Unit 3

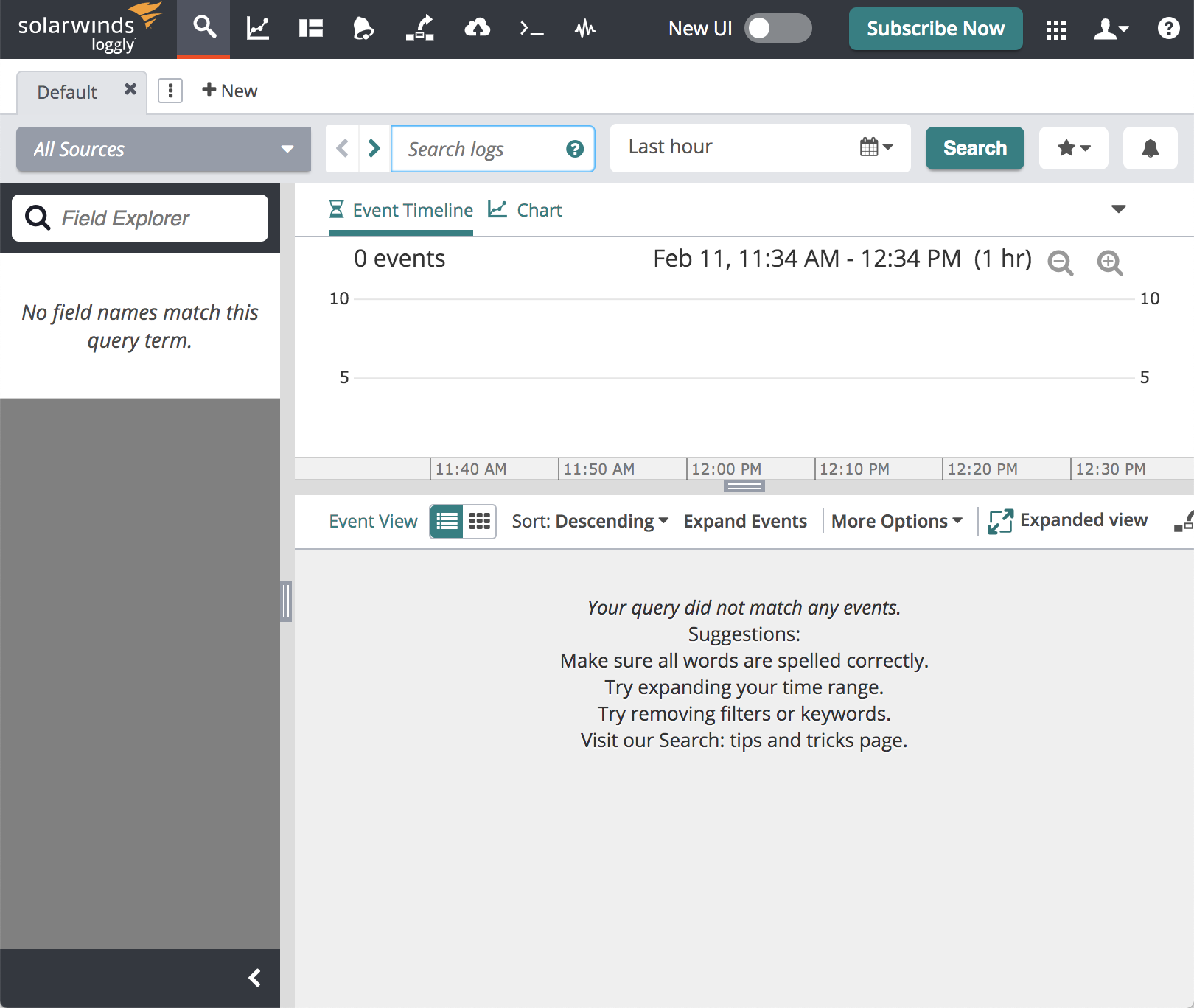
3.2 Logging

Exercise 1

* Import logs into Loggly, count visits by IP address, show top 10 results

Solution

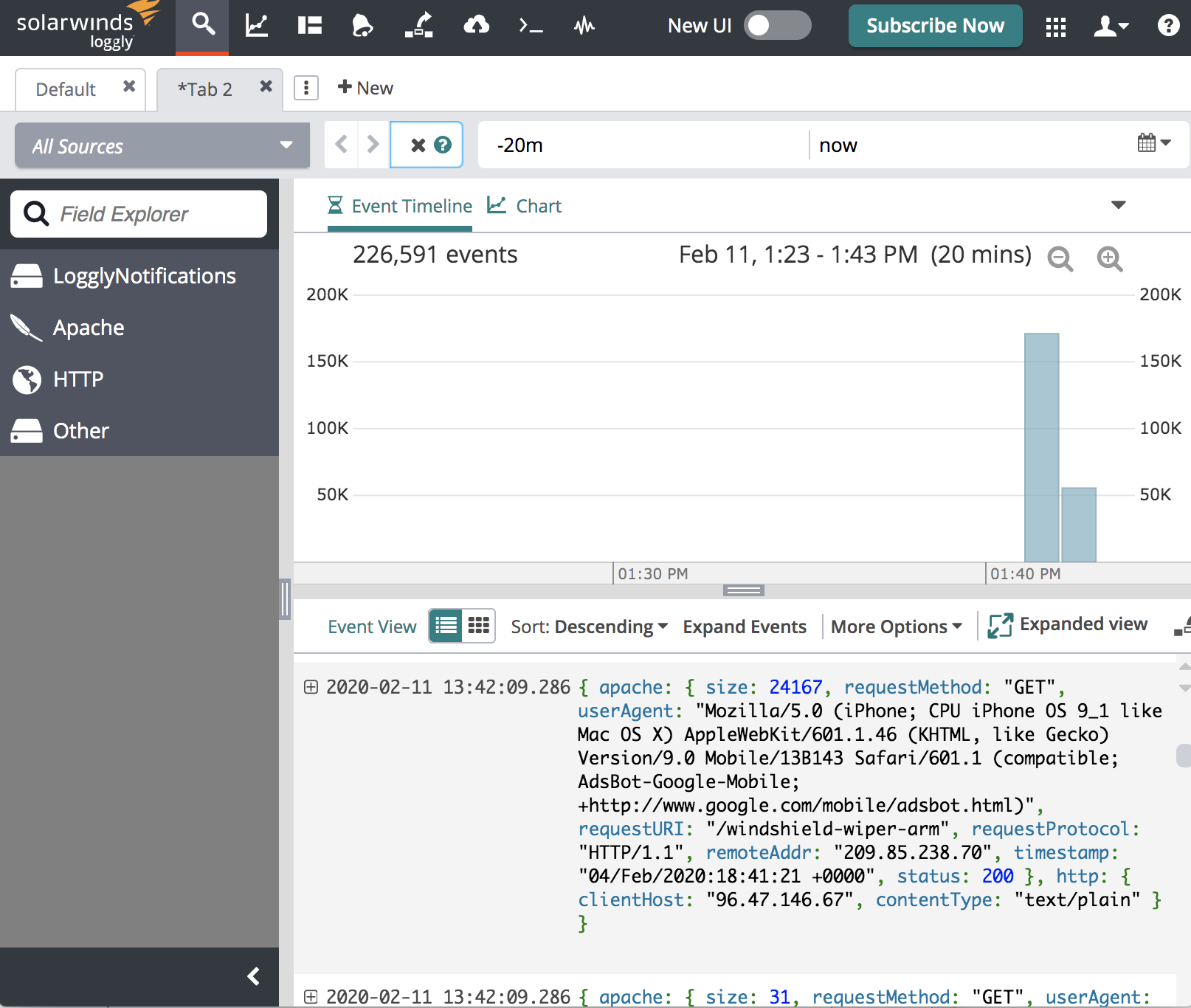
1. Downloads Nginx access logs to local machine
2. Create a new account at loggly.com



Click source setup (cloud with arrow icon) on the top

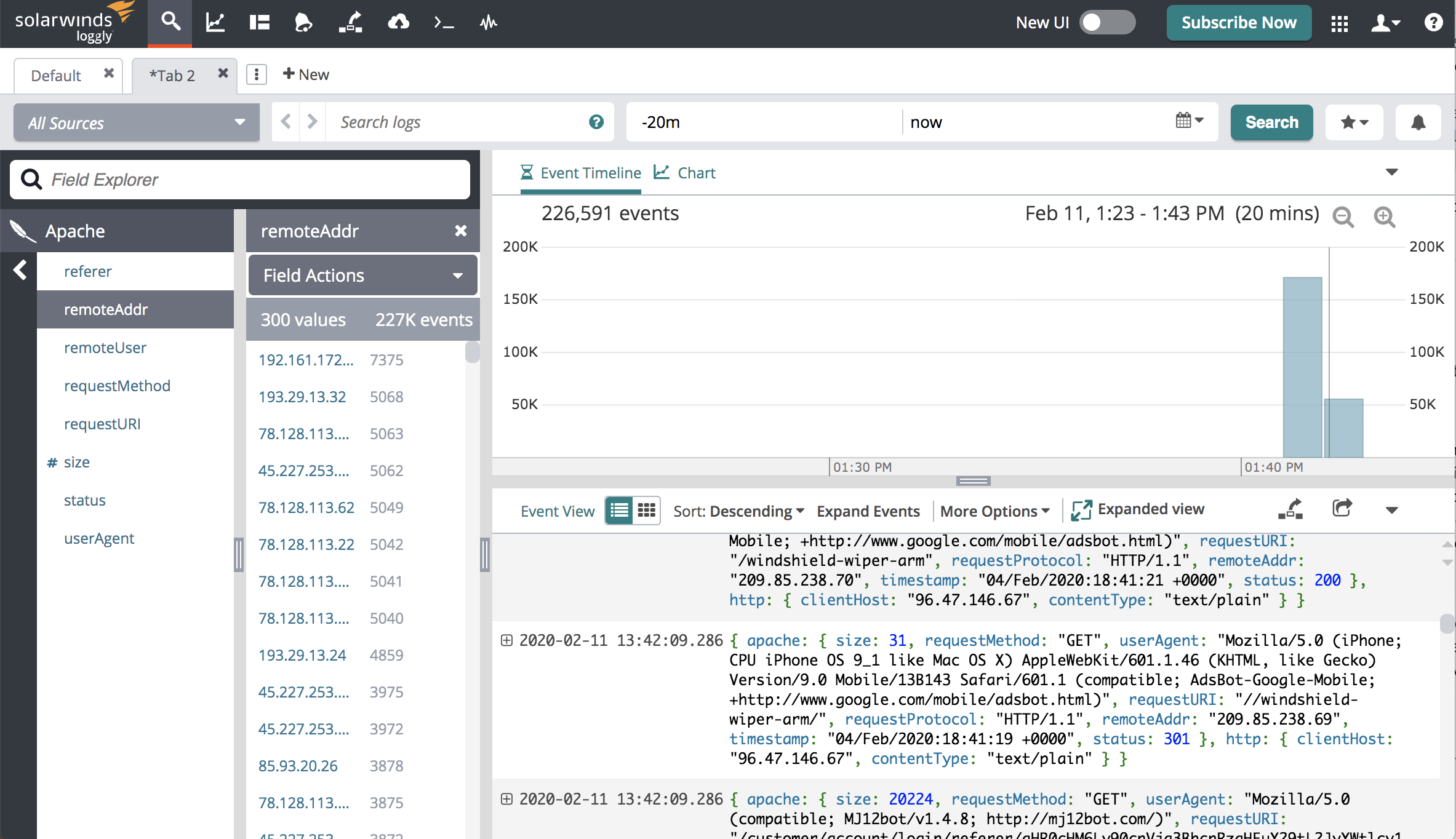
Click Log File and select Browser File Upload

After the file uploads, click Show me my logs link and you should start seeing a list of events and timeline chart

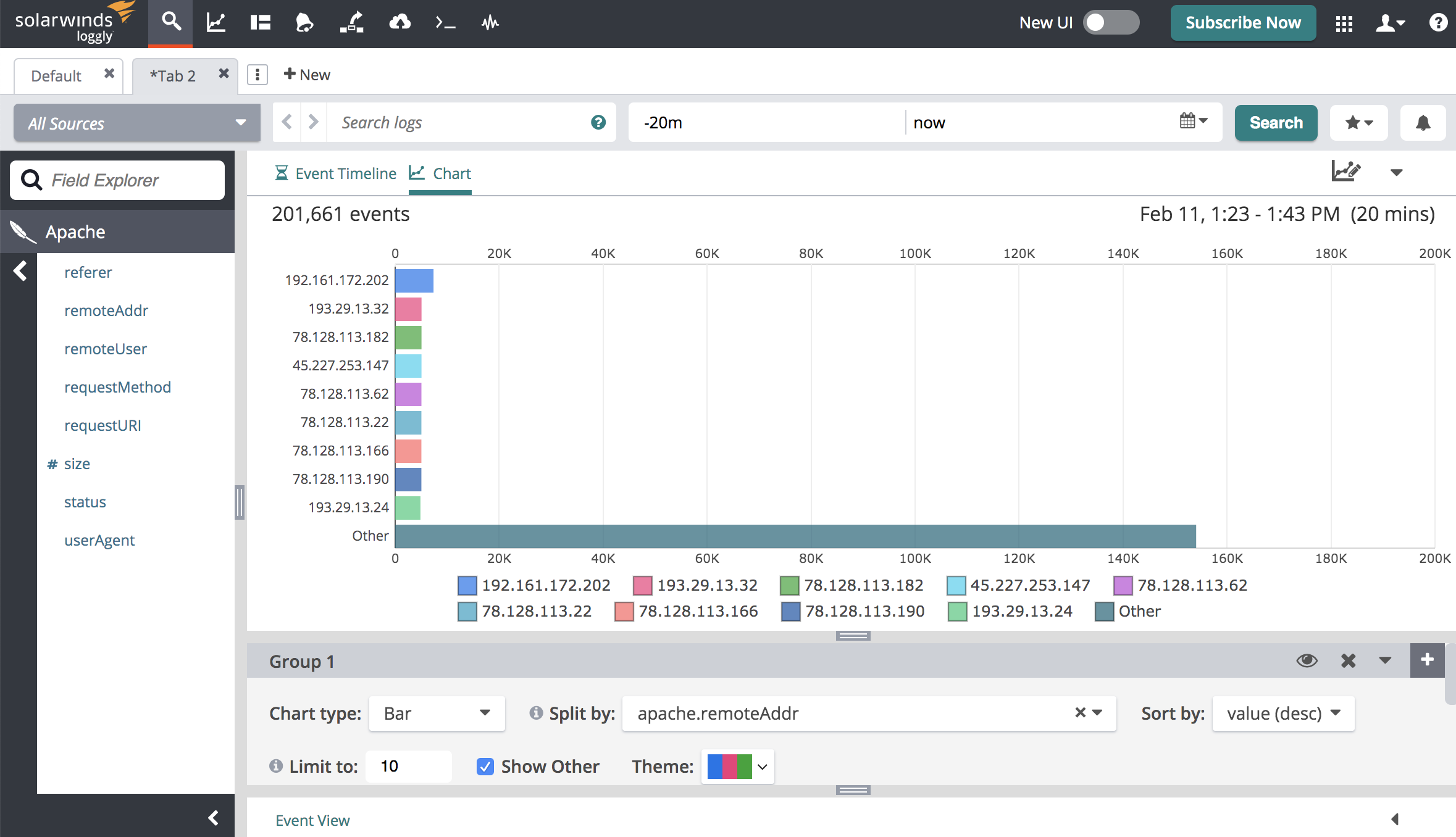


In the left menu, Field Explorer, choose Apache and then remoteAddr

You will see the following



In the Field Actions menu choose View as Bar Chart and you should see top 10 IP addresses that visited the site over last 20 minutes. This can help identify for example a denial of service attack.

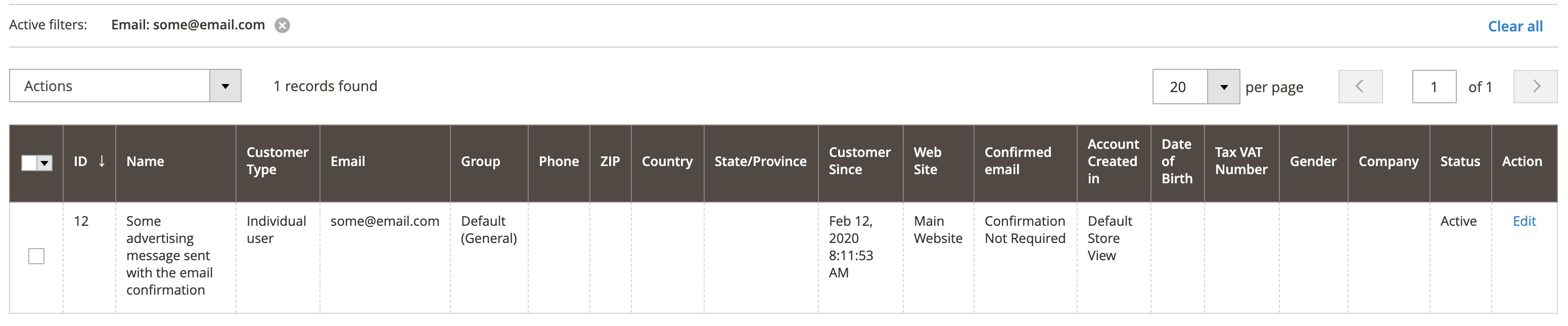


# Exercise 2

While reviewing the customer grid in the Magento admin panel, a business user identified suspicious user signups.

An example of a suspicious customer record is pictured below (pic 2.1).

Current admin locale timezone is set to “Pacific Standard Time (America/Los\_Angeles)” (UTC -8).



Pic. 2.1. Customer Since column has the value “Feb 12, 2020 8:11:53 AM”

## Task

* Identify from which IP address the customer create request was made from (sample access.log file is available in the exercise materials for this investigation);
* Enable the captcha solution for the customer registration page to prevent frontend customers creation by the automated scripts (complete it on your Magento 2 instance);

## Solution

1. Find out the customer creation date from the customer record info.
   1. Can be found in the Magento admin panel at Customers > All Customers grid. Find the appropriate customer record and check the “Customer Since” column value (datetime in the current admin locale timezone).
   2. Can be found in the database in the customer\_entity table, created\_at field (datetime in the UTC timezone).
2. Find the IP address information from the access.log for the request which created the account.
   1. Customer account is created with a POST request /customer/account/createpost
   2. Access.log contains datetime info in the UTC timezone. To find an account creation datetime in a UTC format a conversion must be completed from the admin locale timezone. In this particular case:

Feb 12, 2020 8:11:53 AM PST => Feb 12, 2020 16:11:53 UTC

* 1. Search for the mentioned POST request around the target datetime period in the access.log file. Keep in mind that couple seconds delay is possible between actual record creation in the DB and the web request to be completely processed with the record in the access.log.
  2. In this case, the following record can be found in the access.log:

185.214.164.10 - - [12/Feb/2020:16:11:54 +0000] "POST /customer/account/createpost/ HTTP/1.1" 302 31 "https://www.demostore.com/customer/account/create/" "Opera/9.80 (Windows NT 6.1; U; Distribution 00) Presto/2.10.229 Version/11.60"

* 1. That IP can be added to the WAF blacklist to prevent automatic scripts execution on the website.

1. Enable captcha for the customers registration form. Follow steps described in the documentation: <https://docs.magento.com/m2/ee/user_guide/stores/security-google-recaptcha.html>