Log Analysis Report
Name: Ahmed Mourad Mohamed
ID: 2205010

---

1. Overview

This report analyzes Apache server logs to identify request patterns, failure trends, and potential security concerns. Based on the analysis, recommendations are proposed to reduce failure rates, optimize system performance, manage peak traffic periods, and mitigate potential threats.

---

2. Key Metrics Summary

- **Total Unique IPs:** 1,753
- **Average Requests per Day:** 2,500.00
- **Total Failed Requests (4xx / 5xx):** 220

---

3. Request Types by IP

- **Most Active GET IP:** 66.249.73.135 — (482 requests)
- **Most Active POST IP:** 78.173.140.106 — (3 requests)

---

4. Failure Requests (4xx / 5xx)

- **404 Not Found:** 213

- **500 Internal Server Error:** 3
- **403 Forbidden:** 2
- **416 Range Not Satisfiable:** 2
- **Total: 220**

5. Top User

- GET requests dominated by IP: 66.249.73.135
- POST requests dominated by IP: 78.173.140.106

---

6. Days with Highest Failures

- 19/May/2015 – 66 failures
- 18/May/2015 – 66 failures
- 20/May/2015 – 58 failures
- 17/May/2015 – 30 failures

---

7. Requests by Hour

Hour	Requests
00	361
01	360
02	365
03	354
04	355
05	371
06	366
07	357

Request Trends (Hour by Hour)

- 01 → 02: ↑ Increasing (360 → 365)
- 02 → 03: ↓ Decreasing (365 → 354)
- 03 → 04: ↑ Slight Increase (354 → 355)
- 04 → 05: ↑ Increase (355 → 371)

- 05 → 06: ↓ Decrease (371 → 366)
- 06 → 07: ↓ Decrease (366 → 357)
- 07 → 08: ↓ Decrease (357 → 345)
- 08 → 09: ↑ Increase (345 → 364)
- 09 → 10: ↑ Increase (364 → 443)
- 10 → 11: ↑ Increase (443 → 459)

---

9. Status Code Breakdown

Status Code	Count	Percentage
200	9,126	91.26%
304	445	4.45%
404	213	2.13%
301	164	1.64%
206	45	0.45%
500	3	0.03%
416	2	0.02%
403	2	0.02%

---

10 Failure Patterns by Hour

Hour	Failures	% of Total Failures
00	6	2.73%
01	10	4.55%
02	10	4.55%
03	7	3.18%
04	9	4.09%
05	15	6.82%

Recommendations & Analysis

A. Reducing Failures

- **404 Errors:**
  - Redirect or update broken URLs

    - Analyze request URLs for misconfigurations
- **500 Errors:**
    - Debug server-side issues
    - Enable detailed logging
- **403 & 416 Errors:**
    - Review file permissions
    - Test range handling for large file requests
- **Monitoring & Alerts:**
    - Set up real-time alerts
    - Use tools like ELK or Splunk for log correlation

B. High-Traffic Days & Hours

- **Peak Hour:** 14:00–15:00 (~498 requests/hour)
    - Use caching and scale infrastructure
- **May 18–20, 2015:**
    - Investigate for system overloads or attacks
    - Avoid maintenance during peak periods

C. Security Concerns

- **Suspicious IPs:**
    - 66.249.73.135: Likely Googlebot → Confirm
    - 46.105.14.53 & 130.237.218.86: Possible malicious activity
- **Mitigations:**
    - Reverse DNS lookup
    - Analyze user-agent strings
    - Apply rate-limiting (e.g., 300 req/hr/IP)
    - Use Web Application Firewall (WAF)
    - Keep software up to date
- **Unusual POST Requests:**
    - 78.173.140.106: Investigate payloads
    - Harden input validation and CSRF protection

D. System & Service Improvements

- **Caching & CDN:**
    - Use Redis/Memcached and external CDNs
- **Load Balancing & Auto-Scaling:**
    - Distribute load evenly and scale resources automatically

---

12. Conclusion

The Apache server performs reliably with a low failure rate (2%). However, through better error handling, proactive security measures, and optimized resource management, the system can become even more robust, scalable, and secure