ATTACDET

REAL-TIME ANALYSIS OF WEB TRAFFIC WITH MACHINE LEARNING

Prepared : **Musa ŞANA**

Advisor : **Zeydin PALA**

Kullanılan Kütüphaneler / Teknolojiler

→Scapy

Pythonın network seviyesinde işlemleri yapmamızı sağlayan en güçlü kütüphanesidir.

→Tornado

Python ile geliştirilmiş asenkron çalışan bir web server frameworkdür.

Özellikle real-time yapılmak istenen işlemlerde kullanılır.

→ Chartjs

HTML5 canvas elementini kullanarak birçok grafik formatı oluşturmamızı sağlayan javascript kütüphanesidir.

→ Websocket

Bir döküman/dataset içerisinde geçen kelimelerin önemini, istatistiksel yöntemlerle hesaplayarak bunları birer vektör haline getiren bir yaklaşımdır.

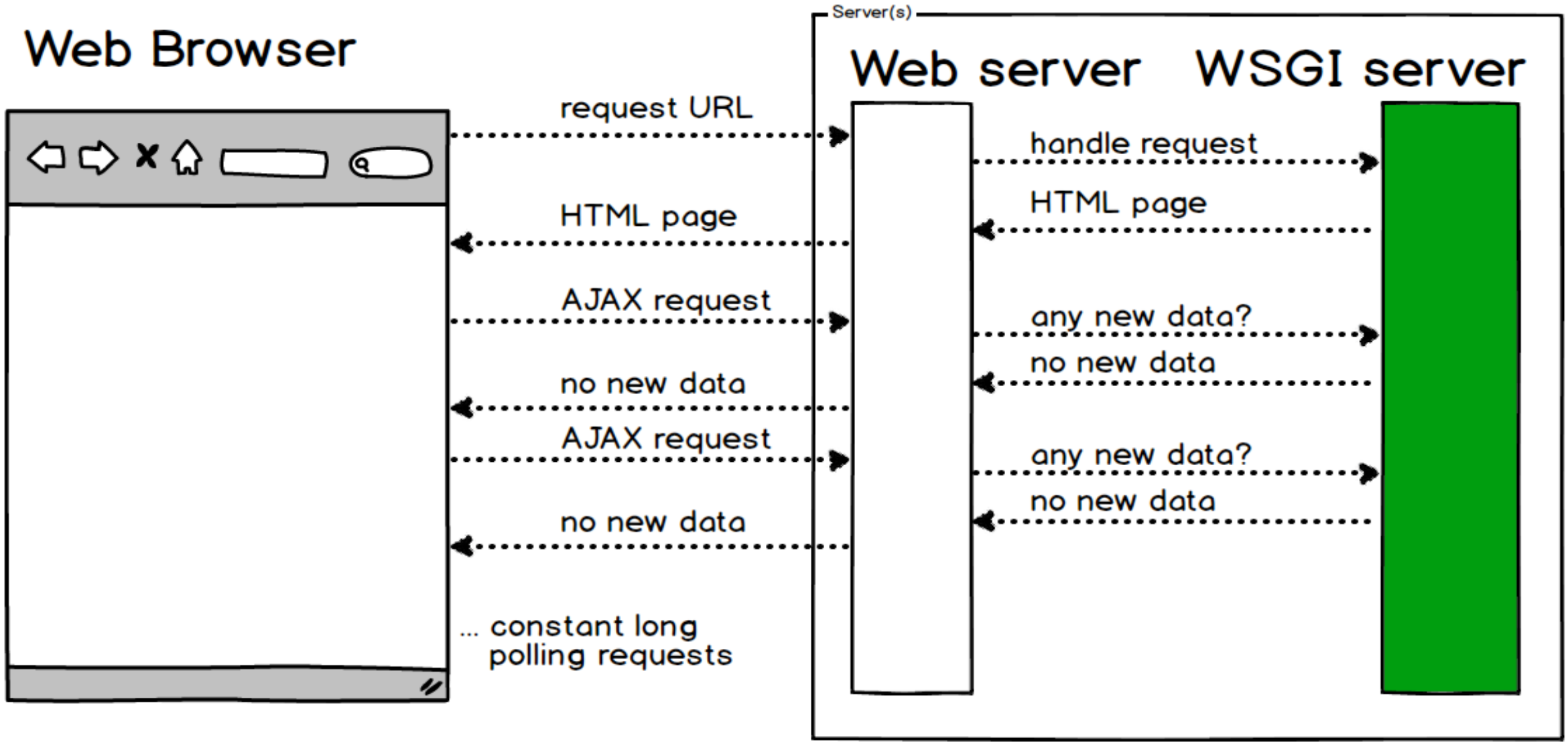
→ Tf-idf (Term Frequency–inverse Document Frequency)

Bir döküman/dataset içerisinde geçen kelimelerin önemini, istatistiksel yöntemlerle hesaplayarak bunları birer vektör haline getiren bir yaklaşımdır.

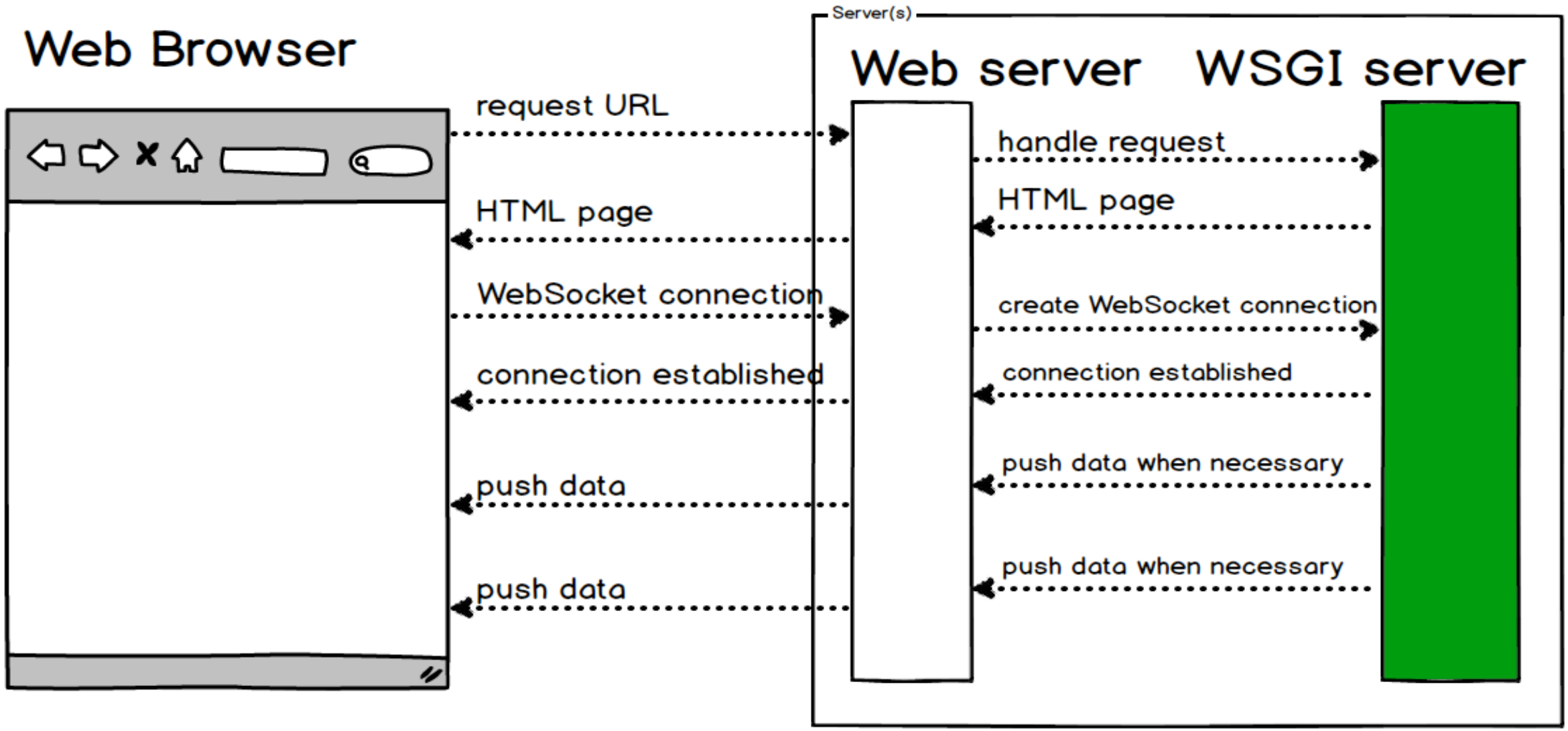
→ Pickle

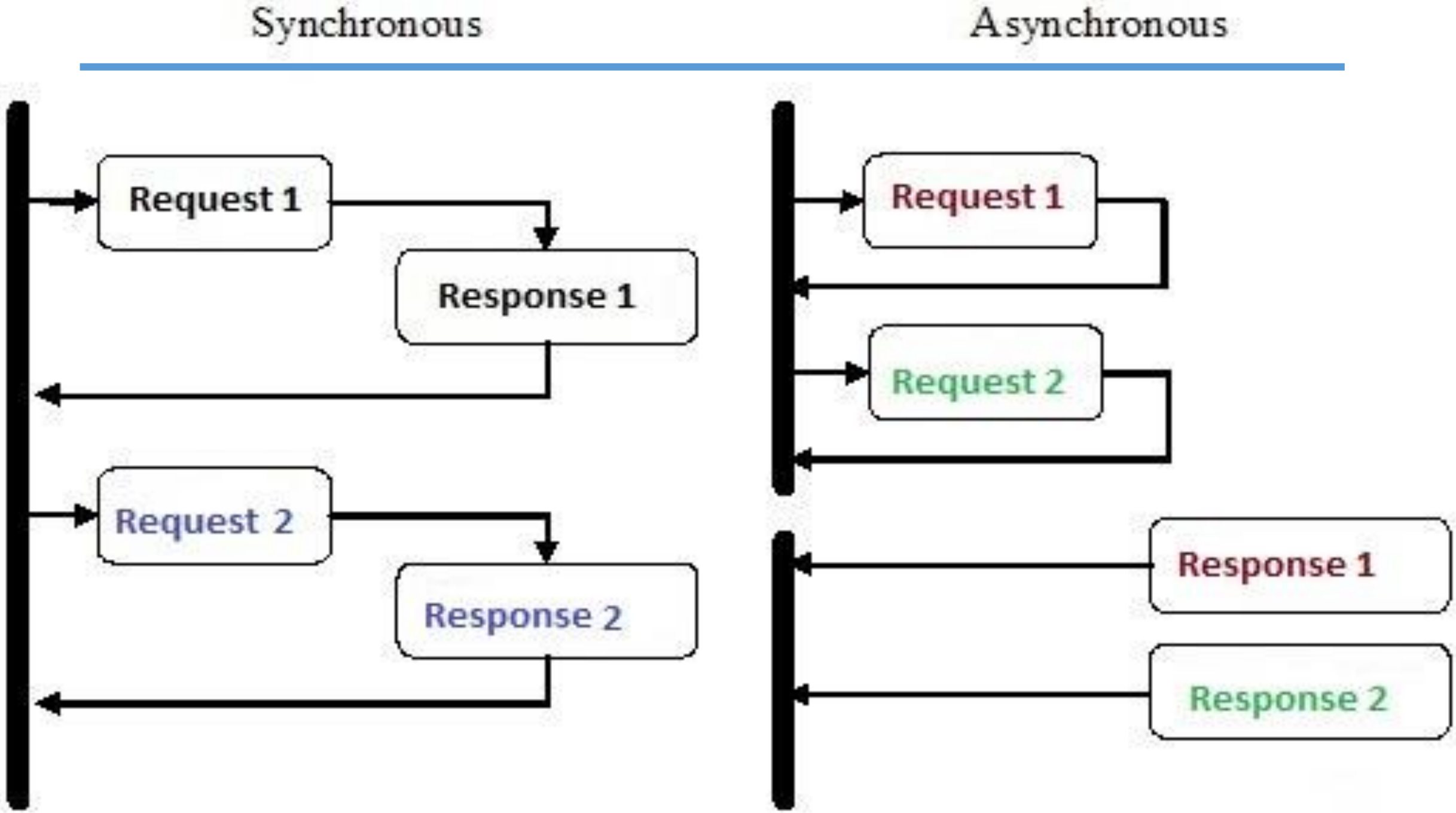
Python objelerini serialize ve de-serialize etmek için kullanılan bir python modolüdür. Projede ‘eğitilmiş makine öğrenmesi modelini’ kaydetmek için kullanıldı.

Long polling via AJAX

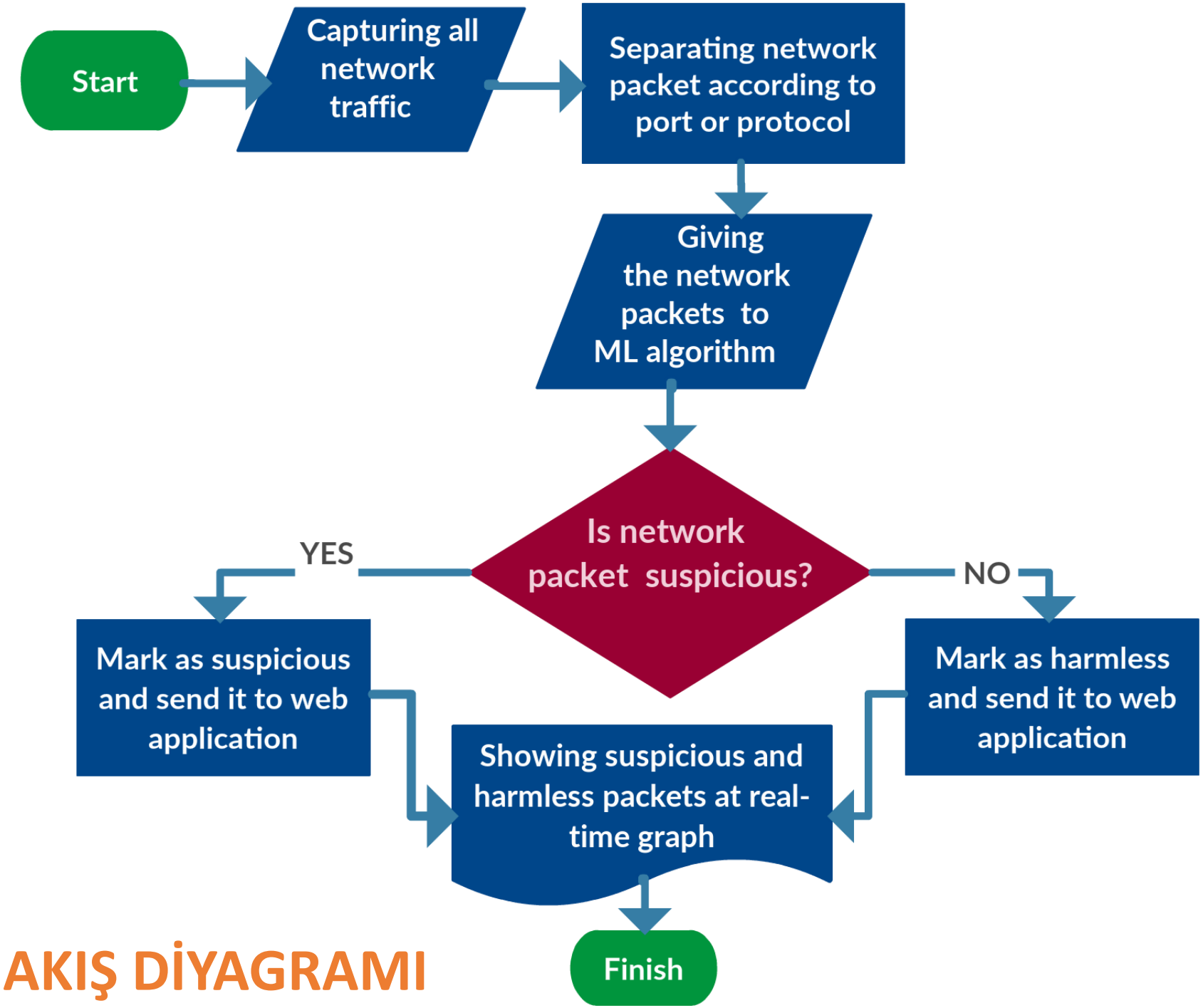


WebSockets


Web Browser
Server(s)
Web server
WSGI server
request URL
handle request
HTML page
HTML page
WebSocket connection
create WebSocket connection
connection established
connection established
push data
push data when necessary
push data
push data when necessary

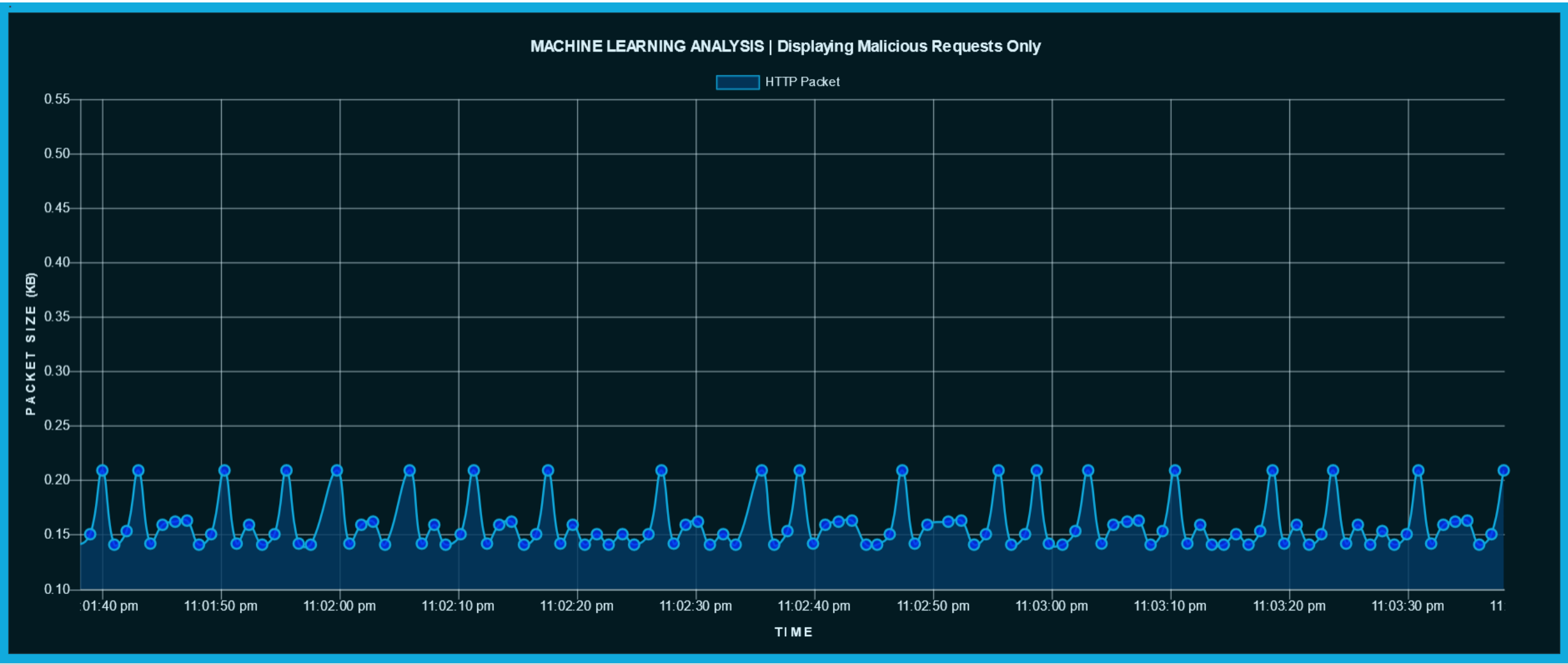

Synchronous
Asynchronous
Request 1
Response 1
Request 2
Response 2
Request 1
Request 2
Response 1
Response 2


01.
Sunucuya gelen/giden tüm http trafiğinin sniff edilmesi
02.
Sniff edilen http paket başlıklarının parse edilerek uygun formata getirilmesi
ATTACDET
Attacdet, makine öğrenmesi yardımıyla bir sunucuya gelen http isteklerini yakalayarak bunların zararlı olup olmadığına yönelik karar vermesi sonucunda bu istatikleri web tabanlı bir uygulamada real-time olarak görselleştirip gösteren bir uygulamadır.
03.
Uygun formata getirilen verinin, makine öğrenmesine verilmesi sonucunda tahmine dayalı cevabın alınması
04.
Makine öğrenmesinin tahmin dayalı sonucu ve diğer verilerin websocket ile web uygulamasına gönderilmesi
05.
WebSocket bağlantısı üzerinden gelen verilerin oluşturulan grafikler üzerinde real-time olarak gösterilmesi

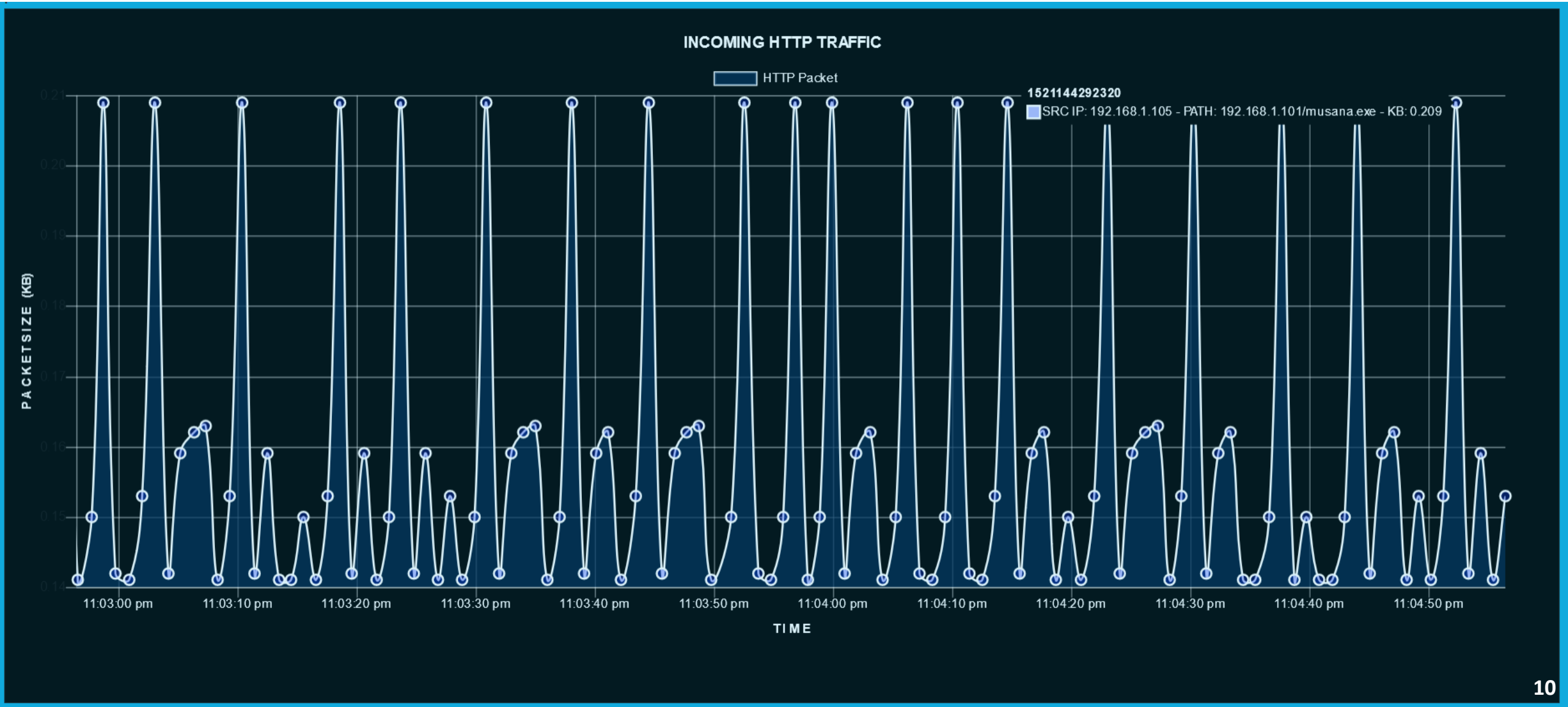


ATTACDET AKIŞ DİYAGRAMI

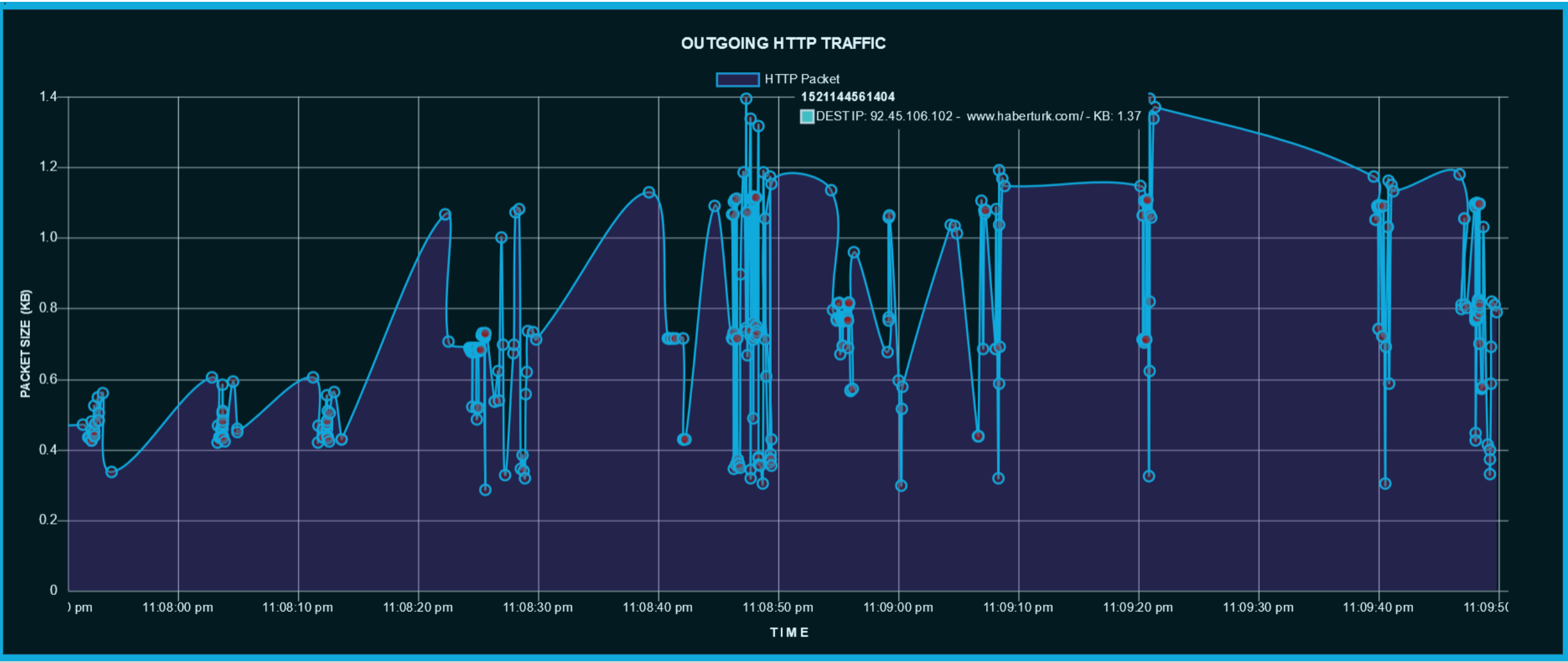
Machine Learning Analysis Graph



Incoming HTTP Traffic Graph



Outgoing HTTP Traffic Graph

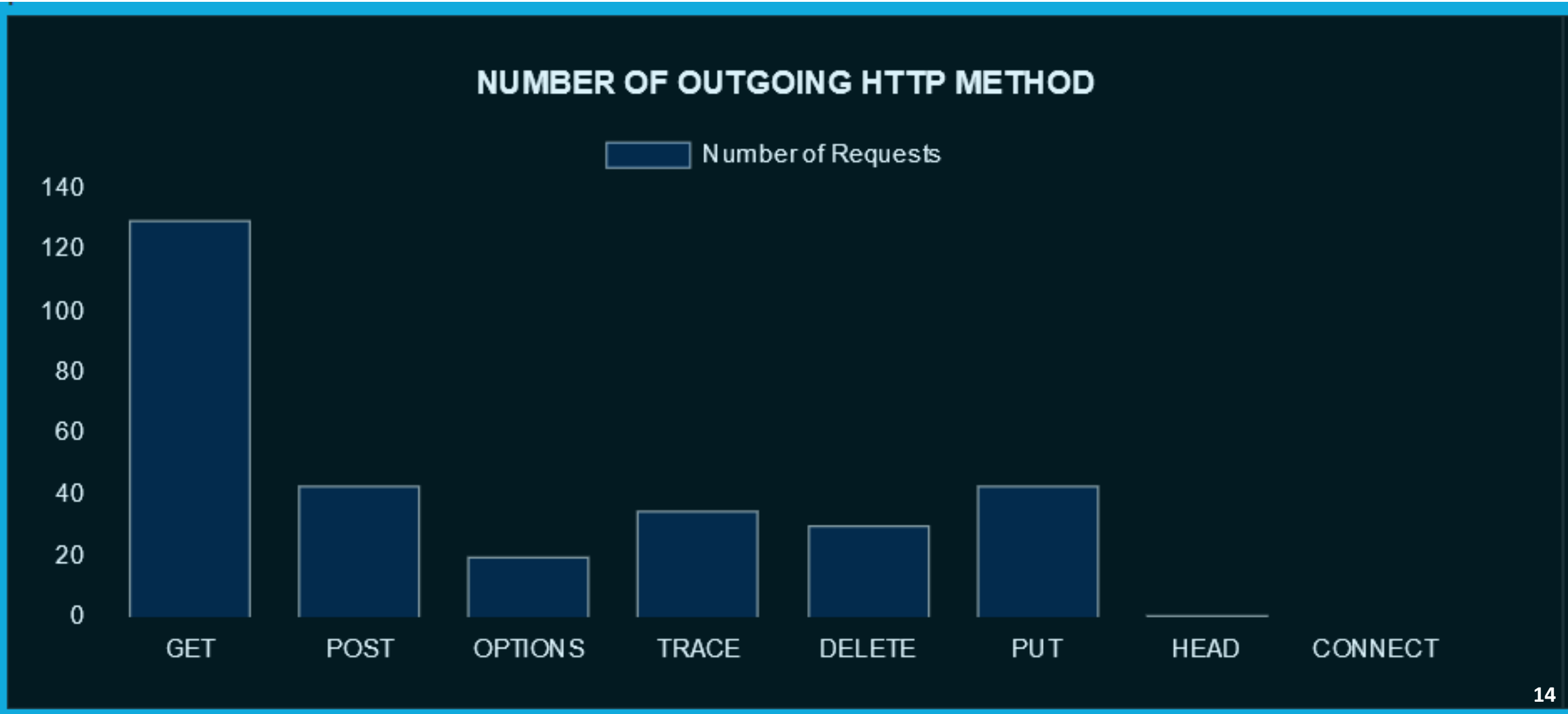


AttacDet Consol Side

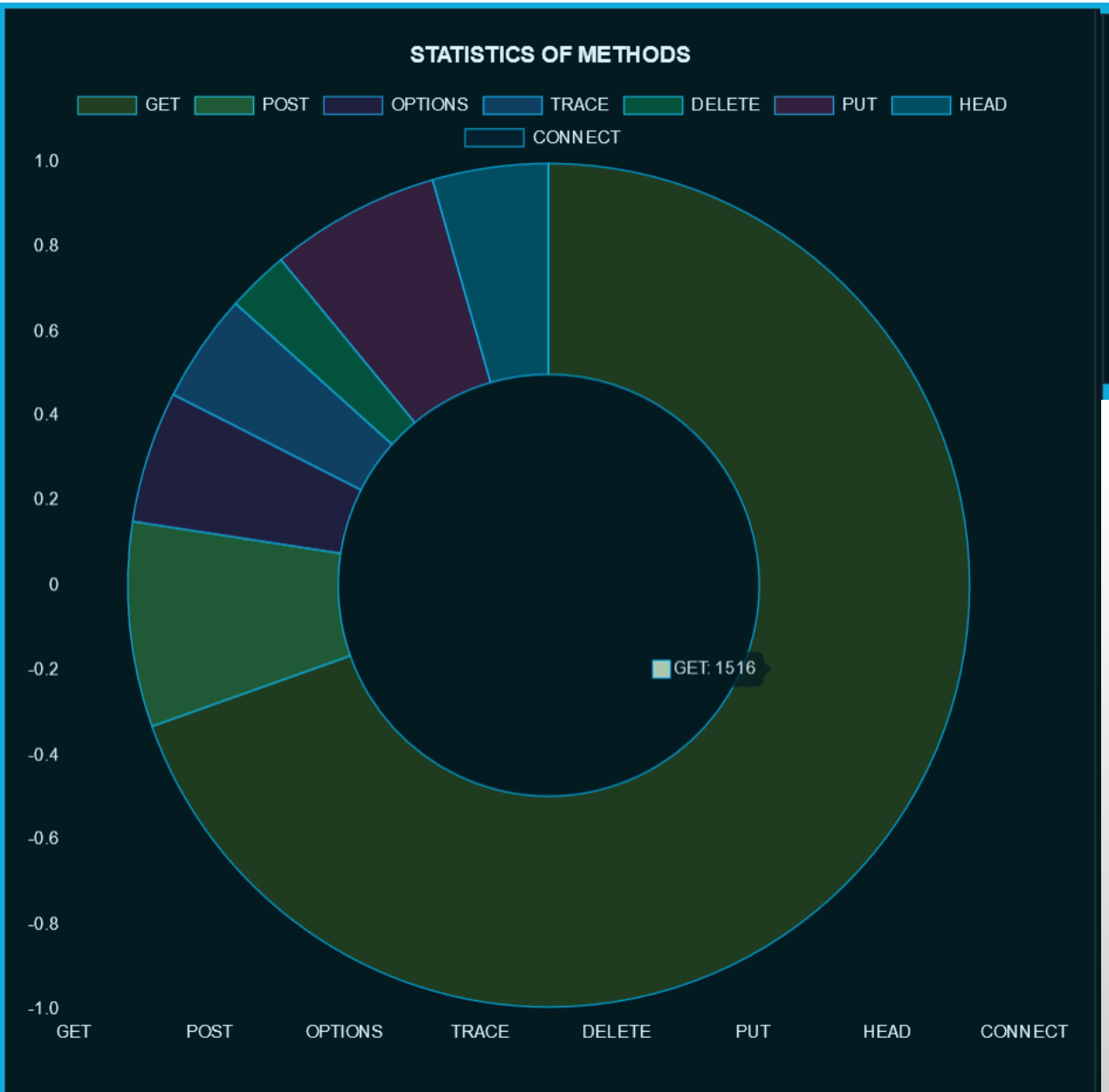
```
xubuntu ~ Desktop remasevum remasevum_Final sudo python3 wso3.py -m 0c:8b:fd:7d:79:81
[*] Training Machine Learning Model...
[*] Training Score (Percent):  97.19  / Float :  0.9718703455410841
[*] Training of Machine Learning Model is Over...
[*] Waiting for WebSocket Connection...
[*] New Client Connected!
[*] Sniffing is Started!
[+] Predict of ML: good          URL: 192.168.1.101/alparslan.edu.tr
[+] Predict of ML: good          URL: 192.168.1.101/itu.edu.tr
[+] Predict of ML: good          URL: 192.168.1.101/musana.org
[+] Predict of ML: good          URL: 192.168.1.101/hacettepe.edu.tr
[+] Predict of ML: good          URL: 192.168.1.101/batman.edu.tr
[+] Predict of ML: bad   URL: 192.168.1.101/backdoor.php
[+] Predict of ML: bad   URL: 192.168.1.101/etc/passwd
[+] Predict of ML: bad   URL: 192.168.1.101/malware.exe
[+] Predict of ML: bad   URL: 192.168.1.101/shell.php
[+] Predict of ML: bad   URL: 192.168.1.101/alparslan.exe
[+] Predict of ML: bad   URL: 192.168.1.101/musana.msi
[+] Predict of ML: bad   URL: 192.168.1.101/batman.exe
[+] Predict of ML: bad   URL: 192.168.1.101/odtu.exe
```

Number Of Incoming HTTP GET Method Graph

Number Of Outgoing HTTP GET Method Graph



Statistic of Methods / POST Data



POST DATA

login=test&password=password&security_level=0&form=submit'
login=test&email=musana%40hotmail.com&password=testpass&password_conf=testpass&secret=123&
mail_activation=&action=create'
par=alparslan.edu.tr&test=value'
username=musana'

Teşekkürler.

Sunum dosyasına musana.net adresinden ulaşabilirsiniz.