

---

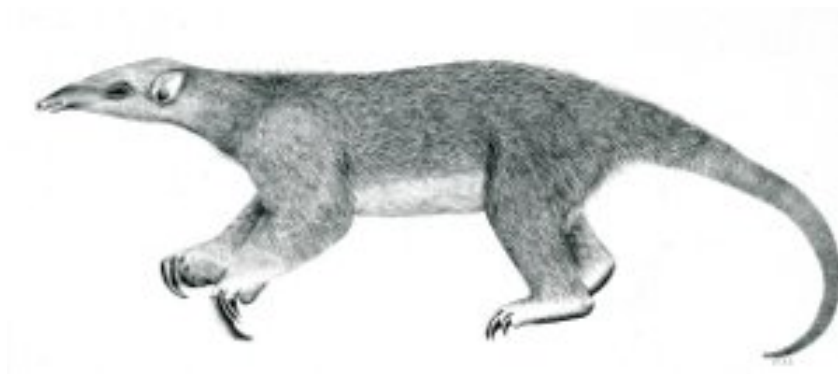
# Tranalyzer2

## Importing Tranalyzer Flows in Splunk



Type of Import: JSON Stream

---



Tranalyzer Development Team

## **Contents**

## 1 Importing Tranalyzer Flows in Splunk

### 1.1 Prerequisites

- Tranalyzer version 0.6.x is installed with standard/default plugins,
- Splunk 6.5.x is installed, Splunk account exists,
- At least one network interface (Ethernet or WLAN) has network traffic.

### 1.2 Select Network Interface

Determine the network interface name by entering the following command:

```
ifconfig
```

at the terminal command line. In the output look for the interface name which has the IP address where the network traffic should be collected from:

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>  
mtu 1500 inet 10.20.6.79 netmask 0xfffffc00 broadcast 10.20.7.255
```

### 1.3 Configure Tranalyzer jsonSink Plugin

Go to *tranalyzer2-0.6.XlmY/trunk/jsonSink/src/jsonSink.h* and set the configuration parameters as needed:

```
#define SOCKET_ON          1 // Whether to output to a socket (1) or file (0)  
#define SOCKET_ADDR "127.0.0.1" // address of the socket  
#define SOCKET_PORT      5000 // port of the socket
```

Set `SOCKET_ON` to 1 to configure the output to a socket. Set the IP address of the destination server which should receive the data stream. If the localhost will be the destination, leave the default setting "127.0.0.1". Set the socket server port of the destination.

### 1.4 Recompile the jsonSink Plugin

Enter the following command:

```
tranalyzer2-0.6.8lm4/trunk/jsonSink/autogen.sh
```

Make sure that the plugin is compiled successfully. In this case the following message will be shown at the command line:

```
Plugin jsonSink copied into USER_DIRECTORY/.tranalyzer/plugins
```

### 1.5 Start Tranalyzer2

Start generating flow records by launching Tranalyzer2 with the interface name determined on the previous step and setting a file name as the command line arguments by entering the command:

```
tranalyzer -i en0 -w test1 &
```

Note that the file name is optional for JSON stream import, if file name is not indicated the records will be shown in the standard output (besides being streamed over the configured TCP socket).

### 1.5.1 Check File Output

Check that the flow records are written to the file by entering the command:

```
tail -f test1_flows.txt
```

Flow records should be shown in the terminal.

### 1.5.2 Collect Traffic

Let Tranalyzer2 run and collect network traffic.

## 1.6 Start Splunk

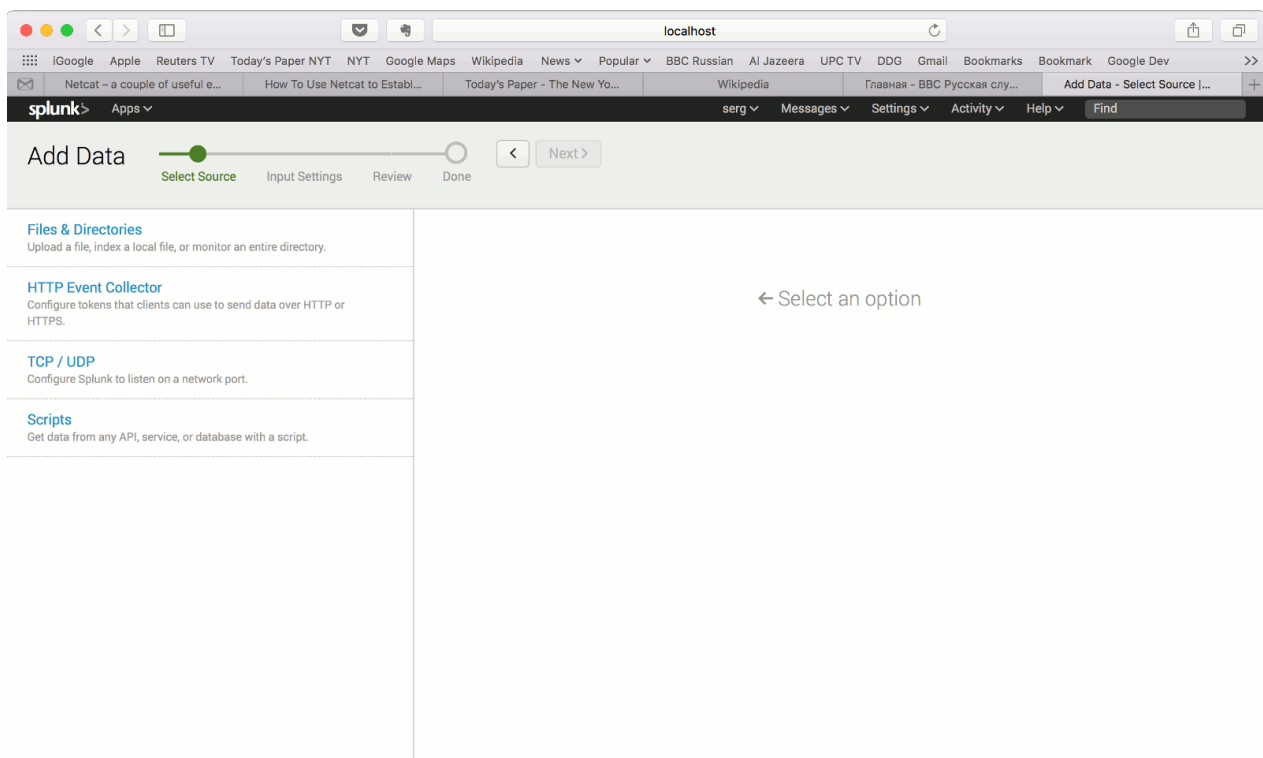
Start Splunk by entering the following command:

```
splunk start
```

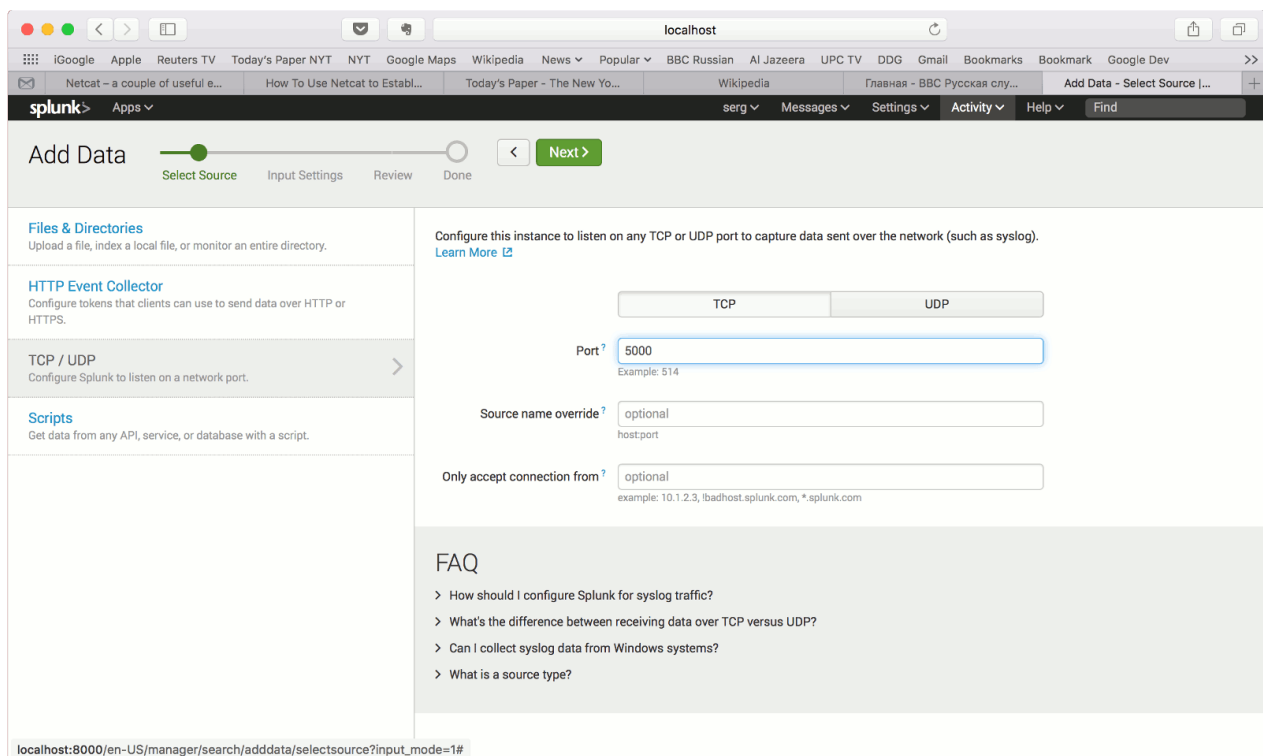
in the directory where Splunk is installed. Wait for the confirmation message that Splunk is up and running:

The Splunk web interface is at `http://splunk_hostname:8000`

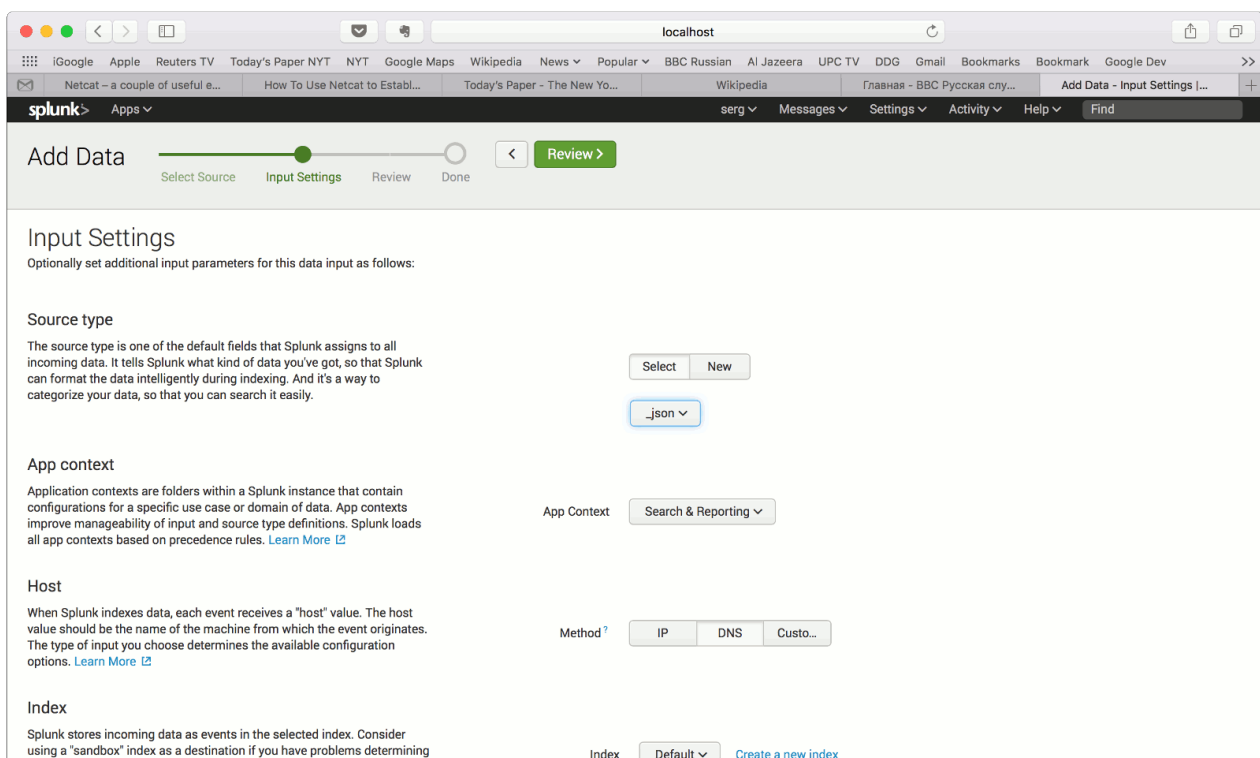
## 1.7 Login to Splunk, Import and Search Data



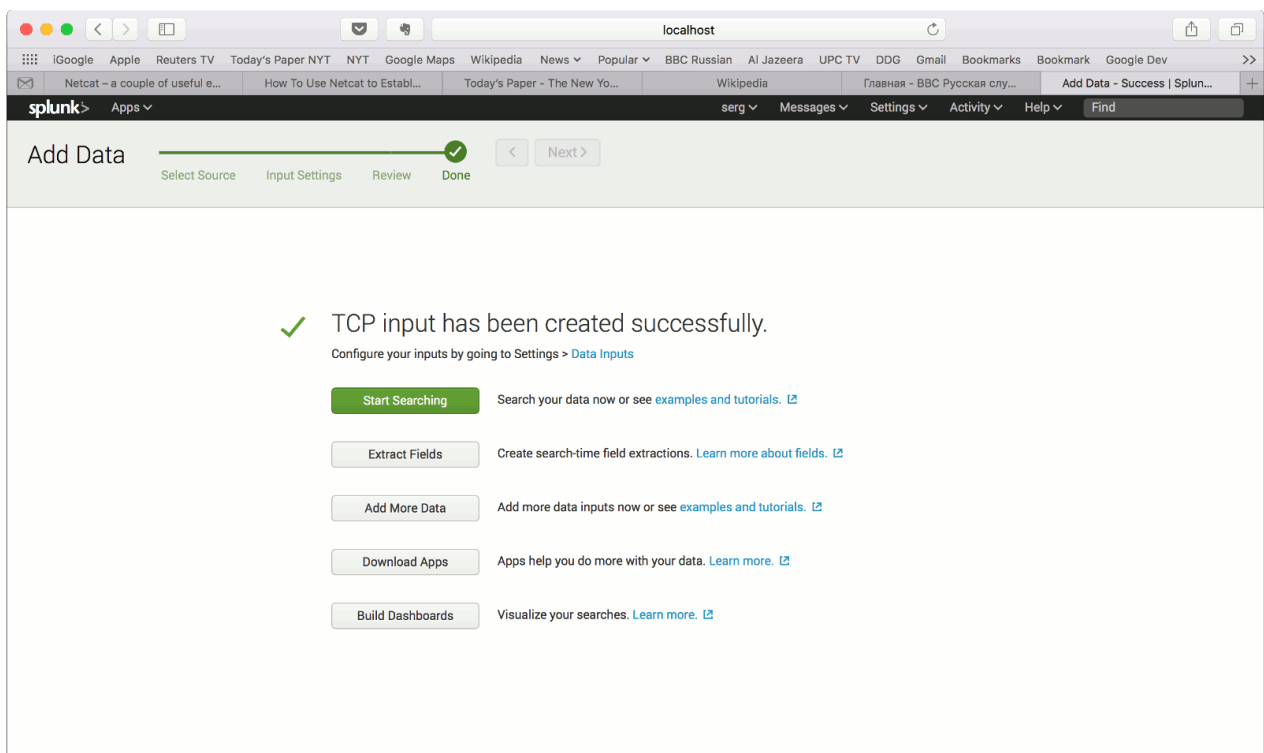
**Figure 1:** Select “Add Data”.



**Figure 2:** Select “TCP/UDP” and set protocol to “TCP” and set the correct port number (same as in the Tranalyzer2 plugin configuration file, in this example — 5000).

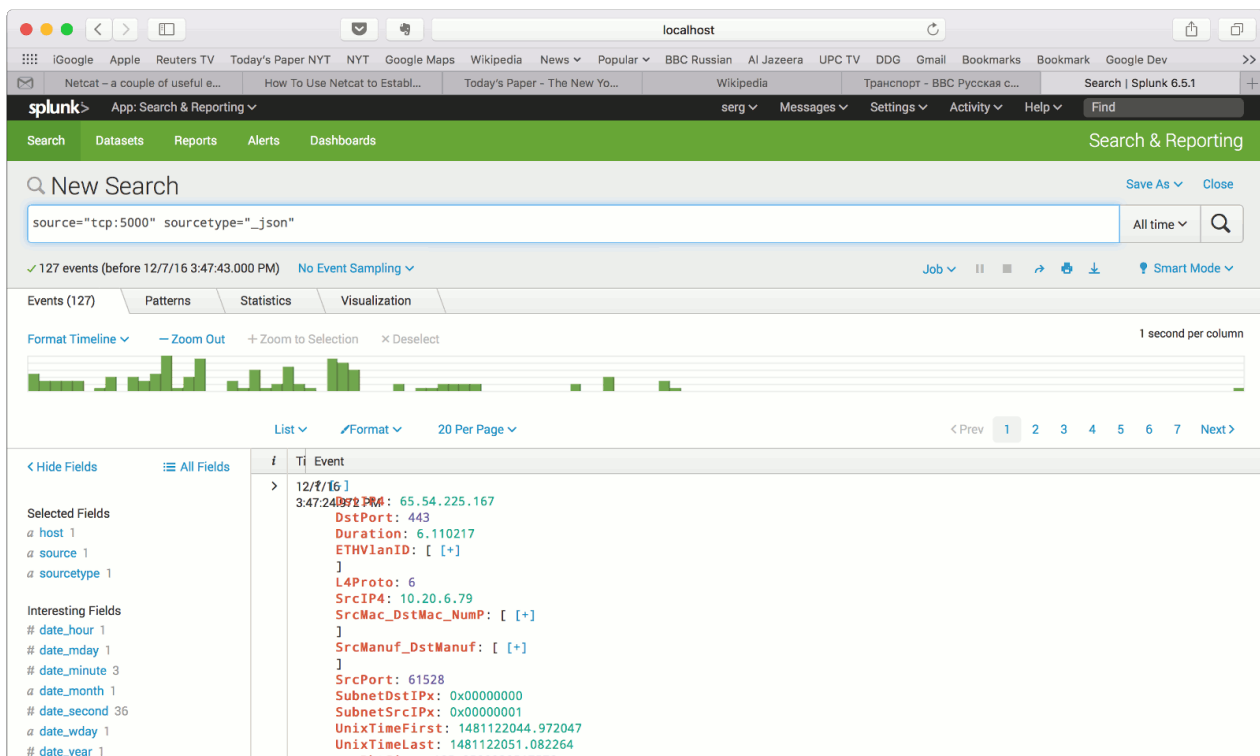


**Figure 3:** Select “\_json” as Source Type and proceed to “Review”.

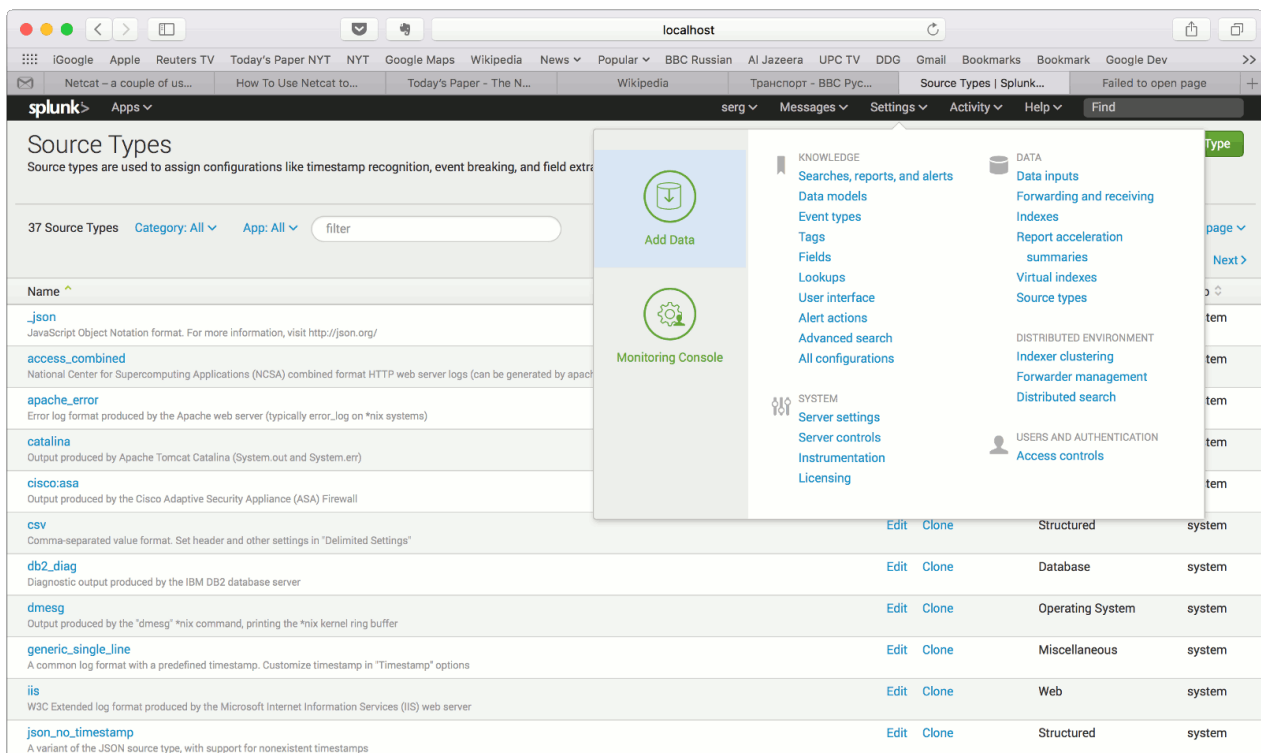


**Figure 4:** Select “Start Searching” to make sure that the data is being received by Splunk.

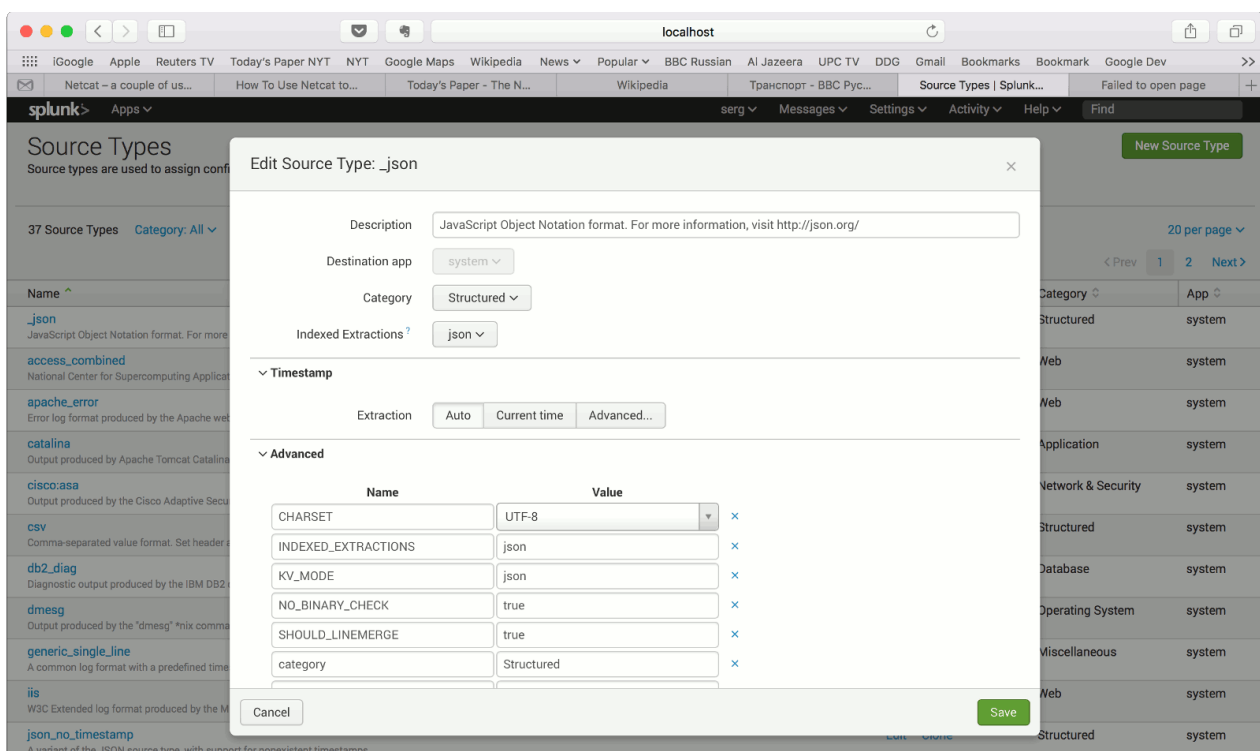




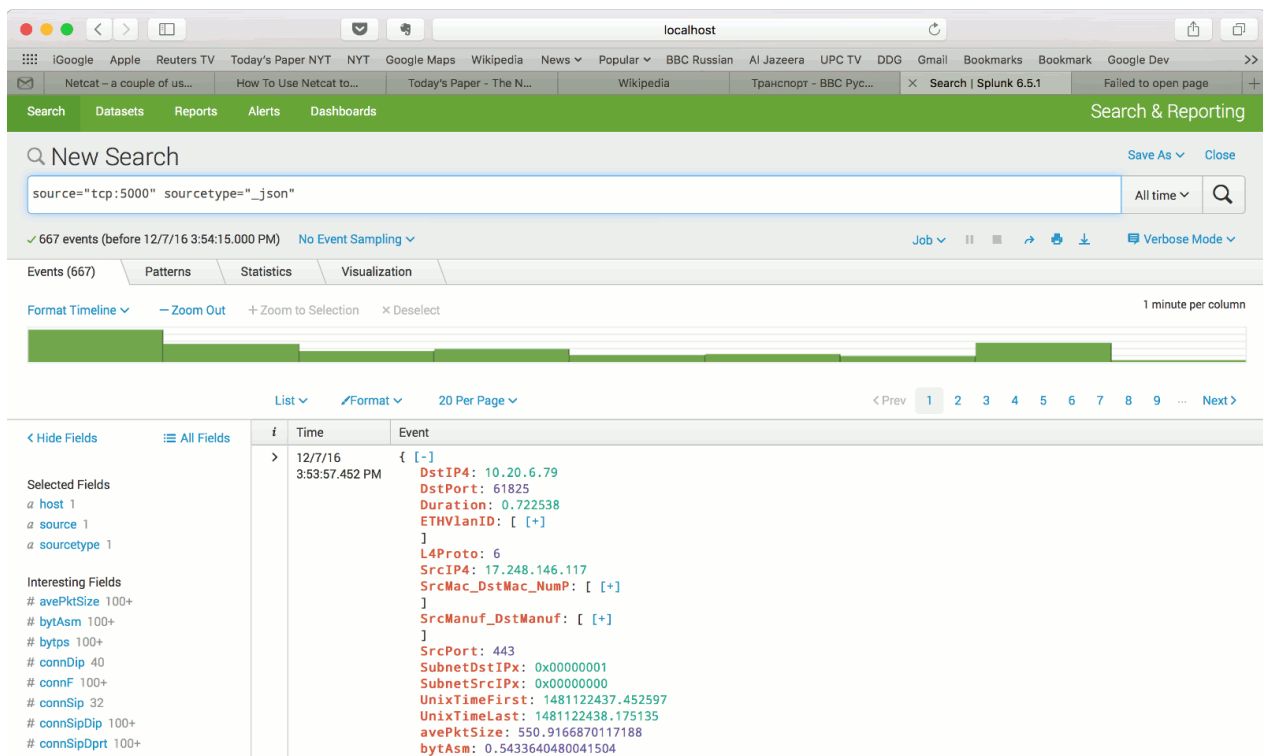
**Figure 5:** Note that the data is being received, but the Tranalyzer2 specific data record field are not shown yet.



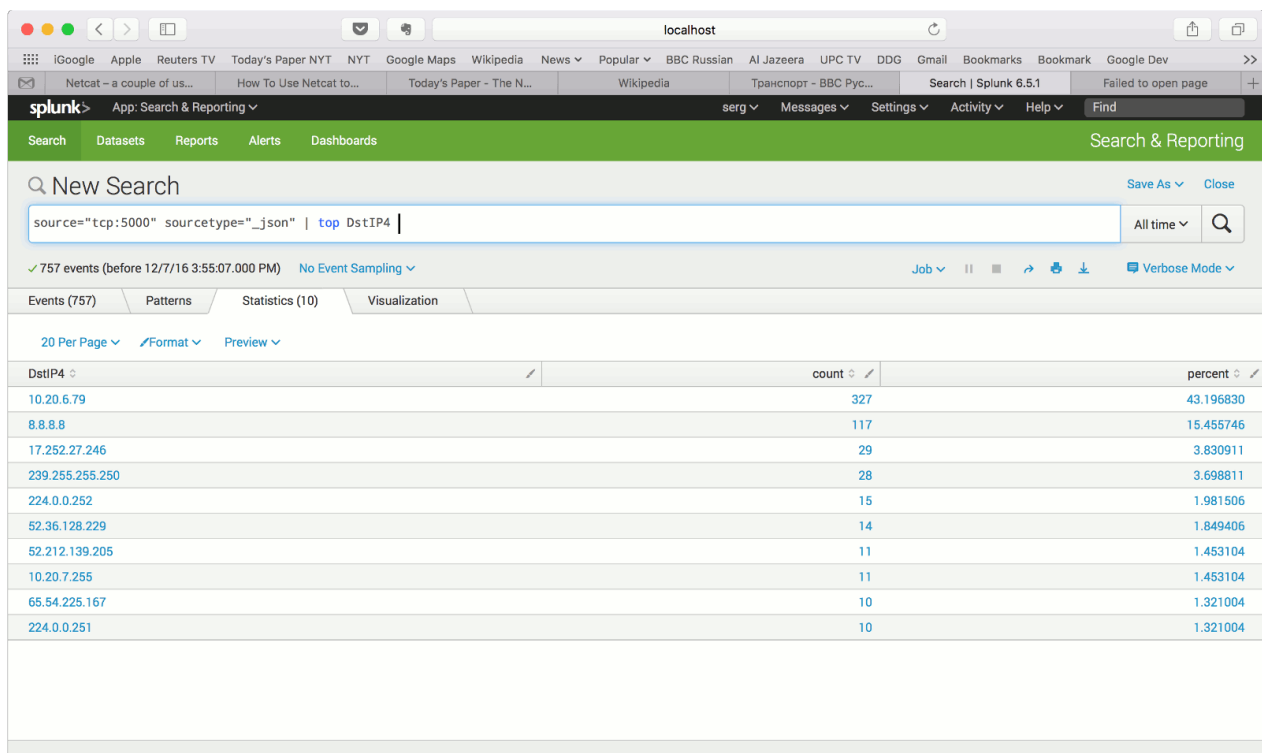
**Figure 6:** Go to “Settings”->”DATA”->”Source Types” and click on “\_json” data source type to edit it.



**Figure 7:** Change option “KV\_MODE” from “none” to “json” and save the changes.



**Figure 8:** Return to the Search window and make sure that the Tranalyzer2 specific fields are recognized by Splunk.



**Figure 9:** Query data, e.g. show top destination IP addresses by number of the records.