PENTESTING RECONNAISSANCE TOOLS

Table of Contents

WIRESHARK 1

WHOIS 4

HOSTING 6

IP2LOCATION 6

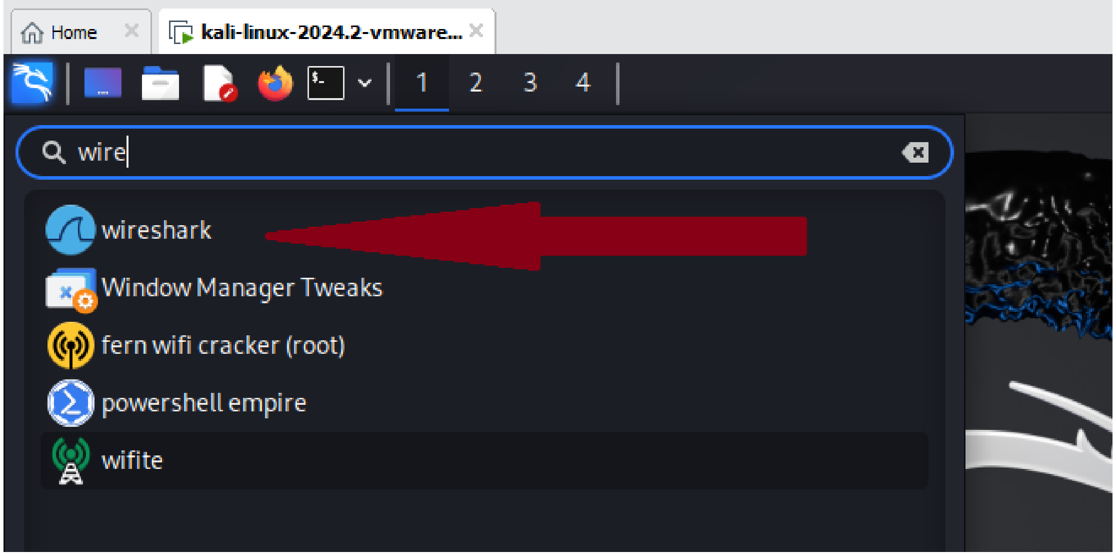
GOOGLE MAPS 8

WAYBACK MACHINE 10

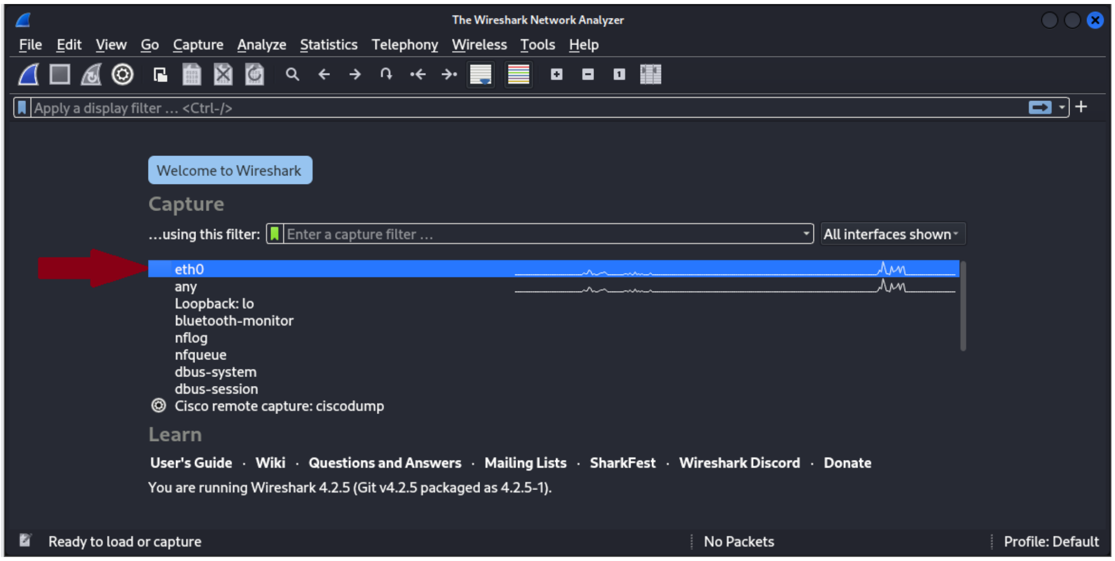
GOOGLE DORKING 13

WIRESHARK

Wireshark is an inbuilt software readily available in Kali Linux Operating Systems (it does not need to be downloaded). Wireshark is an open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security. Saved Captures from the Wireshark application use the file extension .pcapng



While using VMware, in order to record/scan activity from your computer, change the Network Adapter setting to **NAT** (Network Address Translation), but if you're monitoring activity from outside your computer but on the network you are on, Use the Network Adapter setting **Bridged**.

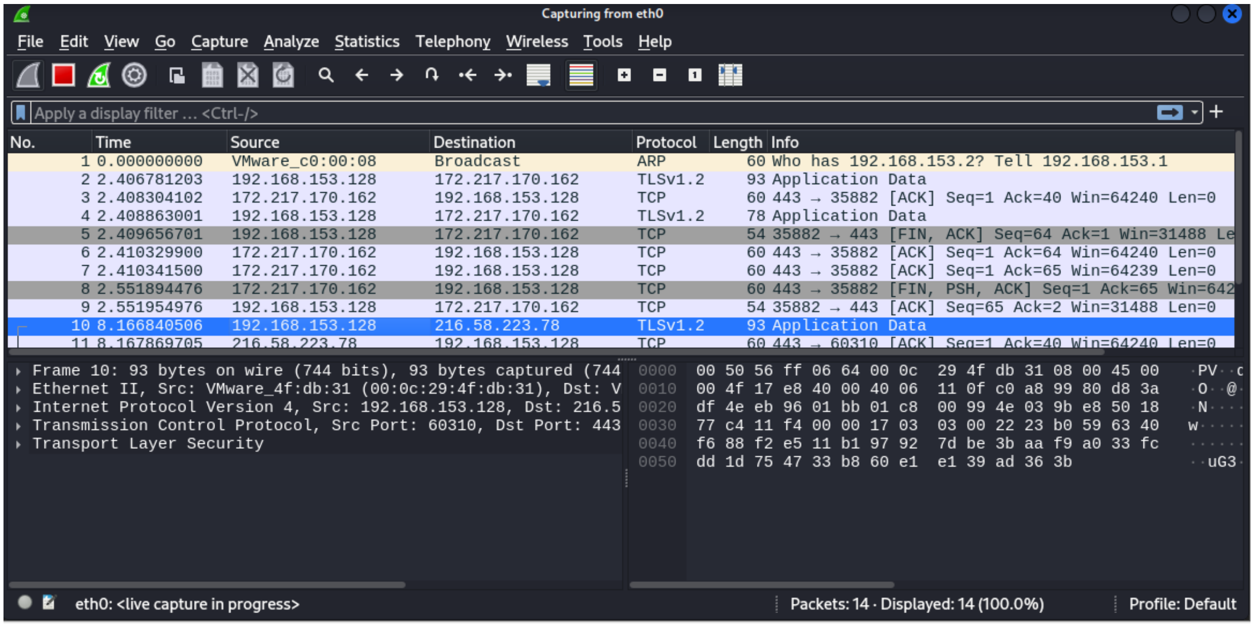

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump

You are running Wireshark 4.2.5 (Git v4.2.5 packaged as 4.2.5-1).

Ready to load or capture | No Packets | Profile: Default

Upon opening Wireshark you will quickly notice "Eth0" is your host machine's network card. When trying to hack into a Wi-Fi network you will need an external network adapter. (Alfa Card Network Adapter.)



```
No.  Time           Source              Destination         Protocol  Length Info
   1 0.000000000    VMware_c0:00:08     Broadcast           ARP           60 Who has 192.168.153.2? Tell 192.168.153.1
   2 2.406781203    192.168.153.128     172.217.170.162     TLSv1.2       93 Application Data
   3 2.408304102    172.217.170.162     192.168.153.128     TCP           60 443 → 35882 [ACK] Seq=1 Ack=40 Win=64240 Len=0
   4 2.408863001    192.168.153.128     172.217.170.162     TLSv1.2       78 Application Data
   5 2.409656701    192.168.153.128     172.217.170.162     TCP           54 35882 → 443 [FIN, ACK] Seq=64 Ack=1 Win=31488 Le
   6 2.410329900    172.217.170.162     192.168.153.128     TCP           60 443 → 35882 [ACK] Seq=1 Ack=64 Win=64240 Len=0
   7 2.410341500    172.217.170.162     192.168.153.128     TCP           60 443 → 35882 [ACK] Seq=1 Ack=65 Win=64239 Len=0
   8 2.551894476    172.217.170.162     192.168.153.128     TCP           60 443 → 35882 [FIN, PSH, ACK] Seq=1 Ack=65 Win=642
   9 2.551954976    192.168.153.128     172.217.170.162     TCP           54 35882 → 443 [ACK] Seq=65 Ack=2 Win=31488 Len=0
  10 8.166840506    192.168.153.128     216.58.223.78       TLSv1.2       93 Application Data
  11 8.167869705    216.58.223.78       192.168.153.128     TCP           60 443 → 60310 [ACK] Seq=1 Ack=40 Win=64240 Len=0
```

```
› Frame 10: 93 bytes on wire (744 bits), 93 bytes captured (744    0000  00 50 56 ff 06 64 00 0c  29 4f db 31 08 00 45 00   ·PV··c
› Ethernet II, Src: VMware_4f:db:31 (00:0c:29:4f:db:31), Dst: V    0010  00 4f 17 e8 40 00 40 06  11 0f c0 a8 99 80 d8 3a   ·O··@·
› Internet Protocol Version 4, Src: 192.168.153.128, Dst: 216.5    0020  df 4e eb 96 01 bb 01 c8  00 99 4e 03 9b e8 50 18   ·N····
› Transmission Control Protocol, Src Port: 60310, Dst Port: 443    0030  77 c4 11 f4 00 00 17 03  03 00 22 23 b0 59 63 40   w·····
› Transport Layer Security                                         0040  f6 88 f2 e5 11 b1 97 92  7d be 3b aa f9 a0 33 fc   ······
                                                                   0050  dd 1d 75 47 33 b8 60 e1  e1 39 ad 36 3b            ··uG3·
```

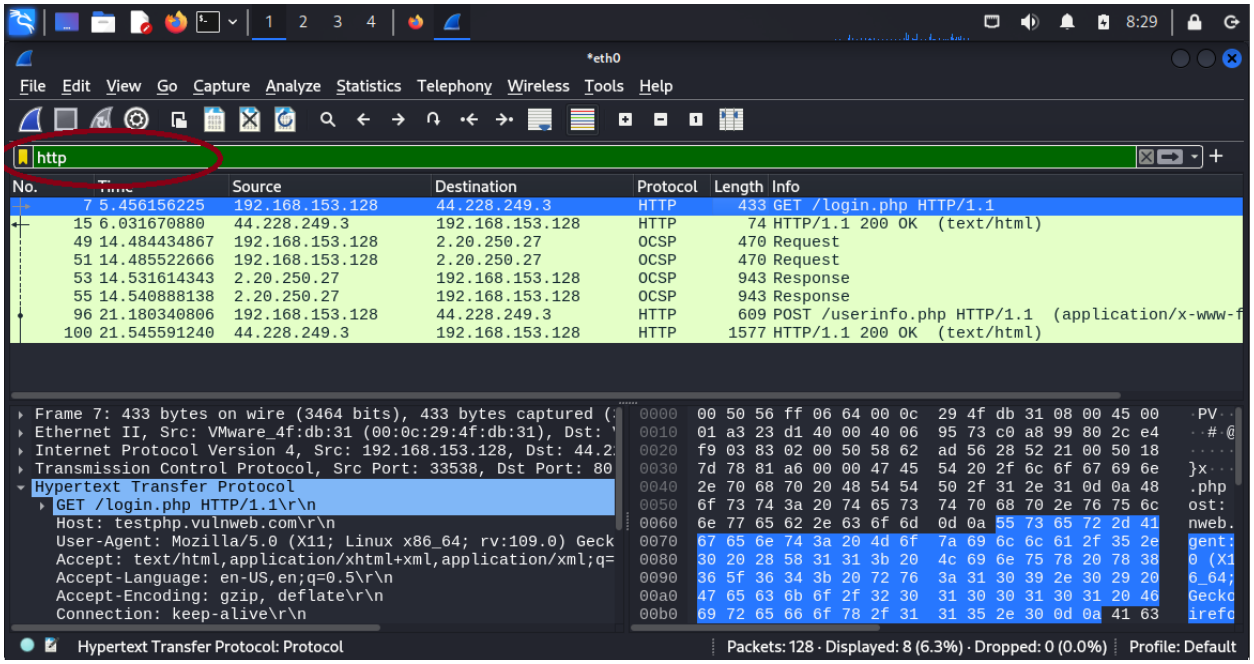
eth0: <live capture in progress>   Packets: 14 · Displayed: 14 (100.0%)   Profile: Default

When you click into the "Eth0" adapter, you will be able to monitor the packets being transferred through the network you are currently connected to. For example you can try opening this webpage on your browser testphp.vulnweb.com/login.php

This webpage is used by learners to use vulnerability scanners and other tools. So for example you want to capture the information you key in specifically into this website, perform the following:

1. Open the website on your browser.
2. Go to Wireshark and make sure that it is not recording any data or reset and clear any old data, (this step reduces traffic information flowing through. Makes it easy to monitor the exact data we're looking for rather than sifting through a lot of figures).
3. Go to back to the browser and type in the Username and Password for the page. Click login and observe what happened on Wireshark. Be sure to stop the recording.
4. Filter out the target protocols and observe for further information.
    a. The packets captured are still plenty which is why it is important to know who or what it is that you're targeting beforehand. Important info may include: The

Protocol for example a website using **HTTP/HTTPS** (Simply type it into the filter), the IP Address of the target machine (ip.addr==192.168.0.100).



```
http
```

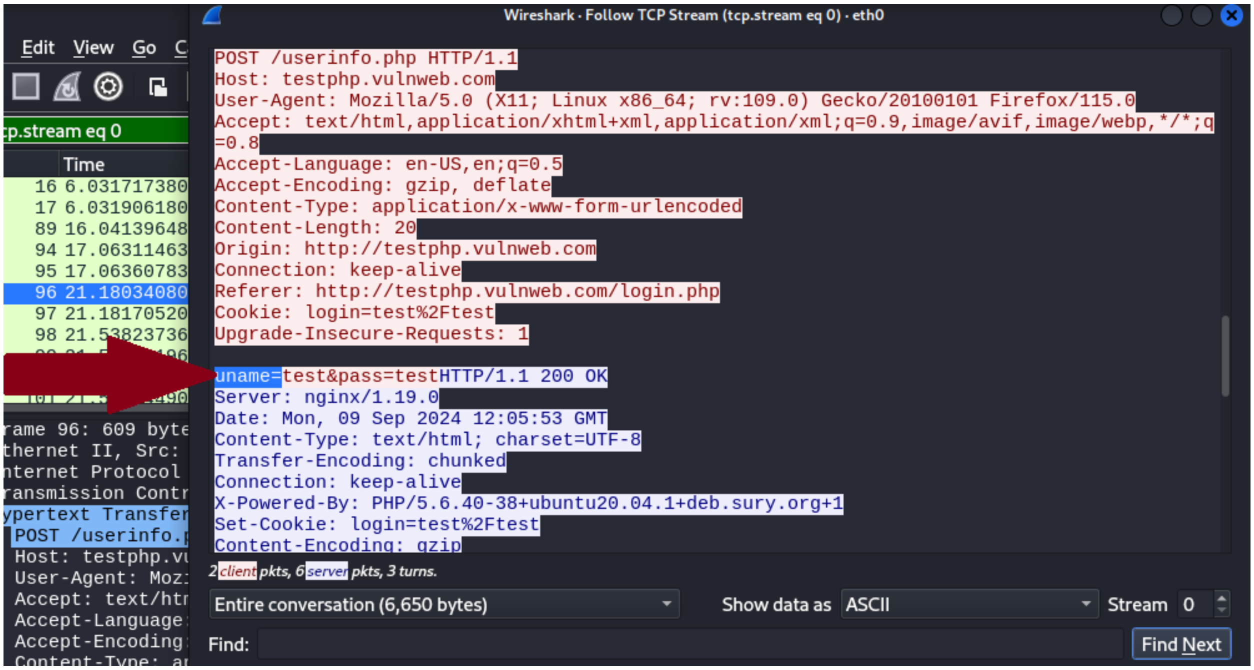
```
No.    Time          Source            Destination       Protocol  Length Info
     7 5.456156225   192.168.153.128   44.228.249.3      HTTP        433 GET /login.php HTTP/1.1
    15 6.031670880   44.228.249.3      192.168.153.128   HTTP         74 HTTP/1.1 200 OK  (text/html)
    49 14.484434867  192.168.153.128   2.20.250.27       OCSP        470 Request
    51 14.485522666  192.168.153.128   2.20.250.27       OCSP        470 Request
    53 14.531614343  2.20.250.27       192.168.153.128   OCSP        943 Response
    55 14.540888138  2.20.250.27       192.168.153.128   OCSP        943 Response
    96 21.180340806  192.168.153.128   44.228.249.3      HTTP        609 POST /userinfo.php HTTP/1.1  (application/x-www-f
   100 21.545591240  44.228.249.3      192.168.153.128   HTTP       1577 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 7: 433 bytes on wire (3464 bits), 433 bytes captured (:
› Ethernet II, Src: VMware_4f:db:31 (00:0c:29:4f:db:31), Dst: '
› Internet Protocol Version 4, Src: 192.168.153.128, Dst: 44.2:
› Transmission Control Protocol, Src Port: 33538, Dst Port: 80
⌄ Hypertext Transfer Protocol
  › GET /login.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Geck
    Accept: text/html,application/xhtml+xml,application/xml;q=
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
```

```
0000  00 50 56 ff 06 64 00 0c  29 4f db 31 08 00 45 00   ·PV··
0010  01 a3 23 d1 40 00 40 06  95 73 c0 a8 99 80 2c e4   ··#·@
0020  f9 03 83 02 00 50 58 62  ad 56 28 52 21 00 50 18   ·····
0030  7d 78 81 a6 00 00 47 45  54 20 2f 6c 6f 67 69 6e   }x···
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php
0050  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost:
0060  6e 77 65 62 2e 63 6f 6d  0d 0a 55 73 65 72 2d 41   nweb.
0070  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent:
0080  30 20 28 58 31 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X1
0090  36 5f 36 34 3b 20 72 76  3a 31 30 39 2e 30 29 20   6_64;
00a0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko
00b0  69 72 65 66 6f 78 2f 31  31 35 2e 30 0d 0a 41 63   irefo
```

```
Hypertext Transfer Protocol: Protocol        Packets: 128 · Displayed: 8 (6.3%) · Dropped: 0 (0.0%)   Profile: Default
```

5. For this example, we know that the website we're monitoring is HTTP, we know that there is a login page and we know that some information was sent through the network to enable the user to login. Now for us to know what exactly what transferred through that network, we need to right click on the exact packet => click on follow => then click on TCP Stream.
    a. **TAKE NOTE:** The information in red is the devices' sent data packet, while the blue section is the response from the server.
    b. From the image below, the highlighted section will reveal the Username and Password that was input. These are the parameters of the data packet sent from the computer to the server.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0
Edit View Go C
p.stream eq 0
Time
2 client pkts, 6 server pkts, 3 turns.
Entire conversation (6,650 bytes)
Show data as ASCII
Stream 0
Find:
Find Next

```
16 6.031717380
17 6.031906180
89 16.04139648
94 17.06311463
95 17.06360783
96 21.18034080
97 21.18170520
98 21.53823736
```

```
rame 96: 609 byte
thernet II, Src:
nternet Protocol
ransmission Contr
ypertext Transfer
 POST /userinfo.p
 Host: testphp.vu
 User-Agent: Moz:
 Accept: text/htr
 Accept-Language:
 Accept-Encoding:
 Content-Type: ar
```

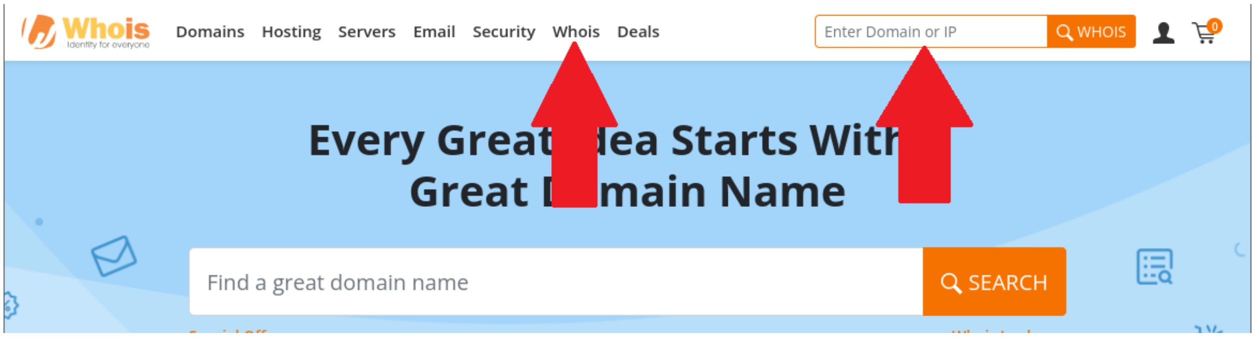
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 09 Sep 2024 12:05:53 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
```

WHOIS

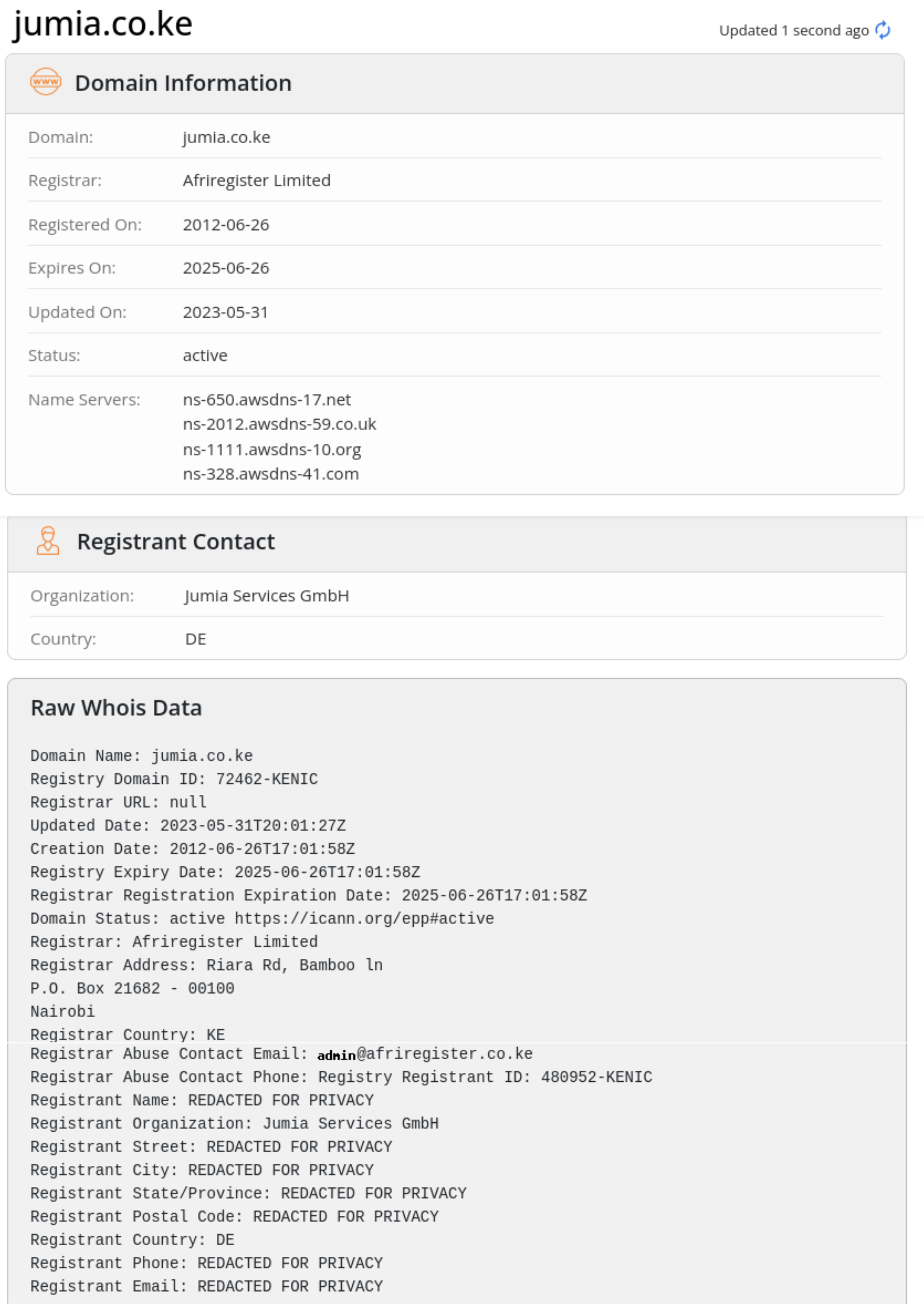
This is a website (whois.com) used to register domains and keeps track of your registered data when claiming a domain. It allows anyone to do a domain lookup (investigating for more information about a specific website). You're able to find out, **who owns** a website, whether it's a company or an individual details provided may include: Name, Email and Phone Number, Country, P.O Box, and Street Info (unless redacted for privacy purposes). You can also find out when the domain was **registered**, when the domain license **expires** and when it was **last updated.**

A similar website is arin.net



Use the Whois Search

From this point onwards, we will perform a full reconnaissance of Jumia through their website jumia.co.ke. See results below:



jumia.co.ke

Updated 1 second ago

Domain Information

Domain:	jumia.co.ke
Registrar:	Afriregister Limited
Registered On:	2012-06-26
Expires On:	2025-06-26
Updated On:	2023-05-31
Status:	active
Name Servers:	ns-650.awsdns-17.net ns-2012.awsdns-59.co.uk ns-1111.awsdns-10.org ns-328.awsdns-41.com

Registrant Contact

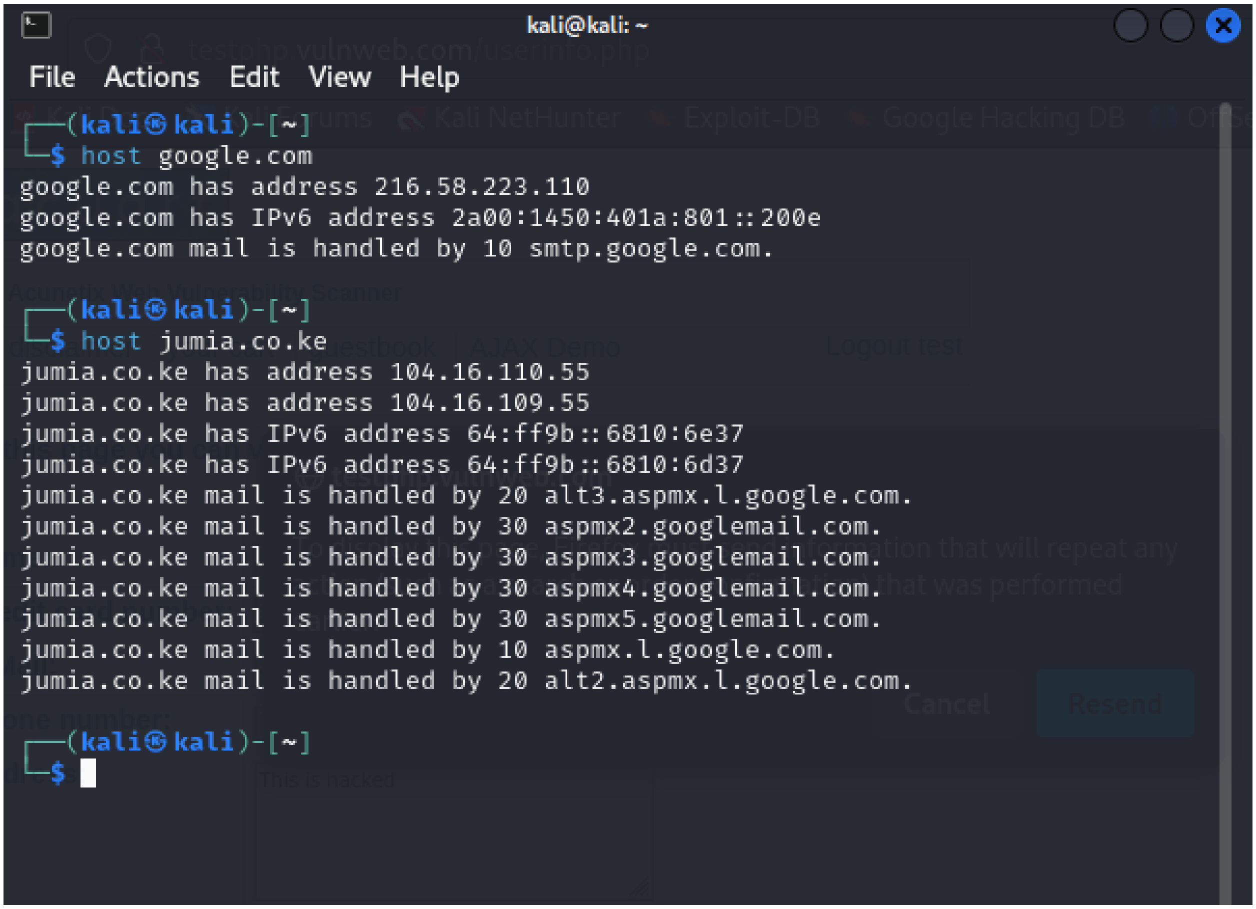
Organization:	Jumia Services GmbH
Country:	DE

Raw Whois Data

```
Domain Name: jumia.co.ke
Registry Domain ID: 72462-KENIC
Registrar URL: null
Updated Date: 2023-05-31T20:01:27Z
Creation Date: 2012-06-26T17:01:58Z
Registry Expiry Date: 2025-06-26T17:01:58Z
Registrar Registration Expiration Date: 2025-06-26T17:01:58Z
Domain Status: active https://icann.org/epp#active
Registrar: Afriregister Limited
Registrar Address: Riara Rd, Bamboo ln
P.O. Box 21682 - 00100
Nairobi
Registrar Country: KE
Registrar Abuse Contact Email: admin@afriregister.co.ke
Registrar Abuse Contact Phone: Registry Registrant ID: 480952-KENIC
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Jumia Services GmbH
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: REDACTED FOR PRIVACY
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: DE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Email: REDACTED FOR PRIVACY
```

HOSTING

To find out the IP Address of a website open the Linux Terminal => use the host key word e.g. host jumia.co.ke



```
┌──(kali㉿kali)-[~]
└─$ host google.com
google.com has address 216.58.223.110
google.com has IPv6 address 2a00:1450:401a:801::200e
google.com mail is handled by 10 smtp.google.com.

┌──(kali㉿kali)-[~]
└─$ host jumia.co.ke
jumia.co.ke has address 104.16.110.55
jumia.co.ke has address 104.16.109.55
jumia.co.ke has IPv6 address 64:ff9b::6810:6e37
jumia.co.ke has IPv6 address 64:ff9b::6810:6d37
jumia.co.ke mail is handled by 20 alt3.aspmx.l.google.com.
jumia.co.ke mail is handled by 30 aspmx2.googlemail.com.
jumia.co.ke mail is handled by 30 aspmx3.googlemail.com.
jumia.co.ke mail is handled by 30 aspmx4.googlemail.com.
jumia.co.ke mail is handled by 30 aspmx5.googlemail.com.
jumia.co.ke mail is handled by 10 aspmx.l.google.com.
jumia.co.ke mail is handled by 20 alt2.aspmx.l.google.com.

┌──(kali㉿kali)-[~]
└─$ 
```

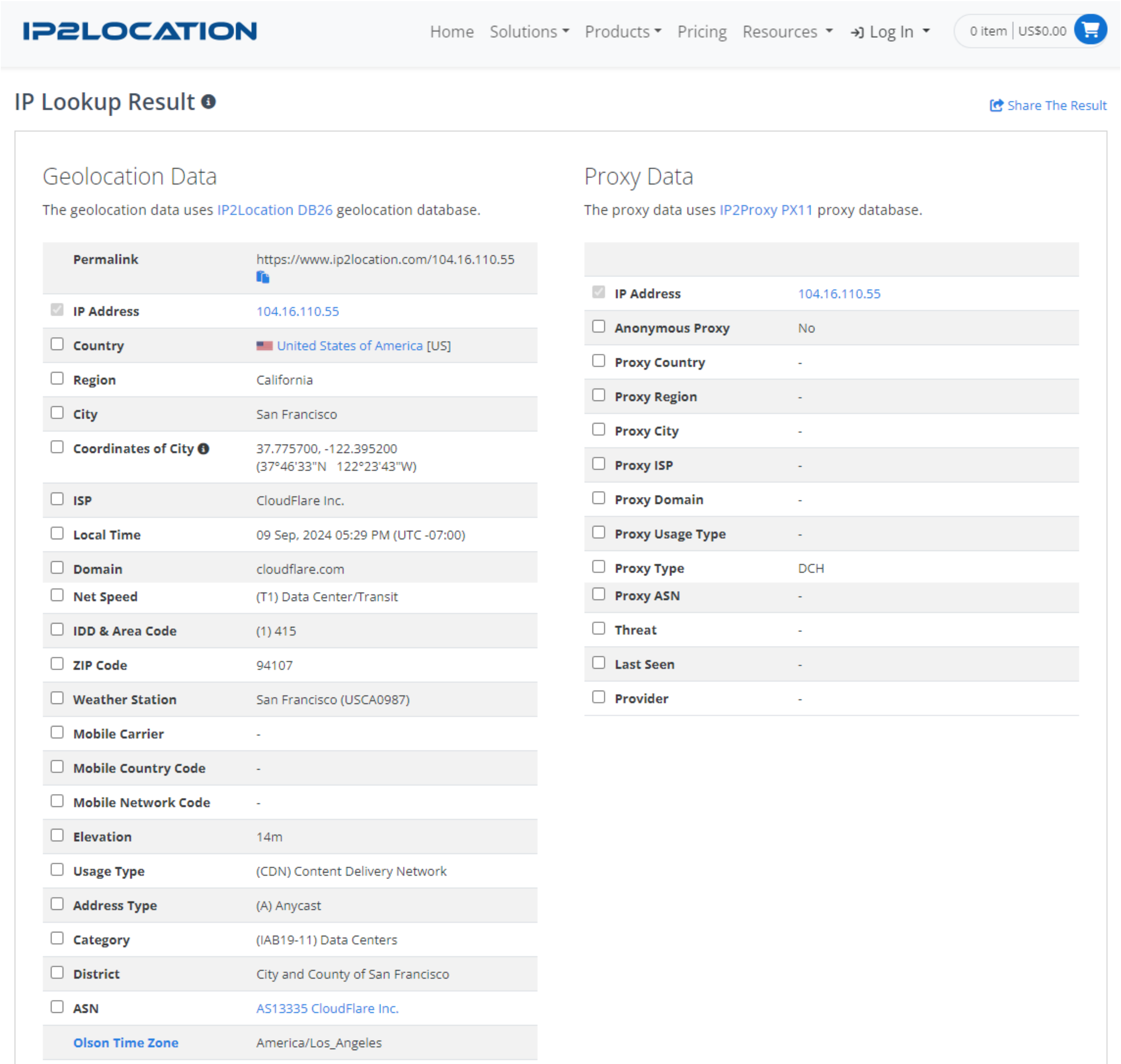
With these IP Addresses you can not only launch a Whois search, but you can now also find out the exact location of the servers using ip2location.

IP2LOCATION

IP2Location is a non-intrusive website (ip2location.com) with IP location lookup technology that retrieves geolocation information with no explicit permission required from users. In simple terms, if you have the IP Address of a hosted website, you can track their location from this website.

Why is this important? Having gathered the IP Address of the target website, it is important to confirm not only the location of the servers but also to perform a further survey of the layout of where the serve is.

Let's continue with the example of Jumia's website and find out more about the physical location of the company's resources.



IP Lookup Result

Geolocation Data

The geolocation data uses IP2Location DB26 geolocation database.

	Permalink	https://www.ip2location.com/104.16.110.55
☑	**IP Address**	104.16.110.55
☐	**Country**	United States of America [US]
☐	**Region**	California
☐	**City**	San Francisco
☐	**Coordinates of City**	37.775700, -122.395200 (37°46'33"N 122°23'43"W)
☐	**ISP**	CloudFlare Inc.
☐	**Local Time**	09 Sep, 2024 05:29 PM (UTC -07:00)
☐	**Domain**	cloudflare.com
☐	**Net Speed**	(T1) Data Center/Transit
☐	**IDD & Area Code**	(1) 415
☐	**ZIP Code**	94107
☐	**Weather Station**	San Francisco (USCA0987)
☐	**Mobile Carrier**	-
☐	**Mobile Country Code**	-
☐	**Mobile Network Code**	-
☐	**Elevation**	14m
☐	**Usage Type**	(CDN) Content Delivery Network
☐	**Address Type**	(A) Anycast
☐	**Category**	(IAB19-11) Data Centers
☐	**District**	City and County of San Francisco
☐	**ASN**	AS13335 CloudFlare Inc.
	Olson Time Zone	America/Los_Angeles

Proxy Data

The proxy data uses IP2Proxy PX11 proxy database.

☑	**IP Address**	104.16.110.55
☐	**Anonymous Proxy**	No
☐	**Proxy Country**	-
☐	**Proxy Region**	-
☐	**Proxy City**	-
☐	**Proxy ISP**	-
☐	**Proxy Domain**	-
☐	**Proxy Usage Type**	-
☐	**Proxy Type**	DCH
☐	**Proxy ASN**	-
☐	**Threat**	-
☐	**Last Seen**	-
☐	**Provider**	-

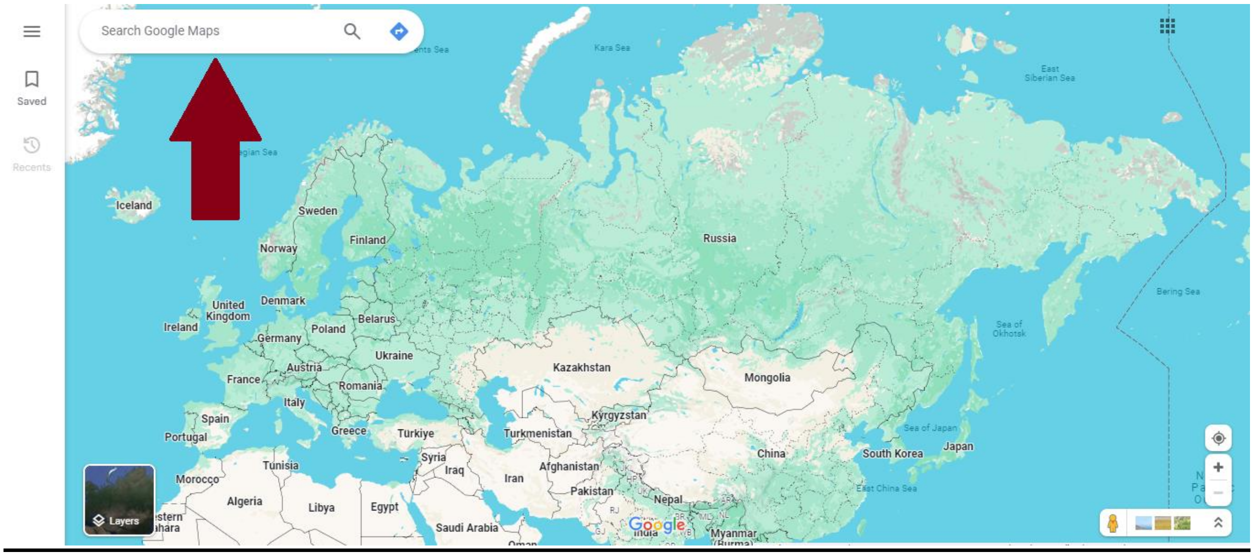
All of this is very important information but take note of the “Coordinates of the City”. Those are Longitude and Latitude showing the exact location of the servers. These can be copied into Google Maps so as to gain a layout of the environment.

GOOGLE MAPS

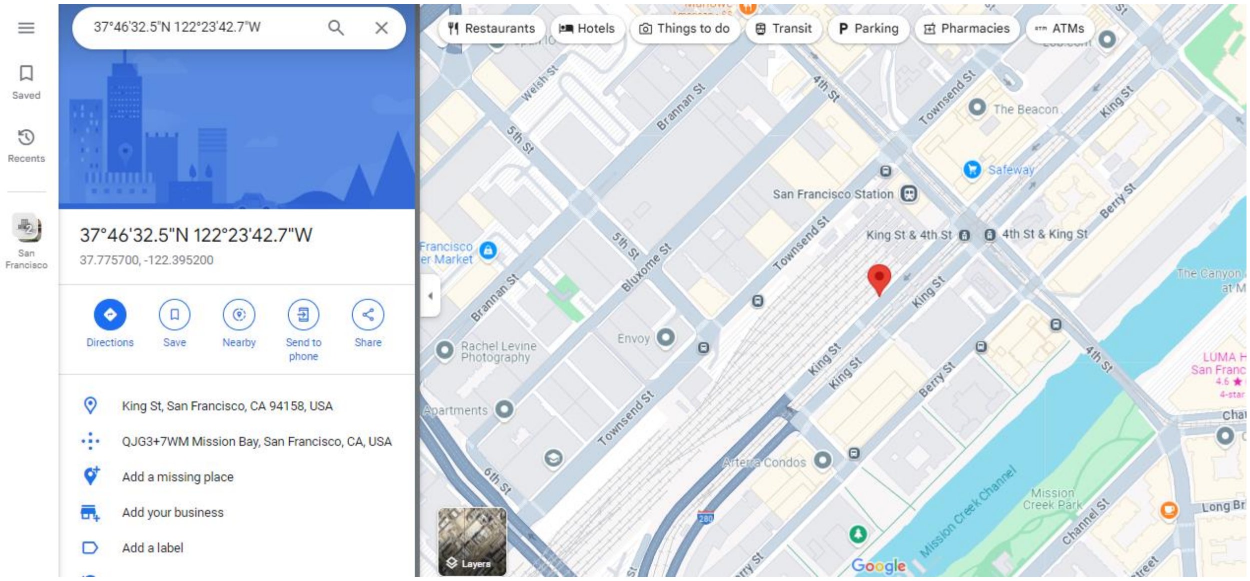
Google Maps is a widely used web mapping service developed by Google. It is valuable tool in reconnaissance because it provides, site assessment, route planning if you’re going to visit the place physically, has street view for casual inspection of buildings and provides a deeper understanding of the geographical layout and any local amenities and business that may be relevant to your mission. Visit maps.google.com to explore the various tools.

Copy the coordinates given from the ip2location website. Take note that the coordinates are split into two types, either one of them will do.

Paste the coordinates to the search box on Google Maps.



If you are unfamiliar with the location it may be difficult to determine which exact building you’re targeting, but you can quickly survey the area around for CCTV cameras, police posts, crowded areas / tourist hotspots and so much more.


37°46'32.5"N 122°23'42.7"W

37°46'32.5"N 122°23'42.7"W

37.775700, -122.395200

King St, San Francisco, CA 94158, USA

QJG3+7WM Mission Bay, San Francisco, CA, USA

Above is the location of the Jumia Servers in San Francisco California.

37°46'33.0"N 122°23'43.0"W

301 King St

San Francisco, California

Google Street View

May 2023 See more dates

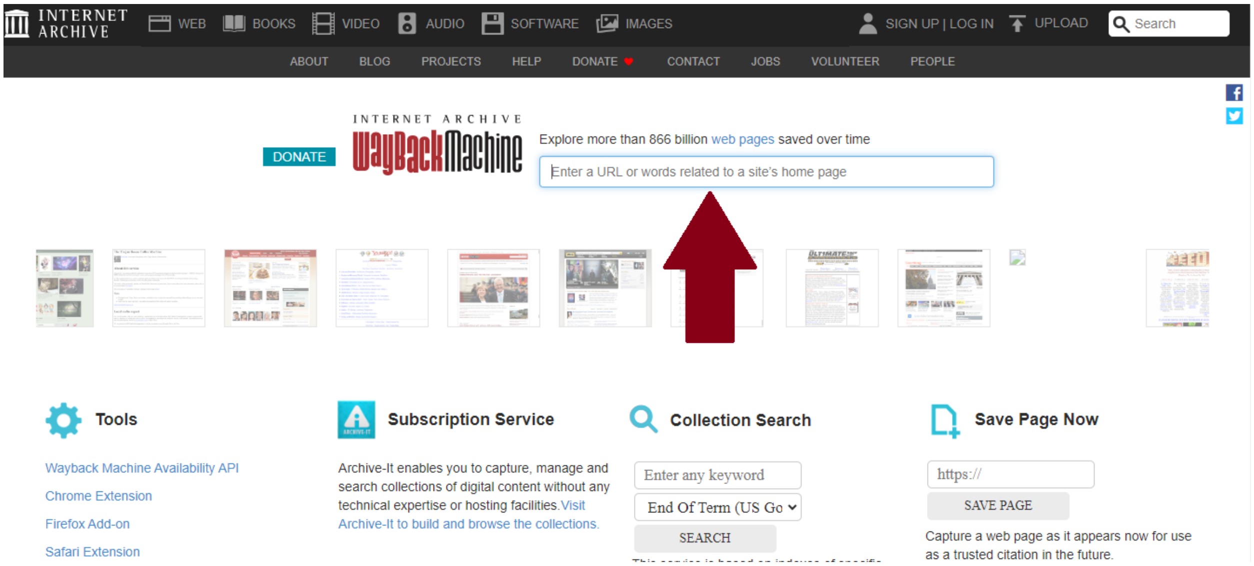
Image capture: May 2023 © 2024 Google Kenya Terms Privacy Report a problem

Using the street view tool, this is the supposed building that may contain the servers. One thing's for sure… They're in here somewhere.

WAYBACK MACHINE

The Wayback Machine is a digital archive of the Internet. It allows users to view archived versions of web pages dating back to the early days of the internet. Users can select different dates to view how a website looked at various points in time, allowing them to see changes and historical content.

As seen in the photo below, this is the [Wayback Machine (web.archive.org)](https://web.archive.org)



Explore more than 866 billion web pages saved over time

Enter a URL or words related to a site's home page

Wayback Machine Availability API

Chrome Extension

Firefox Add-on

Safari Extension

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

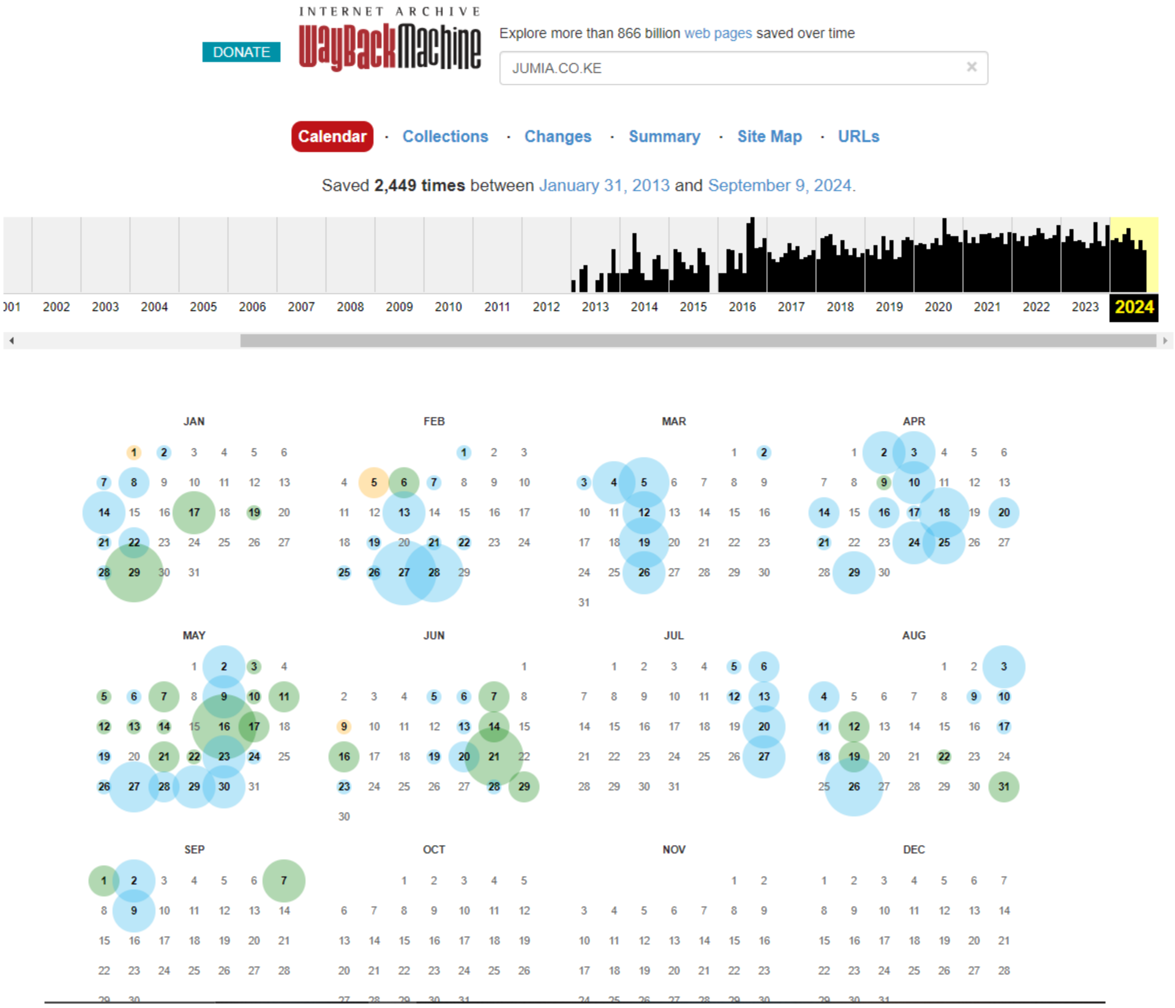
Enter any keyword

End Of Term (US Go

https://

Capture a web page as it appears now for use as a trusted citation in the future.

You can write down any webpage to try and explore the archived data (if any). For example we're going to continue using the Jumia webpage and find out more about it



Explore more than 866 billion web pages saved over time

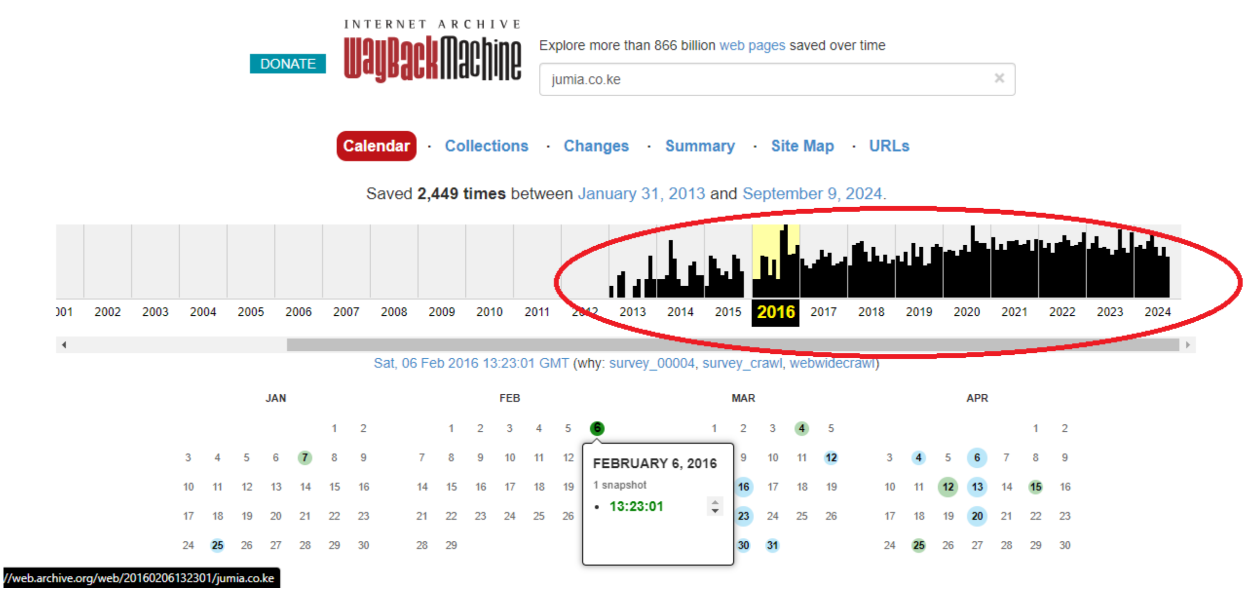
JUMIA.CO.KE

Saved **2,449 times** between January 31, 2013 and September 9, 2024.

From this results page, we can take note of the following things:

- There were 2,449 captures / updates that have been archived in this website.
- The approximate date when the website was first launched / first updated (31st January 2013).
- The last update made to the website (9th September 2013).
- The frequency at which the website is being updated. From the screenshot above we can tell that there were many updates around April and May, probably in preparation for the "Back to School" discounts that guarantees many visitors to their sites.
- The various colours have meanings as well: Blue is a good result; the full page was archived without error, green means a redirect, orange represents a client error and red denotes a server error.

Take note of this highlighted timeline. This is the tool that will allow you to "travel back in time" specifically in relation to the website you are searching. You can click anywhere on the time line, in this example we clicked on 2016. Upon visiting that year, you will notice there are captures that were archived, for example this one on the 6th of February 2016.



Explore more than 866 billion web pages saved over time

jumia.co.ke

Calendar · Collections · Changes · Summary · Site Map · URLs

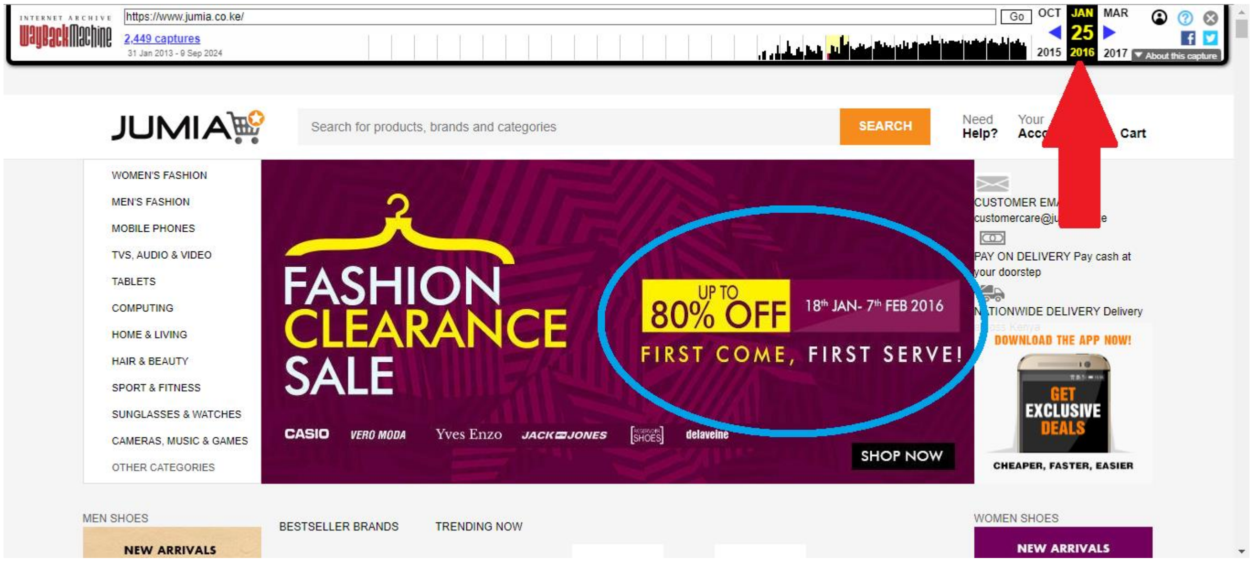
Saved 2,449 times between January 31, 2013 and September 9, 2024.

Sat, 06 Feb 2016 13:23:01 GMT (why: survey_00004, survey_crawl, webwidecrawl)

FEBRUARY 6, 2016
1 snapshot
• 13:23:01

//web.archive.org/web/20160206132301/jumia.co.ke

Upon visiting the capture, you will get the website to open like in the screenshot below. You can confirm the exact date you have travelled to from the top right hand corner. The website itself will take time to load but usually you will get some kind of content to confirm that it is successful, such as what I have highlighted in blue (The discount offers at that point in time).



https://www.jumia.co.ke/

2,449 captures
31 Jan 2013 - 9 Sep 2024

Search for products, brands and categories

GOOGLE DORKING

A Google Dork is a search query that looks for specific information on Google's search engine. It uses advanced search filters that allow to retrieve more efficient results. It is a technique often used by cybersecurity professionals in order to find valuable information about a target. They can be used to find information that you didn't even know existed.

Below is an example of Search Operators you can try.

Operator	**Description**	**Syntax**	**Example**
()	Group multiple terms or operators. Allows advanced expressions	(<term> or <operator>)	inurl:(html | php)
*	Wildcard. Matches any word	<text> * <text>	How to * a computer
""	The given keyword has to match exactly. *case-insensitive*	"<keywords>"	"google"
m..n / m...n	Search for a range of numbers. *n* should be greater than *m*	<number>..<number>	1..100
-	Documents that match the operator are excluded. *NOT-*Operator	-<operator>	-site:youtube.com
+	Include documents that match the operator	+<operator>	+site:youtube.com

Operator	**Description**	**Syntax**	**Example**
|	Logical *OR-Operator*. Only one operator needs to match in order for the overall expression to match	<operator> | <operator>	"google" | "yahoo"
~	Search for synonyms of the given word. Not supported by Google	~<word>	~book
@	Perform a search only on the given social media platform. Rather use **site**	@<socialmedia>	@instagram
after	Search for documents published / indexed after the given date	after:<yy(-mm-dd)>	after:2020-06-03
allintitle	Same as **intitle** but allows multiple keywords seperated by a space	allintitle:<keywords>	allintitle:dog cat
allinurl	Same as **inurl** but allows multiple keywords seperated by a space	allinurl:<keywords>	allinurl:search com

Operator	**Description**	**Syntax**	**Example**
allintext	Same as **intext** but allows multiple keywords seperated by a space	allintext:<keywords>	allintext:math science university
AROUND	Search for documents in which the first word is up to *n* words away from the second word and vice versa	<word1> AROUND(<n>) <word2>	google AROUND(10) good
author	Search for articles written by the given author if applicable	author:<name>	author:Max
before	Search for documents published / indexed before the given date	before:<yy(-mm-dd)>	before:2020-06-03
cache	Search on the cached version of the given website. Uses Google's cache to do so	cache:<domain>	cache:google.com
contains	Search for documents that link to the given fileype. Not supported by Google	contains:<filetype>	contains:pdf

Operator	**Description**	**Syntax**	**Example**
date	Search for documents published within the past *n* months. Not supported by Google	date:<number>	date:3
define	Search for the definition of the given word	define:<word>	define:funny
ext	Search for a specific filetype	ext:<documenttype>	ext:pdf
filetype	Refer to **ext**	filetype:<documenttype>	filetype:pdf
inanchor	Search for the given keyword in a website's anchors	inanchor:<keyword>	inanchor:security
index of	Search for documents containing direct downloads	index of:<term>	index of:mp4 videos
info	Search for information about a website	info:<domain>	info:google.com
intext	Keyword needs to be in the text of the document	intext:<keyword>	intext:news

Operator	**Description**	**Syntax**	**Example**
intitle	Keyword needs to be in the title of the document	intitle:<keyword>	intitle:money
inurl	Keyword needs to be in the URL of the document	inurl:<keyword>	inurl:sheet
link / links	Search for documents whose links contain the given keyword. Useful for finding documents that link to a specific website	link:<keyword>	link:google
location	Show documents based on the given location	location:<location>	location:USA
numrange	Refer to **m..n**	numrange:<number>-<number>	numrange:1-100
OR	Refer to **|**	<operator> OR <operator>	"google" OR "yahoo"
phonebook	Search for related phone numbers associated with the given name	phonebook:<name>	phonebook:"william smith"

Operator	**Description**	**Syntax**	**Example**
relate / related	Search for documents that are related to the given website	relate:<domain>	relate:google.com
safesearch	Exclude adult content such as pornographic videos	safesearch:<keyword>	safesearch:sex
source	Search on a specific news site. Rather use **site**	source:<news>	source:theguardian
site	Search on the given site. Given argument might also be just a TLD such as **com, net**, etc	site:<domain>	site:google.com
stock	Search for information about a market stock	stock:<stock>	stock:dax
weather	Search for information about the weather of the given location	weather:<location>	weather:Miami