# Anomaly Detection in Server Access Log

Fatemeh Shiri
2021/29/06
Rahnema College Machine Learning Tuning Course

# Table of Contents

**01**

## Log Analysis

Process of converting raw log file to csv file

**02**

## Pre-Processing

Working on data and features

**03**

## Model

Using Base Models to find anomalies

**04**

## Next

Next step for fine-tuning and development

# 01
# Log Analysis

Survey of raw access log file

# Log Analysis Survey

## Find Format and structure

- IP [TIME] [Method Path] StatusCode ResponseLength [[UserAgent]] ResponseTime
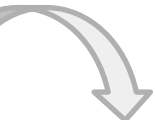
- Blank : '-'

## Process

- Regex
- Manual

## Log Indexing

- Csv File
- Columns : ['line','ClientIp', 'DateTime', 'MethodPath', 'StatCode', 'ResponseLength', 'UserAgent', 'ResponseTime']

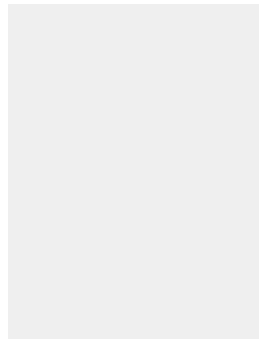- **8** columns
- **1260034** records

41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get css/page.2f0fc69390da8cdff683.css] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 4
20.116.215.189 [2021-5-12T5:6:2.0+0430] [Get templates/service.html] 200 1201 [[Go-http-client/2.0]] 0
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get images/sanjaghmaglogo1.png] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 8
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get images/gadgets/join_pros3.jpg] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 8
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get images/default.jpg] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 4
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get images/sanjagh_logo_purple5.png] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 0
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get js/page.07cb314dc14eef820638.js] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 8
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get js/lazyload.797291581158393f5011.js] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 0
60.56.221.168 [2021-5-12T5:6:2.0+0430] [Get css/font_awesome.min.css] 304 0 [[Mozilla/5.0 (Linux; Android 10; SM-J600F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.181 Mobile Safari/537.36]] 4
60.56.221.168 [2021-5-12T5:6:2.0+0430] [Get css/page.2f0fc69390da8cdff683.css] 304 0 [[Mozilla/5.0 (Linux; Android 10; SM-J600F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.181 Mobile Safari/537.36]] 16
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get fonts/IRANSansWeb_Light.woff2] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 8
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get images/aparat_logo.png] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 4
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get /pages/13401524] 200 52073 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.36]] 20
41.181.1.76 [2021-5-12T5:6:2.0+0430] [Get fonts/sanjagh_icon_font_5.woff] 304 0 [[Mozilla/5.0 (Linux; Android 9; G9) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Mobile Safari/537.36]] 4
35.103.240.193 [2021-5-12T5:6:2.0+0430] [Get fonts/fontawesome_webfont.woff2?v=4.7.0] 304 0 [[Mozilla/5.0 (Linux; Android 6.0; MYA-L22) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Mobile Safari/537.36]] 24
119.82.33.126 [2021-5-12T5:6:2.0+0430] [Get /order/802732418/289354109] 200 54778 [[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.1 Safari/605.1.15 (Appl
35.117.114.180 [2021-5-12T5:6:2.0+0430] [Post /api/cs0/uxEvents] 200 2 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-A105F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile Safari/537.36]] 4
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get css/font_awesome.min.css] 200 30891 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.36]] 4
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get images/default.jpg] 200 25889 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.36]] 8
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get images/gadgets/join_pros3.jpg] 200 34053 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.36]] 8
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get css/page.2f0fc69390da8cdff683.css] 200 50880 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/5
226.152.63.215 [2021-5-12T5:6:2.0+0430] [Get /price/337225318] 200 41075 [[Mozilla/5.0 (Linux; Android 9; SM-A105F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile SamsungBrowser/9.2 Chro
35.117.114.180 [2021-5-12T5:6:2.0+0430] [Get templates/service.html] 200 1201 [[Go-http-client/2.0]] 4
76.212.164.3 [2021-5-12T5:6:2.0+0430] [Get images/default.jpg] 200 20993 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.3
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get images/sanjagh_logo_purple5.png] 200 4680 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.3
4.138.31.112 [2021-5-12T5:6:2.0+0430] [Get js/lazyload.797291581158393f5011.js] 200 10690 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.3
4.138.31.112 [2021-5-12T5:6:3.0+0430] [Get js/sentry.47b4061bac0b8ac89b9c.js] 200 65059 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/53
4.138.31.112 [2021-5-12T5:6:3.0+0430] [Get js/page.07cb314dc14eef820638.js] 200 332023 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/53
29.57.51.148 [2021-5-12T5:6:3.0+0430] [Put /api/v2/token] 200 289 [[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36]] 8
4.138.31.112 [2021-5-12T5:6:3.0+0430] [Get images/aparat_logo.png] 200 1038 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.3
4.138.31.112 [2021-5-12T5:6:3.0+0430] [Get /pages/19392351376] 200 53983 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Sa
4.138.31.112 [2021-5-12T5:6:3.0+0430] [Get fonts/sanjagh_icon_font_5.woff2] 200 8644 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.3
4.138.31.112 [2021-5-12T5:6:3.0+0430] [Get fonts/IRANSansWeb_Light.woff2] 200 28400 [[Mozilla/5.0 (Linux; Android 6.0.1; SM-C5010) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.3
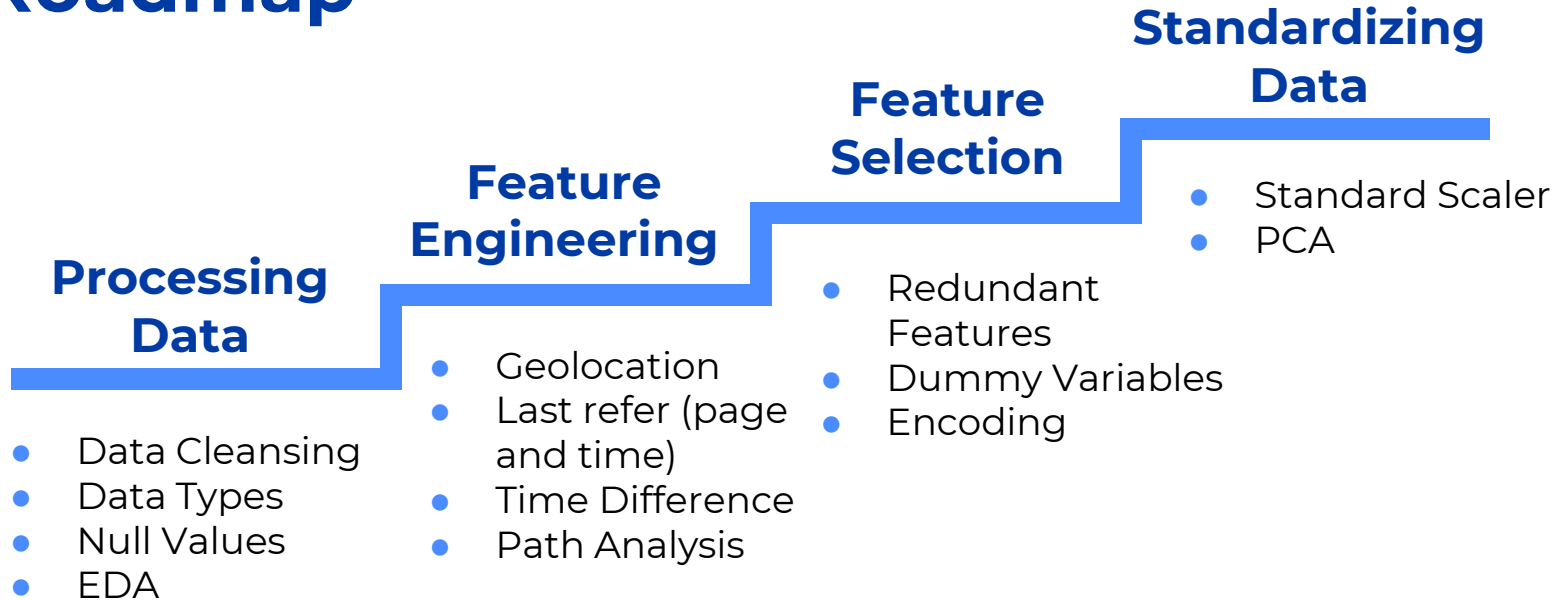- [2021-5-12T5:6:3.0+0430] [Get /] 301 169 [[kube-probe/1.21]] -
60.56.221.168 [2021-5-12T5:6:3.0+0430] [Get images/sanjaghmaglogo1.png] 200 20993 [[Mozilla/5.0 (Linux; Android 10; SM-J600F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.181 Mobile Safari/537.36]] 8
114.130.184.163 [2021-5-12T5:6:3.0+0430] [Put /api/v2/token] 304 0 [[Mozilla/5.0 (Linux; Android 10; SM-A105F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Mobile Safari/537.3
35.117.114.180 [2021-5-12T5:6:3.0+0430] [Get fonts/IRANSansWeb_Light.woff2] 304 0 [[Mozilla/5.0 (Linux; Android 9; SM-A105F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile Safari/537.36]] 0
35.117.114.180 [2021-5-12T5:6:3.0+0430] [Get css/servicePrice.7baaf654ebb8b26cf6b67.css] 200 121322 [[Mozilla/5.0 (Linux; Android 10; SM-J600F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.181 Mobile Safari/537.36]
60.56.221.168 [2021-5-12T5:6:3.0+0430] [Get images/sanjagh_logo_purple5.png] 304 0 [[Mozilla/5.0 (Linux; Android 10; SM-J600F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.181 Mobile Safari/537.36]
226.152.63.215 [2021-5-12T5:6:3.0+0430] [Get css/font_awesome.min.css] 200 30891 [[Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J530F Build/PPR1.180610.011) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/9
226.152.63.215 [2021-5-12T5:6:3.0+0430] [Get images/default.jpg] 200 20993 [[Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J530F Build/PPR1.180610.011) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/9.2 Chr
226.152.63.215 [2021-5-12T5:6:3.0+0430] [Get images/sanjaghmaglogo1.png] 200 25889 [[Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J530F Build/PPR1.180610.011) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser

| | line | ClientIp | DateTime | MethodPath | StatCode | ResponseLength | UserAgent | ResponseTime |
|---|---|---|---|---|---|---|---|---|
| 0 | 207.213.193.143 [2021-5-12T5:6:0.0+0430] [Get ... | 207.213.193.143 | [2021-5-12T5:6:0.0+0430] | [Get /cdn/profiles/1026106239] | 304 | 0 | [[Googlebot-Image/1.0]] | 32 |
| 1 | 207.213.193.143 [2021-5-12T5:6:0.0+0430] [Get ... | 207.213.193.143 | [2021-5-12T5:6:0.0+0430] | [Get images/badge.png] | 304 | 0 | [[Googlebot-Image/1.0]] | 4 |
| 2 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get /... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get /pages/630180847] | 200 | 52567 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 32 |
| 3 | 35.108.208.99 [2021-5-12T5:6:0.0+0430] [Get im... | 35.108.208.99 | [2021-5-12T5:6:0.0+0430] | [Get images/fav_icon2.ico] | 200 | 23531 | [[Mozilla/5.0 (Linux; Android 6.0; CAM-L21) Ap... | 20 |
| 4 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get i... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get images/sanjagh_logo_purple5.png] | 200 | 4680 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 8 |
| 5 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get c... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get css/font_awesome.min.css] | 200 | 30891 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 8 |
| 6 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get i... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get images/default.jpg] | 200 | 20993 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 8 |
| 7 | 207.213.193.143 [2021-5-12T5:6:0.0+0430] [Get ... | 207.213.193.143 | [2021-5-12T5:6:0.0+0430] | [Get /cdn/pro_photo_gallery/226014993] | 304 | 0 | [[Googlebot-Image/1.0]] | 20 |
| 8 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get i... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get images/sanjaghmaglogo1.png] | 200 | 25889 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 8 |
| 9 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get j... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get js/lazyload.797291581158393f5011.js] | 200 | 10690 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 0 |
| 10 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get i... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get images/gadgets/join_pros3.jpg] | 200 | 34053 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 8 |
| 11 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get c... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get css/page.2f0fc69390da8cdff683.css] | 200 | 50880 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 12 |
| 12 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get j... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get js/sentry.47b4061bac0b8ac89b9c.js] | 200 | 65059 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 4 |
| 13 | 35.110.222.153 [2021-5-12T5:6:0.0+0430] [Get j... | 35.110.222.153 | [2021-5-12T5:6:0.0+0430] | [Get js/page.07cb314dc14eef820638.js] | 200 | 332023 | [[Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG S... | 32 |

# 02
## Pre-Processing

# Roadmap

**Processing Data**
- Data Cleansing
- Data Types
- Null Values
- EDA

**Feature Engineering**
- Geolocation
- Last refer (page and time)
- Time Difference
- Path Analysis

**Feature Selection**
- Redundant Features
- Dummy Variables
- Encoding

**Standardizing Data**
- Standard Scaler
- PCA

# Processing Data

## Null values

```
df.isnull().sum()
```

```
line                 0
ClientIp         18090
DateTime             0
MethodPath           0
StatCode             0
ResponseLength       0
UserAgent            0
ResponseTime     19808
dtype: int64
```

| | client_ip | date_time | status_code | response_length | user_agent | response_time | method | path |
|---|---|---|---|---|---|---|---|---|
| 45 | NaN | 2021-05-12 05:06:01+04:30 | 301 | 169 → | kube-probe/1.21 | NaN | Get | / |
| 113 | NaN | 2021-05-12 05:06:03+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 154 | NaN | 2021-05-12 05:06:05+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 181 | NaN | 2021-05-12 05:06:07+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 221 | NaN | 2021-05-12 05:06:09+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 1259794 | NaN | 2021-05-12 15:08:51+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 1259865 | NaN | 2021-05-12 15:08:53+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 1259923 | NaN | 2021-05-12 15:08:55+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 1259968 | NaN | 2021-05-12 15:08:57+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |
| 1260026 | NaN | 2021-05-12 15:08:59+04:30 | 301 | 169 | kube-probe/1.21 | NaN | Get | / |

Imputation with:
Server Ip and 0

## Data Types

```
df.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 1260035 entries, 0 to 1260034
Data columns (total 8 columns):
 #   Column           Non-Null Count    Dtype
---  ------           --------------    -----
 0   client_ip        1260035 non-null  object
 1   date_time        1260035 non-null  datetime64[ns, pytz.FixedOffset(270)]
 2   status_code      1260035 non-null  int64
 3   response_length  1260035 non-null  int64
 4   user_agent       1260035 non-null  object
 5   response_time    1258317 non-null  object
 6   method           1260035 non-null  object
 7   path             1260035 non-null  object
dtypes: datetime64[ns, pytz.FixedOffset(270)](1), int64(2), object(5)
memory usage: 76.9+ MB
```
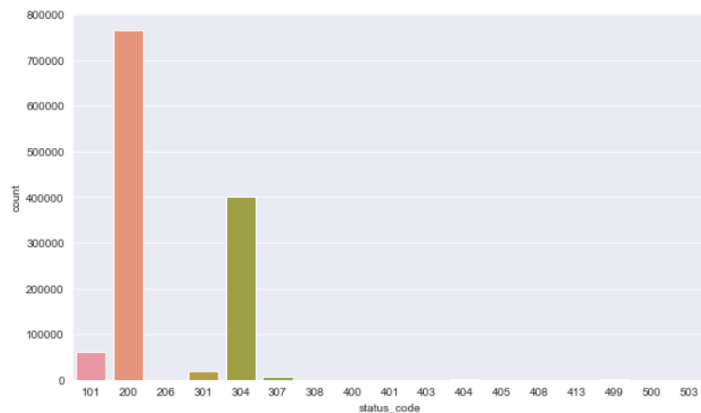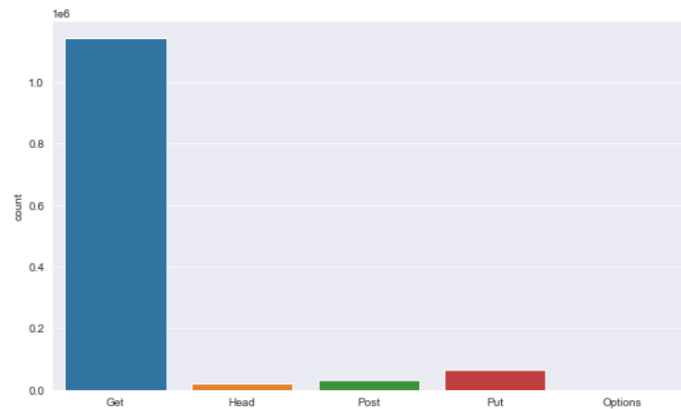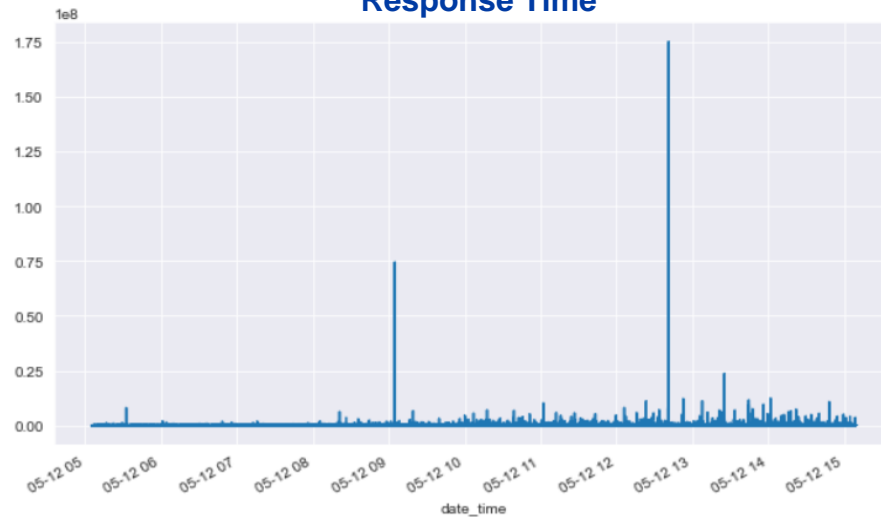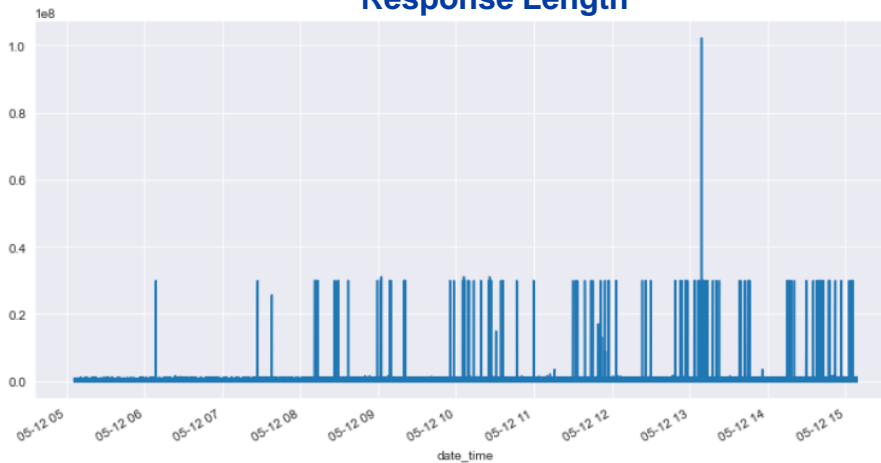
# Feature Engineering

## Geolocation

| | |
|---|---|
| United States | 759912 |
| Japan | 76115 |
| China | 62504 |
| France | 30593 |
| United Kingdom | 27328 |
| Germany | 25054 |
| Republic of Korea | 14544 |
| Russia | 12483 |
| Vietnam | 12038 |
| Mexico | 8768 |

{'cdn': 1,
 'profiles': 2,
 'pro_photo_gallery': 3,
 'images': 4,
 'fonts': 5,
 'js': 6,
 'gadgets': 7,
 'css': 8,
 'pages': 9,
 'order': 10,
 '802732418': 11,
 'api': 12,
 'cs0': 13,
 'uxEvents': 14,
 'price': 15,
 'templates': 16,
 'servicePic': 17,
 'v2': 18,
 'token': 19,
 'icons': 20,
 'service_price_body_pic': 21,
 'connect': 22,
 '1677931481': 23,
 'amp': 24,
 '870544902': 25,
 '591621209': 26,

## Path Analysis
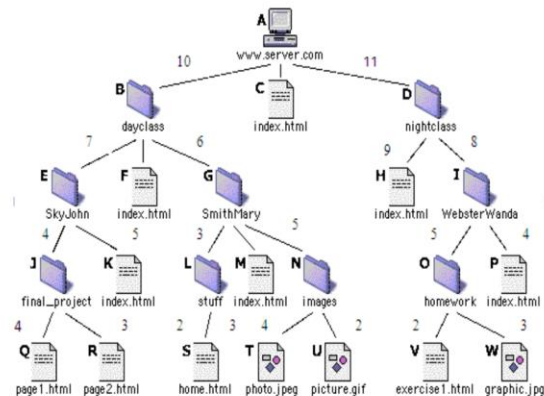


## Time Difference

## Last Refer

# Feature Selection

## Redundant

- Date_time

## Dummies and Encoding

- Method
- Ip, user_agent, path, geolocation, last_refer

| ip_encoded | status_code | response_length | response_time | Head | Options | Post | Put | geo_coded | Le_coded_path | le_last_page | date_time | last_refer | date_differance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11019 | 304 | 0 | 32.0 | 0 | 0 | 0 | 0 | 110 | 4 | 62537.0 | 1.620780e+12 | 0.000000e+00 | 1.620780e+12 |
| 10925 | 200 | 0 | 24.0 | 1 | 0 | 0 | 0 | 110 | 0 | 62537.0 | 1.620780e+12 | 0.000000e+00 | 1.620780e+12 |
| 11019 | 304 | 0 | 16.0 | 0 | 0 | 0 | 0 | 110 | 8 | 4.0 | 1.620780e+12 | 1.620780e+12 | 0.000000e+00 |
| 38695 | 200 | 0 | 20.0 | 1 | 0 | 0 | 0 | 110 | 0 | 62537.0 | 1.620780e+12 | 0.000000e+00 | 1.620780e+12 |
| 11019 | 304 | 0 | 32.0 | 0 | 0 | 0 | 0 | 110 | 8 | 8.0 | 1.620780e+12 | 1.620780e+12 | 0.000000e+00 |

# Standardizing Data
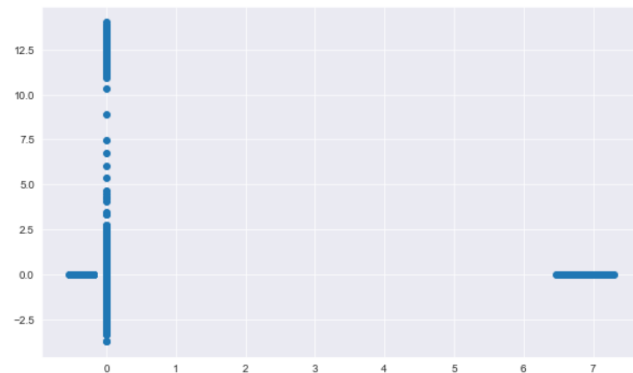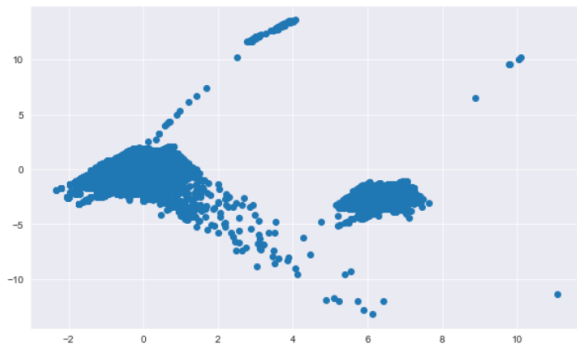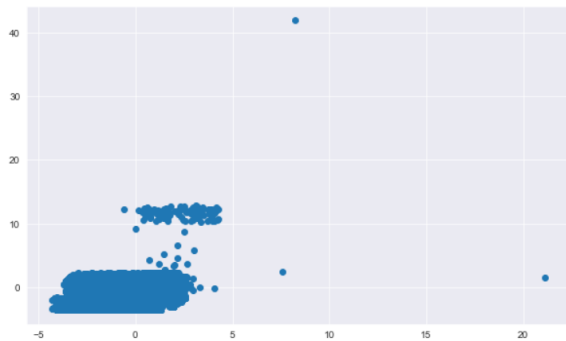
# 03
# Modeling

# Models

## Clustering

- Kmeans
- DBSCAN

## Distance-Based

- LOF
- KNN

## Linear Models

- PCA
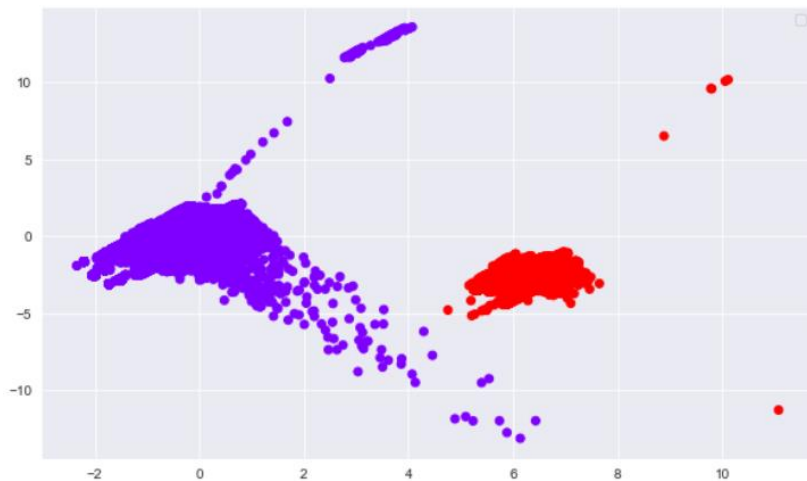- Elliptic Envelope

## Neural Network

- Auto-Encoder
- LSTM

## Tree-Based
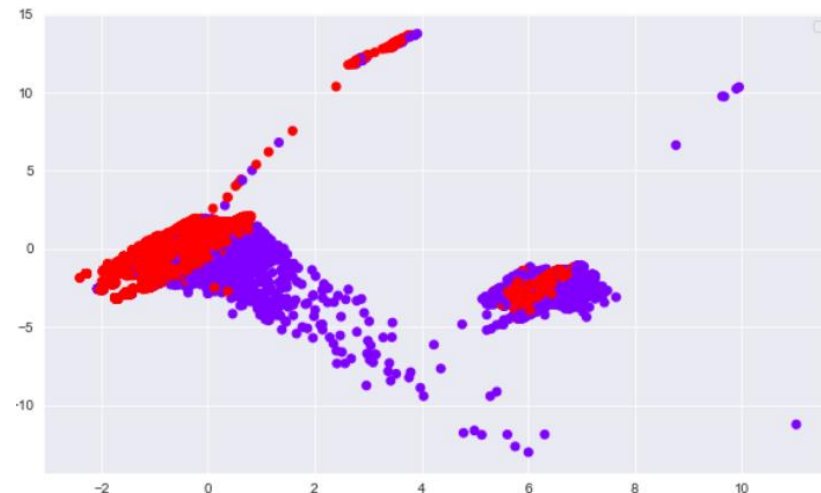
- Isolation Forest

## Kmeans

- n_clusters = 2
- 0 : 1208901 , 1 : 51124



```
(0      6261.251954
 1     11548.317346
Name: response_time, dtype: float64,
 0      6.813739e+04
 1      1.620801e+12
Name: date_differance, dtype: float64)
```
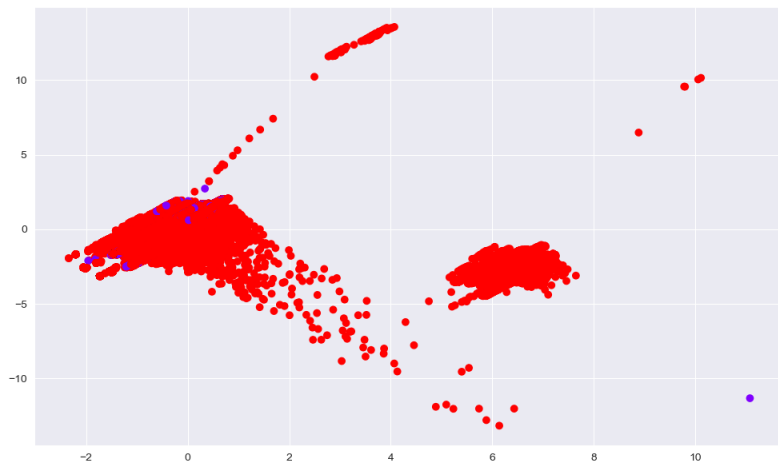
## Isolation Forest

- Contamination = 4%
- -1 : 50393 , 1 : 1209632



```
(-1     95804.064533
  1      2754.371329
Name: response_time, dtype: float64,
 -1      6.872318e+11
  1      3.987185e+10
Name: date_differance, dtype: float64)
```

## LOF
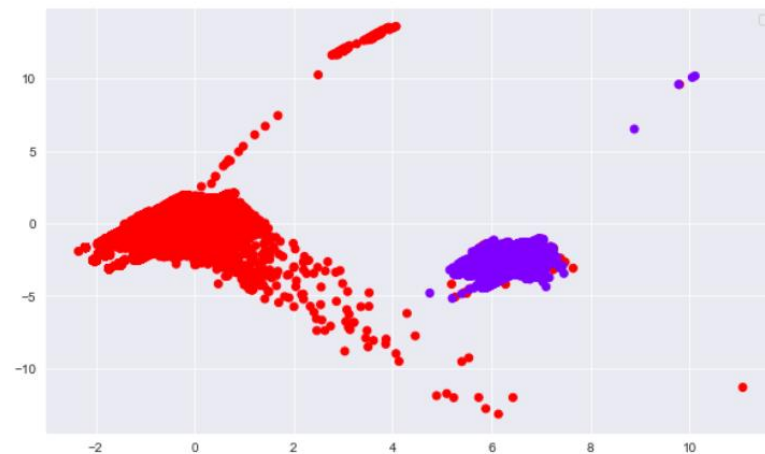
- n_neigbors = 2
- Contamination: 4%
- Distance : 'Manhattan'
- -1 : 50401 , 1 : 1209624



```
-1     2695.742565
 1     6633.269349
Name: response_time, dtype: float64,
-1     3.215968e+07
 1     6.850088e+10
Name: date_difference, dtype: float64)
```
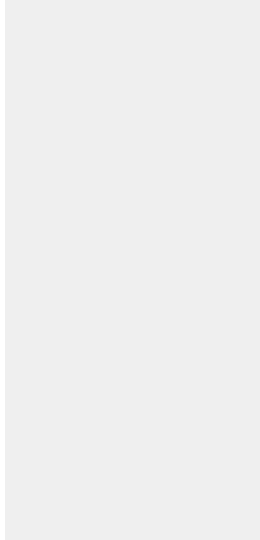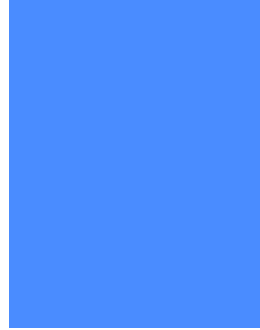
## Elliptic Envelope

- Normal Distribution
- Contamination = 3%
- -1 : 37801 , 1 : 1222224



```
(-1     11430.889924
  1      6322.516048
Name: response_time, dtype: float64,
 -1     1.620806e+12
  1     1.766766e+10
Name: date differance, dtype: float64)
```

# 04
# What's Next?

**Fine-Tune and Test Models**

- Using Sliding Window

- Using Neural Networks

**Develop API**

- Flask

**Reactive Implementation**

# Resources

- ANALYSIS OF WEB LOGS AND WEB USER IN WEB MINING , L.K. Joshila Grace1, V.Maheswari2 , Dhinaharan Nagamalai3

- Anomaly Detection for Application Log Data, Aarish Grover

- Comparative Analysis of Machine Learning-Based Approaches for Anomaly Detection in Vehicular Data, Konstantinos Demestichas, Theodoros Alexakis, Nikolaos Peppes and Evgenia Adamopoulou

- Experience Report: System Log Analysis for Anomaly Detection, Shilin He, Jieming Zhu, Pinjia He, and Michael R. Lyu

- Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection, Max Landauer a, Markus Wurzenberger, Florian Skopik, Giuseppe Settanni, Peter Filzmoser

# Thanks

Do you have any questions?