Mac address lookup API

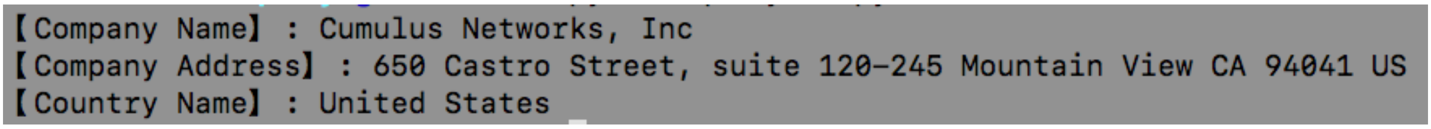
Usage

Command Line

The queryMac.py is used python3, so if you want to run it in your real environment. You need to install python3 and required libs.

```
git clone https://github.com/lvchongen/macquery.git

cd macquery

pip install -r ./requirement.txt

python queryMac.py mac-address  # like 44:38:39:ff:ef:57
```

After running the scripts and pass the mac-address, it would give up results as below:



```
【Company Name】 : Cumulus Networks, Inc
【Company Address】 : 650 Castro Street, suite 120-245 Mountain View CA 94041 US
【Country Name】 : United States
```

Virtual Python Environment

If you want to use virtual environment, please install the virtualenv firstly.

```
git clone https://github.com/lvchongen/macquery.git

virtualenv -p python3 ./venv3

source ./venv3/bin/activate

cd macquery

pip install -r ./requirement.txt

python queryMac.py mac-address  # like 44:38:39:ff:ef:57
```

Docker Container Execution

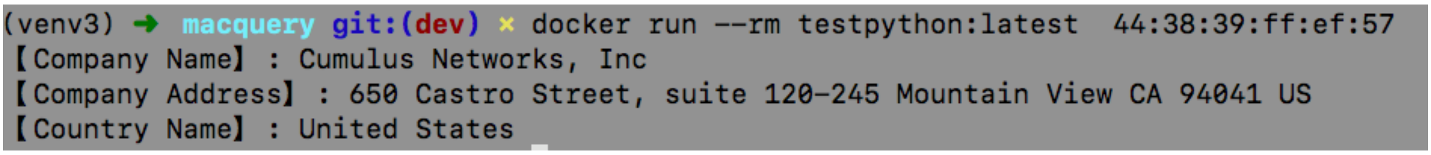
If you want to query mac-address by using docker. I package this script into the docker image. The dockerfile is below:

```
FROM python:3.7

MAINTAINER chlv lvchongen@gmail.com

ADD queryMac.py /

RUN pip install requests

RUN pip install beautifulsoup4

ENTRYPOINT [ "python", "/queryMac.py"]
```

You can build this image and start container to do mac-address query:

```
git clone https://github.com/lvchongen/macquery.git

cd macquery

docker build -t testpython .     # You c gan use different tag for docker image

docker run --rm testpython:latest mac-address  # like 44:38:39:ff:ef:57
```

After running the container it would give us results and delete the unused container.

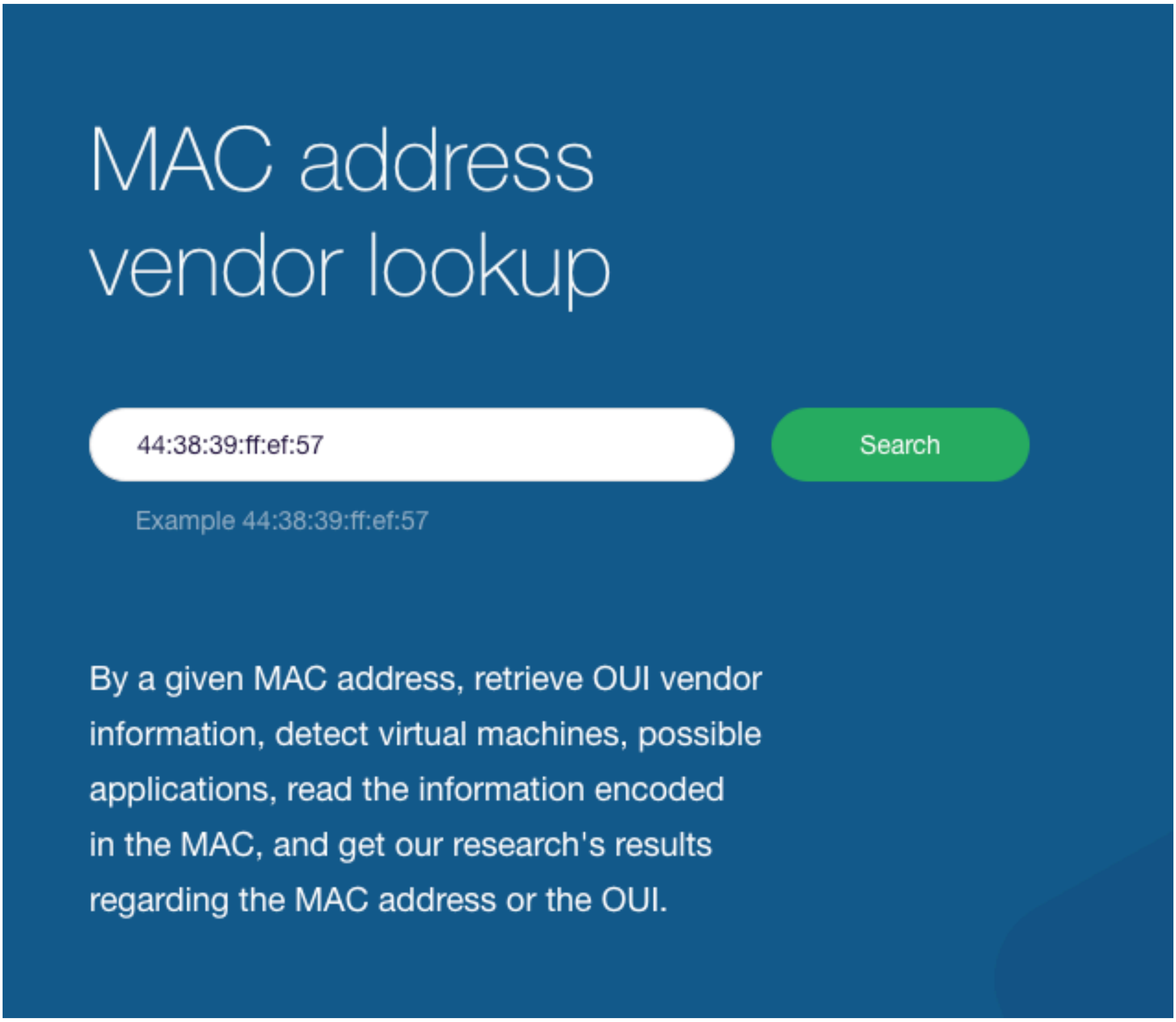


```
(venv3) ➜  macquery git:(dev) ✗ docker run --rm testpython:latest  44:38:39:ff:ef:57
【Company Name】 : Cumulus Networks, Inc
【Company Address】 : 650 Castro Street, suite 120-245 Mountain View CA 94041 US
【Country Name】 : United States
```

Background

People can access the website macaddress.io and search the vendor information by providing mac address.

- Open the URL in browser and input the MAC address in the serach field.



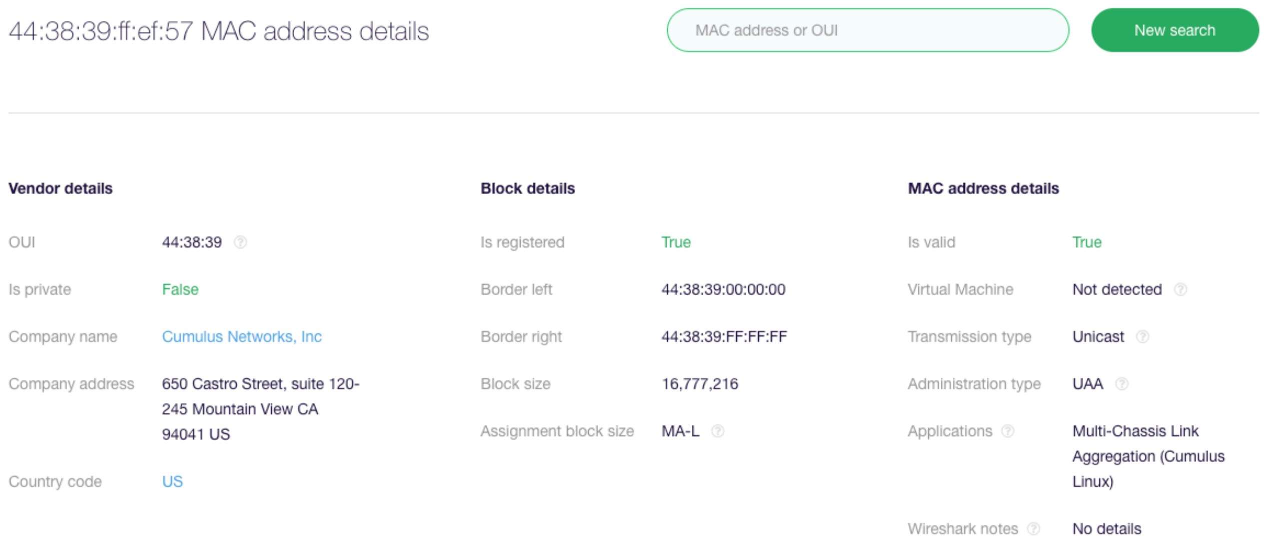
MAC address vendor lookup

44:38:39:ff:ef:57

Example 44:38:39:ff:ef:57

By a given MAC address, retrieve OUI vendor information, detect virtual machines, possible applications, read the information encoded in the MAC, and get our research's results regarding the MAC address or the OUI.

- After click the search button, the browser will give user all informaction about the mac address in redirected url.



44:38:39:ff:ef:57 MAC address details

Vendor details

OUI	44:38:39
Is private	False
Company name	Cumulus Networks, Inc
Company address	650 Castro Street, suite 120-245 Mountain View CA 94041 US
Country code	US

Block details

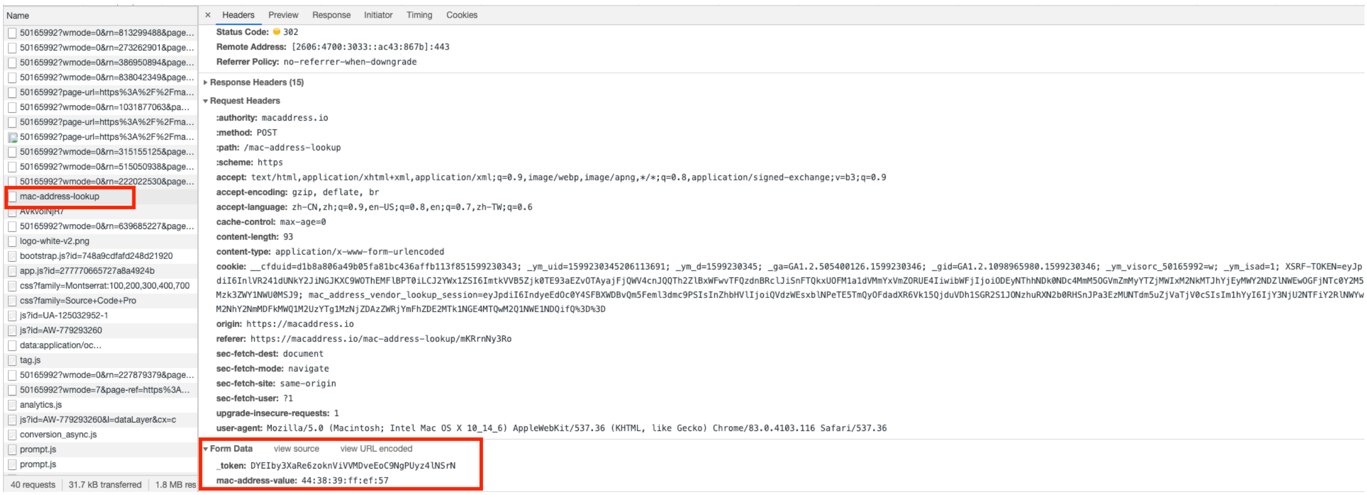
Is registered	True
Border left	44:38:39:00:00:00
Border right	44:38:39:FF:FF:FF
Block size	16,777,216
Assignment block size	MA-L

MAC address details

Is valid	True
Virtual Machine	Not detected
Transmission type	Unicast
Administration type	UAA
Applications	Multi-Chassis Link Aggregation (Cumulus Linux)
Wireshark notes	No details

Interface analysis

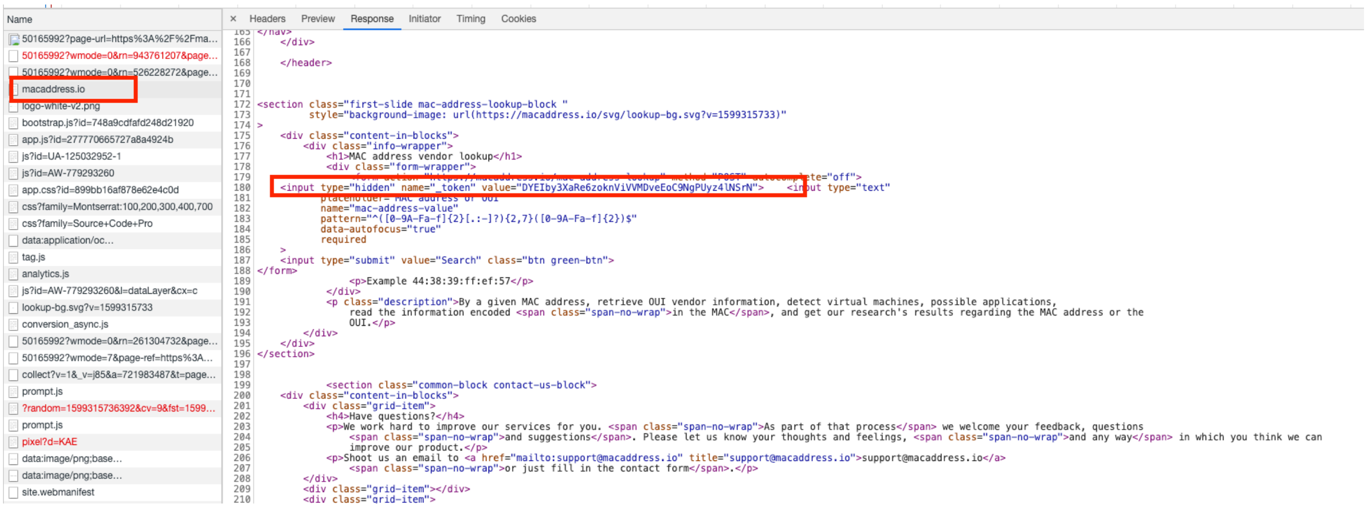
1. We can use develop tools to capture the http request and response in Chrome. After clicking the search button, the website will request this api as below.



```
50165992?wmode=0&rn=813299488&page...
50165992?wmode=0&rn=273262901&page...
50165992?wmode=0&rn=386950894&page...
50165992?wmode=0&rn=838042349&page...
50165992?page-url=https%3A%2F%2Fma...
50165992?wmode=0&rn=1031877063&pa...
50165992?page-url=https%3A%2F%2Fma...
50165992?page-url=https%3A%2F%2Fma...
50165992?wmode=0&rn=315155125&page...
50165992?wmode=0&rn=515050938&page...
50165992?wmode=0&rn=222022530&page...
mac-address-lookup
AVkvoINjR7
50165992?wmode=0&rn=639685227&page...
logo-white-v2.png
bootstrap.js?id=748a9cdfafd248d21920
app.js?id=277770665727a8a4924b
css?family=Montserrat:100,200,300,400,700
css?family=Source+Code+Pro
js?id=UA-125032952-1
js?id=AW-779293260
data:application/oc...
tag.js
50165992?wmode=0&rn=227879379&page...
50165992?wmode=7&page-ref=https%3A...
analytics.js
js?id=AW-779293260&l=dataLayer&cx=c
conversion_async.js
prompt.js
prompt.js
40 requests | 31.7 kB transferred | 1.8 MB res
```

```
Status Code: 302
Remote Address: [2606:4700:3033::ac43:867b]:443
Referrer Policy: no-referrer-when-downgrade
▸ Response Headers (15)
▾ Request Headers
:authority: macaddress.io
:method: POST
:path: /mac-address-lookup
:scheme: https
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-encoding: gzip, deflate, br
accept-language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
cache-control: max-age=0
content-length: 93
content-type: application/x-www-form-urlencoded
cookie: __cfduid=d1b8a806a49b05fa81bc436affb113f851599230343; _ym_uid=1599230345206113691; _ym_d=1599230345; _ga=GA1.2.505400126.1599230346; _gid=GA1.2.1098965980.1599230346; _ym_visorc_50165992=w; _ym_isad=1; XSRF-TOKEN=eyJp
diI6InlVR241dUNkY2JiNGJKXC9WOThEMFlBPT0iLCJ2YWx1ZSI6ImtkVVB5Zjk0TE93aEZvOTAyajFjQWV4cnJQQTh2ZlBxWFwvTFQzdnBRclJiSnFTQkxUOFM1a1dVMmYxVmZORUE4IiwibWFjIjoiODEyNThhNDk0NDc4MmM5OGVmZmMyYTZjMWIxM2NkMTJhYjEyMWY2NDZlNWEwOGFjNTc0Y2M5
Mzk3ZWY1NWU0MSJ9; mac_address_vendor_lookup_session=eyJpdiI6IndyeEdOc0Y4SFBXWDBvQm5Feml3dmc9PSIsInZhbHVlIjoiQVdzWEsxblNPeTE5TmQyOFdadXR6Vk15QjduVDh1SGR2S1JONzhuRXN2b0RHSnJPa3EzMUNTdm5uZjVaTjV0cSIsIm1hYyI6IjY3NjU2NTFiY2RlNWYw
M2NhY2NmMDFkMWQ1M2UzYTg1MzNjZDAzZWRjYmFhZDE2MTk1NGE4MTQwM2Q1NWE1NDQifQ%3D%3D
origin: https://macaddress.io
referer: https://macaddress.io/mac-address-lookup/mKRrnNy3Ro
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
▾ Form Data    view source    view URL encoded
_token: DYEIby3XaRe6zoknViVVMDveEoC9NgPUyz4lNSrN
mac-address-value: 44:38:39:ff:ef:57
```

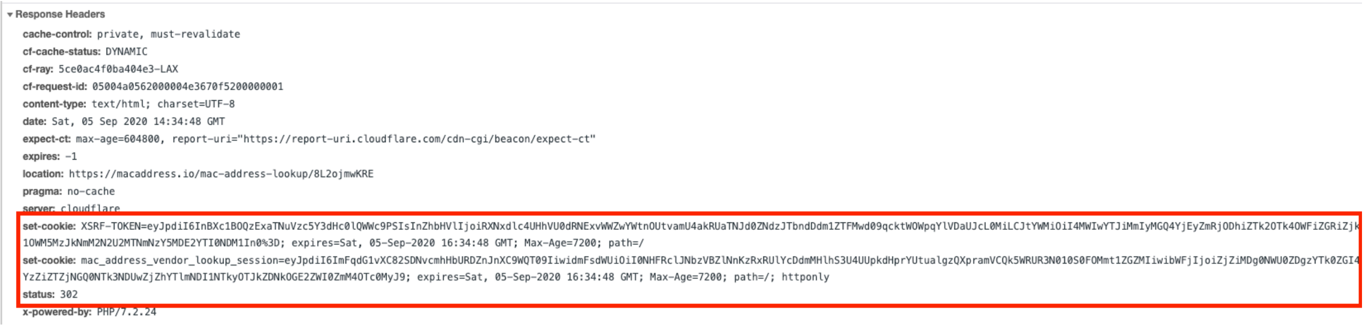
2. The post request need two major parameters: _**token** and **mac-address-value**. The **mac-address-value** is provided by user, and I need to know where is the _**token.** Actually, the token should be genearted by backend because token is the key to access backend. So I try to find it in source code of the html. And the token will be changed every time of accessing.



```
50165992?page-url=https%3A%2F%2Fma...
50165992?wmode=0&rn=943761207&page...
50165992?wmode=0&rn=526228272&page...
macaddress.io
logo-white-v2.png
bootstrap.js?id=748a9cdfafd248d21920
app.js?id=277770665727a8a4924b
js?id=UA-125032952-1
js?id=AW-779293260
app.css?id=899bb16af878e62e4c0d
css?family=Montserrat:100,200,300,400,700
css?family=Source+Code+Pro
data:application/oc...
tag.js
analytics.js
js?id=AW-779293260&l=dataLayer&cx=c
lookup-bg.svg?v=1599315733
conversion_async.js
50165992?wmode=0&rn=261304732&page...
50165992?wmode=7&page-ref=https%3A...
collect?v=1&_v=j85&a=721983487&t=page...
prompt.js
?random=1599315736392&cv=9&fst=1599...
prompt.js
pixel?d=KAE
data:image/png;base...
data:image/png;base...
site.webmanifest
```

```html
</nav>
    </div>

    </header>



<section class="first-slide mac-address-lookup-block "
        style="background-image: url(https://macaddress.io/svg/lookup-bg.svg?v=1599315733)"
>
    <div class="content-in-blocks">
        <div class="info-wrapper">
            <h1>MAC address vendor lookup</h1>
            <div class="form-wrapper">
                <form action="https://macaddress.io/mac-address-lookup" method="POST" autocomplete="off">
    <input type="hidden" name="_token" value="DYEIby3XaRe6zoknViVVMDveEoC9NgPUyz4lNSrN">    <input type="text"
            placeholder="MAC address or OUI"
            name="mac-address-value"
            pattern="^([0-9A-Fa-f]{2}[.:-]?){2,7}([0-9A-Fa-f]{2})$"
            data-autofocus="true"
            required
    >
    <input type="submit" value="Search" class="btn green-btn">
</form>
                <p>Example 44:38:39:ff:ef:57</p>
            </div>
            <p class="description">By a given MAC address, retrieve OUI vendor information, detect virtual machines, possible applications,
                read the information encoded <span class="span-no-wrap">in the MAC</span>, and get our research's results regarding the MAC address or the
                OUI.</p>
        </div>
    </div>
</section>


            <section class="common-block contact-us-block">
    <div class="content-in-blocks">
        <div class="grid-item">
            <h4>Have questions?</h4>
            <p>We work hard to improve our services for you. <span class="span-no-wrap">As part of that process</span> we welcome your feedback, questions
                <span class="span-no-wrap">and suggestions</span>. Please let us know your thoughts and feelings, <span class="span-no-wrap">and any way</span> in which you think we can
                improve our product.</p>
            <p>Shoot us an email to <a href="mailto:support@macaddress.io" title="support@macaddress.io">support@macaddress.io</a>
                <span class="span-no-wrap">or just fill in the contact form</span>.</p>
        </div>
        <div class="grid-item"></div>
        <div class="grid-item">
```

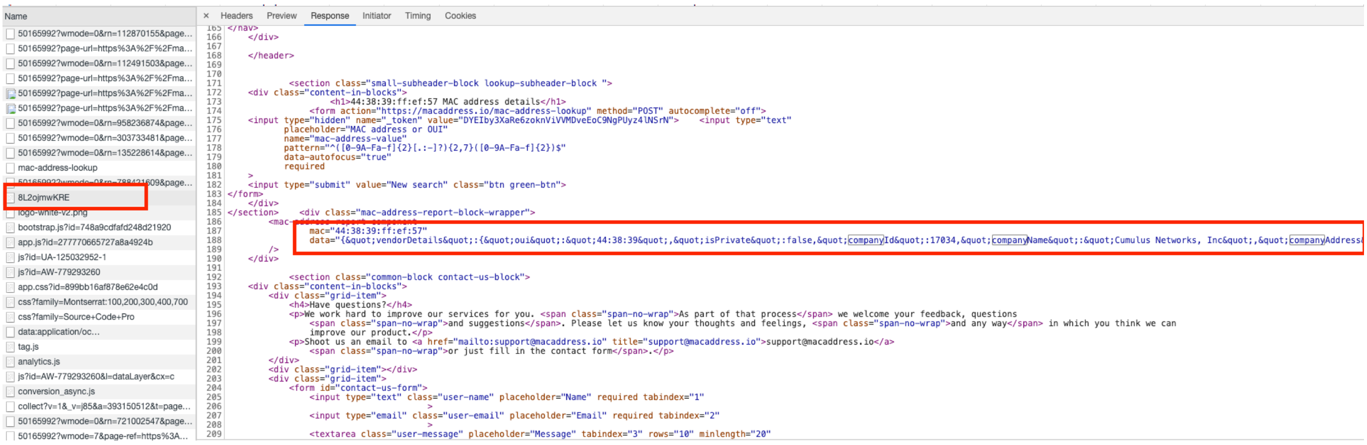
3. From a safety perspective, the backend should know whether the request has permission. In this website the cookie is the major key. We can get the cookie infomation from first response header as below.



▾ Response Headers

```
cache-control: private, must-revalidate
cf-cache-status: DYNAMIC
cf-ray: 5ce0ac4f0ba404e3-LAX
cf-request-id: 05004a0562000004e3670f5200000001
content-type: text/html; charset=UTF-8
date: Sat, 05 Sep 2020 14:34:48 GMT
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
expires: -1
location: https://macaddress.io/mac-address-lookup/8L2ojmwKRE
pragma: no-cache
server: cloudflare
set-cookie: XSRF-TOKEN=eyJpdiI6InBXc1BOQzExaTNuVzc5Y3dHc0lQWWc9PSIsInZhbHVlIjoiRXNxdlc4UHhVU0dRNExvWWZwYWtnOUtvamU4akRUaTNJd0ZNdzJTbndDdm1ZTFMwd09qcktWOWpqYlVDaUJcL0MiLCJtYWMiOiI4MWIwYTJiMmIyMGQ4YjEyZmRjODhiZTk2OTk4OWFiZGRiZjk
1OWM5MzJkNmM2N2U2MTNmNzY5MDE2YTI0NDM1In0%3D; expires=Sat, 05-Sep-2020 16:34:48 GMT; Max-Age=7200; path=/
set-cookie: mac_address_vendor_lookup_session=eyJpdiI6ImFqdG1vXC82SDNvcmhHbURDZnJnXC9WQT09IiwidmFsdWUiOiI0NHFRclJNbzVBZlNnKzRxRUlYcDdmMHlhS3U4UUpkdHprYUtualgzQXpramVCQk5WRUR3N010S0FOMmt1ZGZMIiwibWFjIjoiZjZiMDg0NWU0ZDgzYTk0ZGI4
YzZiZTZjNGQ0NTk3NDUwZjZhYTlmNDI1NTkyOTJkZDNkOGE2ZWI0ZmM4OTc0MyJ9; expires=Sat, 05-Sep-2020 16:34:48 GMT; Max-Age=7200; path=/; httponly
status: 302
x-powered-by: PHP/7.2.24
```

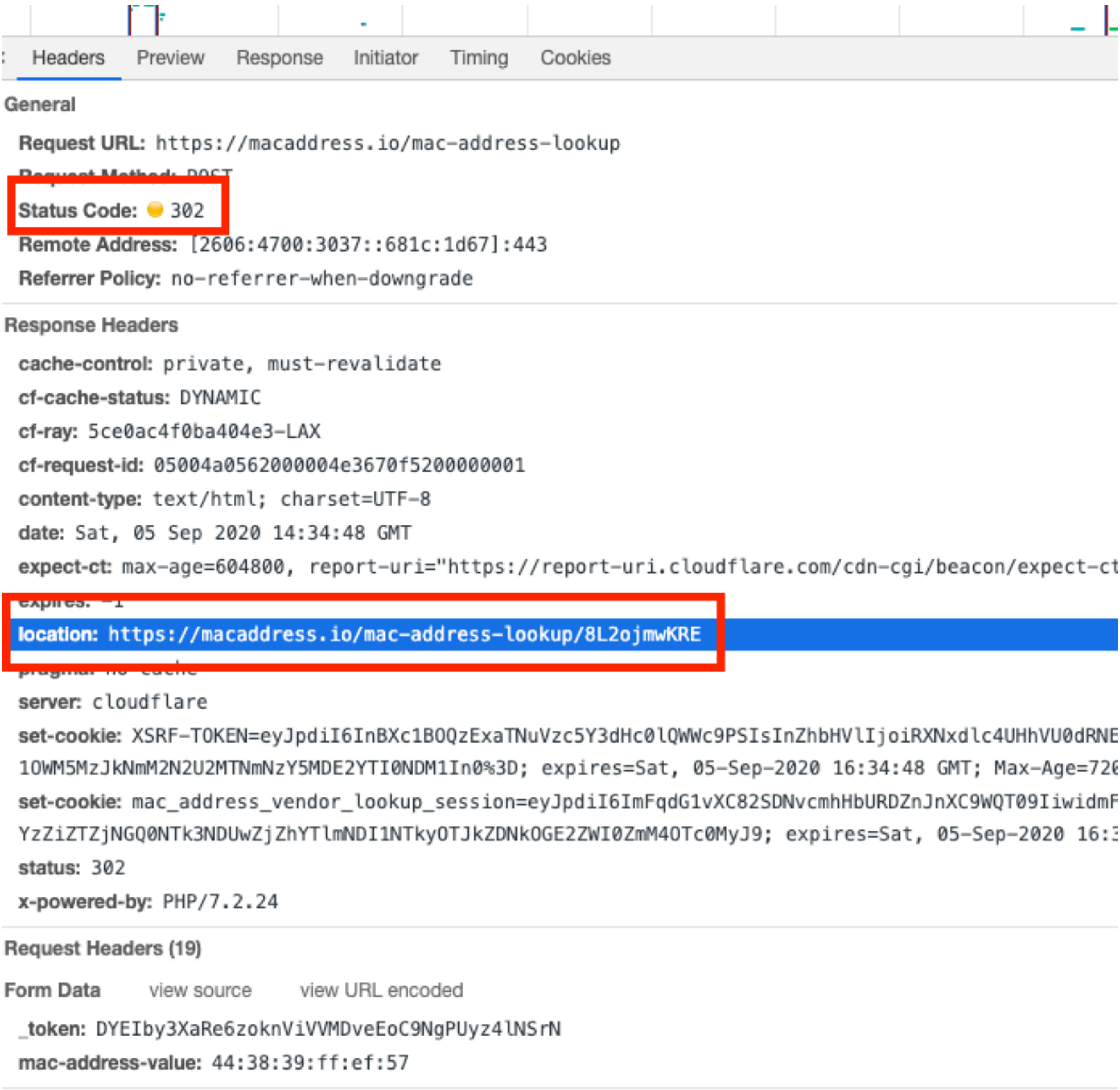
4. After accessing the API **mac-address-lookup**, browser will navigate to redirected url that contains the search results. The status code of http is used to describe the redirect。



```
50165992?wmode=0&rn=112870155&page...
50165992?page-url=https%3A%2F%2Fma...
50165992?wmode=0&rn=112491503&page...
50165992?page-url=https%3A%2F%2Fma...
50165992?page-url=https%3A%2F%2Fma...
50165992?page-url=https%3A%2F%2Fma...
50165992?wmode=0&rn=958236874&page...
50165992?wmode=0&rn=303733481&page...
50165992?wmode=0&rn=135228614&page...
mac-address-lookup
50165992?wmode=0&rn=788421609&page...
8L2ojmwKRE
logo-white-v2.png
bootstrap.js?id=748a9cdfafd248d21920
app.js?id=277770665727a8a4924b
js?id=UA-125032952-1
js?id=AW-779293260
app.css?id=899bb16af878e62e4c0d
css?family=Montserrat:100,200,300,400,700
css?family=Source+Code+Pro
data:application/oc...
tag.js
analytics.js
js?id=AW-779293260&l=dataLayer&cx=c
conversion_async.js
collect?v=1&_v=j85&a=393150512&t=page...
50165992?wmode=0&rn=721002547&page...
50165992?wmode=7&page-ref=https%3A...
```

```html
</nav>
    </div>

    </header>


            <section class="small-subheader-block lookup-subheader-block ">
    <div class="content-in-blocks">
                    <h1>44:38:39:ff:ef:57 MAC address details</h1>
                <form action="https://macaddress.io/mac-address-lookup" method="POST" autocomplete="off">
    <input type="hidden" name="_token" value="DYEIby3XaRe6zoknViVVMDveEoC9NgPUyz4lNSrN">    <input type="text"
            placeholder="MAC address or OUI"
            name="mac-address-value"
            pattern="^([0-9A-Fa-f]{2}[.:-]?){2,7}([0-9A-Fa-f]{2})$"
            data-autofocus="true"
            required
    >
    <input type="submit" value="New search" class="btn green-btn">
</form>
    </div>
</section>    <div class="mac-address-report-block-wrapper">
        <mac-address-report-component
            mac="44:38:39:ff:ef:57"
            data="{&quot;vendorDetails&quot;:{&quot;oui&quot;:&quot;44:38:39&quot;,&quot;isPrivate&quot;:false,&quot;companyId&quot;:17034,&quot;companyName&quot;:&quot;Cumulus Networks, Inc&quot;,&quot;companyAddress
        />
    </div>

            <section class="common-block contact-us-block">
    <div class="content-in-blocks">
        <div class="grid-item">
            <h4>Have questions?</h4>
            <p>We work hard to improve our services for you. <span class="span-no-wrap">As part of that process</span> we welcome your feedback, questions
                <span class="span-no-wrap">and suggestions</span>. Please let us know your thoughts and feelings, <span class="span-no-wrap">and any way</span> in which you think we can
                improve our product.</p>
            <p>Shoot us an email to <a href="mailto:support@macaddress.io" title="support@macaddress.io">support@macaddress.io</a>
                <span class="span-no-wrap">or just fill in the contact form</span>.</p>
        </div>
        <div class="grid-item"></div>
        <div class="grid-item">
            <form id="contact-us-form">
                <input type="text" class="user-name" placeholder="Name" required tabindex="1"
                       >
                <input type="email" class="user-email" placeholder="Email" required tabindex="2"
                       >
                <textarea class="user-message" placeholder="Message" tabindex="3" rows="10" minlength="20"
```

And, the redirect url can be found in lookup api's response header。



General

Request URL: https://macaddress.io/mac-address-lookup
Request Method: POST
Status Code: 302
Remote Address: [2606:4700:3037::681c:1d67]:443
Referrer Policy: no-referrer-when-downgrade

Response Headers

cache-control: private, must-revalidate
cf-cache-status: DYNAMIC
cf-ray: 5ce0ac4f0ba404e3-LAX
cf-request-id: 05004a0562000004e3670f5200000001
content-type: text/html; charset=UTF-8
date: Sat, 05 Sep 2020 14:34:48 GMT
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct
expires: -1
location: https://macaddress.io/mac-address-lookup/8L2ojmwKRE
pragma: no-cache
server: cloudflare
set-cookie: XSRF-TOKEN=eyJpdiI6InBXc1BOQzExaTNuVzc5Y3dHc0lQWWc9PSIsInZhbHVlIjoiRXNxdlc4UHhVU0dRNE
1OWM5MzJkNmM2N2U2MTNmNzY5MDE2YTI0NDM1In0%3D; expires=Sat, 05-Sep-2020 16:34:48 GMT; Max-Age=720
set-cookie: mac_address_vendor_lookup_session=eyJpdiI6ImFqdG1vXC82SDNvcmhHbURDZnJnXC9WQT09IiwidmF
YzZiZTZjNGQ0NTk3NDUwZjZhYTlmNDI1NTkyOTJkZDNkOGE2ZWI0ZmM4OTc0MyJ9; expires=Sat, 05-Sep-2020 16:3
status: 302
x-powered-by: PHP/7.2.24

Request Headers (19)

Form Data view source view URL encoded

_token: DYEIby3XaRe6zoknViVVMDveEoC9NgPUyz4lNSrN
mac-address-value: 44:38:39:ff:ef:57

Based on above desciptions, we know the stpes to query mac information.

1. Access the website macaddress.io to get token.
2. Use mac-address and website to request api **mac-address-lookup** and get redirect url from response header.
3. Access the redirect url and get mac information.

Linux Toolbox

Linux has many commands that can be called in the termincal directly, because system stores the commands under the path `/usr/bin,/usr/local/bin,/usr/sbin` . So if we want to add python scripts to "toolbox" can be called anywhere in terminal. We need to copy/link the script to one of above folders.

Method 1: link file to /usr/local/bin

1. Add the execute path to scrpts

```
#!/usr/bin/env python
```

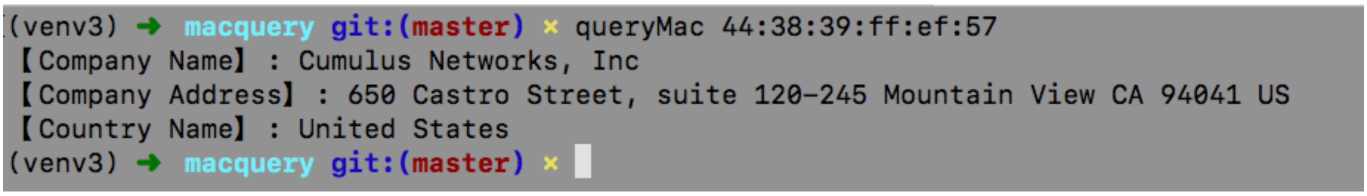
2. Change the permission of python script file.

```
cp queryMac.py queryTool.py

chmod +x quertTool.py
```

1. Link the script to path `/usr/local/bin` :

```
sudo ln -s $PWD/queryTool.py /usr/local/bin/queryMac
```

2. Test this command like



```
[(venv3) ➜  macquery git:(master) ✗ queryMac 44:38:39:ff:ef:57
 【Company Name】 : Cumulus Networks, Inc
 【Company Address】 : 650 Castro Street, suite 120-245 Mountain View CA 94041 US
 【Country Name】 : United States
(venv3) ➜  macquery git:(master) ✗ 
```

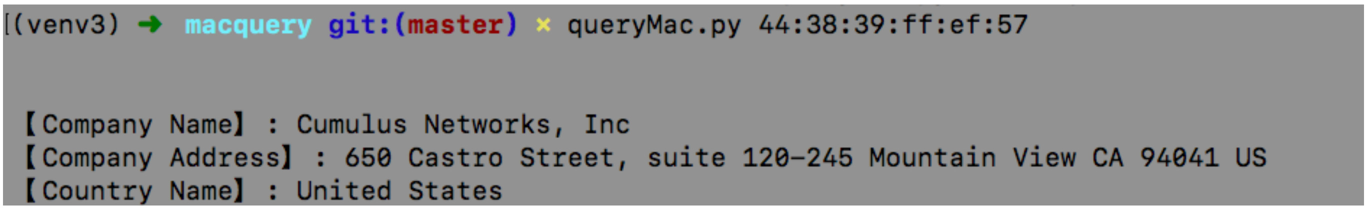
Method 2: using *python setup.py install*

1. Create setup.py file contains below content:

```
from setuptools import setup

setup(
    scripts = [
        'scripts/queryMac.py'  #This is the path of the scripts
    ]
)
```

2. Execute command `python setup.py install`

3. Test this command like:



```
[(venv3) ➜  macquery git:(master) ✗ queryMac.py 44:38:39:ff:ef:57


 【Company Name】 : Cumulus Networks, Inc
 【Company Address】 : 650 Castro Street, suite 120-245 Mountain View CA 94041 US
 【Country Name】 : United States
```