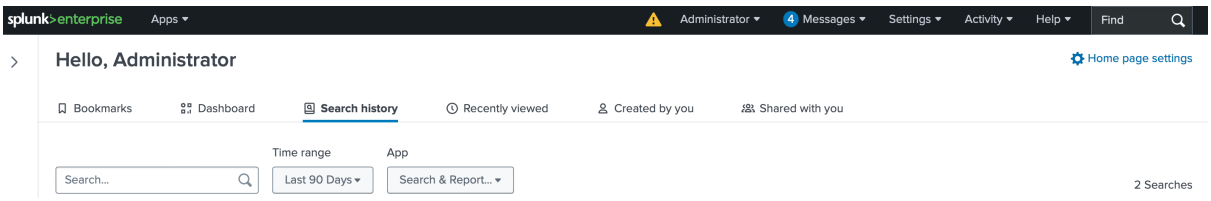
LAB 8 – SIEM

A. Installation and environment set up
   a. Download and follow the instructions here to install SIEM https://help.splunk.com/en/splunk-enterprise/get-started/search-tutorial/10.0/part-1-getting-started/install-splunk-enterprise#a686eb97_b6b4_4692_b0db_daeda6df1f98__macOS_installation_instructions

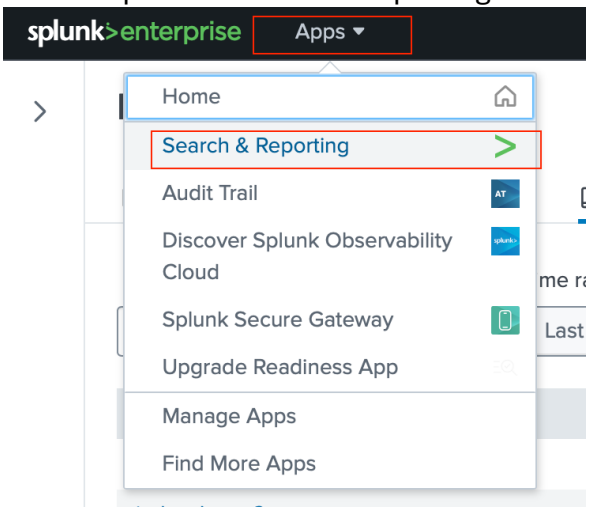
   b. Download and install dataset Botsv2: download and follow the instructions here (see "Installation" section to install the dataset https://github.com/splunk/botsv2
   or follow the below instruction
      - Download Botsv2
      - Unzip/untar the downloaded file into "$SPLUNK_HOME/etc/apps" where $SPLUNK_HOME is the folder that you have installed Splunk.

        Example: in a macbook, you can find the folder "apps" at `/Applications/Splunk/etc/apps`

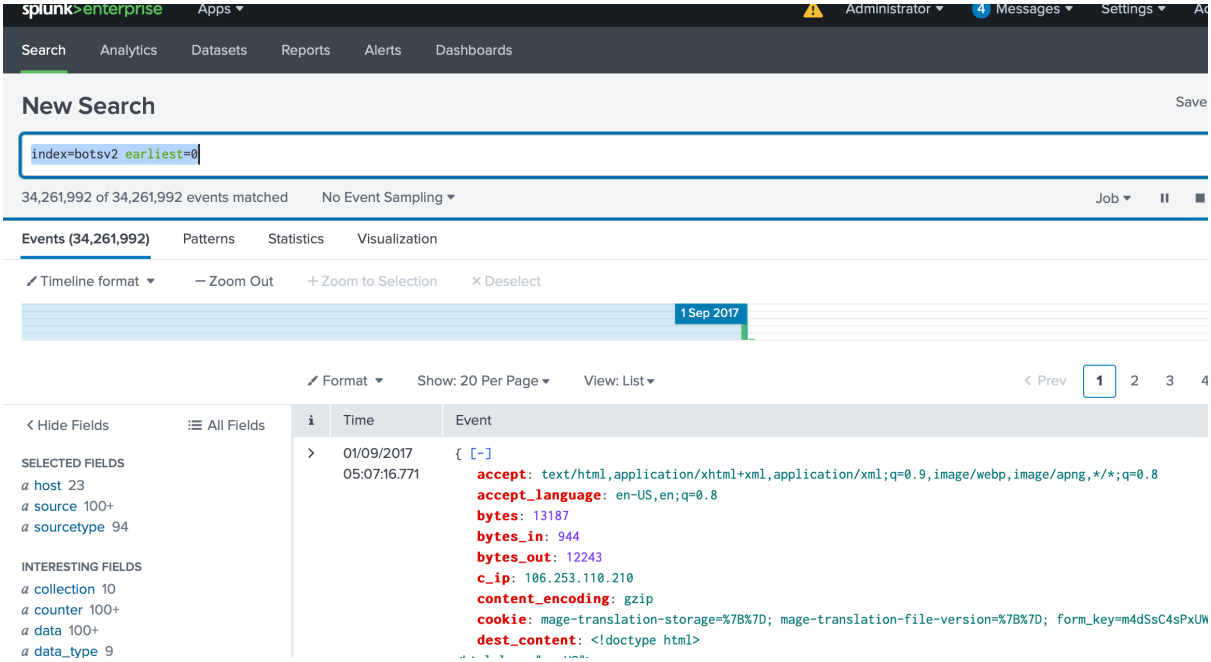
   c. Running Splunk using the web browser: http://localhost:8000/
   You will see the interface as below



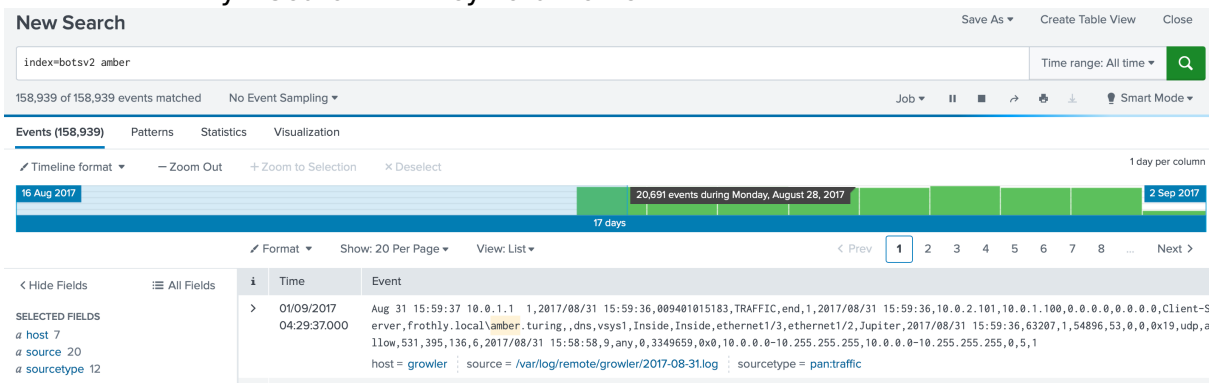
   d. Open "Search and Reporting" function



   e. Run the following search "index=botsv2 earliest=0" to see if it works



f. Try if Search with keyword works



B. Using SIEM for The following questions are based on Try Hack Me-Splunk 2

Scenario: In this exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothly (*a beer company*) to assist them with their recent issues. The focus is on Amber Turing and her communication with a competitor. Example: search for information relevant to "Amber" in the dataset

100 series questions:

[1] Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

[2] Amber found the executive contact information and sent him an email. What image file displayed the executive's contact information? Answer example: /path/image.ext

[3] What is the CEO's name? Provide the first and last name.

[4] What is the CEO's email address?

[5] After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

[6] What is the name of the file attachment that Amber sent to a contact at the competitor?
[7] What is Amber's personal email address?

200 series questions

[1] What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.
[2] What is the public IPv4 address of the server running “www.brewertalk.com”? (Please do NOT access this website)
[3] Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com (Please do NOT access this website)
[4] The IP address from Q#2 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php
[5] What SQL function is being abused on the URI path from the previous question?
[6] What was the value of the cookie that Kevin's browser transmitted to the malicious URL as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an equal sign.
[7] What brewertalk.com username was maliciously created by a spear phishing attack?