**DDOS Attack Detector**

This is a simple real-time DDOS attack detector application based on Kafka messaging system and Spark Streaming. In this application Apache access log data is ingested into Kafka broker and the detector application uses the streaming data to perform real-time analysis to find the DDOS attacks.

**Prerequisite:**

kafka\_2.11

spark-streaming-kafka-0-10\_2.11

spark-core\_2.11

spark-streaming\_2.11

scala\_2.11

Java\_1.8

**Installation:**

Cloudera [Quickstart VM](https://www.cloudera.com/downloads/quickstart_vms/5-13.html)

JDK 1.8

Kafka\_2.2.0

Zookeeper

Eclipse Oxygen (4.7)

Scala Eclipse IDE

**Apache log message sample**

200.4.91.190 - - [25/May/2015:23:11:15 +0000] "GET / HTTP/1.0" 200 3557 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

More can be read on [Apache log](https://httpd.apache.org/docs/2.4/logs.html)

**Steps:**

1. *Start Zookeeper Server* bin/zookeeper-server-start.sh config/zookeeper.properties
2. *Start Kafka Server* bin/kafka-server-start.sh config/server.properties
3. *Run the Detector Application*
4. *Start the consumer* bin/kafka-console-consumer.sh –bootstrap-server localhost:9092 –topic <topicname> --from-beginning
5. *Save the output in a text file*

**Notes:**

1. The application is run on the local machine, but this solution is scalable and can be run on multiple clusters.
2. More sophisticated algorithm can be implemented to find the DDOS attacks.