Log Analysis Report

Taha Abdelwadoud
ID: 2205030

May 10, 2025

Log Analysis Report

Generated on: Sat May 10 09:43:16 AM EDT 2025
Analyzed file: logs.log

1   Key Findings Summary

- **Total Requests:** 10,000

- **Peak Activity:** 2,896 requests on 19/May/2015

- **Critical Issue:** 404 errors (213 occurrences) dominate failures

- **Suspicious Activity:** IP 66.249.73.135 made 482 requests (4.8% of total traffic)
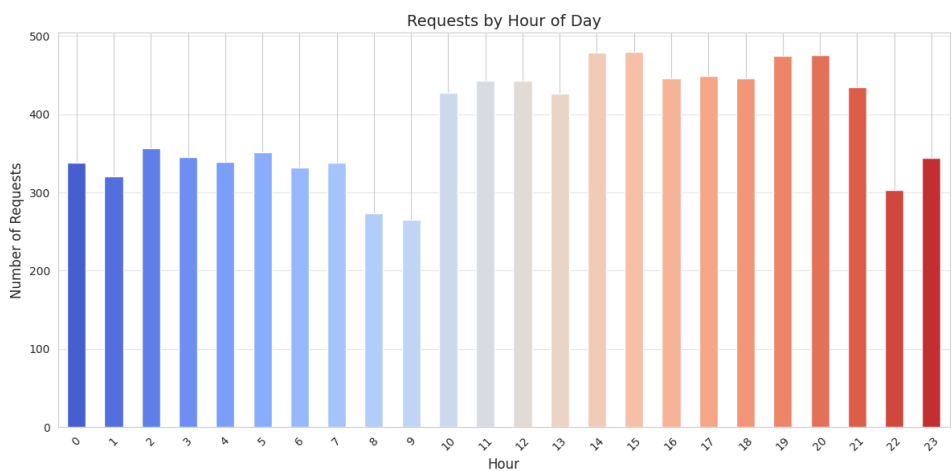
Requests by Hour

Figure 1: Traffic peaks at 14:00–15:00 (498 requests/hour)

2 Detailed Analysis

2.1 Traffic Composition

Metric	Count
GET Requests	9,952 (99.5%)
POST Requests	5 (0.05%)
Unique IPs	1,753

Table 1: Traffic Composition Metrics

Observation: Extremely skewed request methods suggest potential missing POST request logging.

2.2 Top Performers

Most Active IPs:

- 66.249.73.135 (482 requests)

- 46.105.14.53 (364 requests)
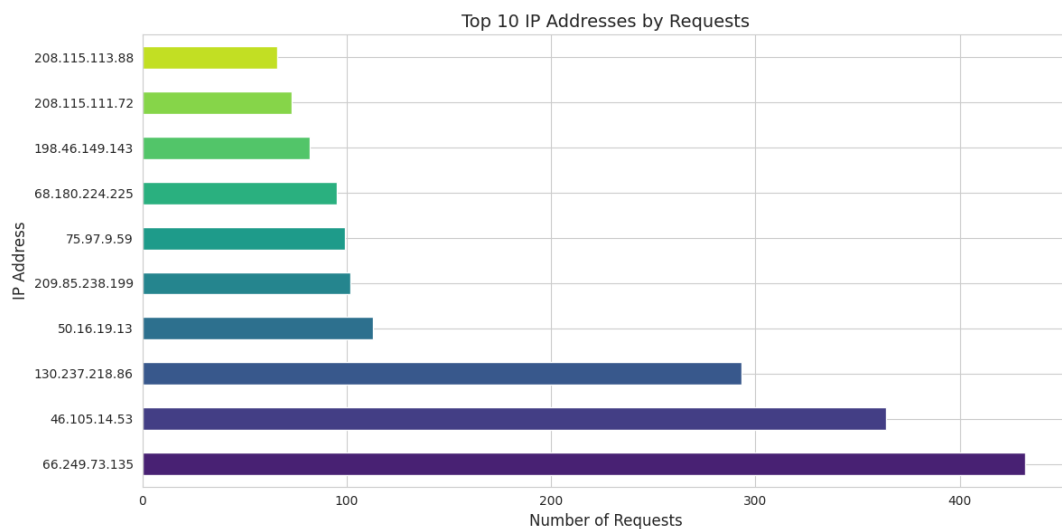
- 130.237.218.86 (357 requests)

Figure 2: Top 10 IPs show possible crawler activity (Googlebot IPs detected)

2.3 Error Analysis

Failure Hotspots:

- **Worst Day:** 19/May/2015 (66 failures)

- **Worst Hour:** 09:00 (18 failures)

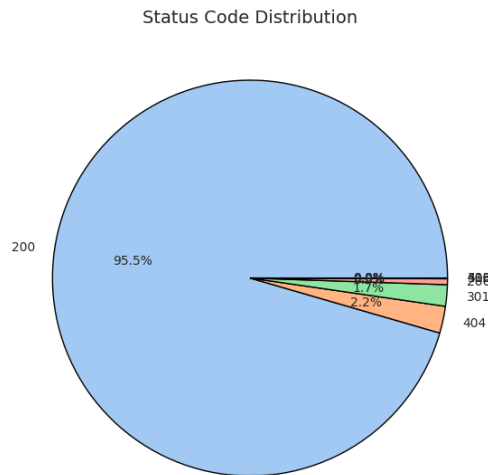| Status Code	Count	Percentage
200 (OK)	9,126	91.26%
404 (Not Found)	213	2.13%
304 (Not Modified)	445	4.45%

Table 2: Status Code Distribution

Figure 3: 404 not found errors represent 2.2% of all failures

2.4 Temporal Patterns

Daily Traffic:

- 17/May/2015: 1,632 requests
- 18/May/2015: 2,893 requests (+77% ↑)
- 19/May/2015: 2,896 requests (Peak)
- 20/May/2015: 2,579 requests

Hourly Pattern:

- **Lowest:** 08:00 (345 requests)
- **Highest:** 14:00 (498 requests)

3 Actionable Recommendations

3.1 Broken Link Fixes

- Audit 404 errors to identify missing resources
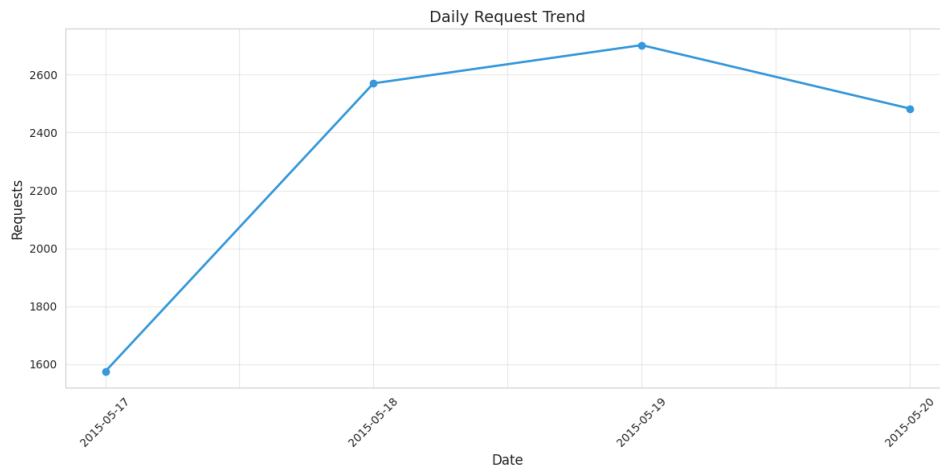- Implement redirects for deprecated endpoints

Figure 4: Sudden traffic surge on May 18–19 requires investigation

3.2   Bot Management

- Verify if top IPs are legitimate crawlers
- Consider rate limiting ($\geq$300 requests/IP/day)

3.3   Capacity Planning

- Scale resources for 14:00–15:00 peak hours
- Monitor traffic surges like May 18–19 spike

3.4   Security Review

- Investigate POST requests from 78.173.140.106
- Check for scraping attempts from high-volume IPs

3.5   Alerting Thresholds

Trigger alerts when:

- Failures > 5% (currently 2.2%)
- Any IP exceeds 400 requests/day