

# Uygulamalı laboratuvar: Mezmo kullanarak bir Ayrıştırma Şablonu oluşturma

Tahmini Gerekli Süre: 60 dk

## Başlarken

Mezmo kullanarak bir Ayrıştırma Şablonu oluşturma uygulamalı laboratuvarına hoş geldiniz.

Bu laboratuvar, alman günlük satırlarını nasıl ayırtacağınızı öğreneceksiniz. Ayrıştırma ekranı ve ayrıştırma mini haritası hakkında bilgi edineceksiniz. Mevcut bazı ayrıştırma fonksyonlarını nasıl kullanacağınızı öğreneceksiniz. Üç değerin hepsini nasıl ayırtacağınızı veya birini nasıl ayırtacağınızı ve şablonları nasıl doğrulayacağınızı öğreneceksiniz.

### Mezmo ayrıştırma:

- Mezmo, yaygın günlük türlerini destekler ve satırları sizin için otomatik olarak ayırtır. Günlük ayrıştırma, günlük verilerini makine tarafından okunabilir hale getirmek için ortak bir formata dönüştürme sürecidir. Ancak, desteklenen günlük türlerinden birine uyumayan bir günlük formatınız varsa, Bir Ayrıştırma Şablon Oluştur veya Alanları Çıkar kullanarak kendi ayrıştırma kurallarınızı oluşturabilirsiniz.
- Özel Ayrıştırma şablonları, aktif şablonların sırasına göre günlüklerinize uygulanır. Örneğin, aynı günlük satırını hedefleyen iki aktif şablonunuz varsa, şablonlar Yönetim Ayrıştırma 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 Ayrıştırma sayfasında sürükleyerek değiştirebilirisiniz.

## 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

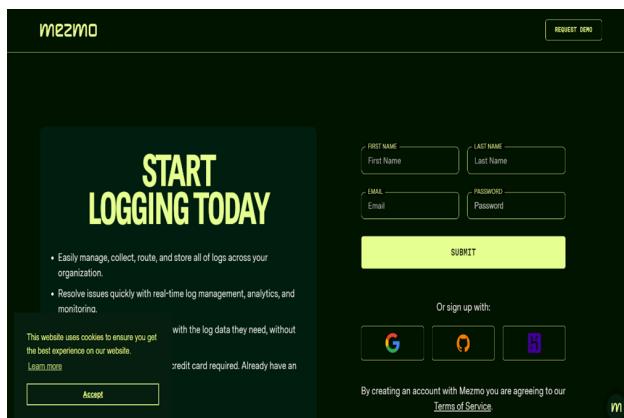
Çoğu durumda, otomatik ayrıştırma ihtiyacınız olan tek şey olabilir, özellikle günlükleriniz yaygın formatlarda ise.

Bu laboratuvari tamamladıktan sonra:

- Bir dizeyi nasıl ayırtacağınızı gösterin.
- Bir zaman damgasını nasıl ayırtacağınızı gösterin.
- Bir sayıyi nasıl ayırtacağınızı gösterin.
- Şablonları nasıl doğrulayacağınızı sergileyin.

## Kurulum : Mezmo ile Kaydolun

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

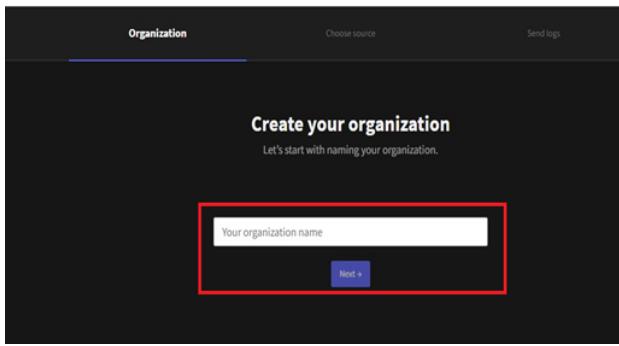


3. Bilgilerinizi girin ve **Gönder** butonuna tıklayın.

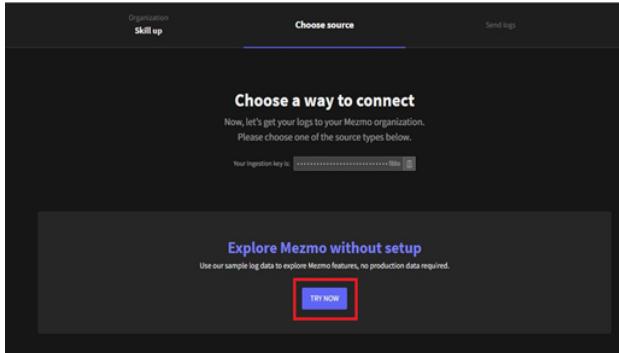


4. E-posta adresinizin geçerliliğini sağlamak için, Mezmo sağladığımız adrese bir doğrulama e-postası gönderecektir. Doğrulama kodunu girin.

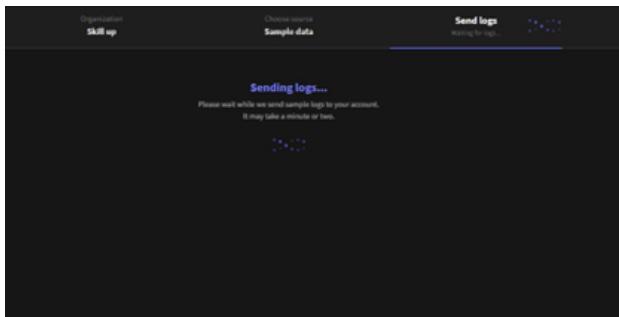
5. Aşağıda gösterildiği gibi **organizasyon adınızı** girin.



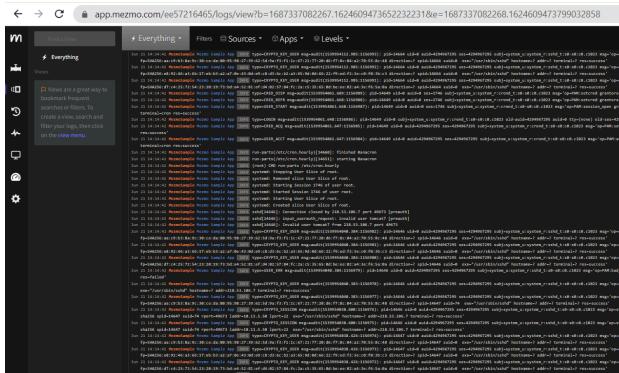
6. Şimdi dene butonuna tıklayın.



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 tarayıcıları 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 Ayırıştır

Log satırından 111.00.11.10'u ayırtıracaksınız.

1. **Ayarlar** simgesine tıklayın ve **Ayırıştırma** seçeneğine tıklayın. Sonraki sayfada **Sablon Oluştur** butonuna tıklayın.

The screenshot shows the Microsoft Edge browser with the address bar set to 'Everything'. The left sidebar has a 'Settings' icon at the top, followed by sections for Organization, Template Library, Categories, Alerts, Archiving, Billing, Integrations, Parsing (which is highlighted with a red box), and Support. The main content area displays a list of system processes. Each process entry includes a small icon, the process name, its full path, CPU usage (e.g., 0.00%), memory usage (e.g., 1.00 MB), and a 'Details' link. For example, one entry is 'Type=CPU% CPU usage=0.00 msid=11595091 100.11595091()', another is 'Type=CLOUD\_XP\_USER acc=msid=11595421 005.11595091()', and so on. The bottom of the page shows navigation links for 'Search', 'Home', 'New tab', and 'Help'.

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

## Manage Parsing

Parsing Templates

No Templates
Lines are custom parsed based on the order of active templates. For more details, please check our <a href="#">Custom Log Parser guide</a> .

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

## Manage Parsing

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

## Manage Parsing

5. Öncelikle, metni daha küçük parçalara avıracaksınız, böylece istediğiniz parçayı kullanabilirsiniz. Extractor Secin kısmında **Avırıcı ile Değer Çıkart** seceneğini seçin.

6. boşluk ve ardından bir tire girin.

7. Artık 24.55.75.102'yi ayrıstırılan 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 ayrıştıracağınız.

1. Kardeş Operatörü oluşturmak için artı işaretini 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://projetc-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 > **Ayırıcı ile Değerleri Çıkar**.

4. Ayırıcıya bir **boşluk** girin.

5. Çıktının her şeyi boşlukla ayırdığını, zaman damgasasının bir kısmını da içerdigini fark edin. Zaman damgasasını düzeltmek için bazı boşlukları korumanız gerekiyor.

(rv:63.0) Gecko/20100101 Firefox/63.0

Extract Values By Delimiter

Delimiter:

Show Empty Elements:

Preserve delimiters between

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

[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 ayırcıları koru seçeneğine tıklayın.

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

8. **Aralarındaki ayırcıları koru** seçeneğine tekrar tıklayın. Hem başlangıç hem de bitiş için çift tırnak “ kullanın. Zaman damgasasının şimdî temizlendiğini, diğer bazı çıktılarla birlikte göreceksiniz.

24.55.75.102

(16/Nov/2018:01:53:22 +0000) "GET /phpmyadmin/doc/html/\_static/underscore.js HTTP/1.1" 200 15147
["http://projetc-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"]

Extract Values By Delimiter

Delimiter:

Show Empty Elements:

Start:  End:

Start:  End:

Preserve delimiters between

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

[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 damgasasından köşeli parantezleri kaldırmanız gerekiyor, böylece teşhis koymak daha kolay olur. Zaman damgasını seçin. [16/Nov/2018:01:53:22 +0000] , operatörü seçin, **Değeri Kısıtl**.

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

11. Çıktınız zaman damgasası olmalıdır.

**Preserve delimiters between**

**Output:** [16/Nov/2018:01:53:22 +0000] "GET /phennyadmin/doc/html/\_static/underscore.js HTTP/1.1" 200  
 - [134] "HTTP://proyecto-oliver.online/phennyadmin/doc/html/index.html"  
 - "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:63.0) Gecko/20100101 Firefox/63.0"

**Trim Value**

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

**Index Range:** Start:  End:

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

**Choose an Operator**

**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 yakaladık.

**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 ayırtıracakız.

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

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

**Preserve delimiters between**

**Output:** [16/Nov/2018:01:53:22 +0000] "GET /phennyadmin/doc/html/\_static/underscore.js HTTP/1.1" 200  
 - [134] "HTTP://proyecto-oliver.online/phennyadmin/doc/html/index.html"  
 - "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:63.0) Gecko/20100101 Firefox/63.0"

**Trim Value**

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

**Index Range:** Start:  End:

**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

3. **200**'ü seçin.

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

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

The screenshot shows the Logstash configuration interface with three main panels:

- Output:** Displays log entries from a file named "phpmyadmin.log". One entry is highlighted with a red box, showing the full URL and status code.
- Input:** Shows the input configuration with the value "200" highlighted by a red box.
- Parsing Result:** Shows the parsed fields: ip\_address (24.55.75.102), timestamp (16/Nov/2018:01:53:22 +0000), and response (200). The "response" field is highlighted with a red box.

#### 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 **Ayrıştırma Şablonu** adımına geri götürür.
3. Satırı **geçerli** olarak işaretleyin ve Bu ayrıştırma şablonunu bu soruya uyan örnek satırlara uygulayın: giriş alanına sorgunuzu girin.

The screenshot shows the "Manage Parsing" interface in the "Test & Verify" step:

- Template Name:** My New Template 2
- Log Line:** A sample log line is shown, with the "response" field highlighted by a red box.
- Sample Lines:** A list of parsed fields: ip\_address (24.55.75.102), timestamp (16/Nov/2018:01:53:22 +0000), and response (200).
- Query:** An input field containing "200" is highlighted by a red box.
- Activate:** A button labeled "Activate" is highlighted with a red box.

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

The screenshot shows the "Manage Parsing" interface in the "Parsing Templates" list:

- Message:** "Please allow up to 15 minutes for changes to active templates to take effect"
- Create Template:** A blue button.
- Filters:** A dropdown menu and a search bar.
- Template Name:** A table showing the active template "My New Template 1" with the status "Active" highlighted by a red box.

Not: Aktif ayrıştırma şablonları, şablon etkinleştirildikten sonra gelen satırlara yalnızca uygulanır. Şablon aktif hale gelmeden önce alınan tüm günlük satırları, ayrıştırma şablonu tarafından ayrıştırılmaz. 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 Ayrıştırma Şablonu oluşturduğunuz.

Bu laboratuvar çalışmasında, mezmo platformuna erişim sağladınız ve keşfettiniz. Verilen örnek günlük satır üzerinde özel ayrıştırma gerçekleştirdiniz ve ip\_address, timestamp, response bilgilerini ayrıştırarak doğruladınız.

**Yazar(lar)**

Pallavi Rai

**Katkıda Bulunan(lar)**

Anamika Agarwal  
Shivam kumar