My query is:

_sourceCategory=Labs/Apache/Access and status_code=404

| logcompare timeshift -24h

🔹 **Line by Line Explanation**

1. _sourceCategory=Labs/Apache/Access and status_code=404

- This filters logs only from the **Apache Access logs** that have an **HTTP 404 (Not Found)** response.
- So you're only analyzing failed requests (pages that don't exist).

---

2. | logcompare timeshift -24h

- logcompare groups logs into patterns/signatures (e.g., similar URLs, user agents, requests).
- Then, it **compares the current time window's log patterns with the same time window 24 hours earlier**.
- timeshift -24h means: "Look at the same time yesterday and compare it with now."

🔹 **How the Results Work**

Looking at your screenshot, you see columns like:

- **Count** → how many times that log pattern occurred in the current time range.
- **% Change** (e.g., +81%, -33%) → how much the count has increased or decreased compared to the same time yesterday.

📌 Example from your screenshot:

- **Signature #2:** Count = 13, +79%
    - This log pattern (type of 404 error) happened 13 times now.
    - Yesterday, it happened only around 7 times → that's a **79% increase**.
- **Signature #6:** Count = 6, -33%
    - This log pattern happened 6 times now.
    - Yesterday, it happened about 9 times → that's a **33% decrease**.

🔹 **Why Logcompare is Useful**

- It helps you **spot unusual changes** in log behavior without manually comparing yesterday's and today's data.
- Instead of going line by line, Sumo Logic highlights which patterns are happening **more often (suspicious increase)** or **less often (possible resolution)**.

🔹 **Example of a Helpful Log Source for Logcompare**

👉 **Authentication Logs (Failed Logins)**

- Query:
- _sourceCategory=Auth/FailedLogins
- | logcompare timeshift -24h
- Why? If failed login attempts from a specific IP or username suddenly spike today compared to yesterday (e.g., +200%), it could indicate a **brute force attack**.

Other examples:

- **Firewall logs** → sudden increase in denied connections.
- **Web server logs** → sudden spike in 500 errors compared to yesterday.

✅ **In summary:**

- logcompare compares **current logs vs. past logs**.
- **Count = raw occurrences now**.
- **% Change = growth or decline compared to yesterday (or specified timeshift)**.
- Great for anomaly detection (e.g., unusual login failures, sudden 404 surges, new types of errors).
