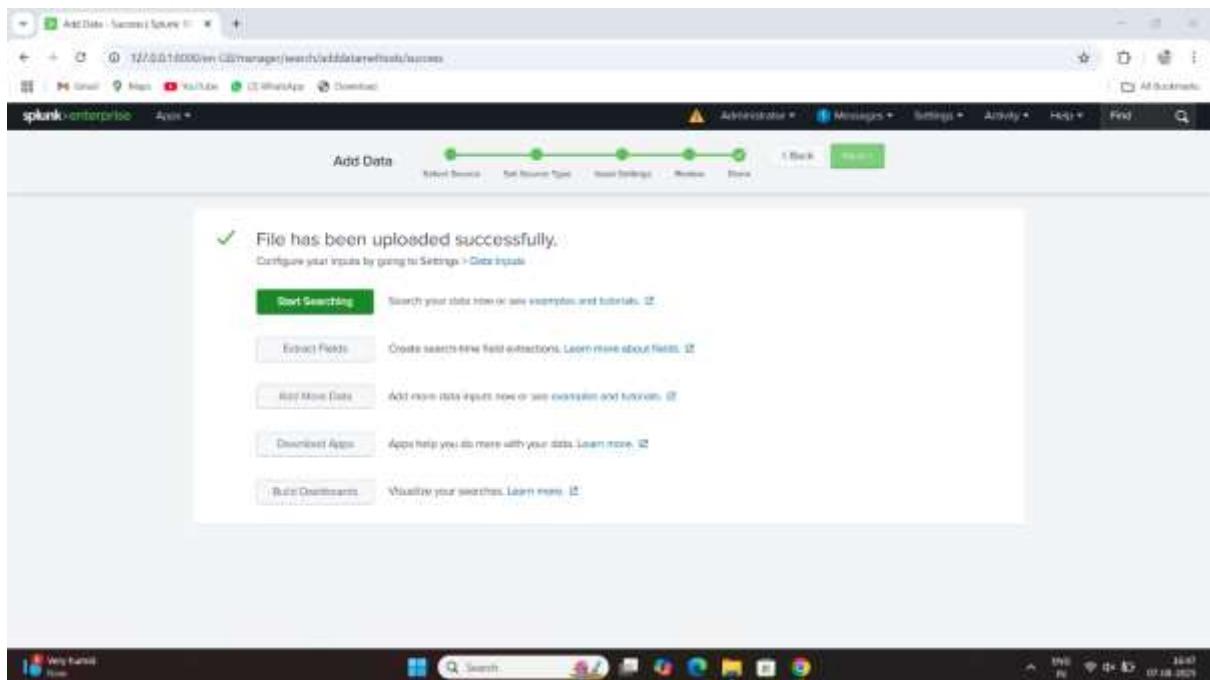
| # | Date | Component | Content |
|---|----------------------------|---------------------|--|
| 1 | 17/03/2025 01:13:38.911 | WindowManager | printResumingDisplayForResuming (app window = ApplicationWindow@194e953 token=Token@4f952 ActivityRecord@1e422f19ff), allowOver = false, startingDisplayed = false, startingMoved = false, selfLaunching = false |
| 2 | 17/03/2025 01:13:38.912 | PowerManagerService | acquire (@com-2230350404, flags=0x1, tag="View Lock", name=com.android.systemui, result=0, uid=10000, pid=2227) |
| 3 | 17/03/2025 01:13:38.913 | PowerManagerService | resetDisplayPolicy("DisplayFeatureSummary@0x211a0000/0x211a0000@true,0x2000000000000000") |
| 4 | 17/03/2025 01:13:38.918 | WindowManager | Skipping AppWindowToken@170796e takeToken@Token@4f959 ActivityRecord@2004890 w0 core:reschedule@0x2000000000000000 |
| 5 | 17/03/2025 01:13:38.959 | NotifyView | visible @ system@this.show@root |
| 6 | 17/03/2025 01:13:38.991 | NotifyView | mVisibility.getVisible is false |

Click on next

Step8 select the input setting

Click on next

Step9 review



Step 10 click on start searching

The image displays two side-by-side screenshots of the Splunk Enterprise web interface. Both screens show a search results page for a query related to Android logs.

Top Screenshot (Search Results):

- Search Bar:** Contains the query: `source="Android_2b_log_structured.log" host="DESKTOP-867F03M" sourcetype="log"`.
- Event Count:** Shows 4,000 events from 07/08/2020 10:47:40,000 to 07/08/2020 10:47:40,000.
- Event View:** Displays a table of 10 selected events. The columns include _id, _index, host, source, sourcetype, and _raw.

| _id | _index | host | source | sourcetype | _raw |
|-----|------------|--------------------------------|-------------------------------|------------|---|
| 1 | IT002/2020 | DESKTOP-867F03M 07/08/09:47 | Android_2b_log_structured.log | log | 2020-07-08T09:47:40,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:47:40,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 2 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 3 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 4 | IT002/2020 | DESKTOP-867F03M 07/08/09:47 | Android_2b_log_structured.log | log | 2020-07-08T09:47:40,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:47:40,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 5 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 6 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 7 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 8 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 9 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |
| 10 | IT003/2020 | DESKTOP-867F03M 07/08/09:48 | Android_2b_log_structured.log | log | 2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log {"host": "DESKTOP-867F03M", "log": "2020-07-08T09:48:00,000Z Android_2b_log_structured.log DESKTOP-867F03M Android_2b_log_structured.log ", "sourcetype": "log"} |

Bottom Screenshot (Content View):

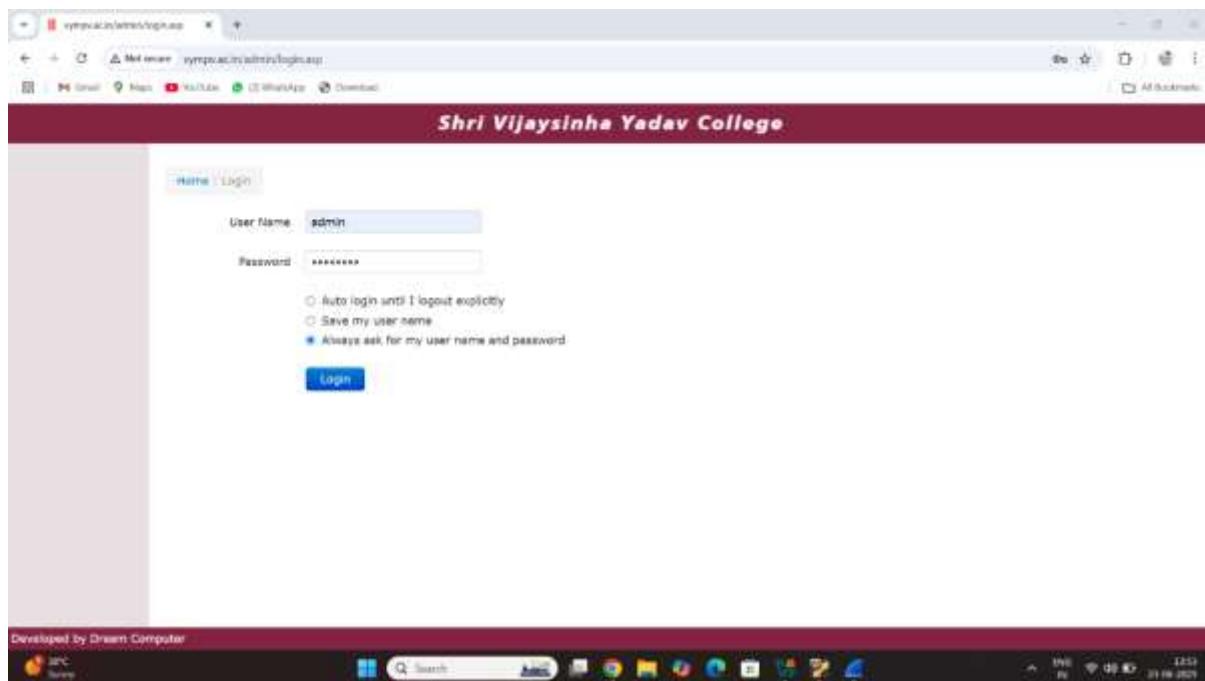
- Report Type:** Top values, ordered by count.
- Results:** Shows the top 10 values and their counts. The top value is `structured.log` with a count of 1,000.
- Event View:** Displays a table of 10 selected events, similar to the top screenshot.

| Value | Count | % |
|----------------|-------|-----|
| structured.log | 1,000 | 100 |

Lab2 identify and investigate various network attack using wireshark

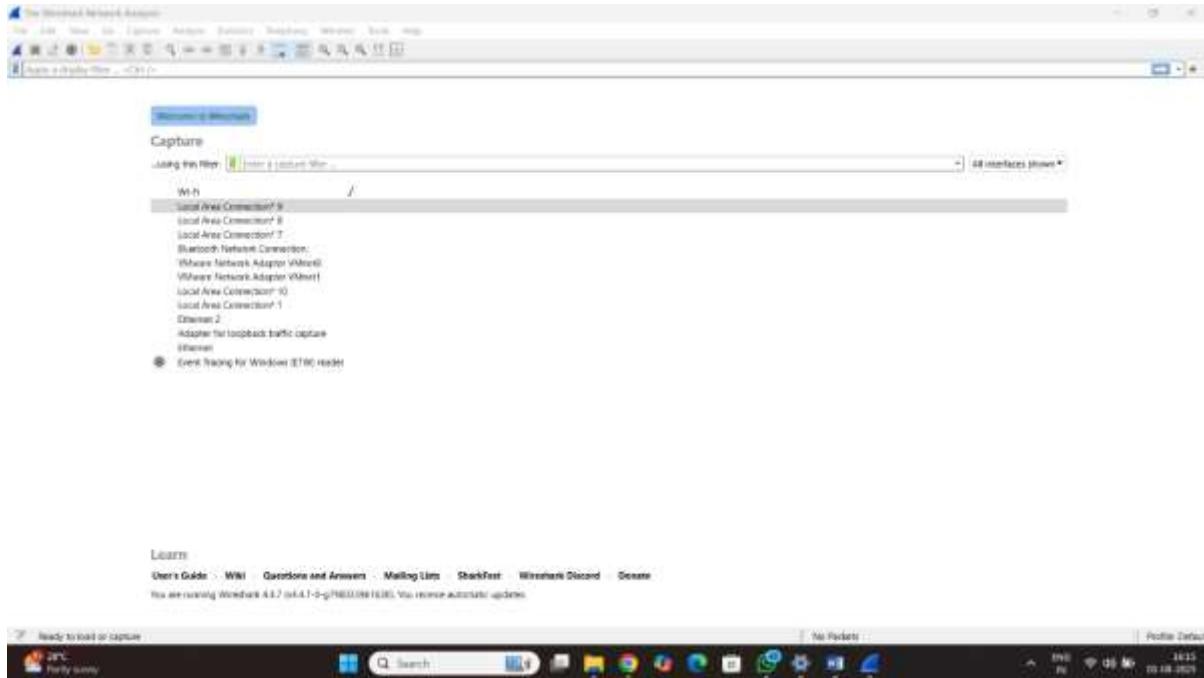
Step1: select the url target I am select the web site
<http://www.vympv.ac.in>

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

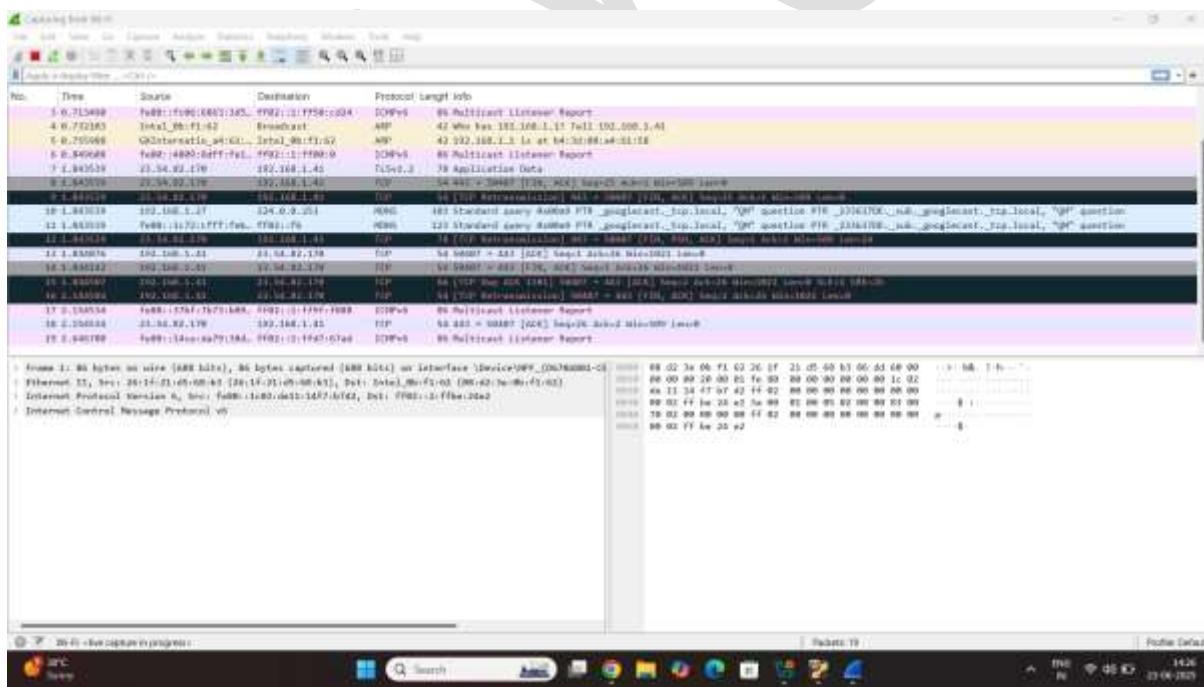


Step3: start the wire shark on network select the Lan

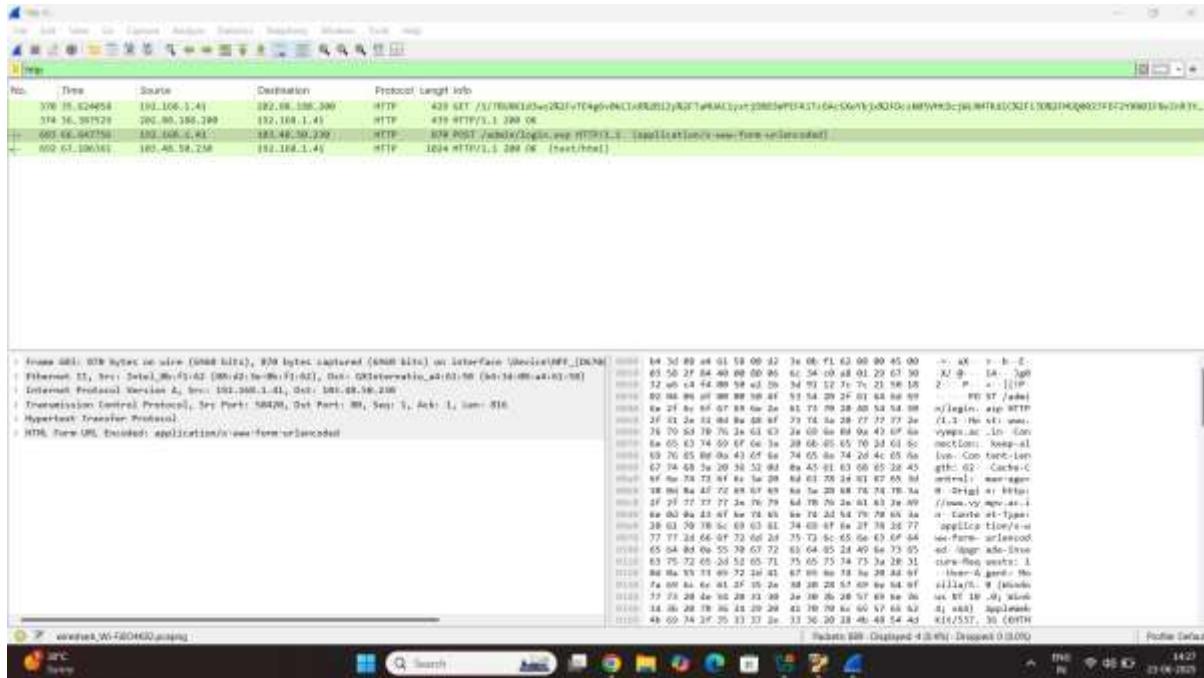
Step4 start the wireshark



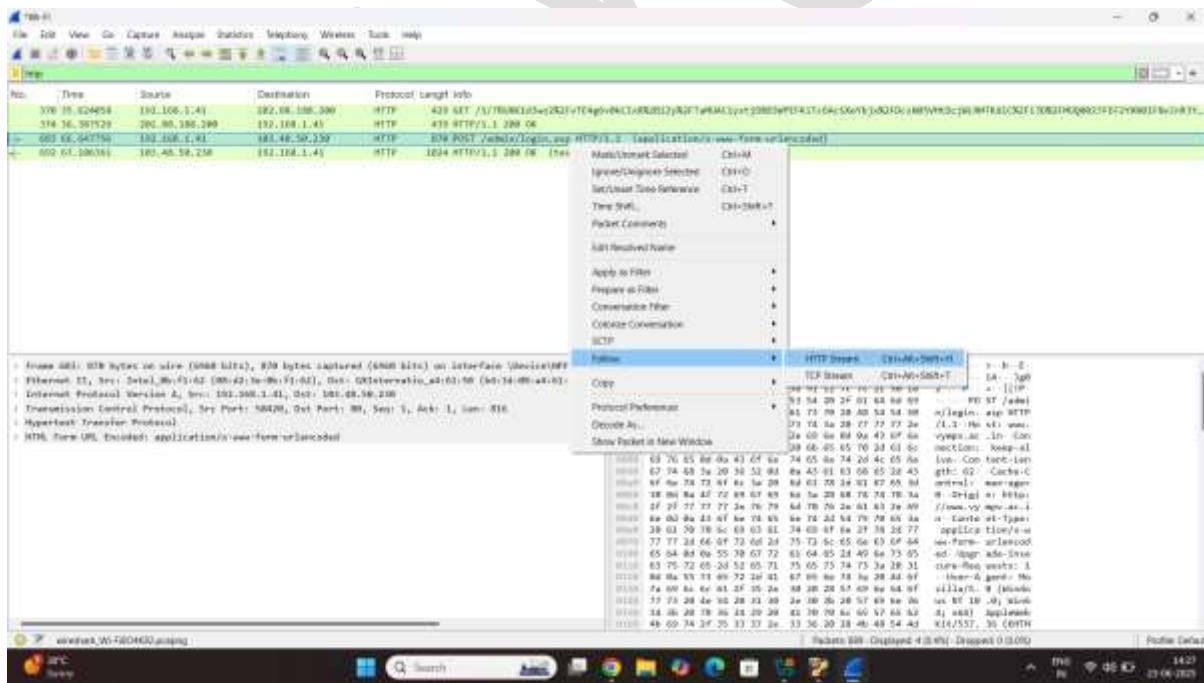
Step5 capture the request of wireshark



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:

