# Ahmed Yasser Ahmed 2205106
# Log File Analysis Report

## 1. Introduction

This report provides insights extracted from web server access logs using the Bash-based script `log_analyzer.sh`. The analysis includes request statistics, IP behavior, error trends, traffic patterns, and suggestions for system improvement and security monitoring.

### 2. Log Format

- IP address

- Date and time

- Request method (GET, POST)

- URL

- HTTP status code

- User agent information

Example log entry:

83.149.9.216 - - [17/May/2015:10:05:03 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"

### 3. Request Statistics

The analysis includes the total number of requests along with a breakdown of HTTP methods:

- Total requests processed
- Number of GET requests
- Number of POST requests

### 4. Unique IP Address Analysis

This section identifies unique client IP addresses making requests:

- Total number of unique IPs
- Request counts per IP, including GET and POST breakdowns

### 5. Error and Failure Analysis

The script analyzes HTTP response codes to detect failed requests (status codes 4xx and 5xx):

- Count and percentage of failure responses
- Identification of the most error-prone day and hour
- IP address responsible for the most failed requests

### 6. Traffic Patterns

Patterns in request volumes over time were analyzed:

- Daily average request count

- Hourly distribution of traffic
- Breakdown of status codes by count and percentage

## 7. User Behavior Analysis

This section outlines which IPs were most active:

- Most active IP overall
- IPs with the most GET and POST requests respectively

## 8. Insights and Recommendations

Based on the data analysis, several operational and security suggestions are made:

- Monitor peak traffic hours for load balancing
- Focus error resolution efforts during hours with high failure rates
- Track high-activity IPs for potential abuse
- Consider implementing rate limiting and security auditing

## 9. Conclusion

This report provides a structured overview of web server activity, with key statistics and insights to help improve system performance, security, and user experience.