

Uygulamalı laboratuvar: Mezmo kullanarak bir Ayırıştırma Şablonu oluşturma

Tahmini Gerekli Süre: **60 dk**

Başlarken

Mezmo kullanarak bir Ayırıştırma Şablonu oluşturma uygulamalı laboratuvarına hoş geldiniz.

Bu laboratuvar, alınan günlük satırlarını nasıl ayırıştıracağınızı öğreneceksiniz. Ayırıştırma ekranı ve ayırıştırma mini haritası hakkında bilgi edineceksiniz. Mevcut bazı ayırıştırma fonksiyonlarını nasıl kullanacağınızı öğreneceksiniz. Üç değerini hepsini nasıl ayırıştıracağınızı veya birini nasıl ayırıştıracağınızı ve şablonları nasıl doğrulayacağınızı öğreneceksiniz.

Mezmo ayırıştırma:

- Mezmo, yaygın günlük türlerini destekler ve satırları sizin için otomatik olarak ayırıştırır. Günlük ayırıştırma, günlük verilerini makine tarafından okunabilir hale getirmek için ortak bir formata dönüştürme sürecidir. Ancak, desteklenen günlük türlerinden birine uymayan bir günlük formatınız varsa, Bir Ayırıştırma Şablonu Oluştur veya Alanları Çıkar kullanarak kendi ayırıştırma kurallarınızı oluşturabilirsiniz.
- Özel Ayırıştırma şablonları, aktif şablonların sırasına göre günlüklerinize uygulanır. Örneğin, aynı günlük satırını hedefleyen iki aktif şablonunuz varsa, şablonlar Yönetim Ayırıştırma sayfasındaki sıraya göre uygulanır.

-Şablon Bir
-Şablon İki

Öncelikle, Şablon Bir gelen günlükler üzerine uygulanacaktır; eğer Şablon İki'de eşleşen bir günlük satırı varsa, o zaman uygulanacaktır. Aktif şablonların sırasını Yönetim Ayırıştırma sayfasında sürükleyerek değiştirebilirsiniz.

Öğrenme Hedefleri:

Bu laboratuvar çalışmasında, standart olmayan günlük formatlarını düzenlemek ve günlükleriniz üzerinde özel dönüşümler gerçekleştirmek için adım adım sihirbazı kullanacaksınız. Bu sayede daha önce erişilemeyen günlük satırlarını kolayca arayabilir ve grafikleyebilirsiniz.

Bu basit bir üç adımlı süreçtir:

-Arama
-Çıkarma
-Doğrulama

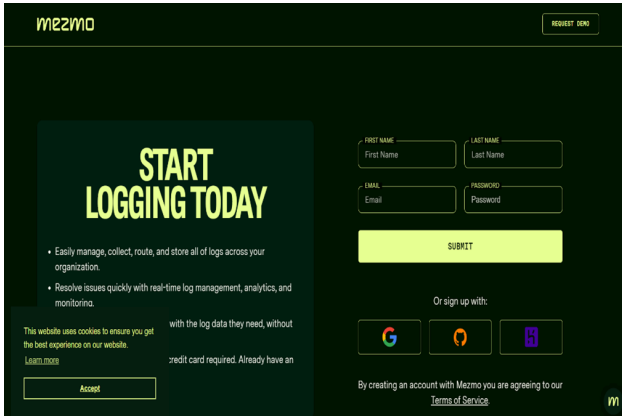
Çoğu durumda, otomatik ayırıştırma ihtiyacınız olan tek şey olabilir, özellikle günlükleriniz yaygın formatlarda ise.

Bu laboratuvarı tamamladıktan sonra:

- Bir dizeyi nasıl ayırıştıracağınızı gösterin.
- Bir zaman damgasını nasıl ayırıştıracağınızı gösterin.
- Bir sayıyı nasıl ayırıştıracağınızı gösterin.
- Şablonları nasıl doğrulayacağınızı sergileyin.

Kurulum : Mezmo ile Kaydolun

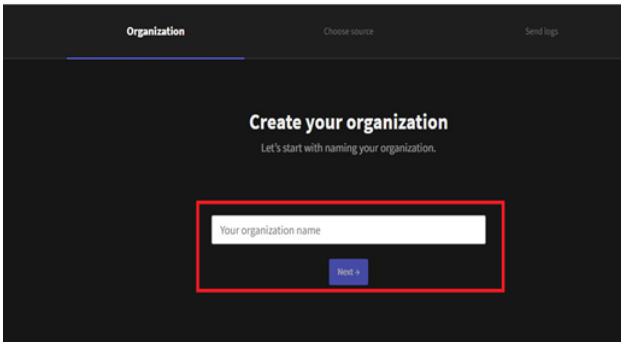
- [Kaydolun](#) bağlantısına tıklayın ve açın.
- Kaydolma sayfasına yönlendirileceksiniz.

The image shows the Mezmo login page. At the top left is the 'me2mo' logo. At the top right is a 'REQUEST DEMO' button. The main content area has a dark background. On the left, there's a section titled 'START LOGGING TODAY' with two bullet points: 'Easily manage, collect, route, and store all of logs across your organization.' and 'Resolve issues quickly with real-time log management, analytics, and monitoring.' Below this is a small text block about cookies: 'This website uses cookies to ensure you get the best experience on our website. Learn more' and 'with the log data they need, without credit card required. Already have an' with an 'Accept' button. On the right, there's a login form with fields for 'FIRST NAME' (First Name), 'LAST NAME' (Last Name), 'EMAIL' (Email), and 'PASSWORD' (Password). Below these is a 'SUBMIT' button. Underneath the submit button, it says 'Or sign up with:' followed by three social media icons: Google, Facebook, and Twitter. At the bottom right, it says 'By creating an account with Mezmo you are agreeing to our Terms of Service' with a link to 'Terms of Service' and the Mezmo logo.

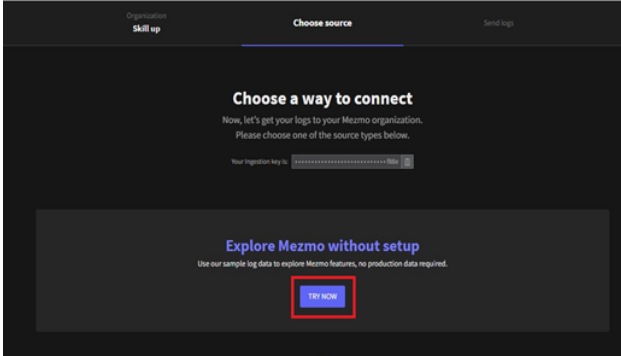
- Bilgilerinizi girin ve **Gönder** butonuna tıklayın.

The image shows the Mezmo verification page. At the top is the Mezmo logo. Below it, it says 'Enter your verification code below' and there are six empty boxes for the code. Below the boxes is a 'Resend Verification Email' button. At the bottom, there is a 'Log Out' button. At the very bottom, there is a footer with 'Terms Privacy © 2013-2023 Mezmo, Inc.'

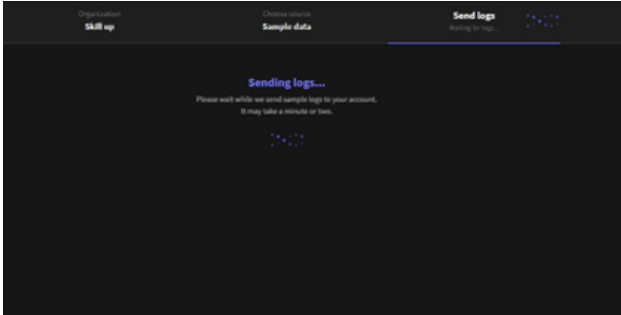
- E-posta adresinizin geçerliliğini sağlamak için, Mezmo sağladığınız adrese bir doğrulama e-postası gönderecektir. Doğrulama kodunu girin.
- Aşağıda gösterildiği gibi **organizasyon adınızı** girin.



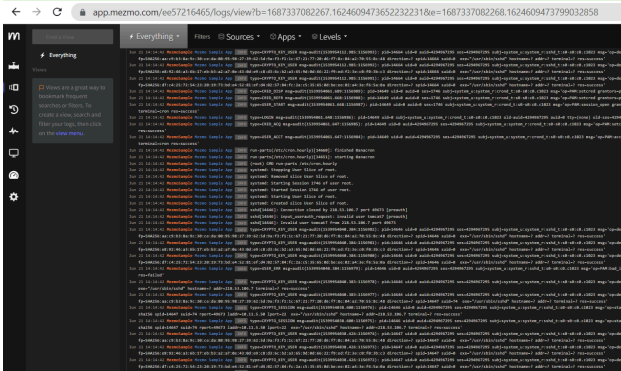
6. Şimdi dene butonuna tıklayın.



7. Örneklenen günlük gönderilirken birkaç saniye bekleyin.



8. Artık Mezmo hesabınızın kontrol paneline veya ana sayfasına yönlendirileceksiniz.



Not: Mezmo'nun ücretsiz deneme süresi yalnızca 14 gündür. Lütfen laboratuvarı ücretsiz deneme süresi içinde tamamlayın.

Günlük bilgileri:

Örnek günlük satırını ele alalım; bu satırda IP adresi, zaman damgası, yanıt bilgisi ve kullanılan web tarayıcısı bulunmaktadır:

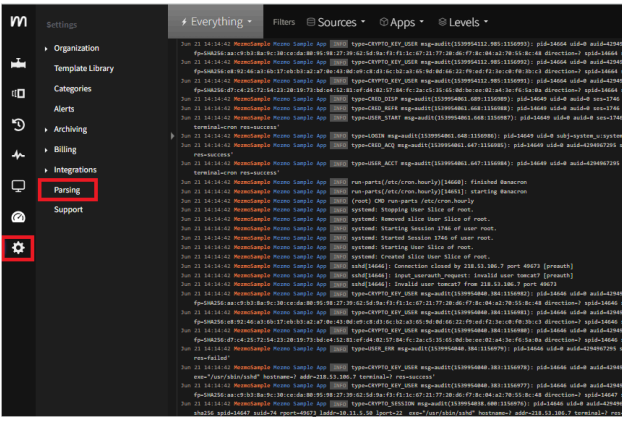
103.93.21.233 - - [15/Nov/2018:18:31:24 +0000] "GET / HTTP/1.1" 200 745 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"

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

Görev 1: Dizeyi Ayrıştır

Log satırından 111.00.11.10'u ayrıştıracaksınız.

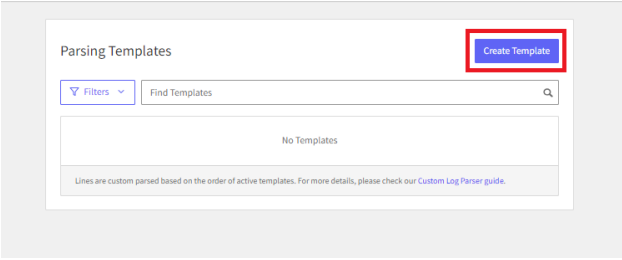
1. Ayarlar simgesine tıklayın ve Ayrıştırma seçeneğine tıklayın. Sonraki sayfada Şablon Oluştur butonuna tıklayın.



2. Sonraki sayfada **Şablon Oluştur** butonuna tıklayın.

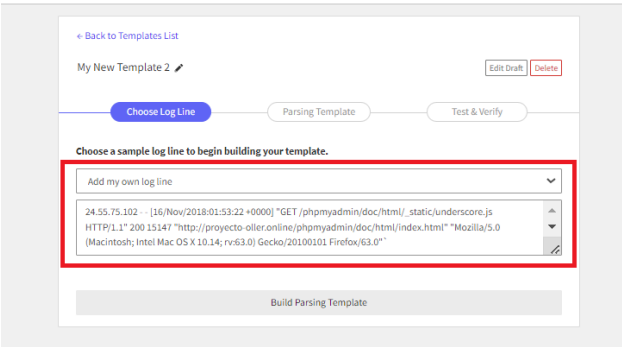


Manage Parsing



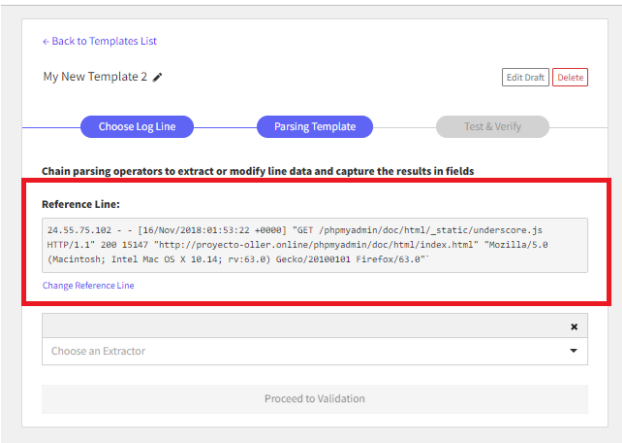
3. Log Satırı Seçin kısmında **Kendi log satırımı ekle** seçeneğini seçin. Girişteki log satırını kullanacaksınız.

Manage Parsing



4. **Ayrıştırma Şablonu Oluştur** butonuna tıklayın. Girdiğiniz satır Referans Satırı olarak göreceksiniz.

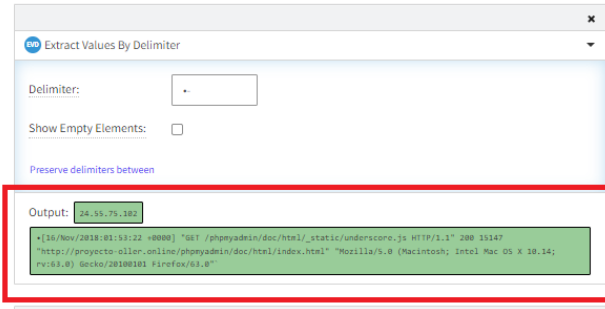
Manage Parsing



5. Öncelikle, metni daha küçük parçalara ayıracaksınız, böylece istediğiniz parçayı kullanabilirsiniz. Extractor Seçin kısmında **Ayrırcı** ile **Değer Çıkart** seçeneğini seçin.

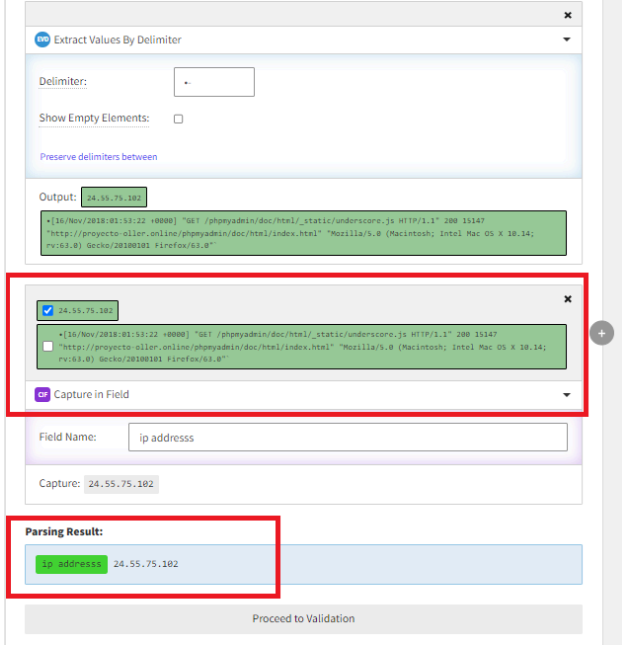
6. **boşluk** ve ardından bir **tire** girin.

7. Artık **24.55.75.102**'yi ayrıştırdın satırların bir parçası olarak görmelisiniz.



8. 24.55.75.102'yi seçin ve **Alanda Yakala** operatörünü seçin. Bir etiket veya Alan Adı olarak **ip_address** verin.

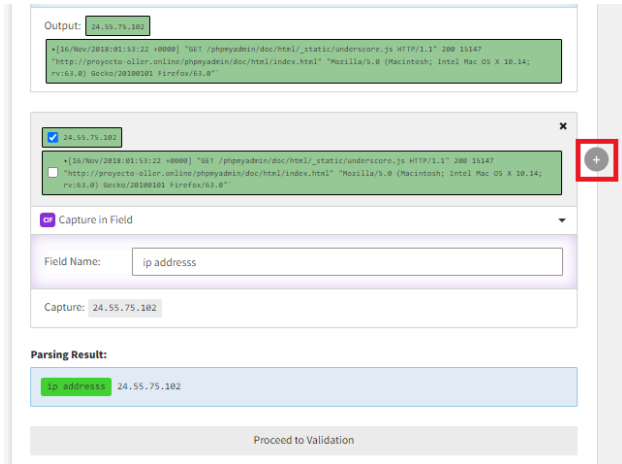
9. Sonuç, ayrıştırma sayfasının altında gösterilmektedir.



Görev 2: Zaman Damgasını Ayrıştır

Log satırından 16/Nov/2018:01:53:22 +0000 zaman damgasını ayrıştıracaksınız.

1. Kardeş Operatörü oluşturmak için **artı işareti** olan çemberi seçin.



2. Zaman damgasını içeren daha uzun çıktıyı kontrol edin.

Preserve delimiters between

Output: 24.55.75.102

```
<[16/Nov/2018:01:53:22 +0000] "GET /phpmyadmin/doc/html/_static/underscore.js HTTP/1.1" 200 15147
"http://projecto-oller.online/phpmyadmin/doc/html/index.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14; rv:63.0) Gecko/20100101 Firefox/63.0"
```

Choose an Operator

Parsing Result:

ip address 24.55.75.102

Proceed to Validation

3. Bir operatör seçin > **Ayrıcı ile Değerleri Çıkar.**

4. Ayrıcıya bir boşluk girin.

5. Çıktının her şeyi boşlukla ayırdığını, zaman damgasının bir kısmını da içerdığını fark edin. Zaman damgasını düzeltmek için bazı boşlukları korumanız gerekiyor.

Extract Values By Delimiter

Delimiter: +

Show Empty Elements: ☐

Preserve delimiters between

Output: [16/Nov/2018:01:53:22 +0000] "GET /phpmyadmin/doc/html/_static/underscore.js HTTP/1.1" 200 15147 "http://projecto-oller.online/phpmyadmin/doc/html/index.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14; rv:63.0) Gecko/20100101 Firefox/63.0"

Choose an Operator

Parsing Result:

ip address 24.55.75.102

Proceed to Validation

6. Aralarındaki ayrıcıları koru seçeneğine tıklayın.

7. Bir sol köşeli parantez [ile başlayın ve bir sağ köşeli parantez] ile bitirin.

8. Aralarındaki ayrıcıları koru seçeneğine tekrar tıklayın. Hem başlangıç hem de bitiş için çift tırnak " kullanın. Zaman damgasının şimdi temizlendiğini, diğer bazı çıktılarla birlikte göreceksiniz.

Extract Values By Delimiter

Delimiter: +

Show Empty Elements: ☐

Start: [End:] ✕

Start: " End: " ✕

Preserve delimiters between

Output: [16/Nov/2018:01:53:22 +0000] "GET /phpmyadmin/doc/html/_static/underscore.js HTTP/1.1" 200 15147 "http://projecto-oller.online/phpmyadmin/doc/html/index.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14; rv:63.0) Gecko/20100101 Firefox/63.0"

Choose an Operator

Parsing Result:

ip address 24.55.75.102

9. Şimdi zaman damgasından köşeli parantezleri kaldırmamız gerekiyor, böylece teşhis koymak daha kolay olur. Zaman damgasını seçin. [16/Nov/2018:01:53:22 +0000] , operatörü seçin, **Değeri Kısalt.**

10. Kısaltma Değeri 0 bazlıdır. Başlangıç için 1, bitiş için -1 girin.

11. Çıktınız zaman damgası olmalıdır.

Trim Value

String: [16/Nov/2018:01:53:22 +0000]

Index Range: Start: 1 End: -1

Output: 16/Nov/2018:01:53:22 +0000

Parsing Result:

ip address 24.55.75.102

Proceed to Validation

12. Operatörü seçin > **Alanda Yakala** ve etiketini **zaman damgası** olarak belirleyin.

13. Şimdiye kadar log satırından iki alan yakaladınız.

Output: 16/Nov/2018:01:53:22 +0000

Capture in Field

Field Name: timestamp

Capture: 16/Nov/2018:01:53:22 +0000

Parsing Result:

ip address 24.55.75.102

timestamp 16/Nov/2018:01:53:22 +0000

Proceed to Validation

Görev 3: Sayıyı Ayrıştır

Log satırından 200'ü ayrıştıracağız.

1. Mini haritayı kullanarak Trim Value'yu seçin. Trim Value turuncudur, mini haritadaki simgelerin üzerine gelerek de bilgi alabilirsiniz. Mini haritayı kullanmak, ayrıştırılan alanlar arasında geçiş yapmanıza olanak tanır. Trim Value'dan başlayarak, 200'ün diğer değerlerden ayrılmış olduğu bir yerden başlayabilir, böylece kullanımı kolaylaşır.

2. **Artı işaretli** olan daireye tıklayarak bir Kardeş Operatörü ekleyin.

Trim Value

String: [16/Nov/2018:01:53:22 +0000]

Index Range: Start: 1 End: 200

Output: 16/Nov/2018:01:53:22 +0000

Parsing Result:

ip address 24.55.75.102

timestamp 16/Nov/2018:01:53:22 +0000

Proceed to Validation

3. **200'ü** seçin.

4. Bir operatör seçin > **Sayıya Dönüştür**.

5. Bir operatör seçin > **Alanda Yakala**. Alan adı **response**.

Preserve delimiters between

Output: [16/Nov/2018:01:53:22 +0000] "GET /phpmyadmin/doc/html/_static/underscore.js HTTP/1.1" 200 15147

"http://proyecto-olier-online/phpmyadmin/doc/html/index.html"

"Mozilla/5.0 (Macintosh; Intel Mac OS X 38.14; rv:63.0) Gecko/20100101 Firefox/63.0"

Convert to Number

Input: 200

Output: 200

Capture in Field

Field Name: response

Capture: 200

Parsing Result:

ip address 24.55.75.182

timestamp 16/Nov/2018:01:53:22 +0000

response 200

Görev 4: Şablonu Doğrula

Bir şablonu aktif hale getirmeden önce, test etmek istediğiniz günlük satırlarının çalıştığından emin olmalısınız.

1. **Günlük satırı** ekleyin ve test edin. Örnek satırı kullanabilirsiniz. Test sırasında, birden fazla satırı test etmek için satırlar eklemeyi unutmayın.
2. Günlük satırlarını geçerli veya geçersiz olarak işaretleyin.
 - a. Bir satır geçersiz olarak işaretlenirse, sizi Ayırıştırma Şablonu adımına geri götürecektir.
3. Satırı geçerli olarak işaretleyin ve Bu ayırıştırma şablonunu bu sorguya uyan örnek satırlara uygulayın: giriş alanına sorgunuzu girin.

Manage Parsing

← Back to Templates List

My New Template 2 [Edit Draft](#) [Delete](#)

Choose Log Line Parsing Template Test & Verify

Set a query and verify parsed output with different sample lines

24.55.75.182 - [16/Nov/2018:01:53:22 +0000] "GET /phpmyadmin/doc/html/_static/underscore.js HTTP/1.1" 200 15147 "http://proyecto-olier-online/phpmyadmin/doc/html/index.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:63.0) Gecko/20100101 Firefox/63.0"

ip address 24.55.75.182

timestamp 16/Nov/2018:01:53:22 +0000

response 200

Validated

Mark as Invalid

Add line

Apply this parsing template to sample lines matching this query:

200

A query is required to define which lines this template applies to.

Activate

4. **Aktif Et** butonuna tıkladığınızda **açık** durumu göreceksiniz. Ve uygulama günlükleriniz için etkili olması 15 dakika sürecektir.

Manage Parsing

Please allow up to 15 minutes for changes to active templates to take effect

Parsing Templates [Create Template](#)

Filters Find Templates

Template Name Status

My New Template 1 [on](#) [x](#)

06/23/2023 17:32

Lines are custom parsed based on the order of active templates. For more details, please check our [Custom Log Parser guide](#).

Not: Aktif ayırıştırma şablonları, şablon etkinleştirildikten sonra gelen satırlara yalnızca uygulanır. Şablon aktif hale gelmeden önce alınan tüm günlük satırları, ayırıştırma şablonu tarafından ayırıştırılmaz.

Uygulamanız yeni günlükler ürettiğinde, uygulama günlüklerinizi analiz etmenize yardımcı olan eşleşen verileri size sunar, böylece uygulamanızın doğru çalışıp çalışmadığını bilirsiniz.

Özet

Tebrikler! Mezmo kullanarak bir Ayırıştırma Şablonu oluşturdunuz.

Bu laboratuvar çalışmasında, mezmo platformuna erişim sağladınız ve keşfettiniz. Verilen örnek günlük satırı üzerinde özel ayrıştırma gerçekleştirdiniz ve ip_address, timestamp, response bilgilerini ayrıştırarak doğruladınız.

Yazar(lar)

Pallavi Rai

Katkıda Bulunan(lar)

Anamika Agarwal
Shivam kumar