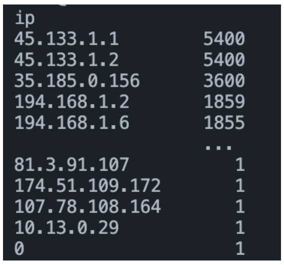
IEUK Engineering Skills Project 2025: Abnormal Server Traffic Problem

The recent successful podcast and newsletter have resulted in a dramatic increase in subscriptions subsequently ending in traffic and severe server outages. Parts of the website crash every few days due to the volume of visitors. There is suspicion of these traffic being caused by non-human factors.

The website logs provide each client's internet protocol (IP) address, country code, timestamp of when the server received the request, request method, request path, request protocol version, request status, size of the response body, a user-agent header and ultimately the server's processing time for this request in milliseconds; these fields form the blueprint for spotting anomalous or malicious traffic such as. brute-force attacks and malformed requests.

After analysing the logs using `analyser.py`, a few key points that draw attention are an unusually high volume of repeated and invalid IPs, unexpected request types, and error-generating patterns reminiscent of brute-force attacks. To address this problem in real time, a program is needed to check the logs frequently, the `checker.py` process demonstrates a real-time checker for the logs where the program flags all of the explained suspicious behaviours and generates a list of suspicious IPs. This checker is a light-weight program that returns a list of all suspicious IPs without a significant change in the website's costs making it a sustainable tool and it can be ran from containers such as Docker meaning that it can be ran along with live logs as an ideal solution.



```
ip
45.133.1.1         5400
45.133.1.2         5400
35.185.0.156       3600
194.168.1.2        1859
194.168.1.6        1855
                    ...
81.3.91.107           1
174.51.109.172        1
107.78.108.164        1
10.13.0.29            1
0                     1
```

The next steps include integrating automated solutions such as rate-limiting or blocking flagged IPs and adding a human-verification (CAPTCHA) step throughout the website on critical endpoints. These crucial security measures that ensure the website is safe from unexpected attack or traffic can be triggered dynamically whenever the checker detects abnormal activity.