Hands-on lab: Create a Parsing Template using Mezmo

Estimated Time Needed: **60 mins**

Getting Started

Welcome to the hands-on lab to create a Parsing Template using Mezmo.

In this lab, you will learn how to parse ingested log lines. You will learn about the parsing screen and, the parsing mini-map. You will learn how to use some of the available parsing functions. You will learn how to parse all three values or parse one and to validate templates.

Mezmo parsing:

- Mezmo supports common log types and parses the lines automatically for you. Log parsing is the process of converting log data into a common format to make them machine-readable. However, if you have a log format that does not fit one of the supported log types, you can create your own parsing rules using Create a Parsing Template or do a one-time log extraction using Extract Fields.
- Custom Parsing templates are applied to your logs based on the order of active templates. For example, if you have two active templates that target the same log line, then the templates are applied in the order on the Manage Parsing page.

  -Template One
  -Template Two

  First, Template One will be applied to incoming logs, if there is a matching log line in Template Two, it will then be applied. You can change the order of active templates by dragging them on the Manage Parsing page.

Learning Objectives:

In this lab, you will be using the step-by-step wizard to wrangle non-standard log formats and run custom transformations on your logs, allowing you to easily search and graph log lines that were previously off-limits.

It is a simple three-step process:
-Search
-Extract
-Validate

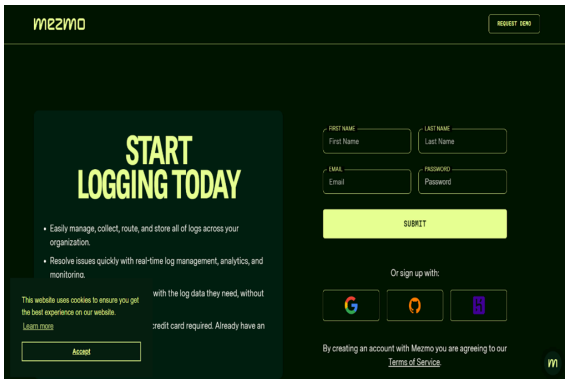
For most cases, automatic parsing may be all you need, especially if your logs are in common formats.

After completing this lab:

- Demonstrate how to parse a string.
- Show how to parse a timestamp.
- Display how to parse a number.
- Exhibit how to validate templates

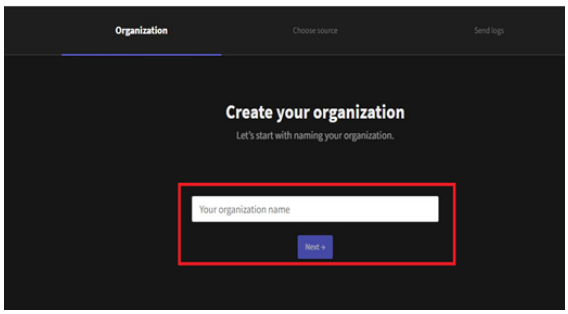
Set-up : Sign up with Mezmo

1. Click and open the link Sign up
2. You will be directed to the sign-up page

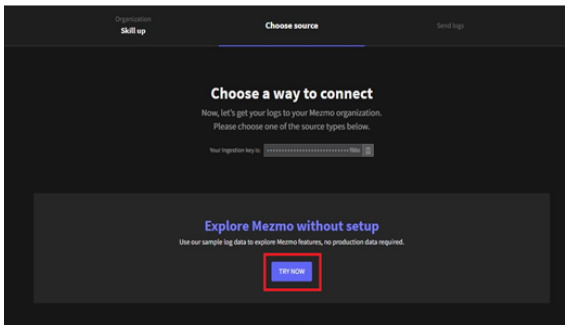


3. Enter your details and click **Submit**

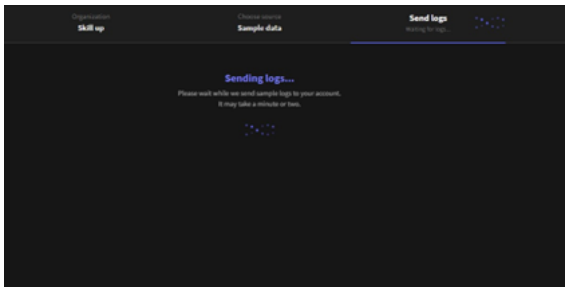
4. To ensure the validity of your email address, Mezmo will send a verification email to the address you provided. Enter the verification code
5. Enter your **organization name** as shown below



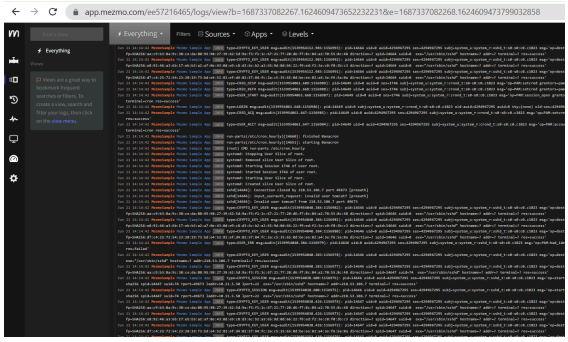
6. Click **Try now**



7. Wait for a few seconds while the sampled log is being sent



8. Now, you will be redirected to your Mezmo account **dashboard** or **homepage**



Note: The mezmo free trial period is for 14 days only. Kindly complete the lab within the free trial period.

Logs information:

Let's take the example log line which has ip address, timestamp, response information, and web browsers used:

```
103.93.21.233 - - [15/Nov/2018:18:31:24 +0000] "GET / HTTP/1.1" 200 745 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
```

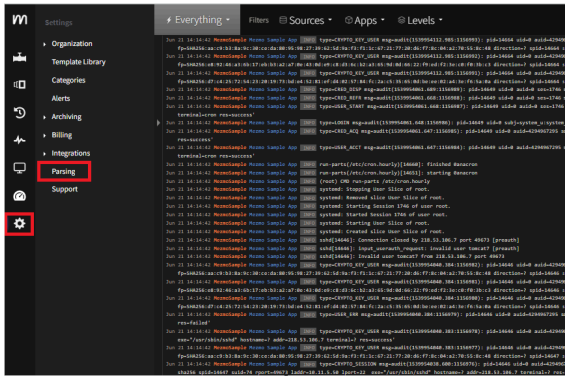
You will use the above log lines throughout and perform custom parsing to parse the three values mentioned below:

- **ip_address:** 103.93.21.233
- **timestamp:** 15/Nov/2018:18:31:24 +0000
- **response:** 200

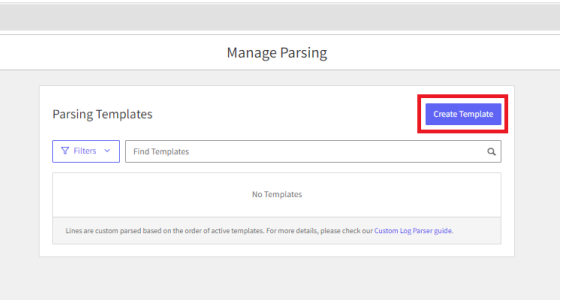
Task 1: Parse The String

You are going to parse 111.00.11.10 from the log line.

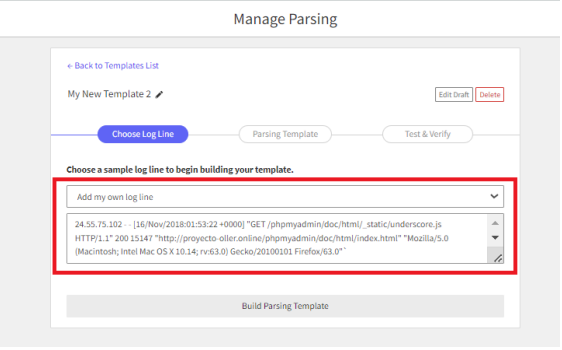
1. Click the **setting** icon and click the **Parsing**. and on the next page click **Create Template**.



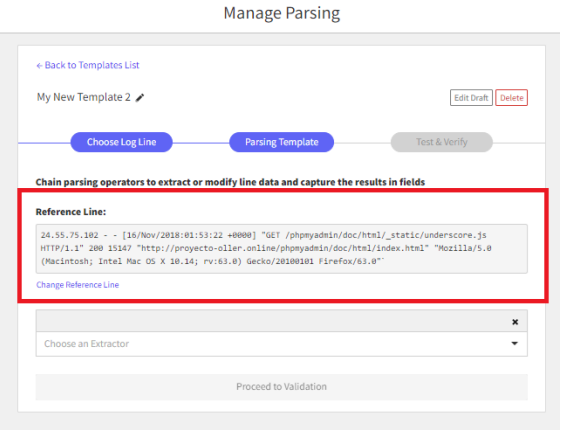
2. On the next page click **Create Template**.



3. In Choose a Log Line, select **Add my own log line**. You will be using the log line from the introduction.



4. Click **Build a Parsing Template**. You will see the line you entered as a Reference Line.



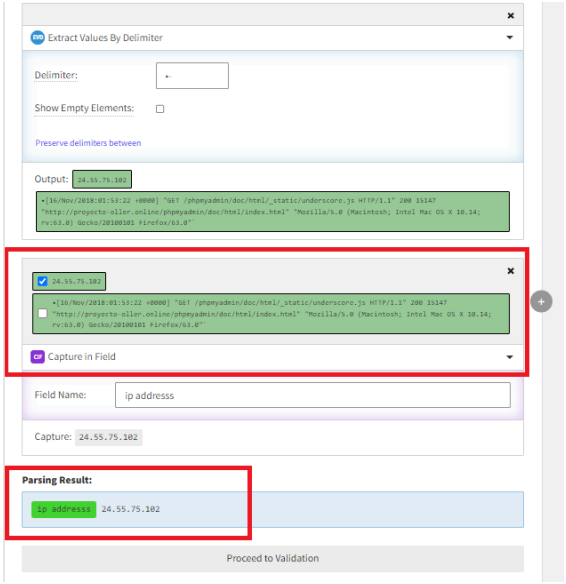
5. First, you are going to break the text down into smaller parts so you can use the part you want. In Choose an Extractor, select **Extract Value By Delimiter**.

6. Enter a **space** and then a **dash**.

7. Now you should see **24.55.75.102** as part of the lines parsed.

8. Select **24.55.75.102** and choose the operator **Capture in Field**. Give a label or Field Name **ip_address**.

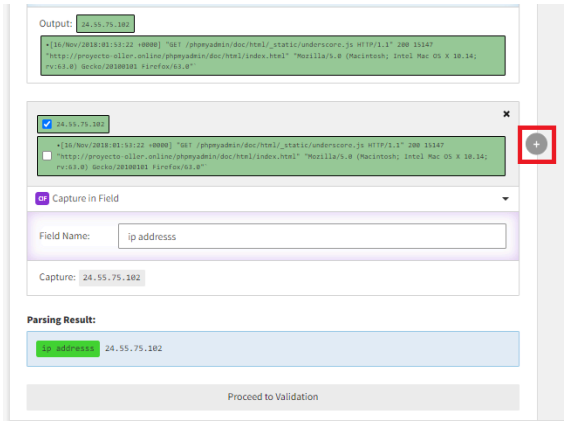
9. The result is shown at the bottom of the parsing page.



Task 2: Parse a Timestamp

You will parse 16/Nov/2018:01:53:22 +0000 from the log line.

1. Select the circle with the **plus sign** to create a Sibling Operator.

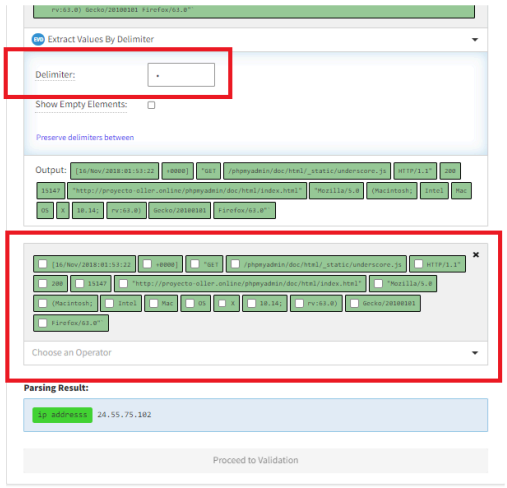


2. Check the longer output that includes the timestamp.

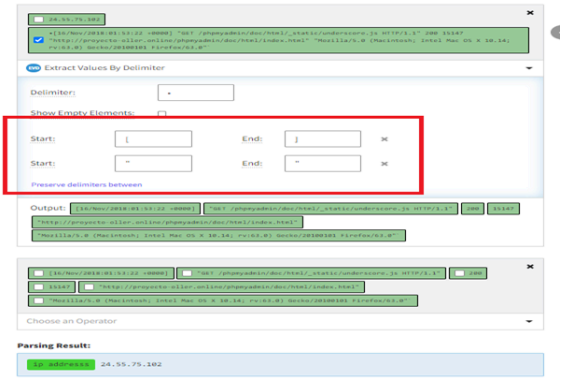
3. Choose an operator > **Extract Values by Delimiter**.

4. Enter a **space** into the delimiter.

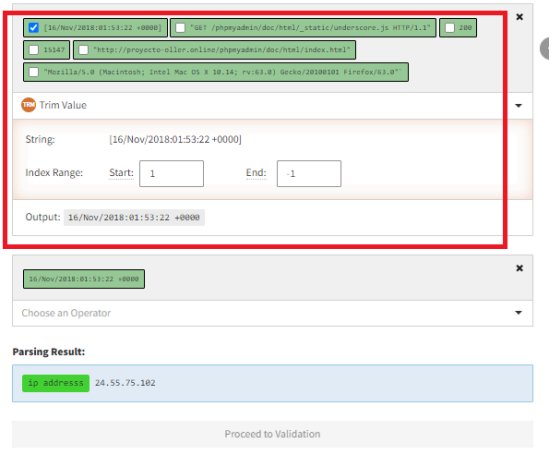
5. Notice the output has split everything by space, including part of timestamp. To fix the timestamp, you need to preserve some of the spaces.



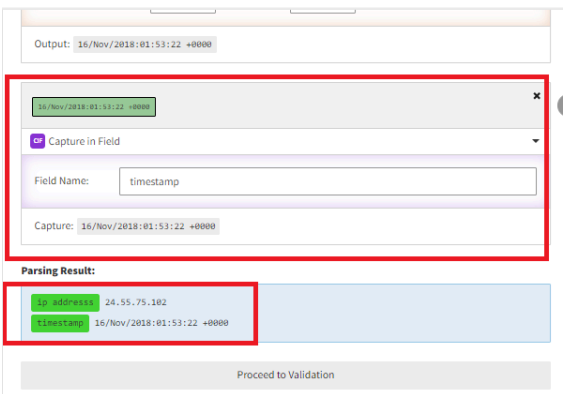
6. Click **Preserve delimiters between**.
7. Start use a left square bracket [and end use a right square bracket] .
8. Click **Preserve delimiters between** again. Use double quotes " for both start and end. You will notice that the timestamp is now cleaned up, along with some of other output.



9. Now you need to remove the brackets from the timestamp, so it's easier to run the diagnosis against. Select the timestamp. [16/Nov/2018:01:53:22 +0000] , choose operator, **Trim Value**.
10. Trim Value is 0 based on counting. Start, enter **1**, for end enter **-1**.
11. Your output should be the timestamp.



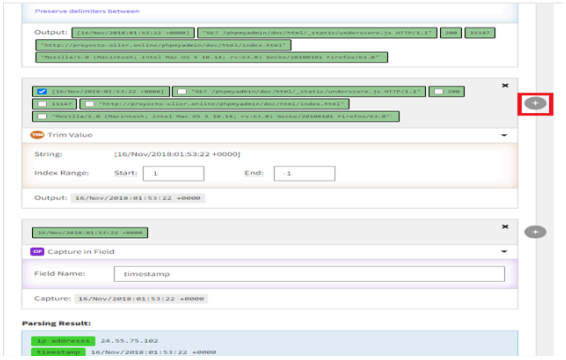
12. Choose operator > **Capture in Field** and label it **timestamp**.
13. So far, you have captured two fields from the log line.



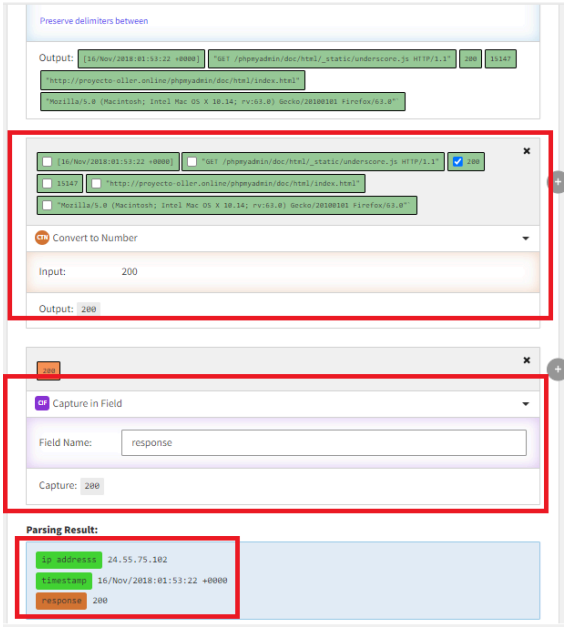
Task 3: Parse The Number

You are going to parse 200 from the log line.

1. Using the mini map, select Trim Value. Trim Value is orange, you can also hover over the icons in the mini map. Using the mini map lets you jump between parsed areas. By starting from Trim Value, you can start from a place where the 200 is already separated from the other values, making it easier to use.
2. Click on circle with the **plus sign** to add a Sibling Operator.



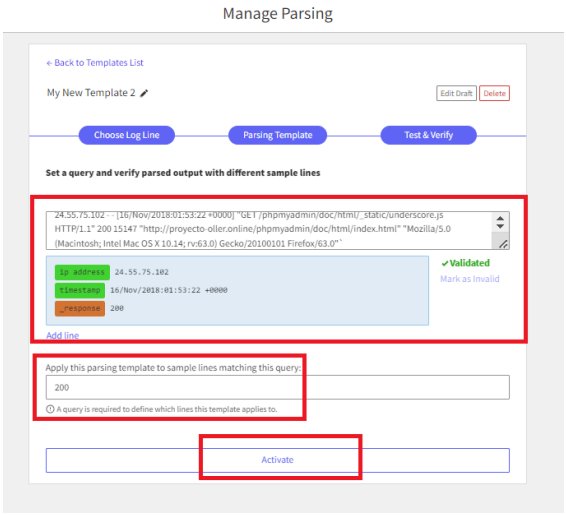
3. Select **200**.
4. Choose an operator > **Convert to Number**.
5. Choose an operator > **Capture in Field**. Field name is **response**.



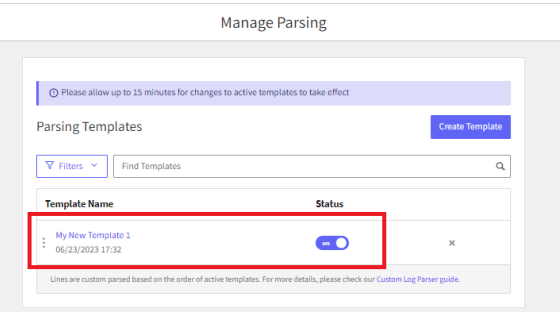
Task 4: Validate Template

Before you can make a template active, you must check that the log lines you want are working.

1. Add a **log line** to test against in Add Line. You can use the example line. When testing you want to be sure to test multiple lines by adding lines.
2. Mark the log lines as valid or invalid.
   a. If a line is marked as invalid, you will be taken back to the Parsing Template step.
3. Mark the line valid and enter your query in the Apply this parsing template to sample lines matching this query: input field.



4. On clicking the **Activate** button then you will see the **on** Status. And it will take 15 minutes to take effect for your application logs.



Note: Active parsing templates are only applied to the lines that come in after the template has been enabled. All log lines that were ingested prior to the template becoming active are not parsed by the parsing template.

And whenever your application generates new logs it will give you matched data from the logs that are helpful in analyzing your application logs so that you know whether your application is working correctly or not.

Summary

Congratulations! You just created a Parsing Template using Mezmo.

In this lab, you have accessed and explored the mezmo platform. You have performed the custom parsing on the example log line provided and parsed ip_address, timestamp, response and validated it.

Author(s)

Pallavi Rai

Contributor(s)

Anamika Agarwal
Shivam kumar