HOW TO USE URLSCAN

BANGALY KOITA

Cover all the details you need to know while using urlscan.io

HOW TO USE URLSCAN

BANGALY KOITA

Vienna – Austria

Version 1.0

23.03.2023

Learn how to use URLSCAN during your investigation

Collect, Analyze, Investigate, and Report

Author: Bangaly Koita

About the Author

Bangaly Koita is a Cyber Security Analyst with 7 years of experience, he worked in different positions such as Support IT, Security Analyst, and Cyber Threat Intelligence.

He holds many certifications such as CISSP, CompTIA SEC +, CompTIA NETWORK +, CompTIA CYSA +, CCNA CYBER OPS, ITIL, and others.

As a passionate person in Cyber security especially in Cyber Threat Intelligence, he decided to create a blog named osintafrica.net to share his experience and knowledge and provide user awareness and training for the worldwide community.

Website: osintafrica.net

LinkedIn: OSINTAFRICA: Overview | LinkedIn

Facebook: OsintAfrica Facebook

Twitter: OSINTAFRICA (@OSINTAFRICA89) / Twitter

Contents

1. Introduction

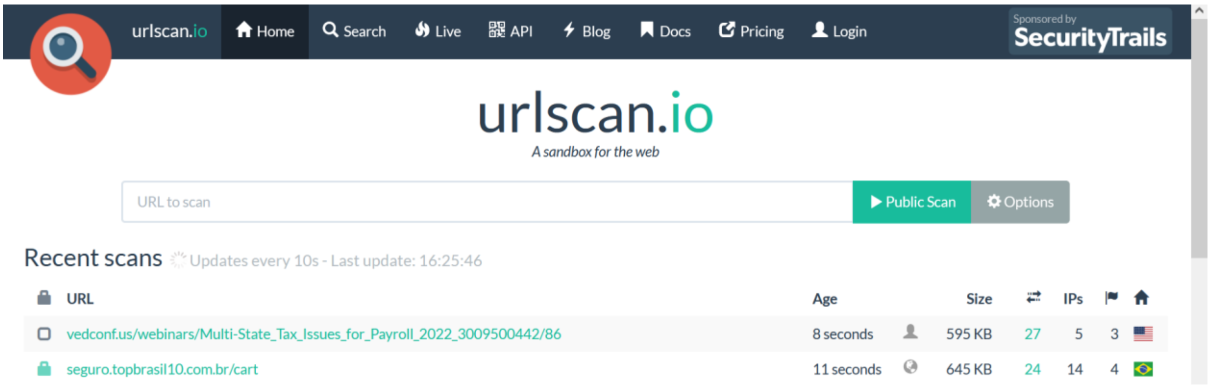
URLSCAN is used to perform different types of web scans and to analyze different IOCs such as IP address, domains, Hashes, filenames, and others.

URLSCAN is a tool used by different security teams such as Security Analyst, Cyber Threat Intelligence, Threat Hunting, Incident response team, and others.

The tool is divided into 2 versions (community version and paid version).

We will focus on the community version that is available for free.

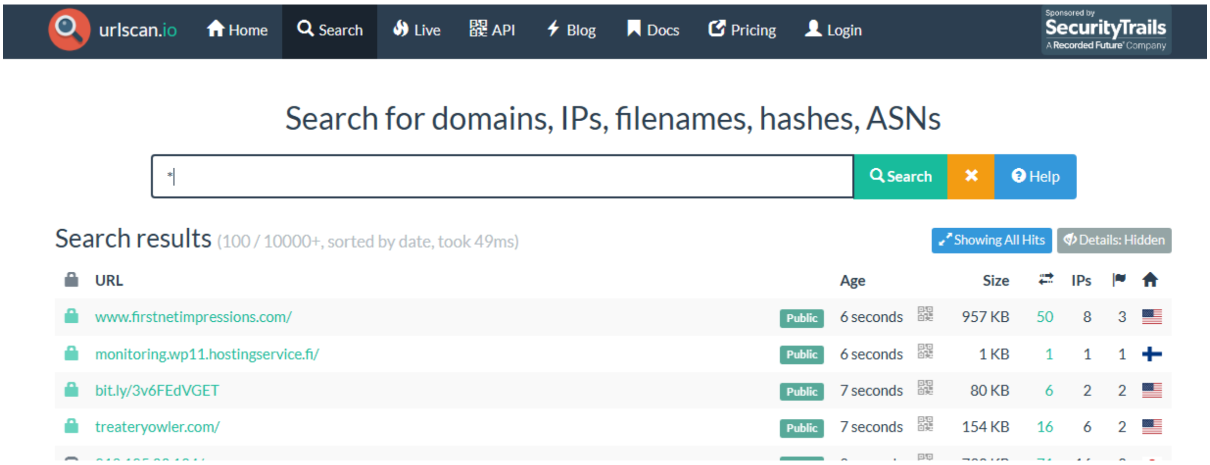
NB: In our case, we need two menus (Home and Search).



Recent scans Updates every 10s - Last update: 16:25:46

URL	Age	Size	⇄	IPs	⚑	⌂
vedconf.us/webinars/Multi-State_Tax_Issues_for_Payroll_2022_3009500442/86	8 seconds	595 KB	27	5	3	
seguro.topbrasil10.com.br/cart	11 seconds	645 KB	24	14	4	

Figure 1 URLSCAN Home dashboard


urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
Sponsored by SecurityTrails A Recorded Future Company
Search for domains, IPs, filenames, hashes, ASNs
*
Search
✖
Help
Showing All Hits
Details: Hidden

Search results (100 / 10000+, sorted by date, took 49ms)

URL		Age	Size	⇄	IPs	⚑	⌂
www.firstnetimpressions.com/	Public	6 seconds	957 KB	50	8	3	
monitoring.wp11.hostingservice.fi/	Public	6 seconds	1 KB	1	1	1	
bit.ly/3v6FEdVGET	Public	7 seconds	80 KB	6	2	2	
treateryowler.com/	Public	7 seconds	154 KB	16	6	2	

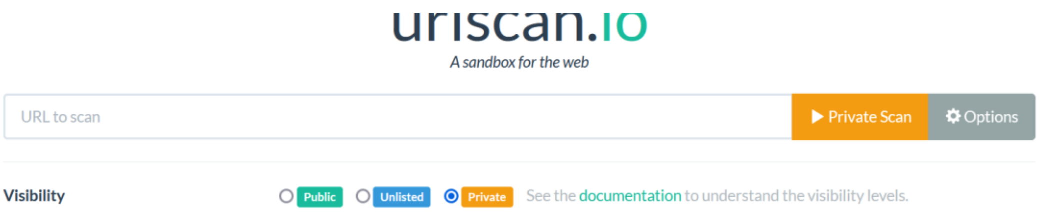
Figure 2 URLSCAN Search dashboard

2. HOME

Once we click on this menu, we can see the scanned queries by the users from different locations.

By default, the tool shows the public scan mode, if you want to leave the default mode and scan anything, the scan will be visible to everyone.

So, we advise you to click on **option** and used the **private mode** if you do not want other people to see the query you entered, this option can also help to avoid alerting the threat actor about your findings.



urlscan.io

A sandbox for the web

URL to scan ▶ Private Scan ⚙ Options

Visibility ○ Public ○ Unlisted ● Private See the documentation to understand the visibility levels.

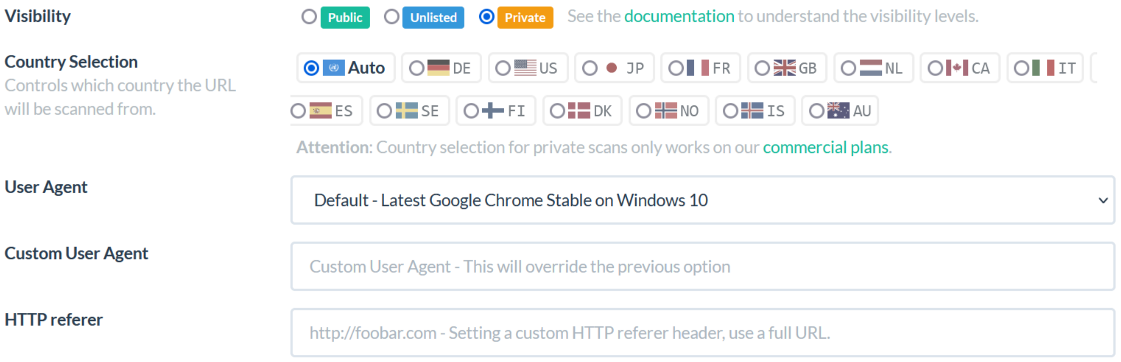
Figure 3 Scans options

URLSCAN can **anonymize** your identity. For instance,

- If you want to hide your location, you can click on "country selection" or auto (be aware that the Country selection for the private mode works only on the Commercial plans)
- You can change the "User Agent". For example, if the website you want to scan is for a mobile phone – you can choose one of the Android User Agents.

You can also customize your own User Agent.

- The "HTTP referer" can be used to custom the HTTP header before scanning.



Visibility ○ Public ○ Unlisted ● Private See the documentation to understand the visibility levels.

Country Selection
Controls which country the URL will be scanned from.

● Auto ○ DE ○ US ○ JP ○ FR ○ GB ○ NL ○ CA ○ IT
○ ES ○ SE ○ FI ○ DK ○ NO ○ IS ○ AU

Attention: Country selection for private scans only works on our commercial plans.

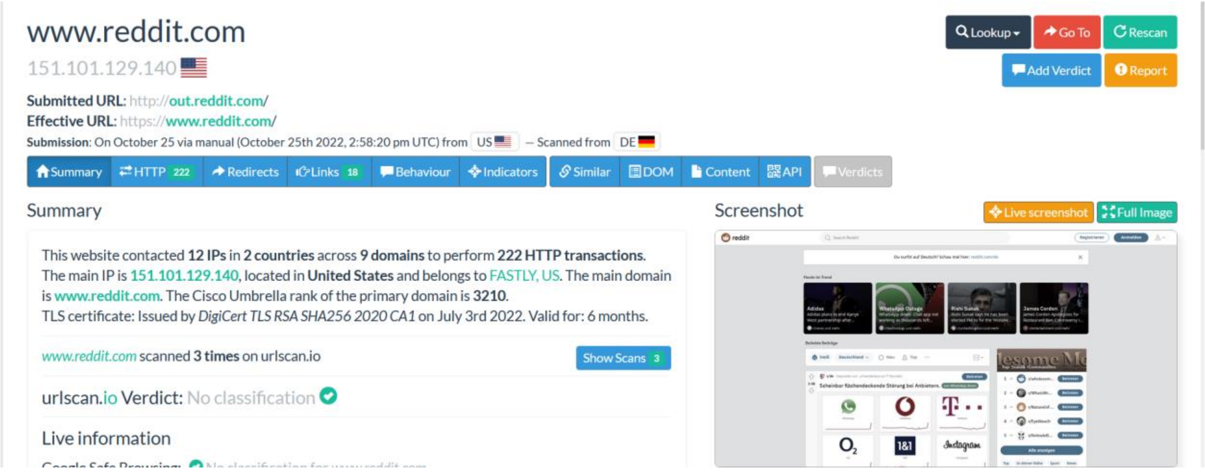
User Agent: Default - Latest Google Chrome Stable on Windows 10

Custom User Agent: Custom User Agent - This will override the previous option

HTTP referer: http://foobar.com - Setting a custom HTTP referer header, use a full URL.

Figure 4 customize your User Agent

Now, let's scan in a **private mode** a URL in hazard and analyze its behavior.



www.reddit.com

151.101.129.140

Submitted URL: http://out.reddit.com/
Effective URL: https://www.reddit.com/
Submission: On October 25 via manual (October 25th 2022, 2:58:20 pm UTC) from US — Scanned from DE

Summary

This website contacted **12 IPs** in **2 countries** across **9 domains** to perform **222 HTTP transactions.** The main IP is 151.101.129.140, located in **United States** and belongs to FASTLY, US. The main domain is www.reddit.com. The Cisco Umbrella rank of the primary domain is **3210**.
TLS certificate: Issued by *DigiCert TLS RSA SHA256 2020 CA1* on July 3rd 2022. Valid for: 6 months.

www.reddit.com scanned **3 times** on urlscan.io

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for www.reddit.com

Screenshot

Figure 5 Private scans

After submitting the URL, we can see the IP address 151.101.129.140 from the submitted URL following the submitted URL and the effective information.

From the right side, we have 5 menus.

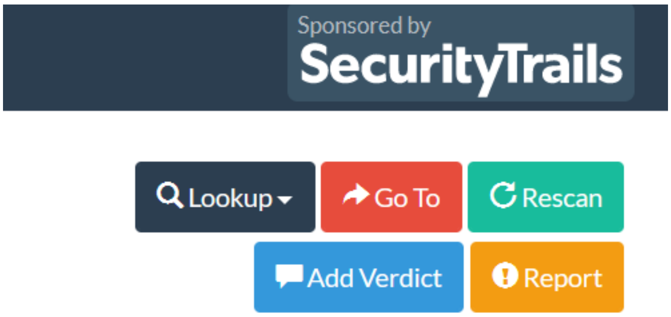


Figure 6 Other tools available on URLSCAN

The menu **"Lookup"** allows you to find different tools such as Virus Total, crt.sh, and Riskiq …. The tools can help you find more details about the submitted domain (click on each of them to learn more about it).

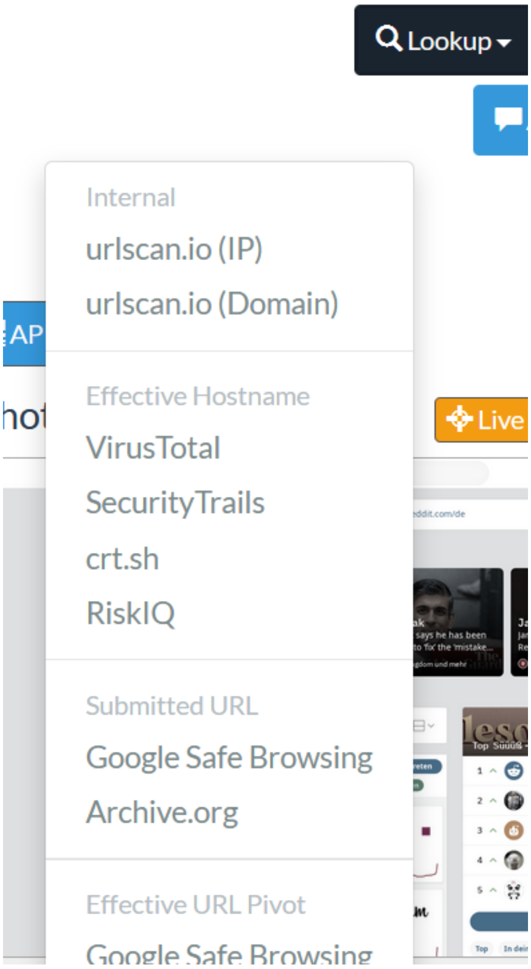


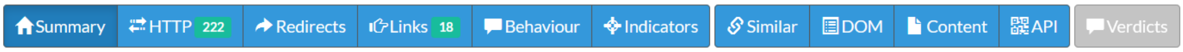
Figure 7 Choosing tools for your analyzing

The option **"Go To"** brings you to the domain submitted webpage (be careful before you click on it in case it is a malicious domain, you might be compromised).

The option **"Rescan"** is used to rescan the submitted URL.

The options **"Add Verdict" and "Report"** are used to add some comments about the submitted domain and contain some details about the scan report.

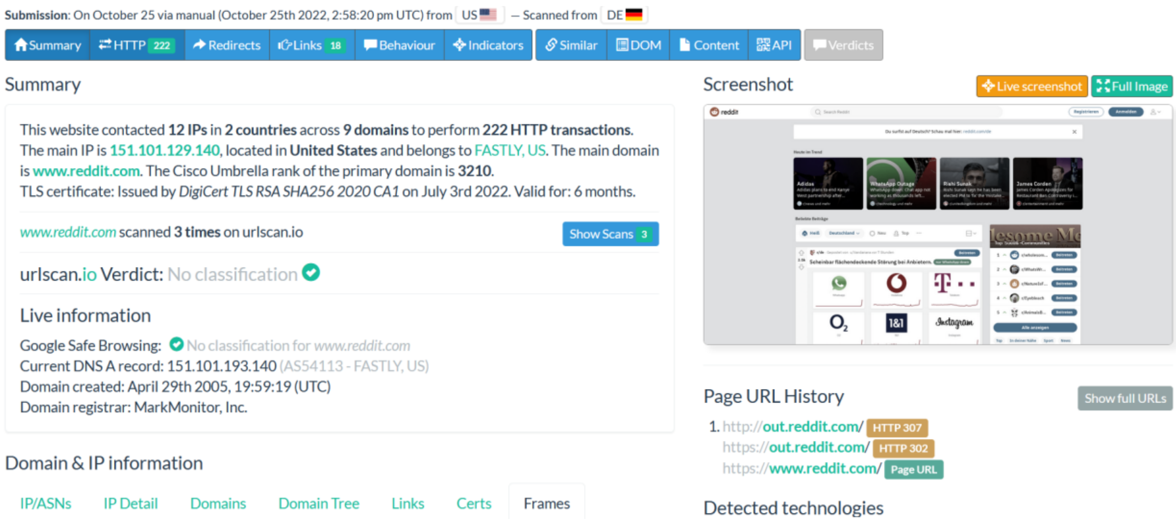
In the next section, we describe in detail the 11 Menus in **blue color.**



2.1 SUMMARY

Click on the "Summary button" to find more details about the menu.

The menu contains all details about the submitted domain.


Submission: On October 25 via manual (October 25th 2022, 2:58:20 pm UTC) from US — Scanned from DE

Summary

This website contacted **12 IPs** in **2 countries** across **9 domains** to perform **222 HTTP transactions**. The main IP is 151.101.129.140, located in **United States** and belongs to FASTLY, US. The main domain is www.reddit.com. The Cisco Umbrella rank of the primary domain is **3210**.
TLS certificate: Issued by *DigiCert TLS RSA SHA256 2020 CA1* on July 3rd 2022. Valid for: 6 months.

www.reddit.com scanned **3 times** on urlscan.io

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *www.reddit.com*
Current DNS A record: 151.101.193.140 (AS54113 - FASTLY, US)
Domain created: April 29th 2005, 19:59:19 (UTC)
Domain registrar: MarkMonitor, Inc.

Domain & IP information

Screenshot

Page URL History

1. http://out.reddit.com/ HTTP 307
https://out.reddit.com/ HTTP 302
https://www.reddit.com/ Page URL

Detected technologies

Figure 8 Summary dashboard

Figure 7 (Figure 9 Summary dashboard) shows in particular:

- The number of domains and IPs that were contacted by the submitted domain,
- The main IP address with a location and the domain hosting provider are also available,
- The certificate detail used by the website with his validity period,
- The website was scanned 3 times,

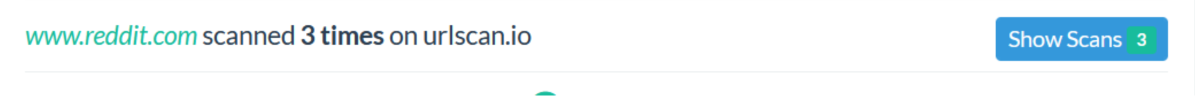
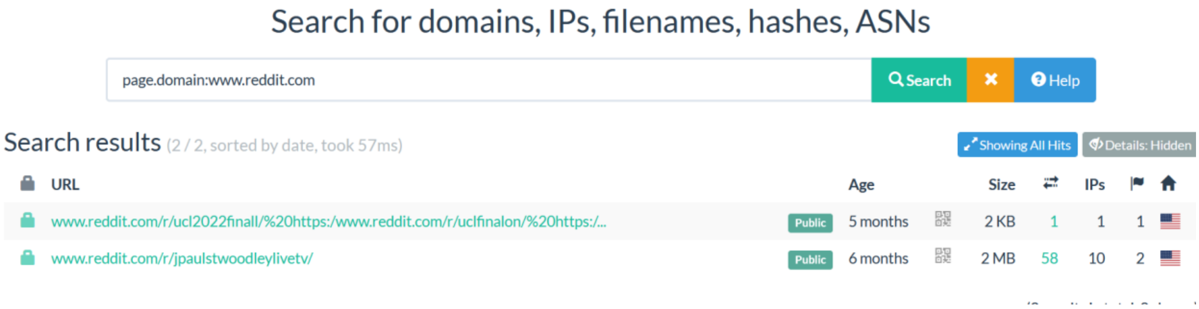

www.reddit.com scanned **3 times** on urlscan.io

Figure 10 Shows the number of times the website was scanned

- **Show scan**

This submenu shows you the number of times the domain has been already scanned. You can click on each scan to have more details such as how the domain looks at the time it was scanned, the IP address, ASN behind the domain at the time it was scanned.


Search for domains, IPs, filenames, hashes, ASNs

page.domain:www.reddit.com

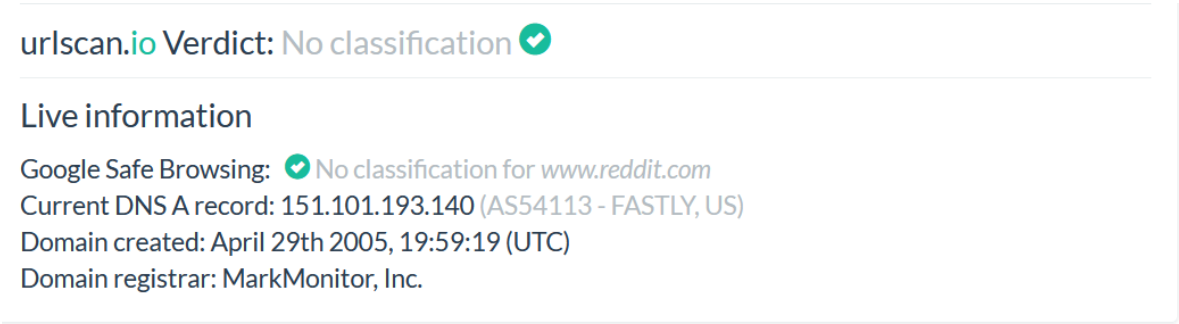
Search results (2 / 2, sorted by date, took 57ms)

URL		Age		Size	⇄	IPs		
www.reddit.com/r/ucl2022finall/%20https:/www.reddit.com/r/uclfinalon/%20https:/...	Public	5 months		2 KB	1	1	1	
www.reddit.com/r/jpaulstwoodleylivetv/	Public	6 months		2 MB	58	10	2	

Figure 11 scanned links or domains

- **Domain classification**

The second part of the Summary menu is the classification of the domain provided by Google Safe Browsing.



urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *www.reddit.com*
Current DNS A record: 151.101.193.140 (AS54113 - FASTLY, US)
Domain created: April 29th 2005, 19:59:19 (UTC)
Domain registrar: MarkMonitor, Inc.

Figure 12 Domain classification

The figure shows that Google Safe Browsing classified the domain as **"No classification"** which means that the domain is cleaned following the rating score available on Google Safe Browsing.

- **Domain and IP information**

7 submenus are available:

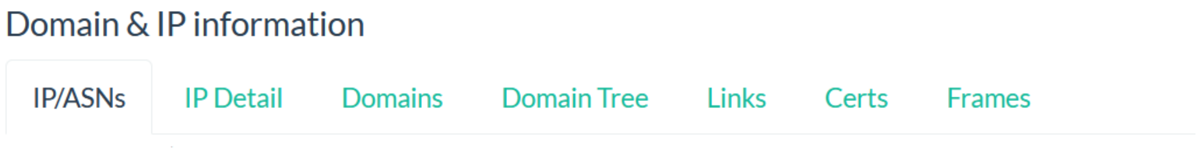
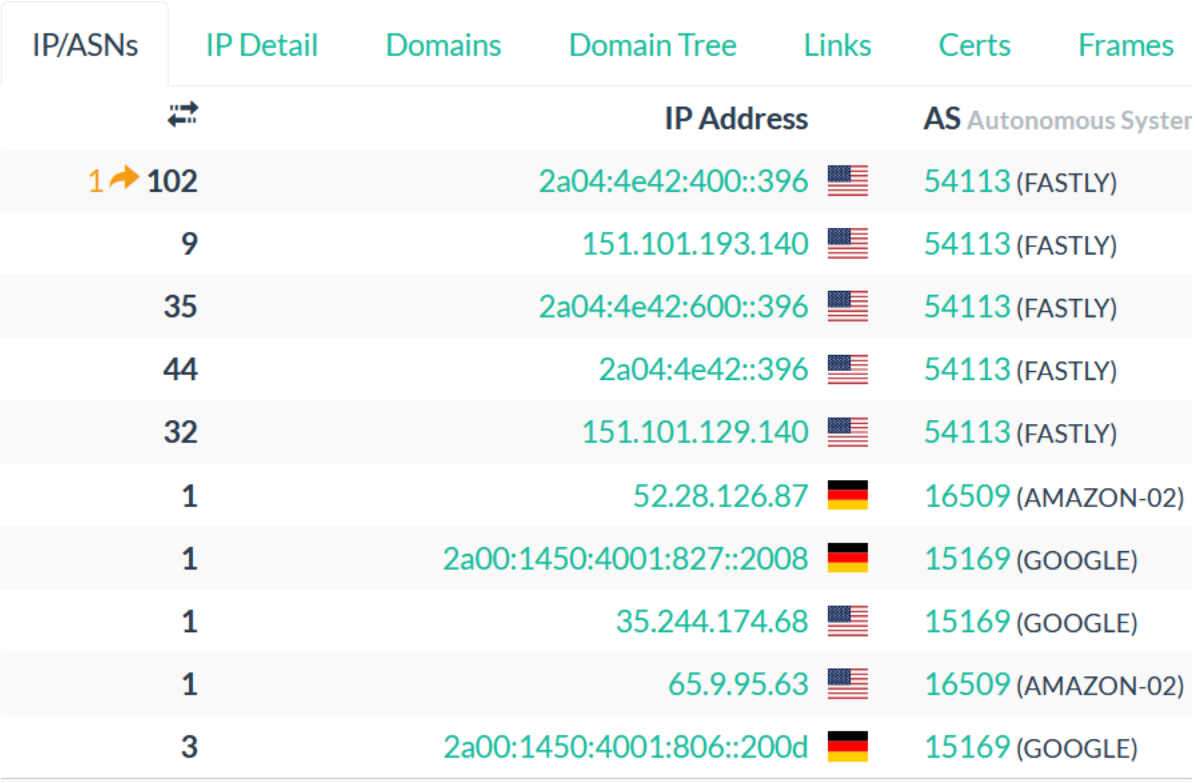


Figure 13 Domain and IP information

The menu IP/ASNs contains the information about all the IP addresses contacted by the domain while being submitted with their ASN (Autonomous System Number).



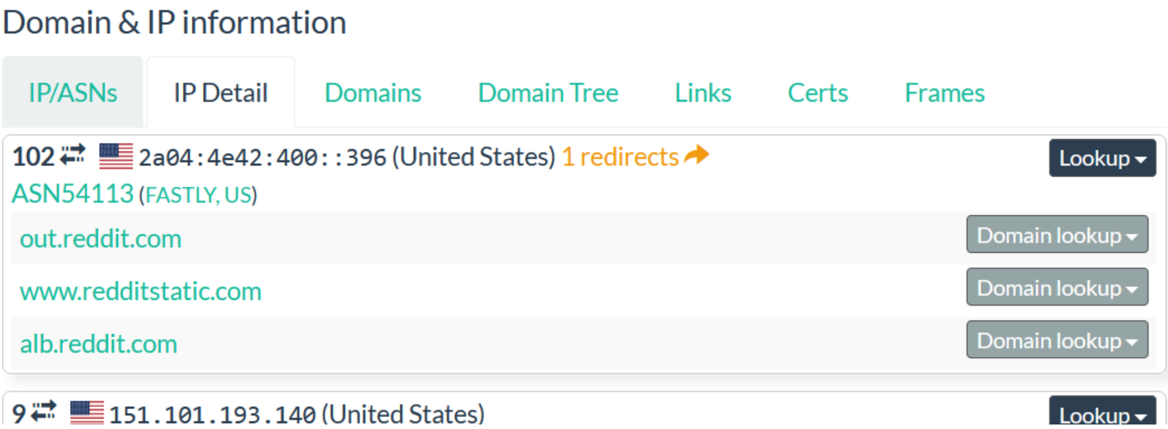
IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

⇄	IP Address		AS Autonomous Syster
1 ➦ 102	2a04:4e42:400::396	🇺🇸	54113 (FASTLY)
9	151.101.193.140	🇺🇸	54113 (FASTLY)
35	2a04:4e42:600::396	🇺🇸	54113 (FASTLY)
44	2a04:4e42::396	🇺🇸	54113 (FASTLY)
32	151.101.129.140	🇺🇸	54113 (FASTLY)
1	52.28.126.87	🇩🇪	16509 (AMAZON-02)
1	2a00:1450:4001:827::2008	🇩🇪	15169 (GOOGLE)
1	35.244.174.68	🇺🇸	15169 (GOOGLE)
1	65.9.95.63	🇺🇸	16509 (AMAZON-02)
3	2a00:1450:4001:806::200d	🇩🇪	15169 (GOOGLE)

Figure 14 Information on IP contacted

You can click on each IP address and ASN to find more information.

The submenus “**IP Detail” “Domains”** and **“Domain Tree”** contain some information about the IPs and the domains contacted by the submitted domain. You can click on each section to see the information available.



Domain & IP information

IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

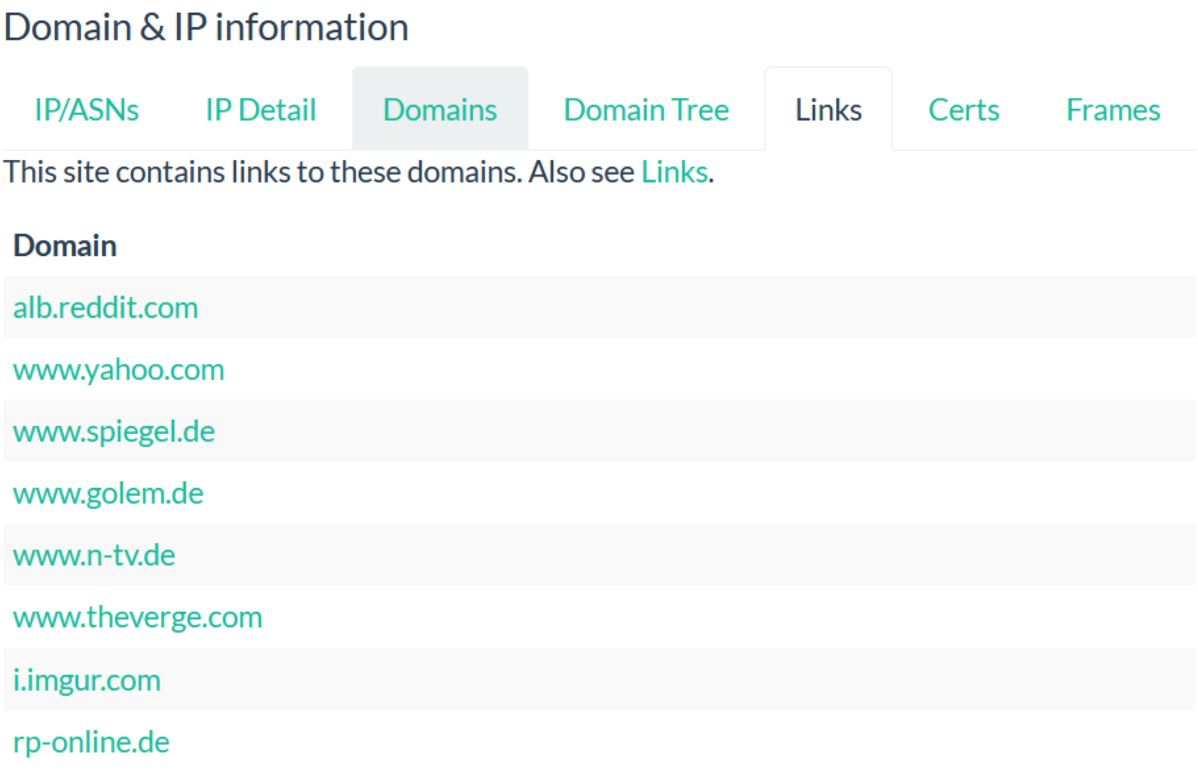
102 ⇄ 🇺🇸 2a04:4e42:400::396 (United States) 1 redirects ➦ | Lookup ▾
ASN54113 (FASTLY, US)

out.reddit.com | Domain lookup ▾
www.redditstatic.com | Domain lookup ▾
alb.reddit.com | Domain lookup ▾

9 ⇄ 🇺🇸 151.101.193.140 (United States) | Lookup ▾

Figure 15 Details related to the IP address

The submenu “**LINK”** contains all the links redirecting to others domains or URLs.



Domain & IP information

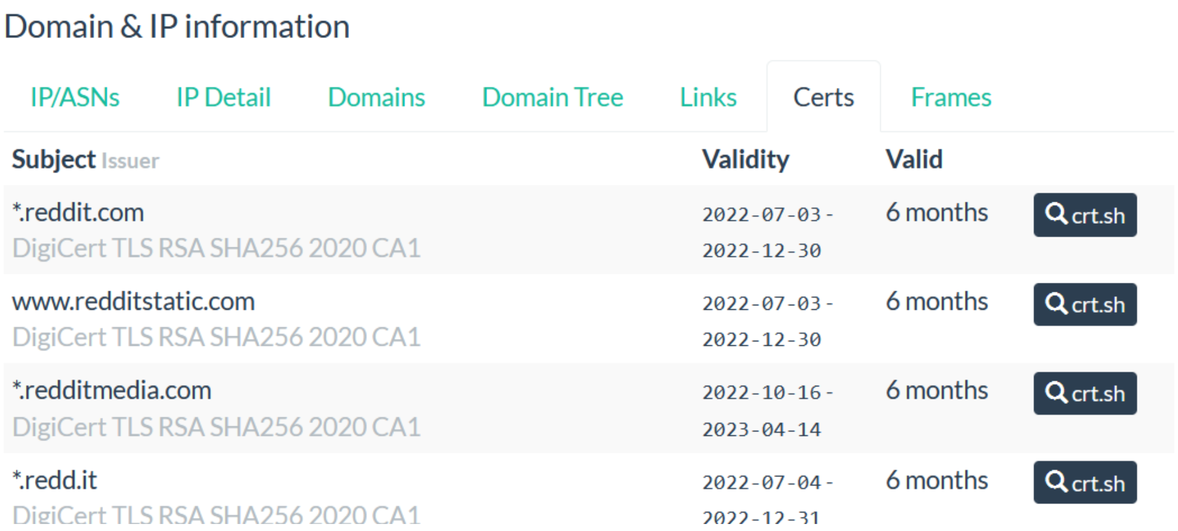
This site contains links to these domains. Also see Links.

Domain
alb.reddit.com
www.yahoo.com
www.spiegel.de
www.golem.de
www.n-tv.de
www.theverge.com
i.imgur.com
rp-online.de

Figure 16 Links on the website

You can click on each link to get more details about it.

The submenu **"Certs"** contains the list of all certificates used by the submitted domain with the validity period.

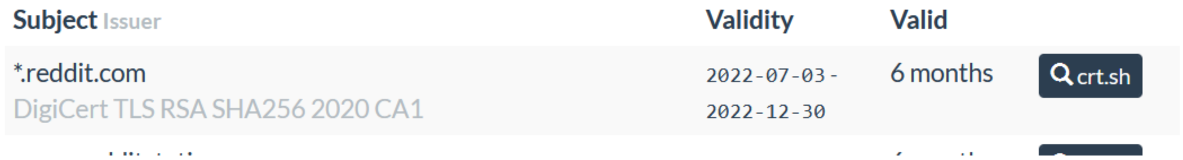


Domain & IP information

Subject Issuer	Validity	Valid	
*.reddit.com DigiCert TLS RSA SHA256 2020 CA1	2022-07-03 - 2022-12-30	6 months	crt.sh
www.redditstatic.com DigiCert TLS RSA SHA256 2020 CA1	2022-07-03 - 2022-12-30	6 months	crt.sh
*.redditmedia.com DigiCert TLS RSA SHA256 2020 CA1	2022-10-16 - 2023-04-14	6 months	crt.sh
*.redd.it DigiCert TLS RSA SHA256 2020 CA1	2022-07-04 - 2022-12-31	6 months	crt.sh

Figure 17 Certificates used by the website

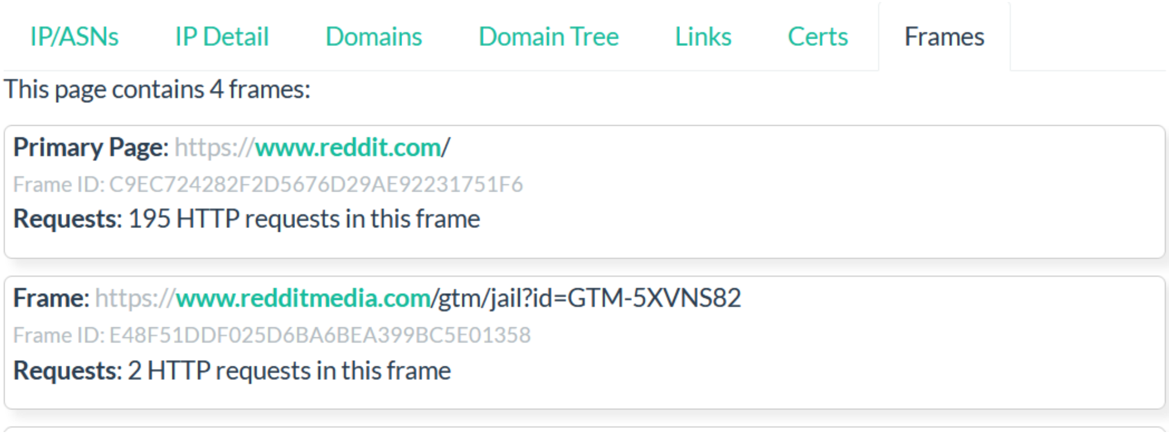
You can click on the **crt.sh** on the right side to get more details about the certificate



Subject Issuer	**Validity**	**Valid**	
*.reddit.com DigiCert TLS RSA SHA256 2020 CA1	2022-07-03 - 2022-12-30	6 months	crt.sh

Figure 18 Click on Cert.sh for more details

The submenu **"Frames"** shows you if the website is using any URL Frames.



This page contains 4 frames:

Primary Page: https://www.reddit.com/
Frame ID: C9EC724282F2D5676D29AE92231751F6
Requests: 195 HTTP requests in this frame

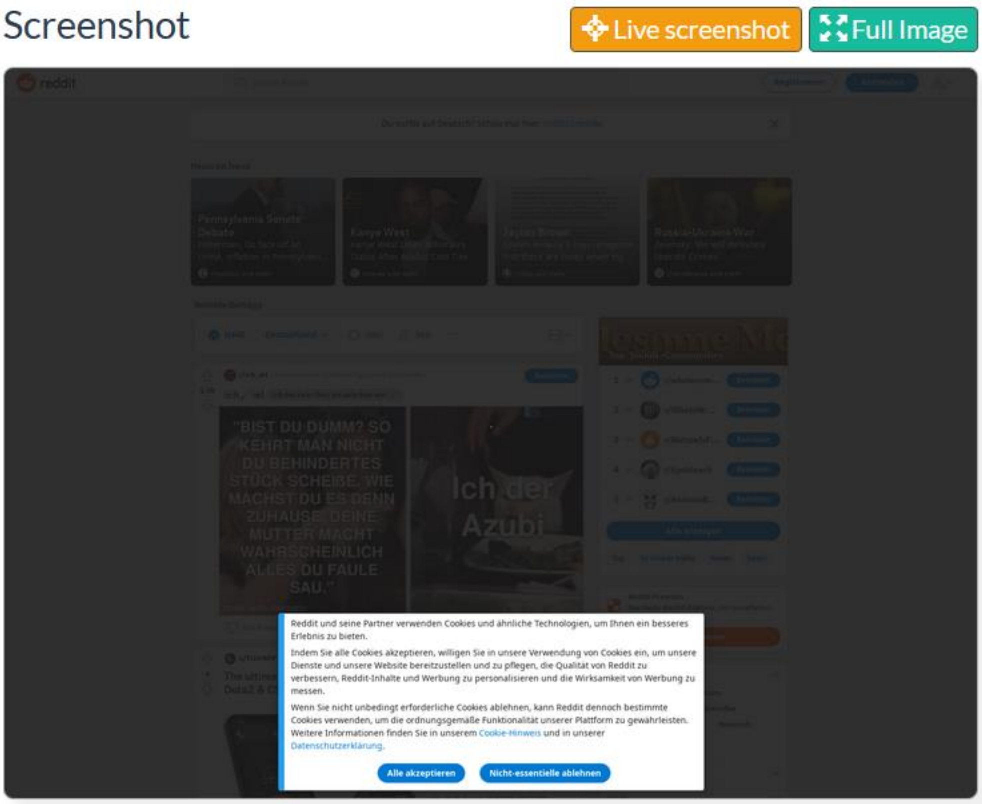
Frame: https://www.redditmedia.com/gtm/jail?id=GTM-5XVNS82
Frame ID: E48F51DDF025D6BA6BEA399BC5E01358
Requests: 2 HTTP requests in this frame

Figure 19 URL Frame used by the website

- **Image**

After describing different submenus from the Summary, from the right side, once the domain has been submitted, the main image from the website will appear in real-time.

We can see how the website behind the domain submitted looks like. This is very important during an investigation, for example when you are analyzing a phishing issue, it is necessary to view the website without connecting directly to it.


Screenshot
Live screenshot
Full Image
reddit
"BIST DU DUMM? SO KEHRT MAN NICHT DU BEHINDERTES STÜCK SCHEIßE. WIE MACHST DU ES DENN ZUHAUSE. DEINE MUTTER MACHT WAHRSCHEINLICH ALLES DU FAULE SAU."
Ich der Azubi
Alle akzeptieren
Nicht-essentielle ablehnen

Reddit und seine Partner verwenden Cookies und ähnliche Technologien, um Ihnen ein besseres Erlebnis zu bieten.

Indem Sie alle Cookies akzeptieren, willigen Sie in unsere Verwendung von Cookies ein, um unsere Dienste und unsere Website bereitzustellen und zu pflegen, die Qualität von Reddit zu verbessern, Reddit-Inhalte und Werbung zu personalisieren und die Wirksamkeit von Werbung zu messen.

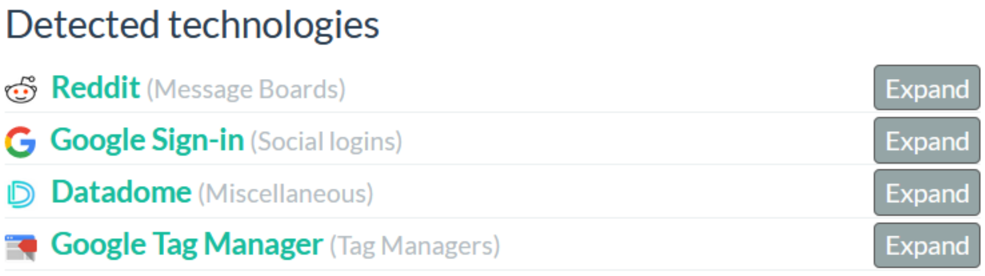
Wenn Sie nicht unbedingt erforderliche Cookies ablehnen, kann Reddit dennoch bestimmte Cookies verwenden, um die ordnungsgemäße Funktionalität unserer Plattform zu gewährleisten. Weitere Informationen finden Sie in unserem Cookie-Hinweis und in unserer Datenschutzerklärung.

Figure 20 Image of the website scanned

You can click on **"Live screenshots"** and **"Full Image"** to have better visibility of the image.

- **Detected technologies**

Here, we can find some technologies used by the domain. Notice that this is very important for you as an analyst. For example, when the website is compromised, the threat actor might embed malicious code into the website, by checking this, you might find out the malicious code embedded within your website, checking this, can also help you to find some technologies that need to be updated or are not in use anymore.



Detected technologies

Reddit (Message Boards) Expand

Google Sign-in (Social logins) Expand

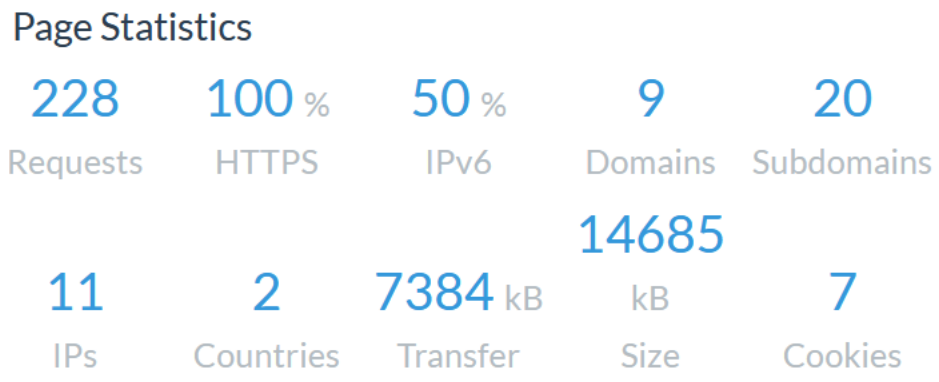
Datadome (Miscellaneous) Expand

Google Tag Manager (Tag Managers) Expand

Figure 21 Technologies available on the website

- **Page Statistics**

This section shows you the whole details about the submitted URL such as HTTP request, domains, subdomains, cookies, IP, etc …



Page Statistics

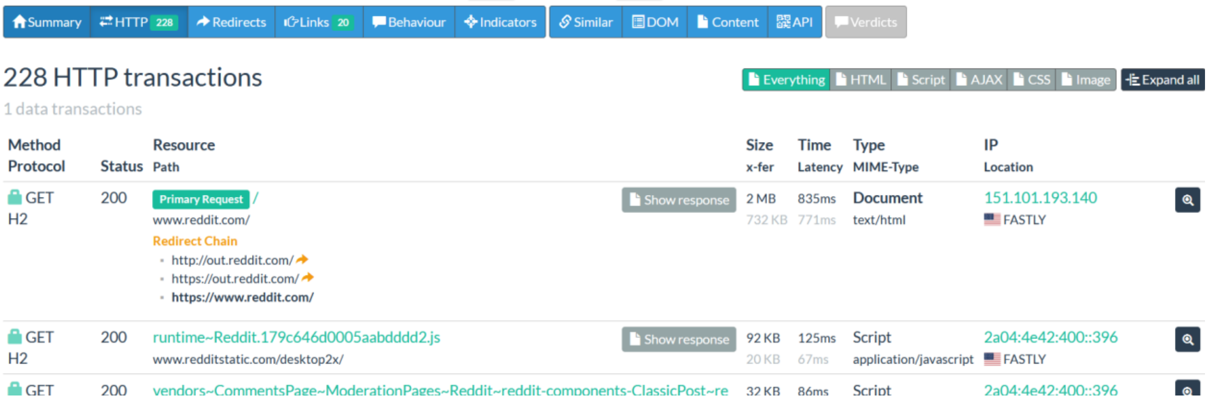
228	100 %	50 %	9	20
Requests	HTTPS	IPv6	Domains	Subdomains
11	2	7384 kB	14685 kB	7
IPs	Countries	Transfer	Size	Cookies

Figure 22 Statistic of the URL scanned

2.2 HTTP

In this menu, we can see all the HTTP transactions after the URL has been submitted.

The HTTP transactions consist of all the resources (HTLM, Script, AJAX, Images …) the website uses.



228 HTTP transactions

1 data transactions

Method Protocol	Status	Resource Path	Size x-fer	Time Latency	Type MIME-Type	IP Location
GET H2	200	Primary Request / www.reddit.com/ Redirect Chain • http://out.reddit.com/ • https://out.reddit.com/ • https://www.reddit.com/	2 MB 732 KB	835ms 771ms	Document text/html	151.101.193.140 FASTLY
GET H2	200	runtime~Reddit.179c646d0005aabdddd2.js www.redditstatic.com/desktop2x/	92 KB 20 KB	125ms 67ms	Script application/javascript	2a04:4e42:400::396 FASTLY
GET	200	vendors~CommentsPage~ModerationPages~Reddit~reddit-components-ClassicPost~re	32 KB	86ms	Script	2a04:4e42:400::396

Figure 23 HTTP transactions after the URL submission

This section is very useful for the analyst.

Click on one of the options available

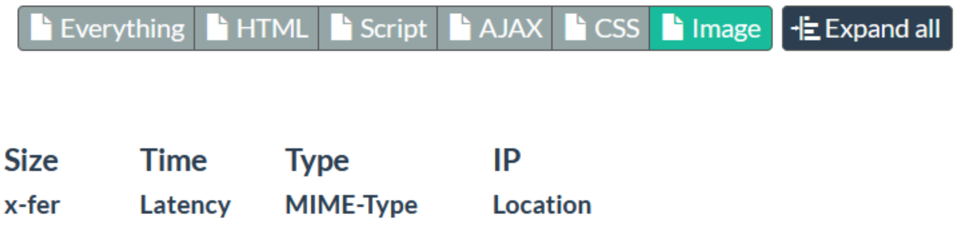
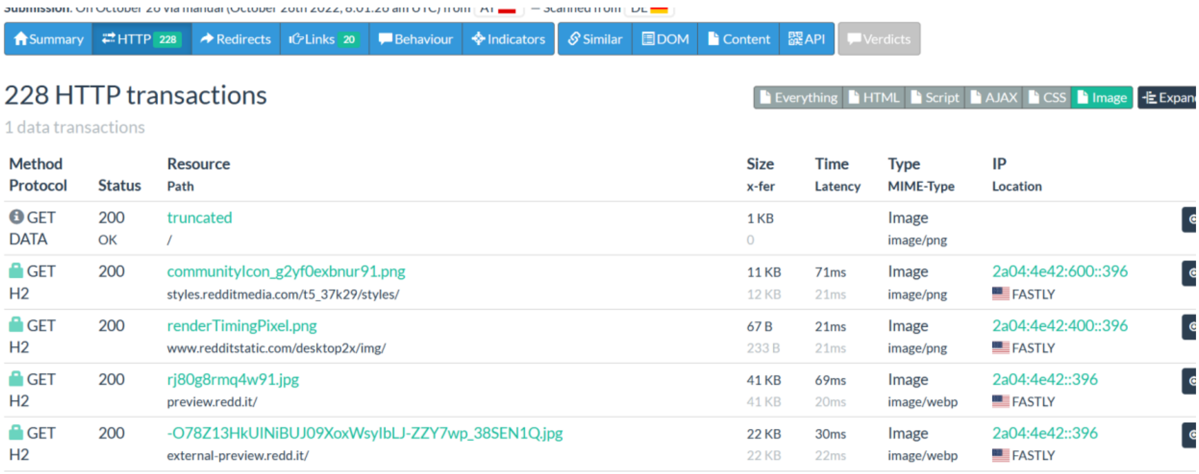


Figure 24 Images available after submitting the URL

In our case, we click on the button **“Image”** to find the image described in the section **Image** and all the files used by the image.



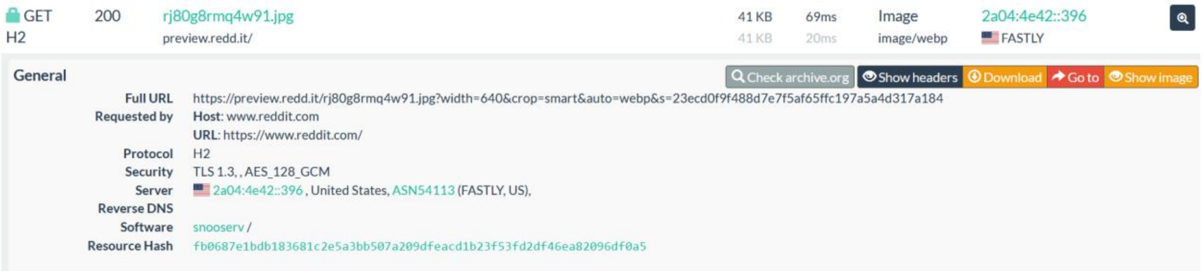
228 HTTP transactions

1 data transactions

Method Protocol	Status	Resource Path	Size x-fer	Time Latency	Type MIME-Type	IP Location
GET DATA	200 OK	truncated /	1 KB 0		Image image/png	
GET H2	200	communityIcon_g2yf0exbnur91.png styles.redditmedia.com/t5_37k29/styles/	11 KB 12 KB	71ms 21ms	Image image/png	2a04:4e42:600::396 FASTLY
GET H2	200	renderTimingPixel.png www.redditstatic.com/desktop2x/img/	67 B 233 B	21ms 21ms	Image image/png	2a04:4e42:400::396 FASTLY
GET H2	200	rj80g8rmq4w91.jpg preview.redd.it/	41 KB 41 KB	69ms 20ms	Image image/webp	2a04:4e42::396 FASTLY
GET H2	200	-O78Z13HkUlNiBUJ09XoxWsylbLJ-ZZY7wp_38SEN1Q.jpg external-preview.redd.it/	22 KB 22 KB	30ms 22ms	Image image/webp	2a04:4e42::396 FASTLY

Figure 25 Images available after submitting the URL 2

Click on the “expand” sign to see more details about each file.



GET H2	200	rj80g8rmq4w91.jpg preview.redd.it/	41 KB 41 KB	69ms 20ms	Image image/webp	2a04:4e42::396 FASTLY

General

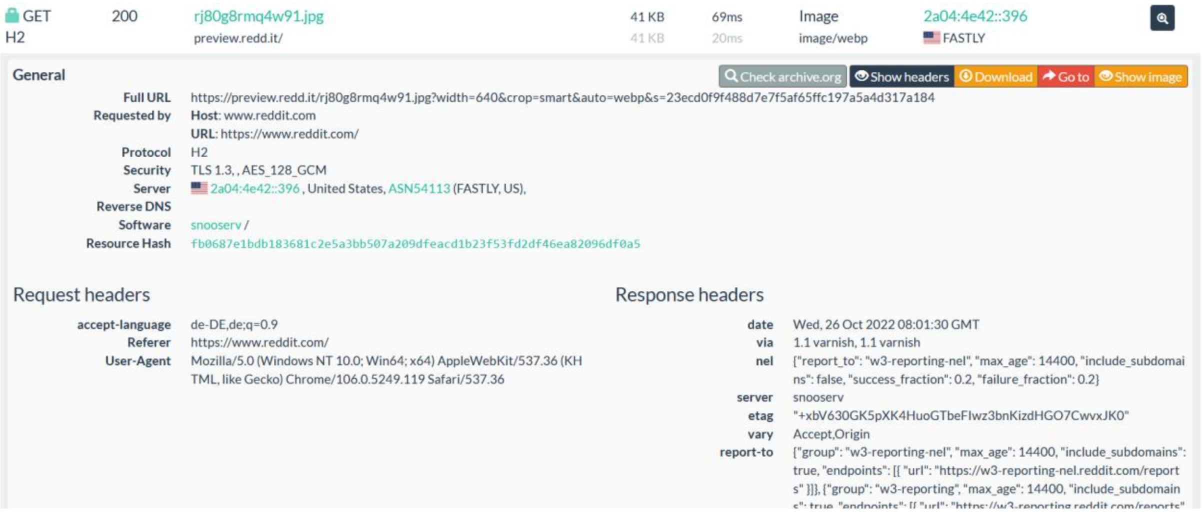
Full URL https://preview.redd.it/rj80g8rmq4w91.jpg?width=640&crop=smart&auto=webp&s=23ecd0f9f488d7e7f5af65ffc197a5a4d317a184
Requested by **Host**: www.reddit.com
URL: https://www.reddit.com/
Protocol H2
Security TLS 1.3, , AES_128_GCM
Server 2a04:4e42::396 , United States, ASN54113 (FASTLY, US),
Reverse DNS
Software snooserv /
Resource Hash fb0687e1bdb183681c2e5a3bb507a209dfeacd1b23f53fd2df46ea82096df0a5

Figure 26 Image expanded to see more details

We can observe that:

- **The Full URL** shows the requested image from the **Host**: www.reddit.com.
- We can find others information such as the **server’s name used, the TLS protocol version used, the Hash of the image used, the software** used, and others …

Click on the **Show headers** to find the details about the request headers and the response headers from the server side.



GET 200 rj80g8rmq4w91.jpg 41 KB 69ms Image 2a04:4e42::396
H2 preview.redd.it/ 41 KB 20ms image/webp FASTLY

General

Full URL https://preview.redd.it/rj80g8rmq4w91.jpg?width=640&crop=smart&auto=webp&s=23ecd0f9f488d7e7f5af65ffc197a5a4d317a184
Requested by **Host**: www.reddit.com
URL: https://www.reddit.com/
Protocol H2
Security TLS 1.3, , AES_128_GCM
Server 2a04:4e42::396 , United States, ASN54113 (FASTLY, US),
Reverse DNS
Software snooserv /
Resource Hash fb0687e1bdb183681c2e5a3bb507a209dfeacd1b23f53fd2df46ea82096df0a5

Request headers

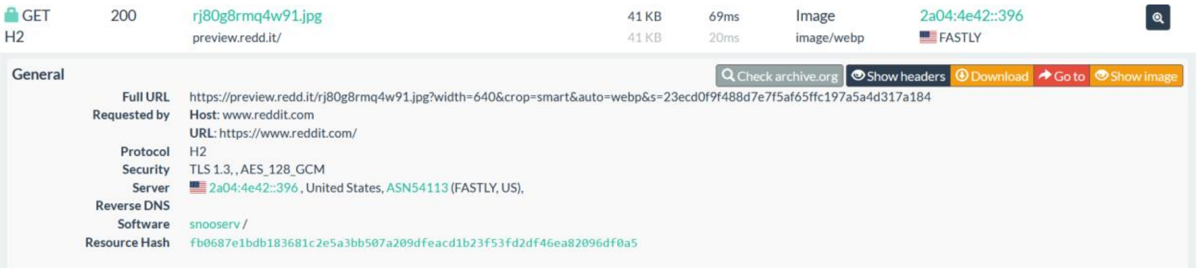
accept-language de-DE,de;q=0.9
Referer https://www.reddit.com/
User-Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.119 Safari/537.36

Response headers

date Wed, 26 Oct 2022 08:01:30 GMT
via 1.1 varnish, 1.1 varnish
nel {"report_to": "w3-reporting-nel", "max_age": 14400, "include_subdomains": false, "success_fraction": 0.2, "failure_fraction": 0.2}
server snooserv
etag "+xbV630GK5pXK4HuoGTbeFlwz3bnKizdHGO7CwvxJK0"
vary Accept,Origin
report-to {"group": "w3-reporting-nel", "max_age": 14400, "include_subdomains": true, "endpoints": [{ "url": "https://w3-reporting-nel.reddit.com/reports" }]}, {"group": "w3-reporting", "max_age": 14400, "include_subdomains": true, "endpoints": [{ "url": "https://w3-reporting.reddit.com/reports"

Figure 27 Show the details of the headers

A click on check **archive.org** leads you to the website https://web.archive.org (You can Google search to find more information about it)



GET 200 rj80g8rmq4w91.jpg 41 KB 69ms Image 2a04:4e42::396
H2 preview.redd.it/ 41 KB 20ms image/webp FASTLY

General

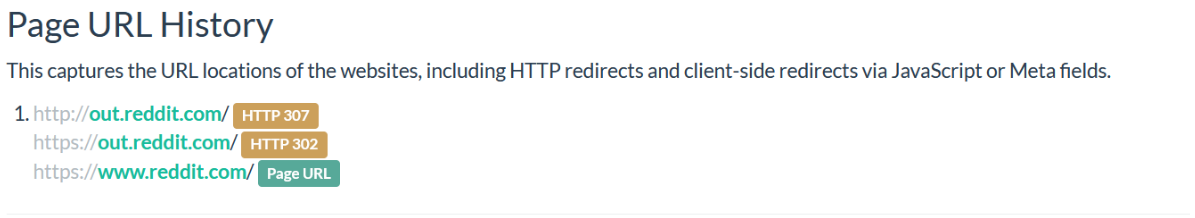
Full URL https://preview.redd.it/rj80g8rmq4w91.jpg?width=640&crop=smart&auto=webp&s=23ecd0f9f488d7e7f5af65ffc197a5a4d317a184
Requested by **Host**: www.reddit.com
URL: https://www.reddit.com/
Protocol H2
Security TLS 1.3, , AES_128_GCM
Server 2a04:4e42::396 , United States, ASN54113 (FASTLY, US),
Reverse DNS
Software snooserv /
Resource Hash fb0687e1bdb183681c2e5a3bb507a209dfeacd1b23f53fd2df46ea82096df0a5

Figure 28 Archive.org

Click on each option (HTLM, Script, AJAX, Images) available to learn more about.

2.3 REDIRECT

Here, you find all the redirect links on the website.



Page URL History

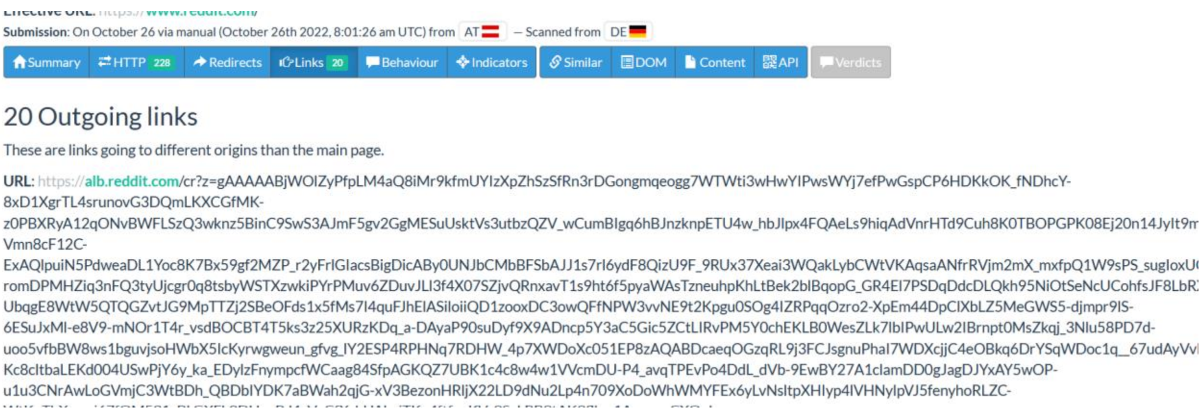
This captures the URL locations of the websites, including HTTP redirects and client-side redirects via JavaScript or Meta fields.

1. http://out.reddit.com/ HTTP 307
   https://out.reddit.com/ HTTP 302
   https://www.reddit.com/ Page URL

Figure 29 Redirecting links on the website

2.4 LINKS

The page contains all the links available on the website.



Effective URL: https://www.reddit.com/

Submission: On October 26 via manual (October 26th 2022, 8:01:26 am UTC) from AT — Scanned from DE

20 Outgoing links

These are links going to different origins than the main page.

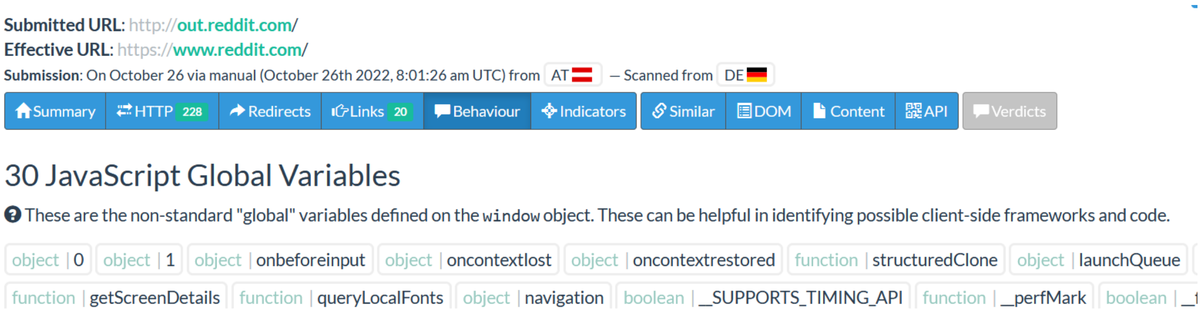
URL: https://alb.reddit.com/cr?z=gAAAAABjWOIZyPfpLM4aQ8iMr9kfmUYIzXpZhSzSfRn3rDGongmqeogg7WTWti3wHwYIPwsWYj7efPwGspCP6HDKkOK_fNDhcY-8xD1XgrTL4srunovG3DQmLKXCGfMK-z0PBXRyA12qONvBWFLSzQ3wknz5BinC9SwS3AJmF5gv2GgMESuUsktVs3utbzQZV_wCumBlgq6hBJnzknpETU4w_hbJlpx4FQAeLs9hiqAdVnrHTd9Cuh8K0TBOPGPK08Ej20n14Jylt9m
Vmn8cF12C-ExAQlpuiN5PdweaDL1Yoc8K7Bx59gf2MZP_r2yFrIGlacsBigDicAByOUNJbCMbBFSbAJJ1s7rl6ydF8QizU9F_9RUx37Xeai3WQakLybCWtVKAqsaANfrRVjm2mX_mxfpQ1W9sPS_sugloxU
romDPMHZiq3nFQ3tyUjcgr0q8tsbyWSTXzwkiPYrPMuv6ZDuvJLI3f4X07SZjvQRnxavT1s9ht6f5pyaWAsTzneuhpKhLtBek2blBqopG_GR4EI7PSDqDdcDLQkh95NiOtSeNcUCohfsJF8LbR
UbqgE8WtW5QTQGZvtJG9MpTTZj2SBeOFds1x5fMs7l4quFJhEIASiloiiQD1zooxDC3owQFfNPW3vvNE9t2Kpgu0SOg4IZRPqqOzro2-XpEm44DpClXbLZ5MeGWS5-djmpr9IS-6ESuJxMl-e8V9-mNOr1T4r_vsdBOCBT4T5ks3z25XURzKDq_a-DAyaP90suDyf9X9ADncp5Y3aC5Gic5ZCtLIRvPM5Y0chEKLB0WesZLk7lblPwULw2IBrnpt0MsZkqj_3Nlu58PD7d-uoo5vfbBW8ws1bguvjsoHWbX5lcKyrwgweun_gfvg_lY2ESP4RPHNq7RDHW_4p7XWDoXc051EP8zAQABDcaeqOGzqRL9j3FCJsgnuPhal7WDXcjjC4eOBkq6DrYSqWDoc1q__67udAyVv
Kc8cltbaLEKd004USwPjY6y_ka_EDylzFnympcfWCaag84SfpAGKQZ7UBK1c4c8w4w1VVcmDU-P4_avqTPEvPo4DdL_dVb-9EwBY27A1clamDD0gJagDJYxAY5wOP-u1u3CNrAwLoGVmjC3WtBDh_QBDblYDK7aBWah2qjG-xV3BezonHRljX22LD9dNu2Lp4n709XoDoWhWMYFEx6yLvNsltpXHlyp4lVHNylpVJ5fenyhoRLZC-

Figure 30 Links available on the website

You can click on each of them or scan each of them for more details

2.5 BEHAVIOUR

The menu contains information about the Security Headers, the Cookies, and the JavaScript global variables used by the website.



Submitted URL: http://out.reddit.com/
Effective URL: https://www.reddit.com/
Submission: On October 26 via manual (October 26th 2022, 8:01:26 am UTC) from AT — Scanned from DE

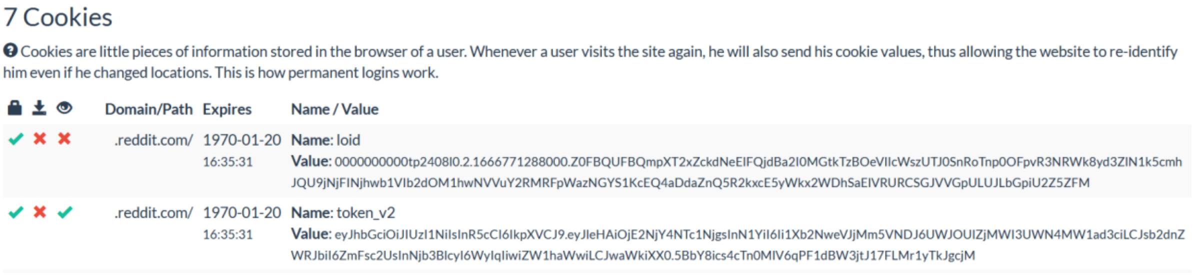
30 JavaScript Global Variables

These are the non-standard "global" variables defined on the `window` object. These can be helpful in identifying possible client-side frameworks and code.

object | 0 — object | 1 — object | onbeforeinput — object | oncontextlost — object | oncontextrestored — function | structuredClone — object | launchQueue

function | getScreenDetails — function | queryLocalFonts — object | navigation — boolean | __SUPPORTS_TIMING_API — function | __perfMark — boolean | _

Figure 31 Variable used by the website

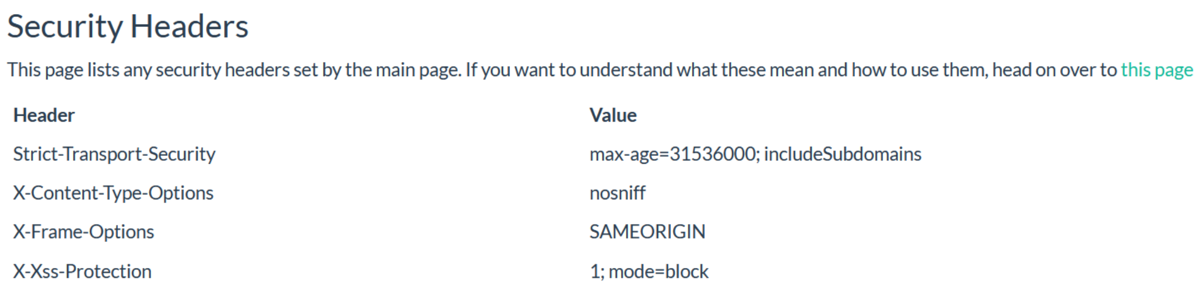


7 Cookies

Cookies are little pieces of information stored in the browser of a user. Whenever a user visits the site again, he will also send his cookie values, thus allowing the website to re-identify him even if he changed locations. This is how permanent logins work.

🔒	⤓	👁	Domain/Path	Expires	Name / Value
✓	✗	✗	.reddit.com/	1970-01-20 16:35:31	**Name**: loid **Value**: 0000000000tp2408l0.2.1666771288000.Z0FBQUFBQmpXT2xZckdNeElFQjdBa2l0MGtkTzBOeVllcWszUTJ0SnRoTnp0OFpvR3NRWk8yd3ZIN1k5cmhJQU9jNjFINjhwb1Vlb2dOM1hwNVVuY2RMRFpWazNGYS1KcEQ4aDdaZnQ5R2kxcE5yWkx2WDhSaElVRURCSGJVVGpULUJLbGpiU2Z5ZFM
✓	✗	✓	.reddit.com/	1970-01-20 16:35:31	**Name**: token_v2 **Value**: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2NjY4NTc1NjgsInN1YiI6Ii1Xb2NweVJjMm5VNDJ6UWJOUlZjMWI3UWN4MW1ad3ciLCJsb2dnZWRJbiI6ZmFsc2UsInNjb3BlcyI6WylqIiwiZW1haWwiLCJwaWkiXX0.5BbY8ics4cTn0MIV6qPF1dBW3jtJ17FLMr1yTkJgcjM

Figure 32 Cookies used by the website



Security Headers

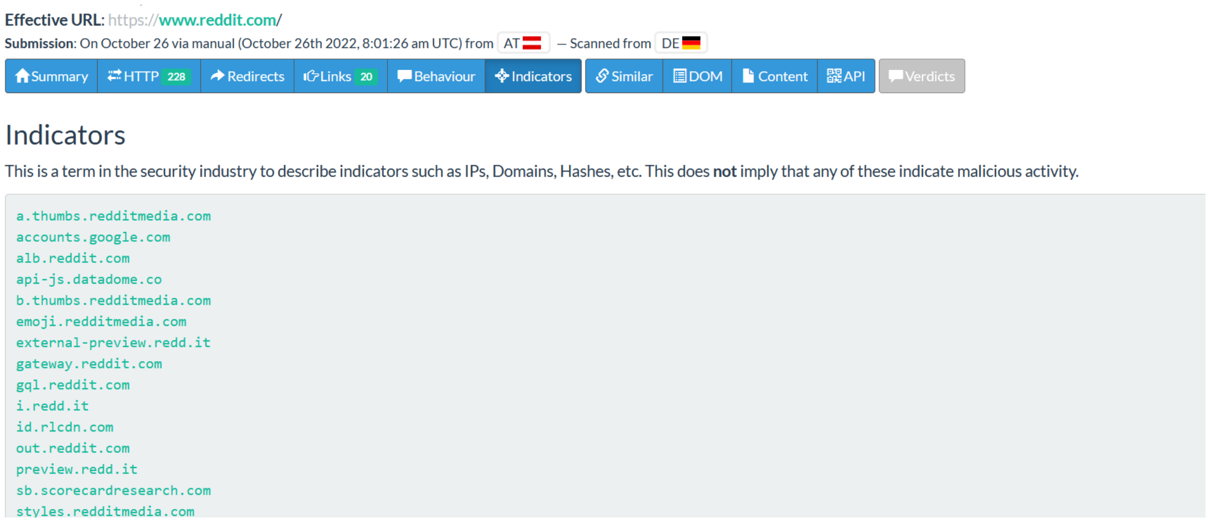
This page lists any security headers set by the main page. If you want to understand what these mean and how to use them, head on over to this page

Header	Value
Strict-Transport-Security	max-age=31536000; includeSubdomains
X-Content-Type-Options	nosniff
X-Frame-Options	SAMEORIGIN
X-Xss-Protection	1; mode=block

Figure 33 Security headers

2.6 INDICATORS

This menu contains all the domains, IP addresses, and hashes used by the websites.



Effective URL: https://www.reddit.com/

Submission: On October 26 via manual (October 26th 2022, 8:01:26 am UTC) from AT — Scanned from DE

Indicators

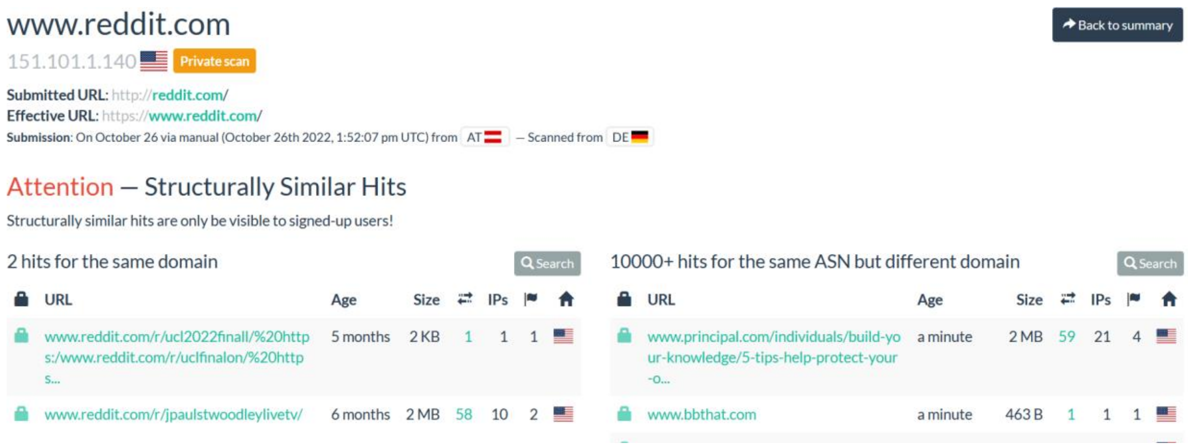
This is a term in the security industry to describe indicators such as IPs, Domains, Hashes, etc. This does **not** imply that any of these indicate malicious activity.

```
a.thumbs.redditmedia.com
accounts.google.com
alb.reddit.com
api-js.datadome.co
b.thumbs.redditmedia.com
emoji.redditmedia.com
external-preview.redd.it
gateway.reddit.com
gql.reddit.com
i.redd.it
id.rlcdn.com
out.reddit.com
preview.redd.it
sb.scorecardresearch.com
styles.redditmedia.com
```

Figure 34 Indicators used by the website

2.7 SIMILAR

This menu shows some information about the URLs, ASN numbers, IP address, and domains scanned on the website.



www.reddit.com

151.101.1.140 🇺🇸 Private scan

Submitted URL: http://reddit.com/

Effective URL: https://www.reddit.com/

Submission: On October 26 via manual (October 26th 2022, 1:52:07 pm UTC) from AT — Scanned from DE

Attention — Structurally Similar Hits

Structurally similar hits are only be visible to signed-up users!

2 hits for the same domain

🔒	URL	Age	Size	⇄	IPs	⚑	🏠
🔒	www.reddit.com/r/ucl2022finall/%20https:/www.reddit.com/r/uclfinalon/%20https...	5 months	2 KB	1	1	1	🇺🇸
🔒	www.reddit.com/r/jpaulstwoodleylivetv/	6 months	2 MB	58	10	2	🇺🇸

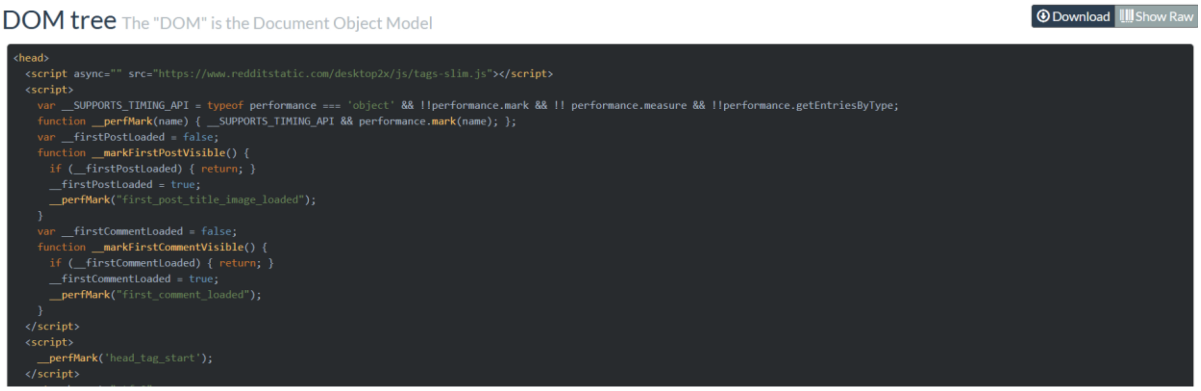
10000+ hits for the same ASN but different domain

🔒	URL	Age	Size	⇄	IPs	⚑	🏠
🔒	www.principal.com/individuals/build-your-knowledge/5-tips-help-protect-your-o...	a minute	2 MB	59	21	4	🇺🇸
🔒	www.bbthat.com	a minute	463 B	1	1	1	🇺🇸

Figure 35 Websites with some similarities

2.8 DOM

This menu is very useful as it has the whole map of the website such as the scripts used by the website, the HTML code used by the website, and others.



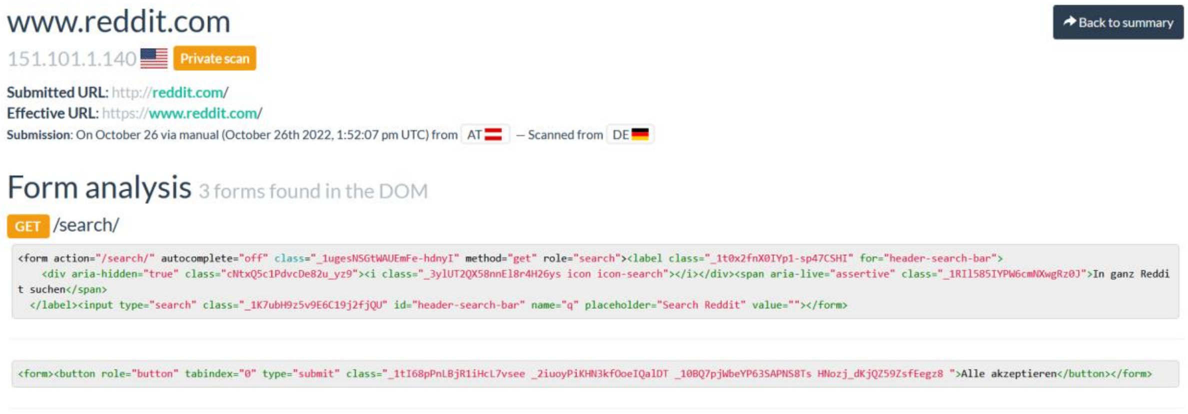
DOM tree The "DOM" is the Document Object Model

```
<head>
  <script async="" src="https://www.redditstatic.com/desktop2x/js/tags-slim.js"></script>
  <script>
    var __SUPPORTS_TIMING_API = typeof performance === 'object' && !!performance.mark && !! performance.measure && !!performance.getEntriesByType;
    function __perfMark(name) { __SUPPORTS_TIMING_API && performance.mark(name); };
    var __firstPostLoaded = false;
    function __markFirstPostVisible() {
      if (__firstPostLoaded) { return; }
      __firstPostLoaded = true;
      __perfMark("first_post_title_image_loaded");
    }
    var __firstCommentLoaded = false;
    function __markFirstCommentVisible() {
      if (__firstCommentLoaded) { return; }
      __firstCommentLoaded = true;
      __perfMark("first_comment_loaded");
    }
  </script>
  <script>
    __perfMark('head_tag_start');
  </script>
```

Figure 36 Website map (structure and content of a document on the web)

2.9 CONTENT

the Form (Google search for Form object DOM) used in DOM is available.



www.reddit.com

151.101.1.140 Private scan

Submitted URL: http://reddit.com/

Effective URL: https://www.reddit.com/

Submission: On October 26 via manual (October 26th 2022, 1:52:07 pm UTC) from AT — Scanned from DE

Form analysis 3 forms found in the DOM

GET /search/

```
<form action="/search/" autocomplete="off" class="_1ugesNSGtWAUEmFe-hdnyI" method="get" role="search"><label class="_1t0x2fnX0IYp1-sp47CSHI" for="header-search-bar">
    <div aria-hidden="true" class="cNtxQ5c1PdvcDe82u_yz9"><i class="_3ylUT2QX58nnEl8r4H26ys icon icon-search"></i></div><span aria-live="assertive" class="_1RI1585IYPW6cmNXwgRz0J">In ganz Reddit suchen</span>
  </label><input type="search" class="_1K7ubH9z5v9E6C19j2fjQU" id="header-search-bar" name="q" placeholder="Search Reddit" value=""></form>
```

```
<form><button role="button" tabindex="0" type="submit" class="_1tI68pPnLBjR1iHcL7vsee _2iuoyPiKHN3kfOoeIQalDT _10BQ7pjWbeYP63SAPNS8Ts HNozj_dKjQZ59ZsfEegz8 ">Alle akzeptieren</button></form>
```

Figure 37 Content

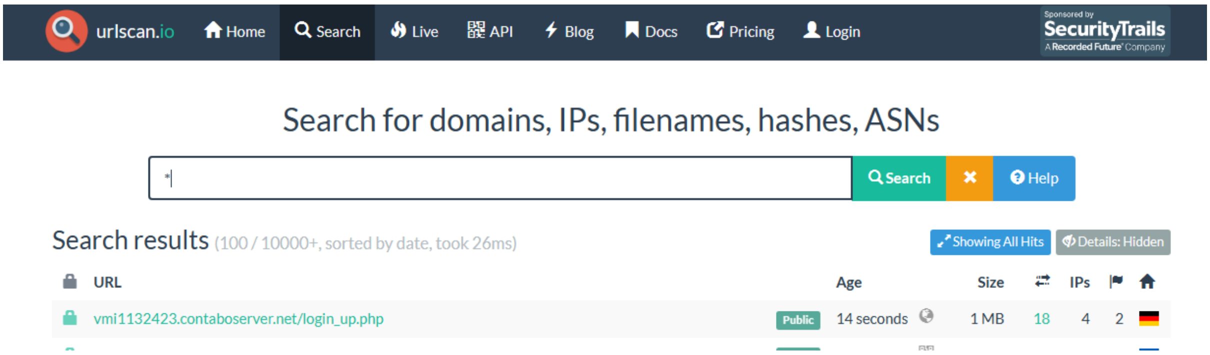
2.10 API

The API used by URLSCAN to get the information from the servers

3 SEARCHES

URLSCAN can help to perform different types of searches to find more information about an indicator such as IP address, domain, file, hash, ASN number, and others.

Click on the “**Search**” button.



Search for domains, IPs, filenames, hashes, ASNs

*|

Search ✖ Help

Search results (100 / 10000+, sorted by date, took 26ms)

Showing All Hits | Details: Hidden

🔒	URL		Age	Size	⇄	IPs	⚑	⌂
🔒	vmi1132423.contaboserver.net/login_up.php	Public	14 seconds	1 MB	18	4	2	🇩🇪

Figure 38 Searches types available

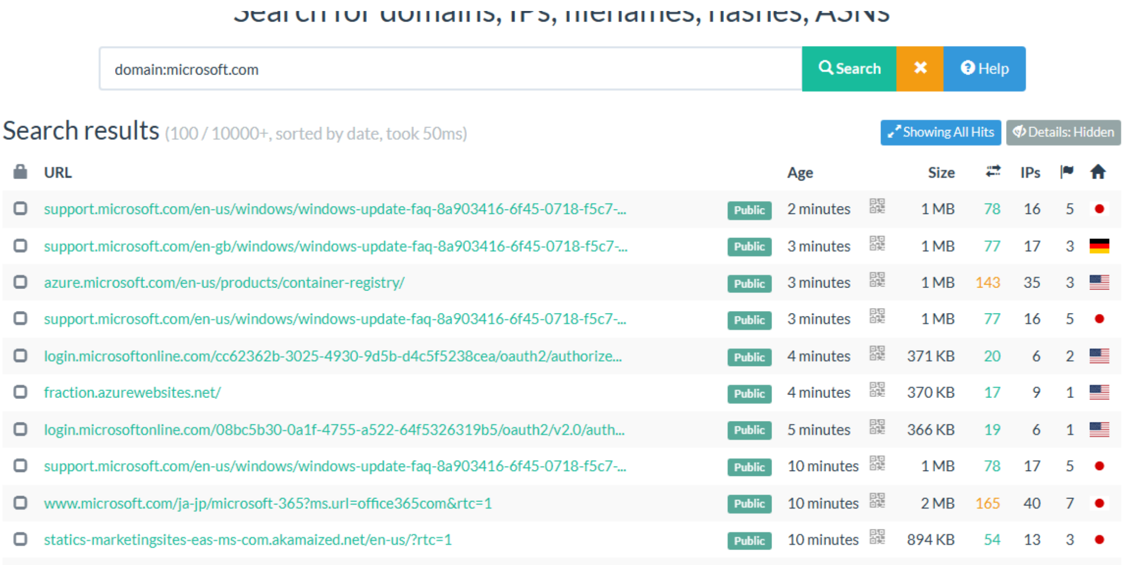
It is very important to first read the documentation. Click on the "**Help**" button to read about how to perform different searches.

Let's give some examples of queries that we can perform in the Search menu.

- **Example 1: Search for the domain**

If you want to find more information about a specific domain such as how the domain looked before and the connection between the domain with others domains or websites, you can use the "domain:" query. For this purpose, let's adopt the website microsoft.com.

[Search - urlscan.io]



Search for domains, IPs, filenames, hashes, ASNs

domain:microsoft.com

Search ✖ Help

Search results (100 / 10000+, sorted by date, took 50ms)

Showing All Hits | Details: Hidden

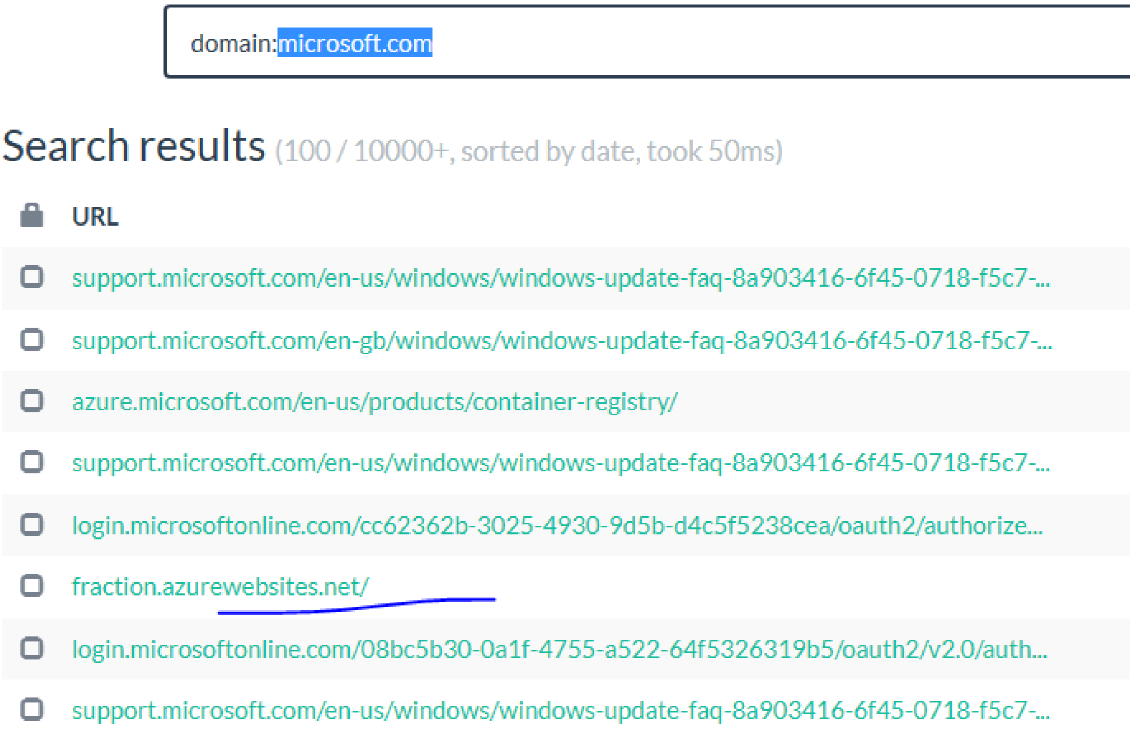
🔒	URL		Age	Size	⇄	IPs	⚑	⌂
□	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	2 minutes	1 MB	78	16	5	●
□	support.microsoft.com/en-gb/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	3 minutes	1 MB	77	17	3	🇩🇪
□	azure.microsoft.com/en-us/products/container-registry/	Public	3 minutes	1 MB	143	35	3	🇺🇸
□	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	3 minutes	1 MB	77	16	5	●
□	login.microsoftonline.com/cc62362b-3025-4930-9d5b-d4c5f5238cea/oauth2/authorize...	Public	4 minutes	371 KB	20	6	2	🇺🇸
□	fraction.azurewebsites.net/	Public	4 minutes	370 KB	17	9	1	🇺🇸
□	login.microsoftonline.com/08bc5b30-0a1f-4755-a522-64f5326319b5/oauth2/v2.0/auth...	Public	5 minutes	366 KB	19	6	1	🇺🇸
□	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	10 minutes	1 MB	78	17	5	●
□	www.microsoft.com/ja-jp/microsoft-365?ms.url=office365com&rtc=1	Public	10 minutes	2 MB	165	40	7	●
□	statics-marketingsites-eas-ms-com.akamaized.net/en-us/?rtc=1	Public	10 minutes	894 KB	54	13	3	●

Figure 39 Find a connection with other domains

Figure 38 shows the results of the search, in particular, the domain Microsoft.com with different subdomains related to Microsoft.com and other domains or websites where Microsoft.com was mentioned following along with the time and the location it was scanned.

If you click on each link where Microsoft.com is mentioned, you can see how the domain was at the time scanned. This technique can also help you as an analyst to find out how the domain looked in the past. Many phishing websites changed the website interface after abusing many people over the internet so this technic can reveal such activity.

As you see, they are some domains or subdomains where Microsoft.com is not mentioned, therefore, we need to find out the relation between Microsoft.com and the domain.



domain:microsoft.com

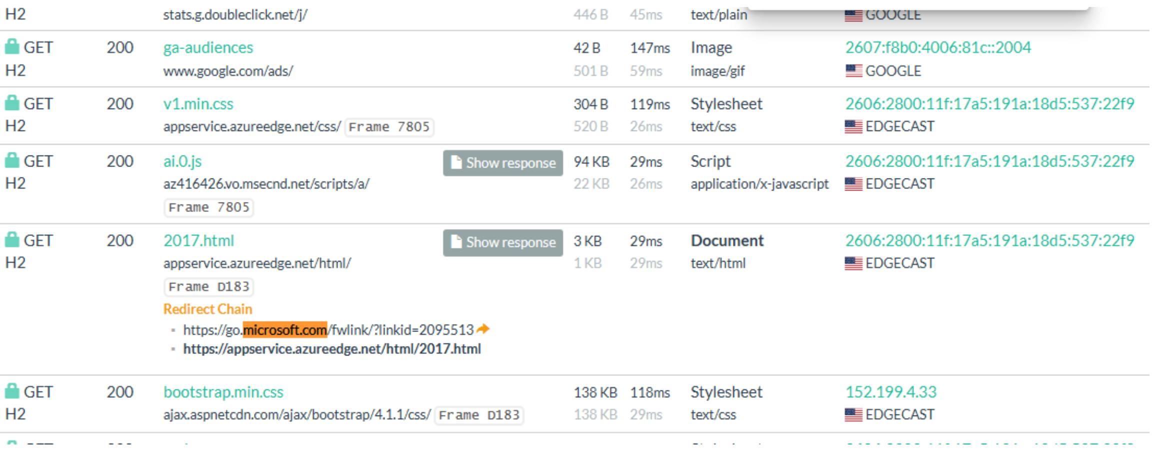
Search results (100 / 10000+, sorted by date, took 50ms)

URL

- support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...
- support.microsoft.com/en-gb/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...
- azure.microsoft.com/en-us/products/container-registry/
- support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...
- login.microsoftonline.com/cc62362b-3025-4930-9d5b-d4c5f5238cea/oauth2/authorize...
- fraction.azurewebsites.net/
- login.microsoftonline.com/08bc5b30-0a1f-4755-a522-64f5326319b5/oauth2/v2.0/auth...
- support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...

Figure 40 Relationship between domains

Click on fraction.azurewebsites.net, go to HTTP transaction, search for Microsoft.com



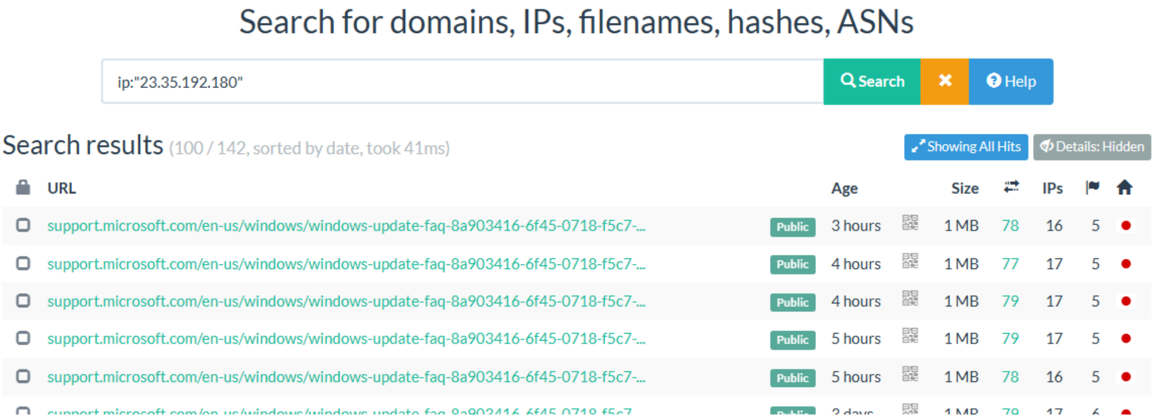
H2		stats.g.doubleclick.net/j/		446 B	45ms	text/plain	GOOGLE
GET H2	200	ga-audiences www.google.com/ads/		42 B 501 B	147ms 59ms	Image image/gif	2607:f8b0:4006:81c::2004 GOOGLE
GET H2	200	v1.min.css appservice.azureedge.net/css/ Frame 7805		304 B 520 B	119ms 26ms	Stylesheet text/css	2606:2800:11f:17a5:191a:18d5:537:22f9 EDGECAST
GET H2	200	ai.0.js az416426.vo.msecnd.net/scripts/a/ Frame 7805	Show response	94 KB 22 KB	29ms 26ms	Script application/x-javascript	2606:2800:11f:17a5:191a:18d5:537:22f9 EDGECAST
GET H2	200	2017.html appservice.azureedge.net/html/ Frame D183 Redirect Chain • https://go.microsoft.com/fwlink/?linkid=2095513 • https://appservice.azureedge.net/html/2017.html	Show response	3 KB 1 KB	29ms 29ms	Document text/html	2606:2800:11f:17a5:191a:18d5:537:22f9 EDGECAST
GET H2	200	bootstrap.min.css ajax.aspnetcdn.com/ajax/bootstrap/4.1.1/css/ Frame D183		138 KB 138 KB	118ms 29ms	Stylesheet text/css	152.199.4.33 EDGECAST

Figure 41 Relationship between domains 2

As you can see, Microsoft.com is used as a redirect chain. This technic is often used by the threat actor to hide their activities and it can be also used to find the correlation between the domains.

- **Example 2: Search for IPs**

Search - urlscan.io



Search for domains, IPs, filenames, hashes, ASNs

ip:"23.35.192.180"

Search results (100 / 142, sorted by date, took 41ms)

🔒	URL		Age		Size	⇄	IPs	⚑	⌂
☐	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	3 hours		1 MB	78	16	5	●
☐	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	4 hours		1 MB	77	17	5	●
☐	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	4 hours		1 MB	79	17	5	●
☐	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	5 hours		1 MB	79	17	5	●
☐	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	5 hours		1 MB	78	16	5	●
☐	support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7	Public	3 days		1 MB	79	17	6	●

Figure 42 Using different types of searches

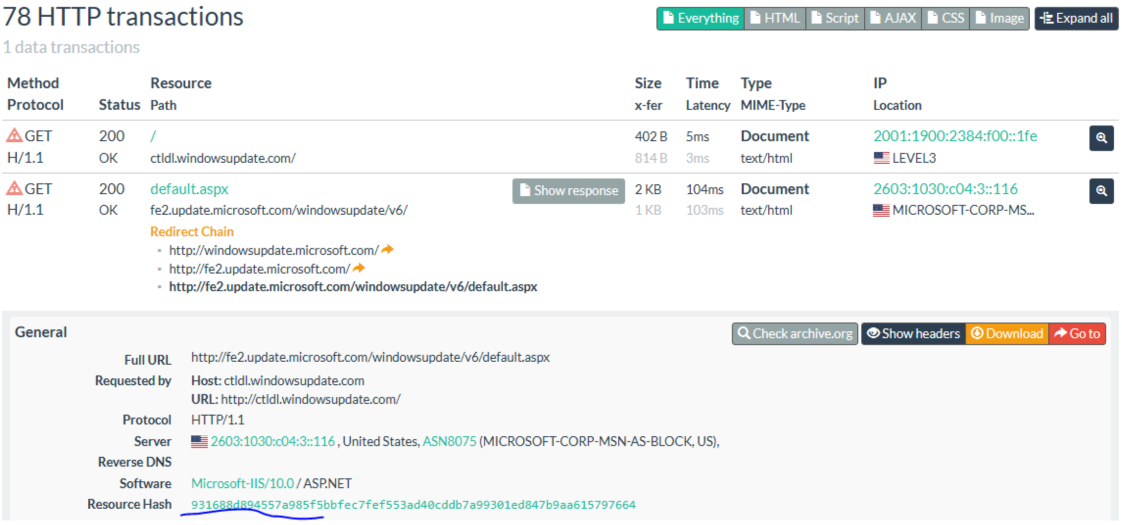
As you see in figure 41, we entered the IP address 23.35.192.180 and we got the domains and subdomains behind the IP address. This technique can be used to find phishing-related domains behind an IP address.

- **Example 3: Search for Hashes**

The hash can help you to make a correlation between the domains. Usually, the threat actor can use the same file but changed the domain, so this technic is a good one to find such activity.

For instance:

Click Microsoft.com, go to HTTP transaction, and expand one http transaction request where the hash is available.



78 HTTP transactions

1 data transactions

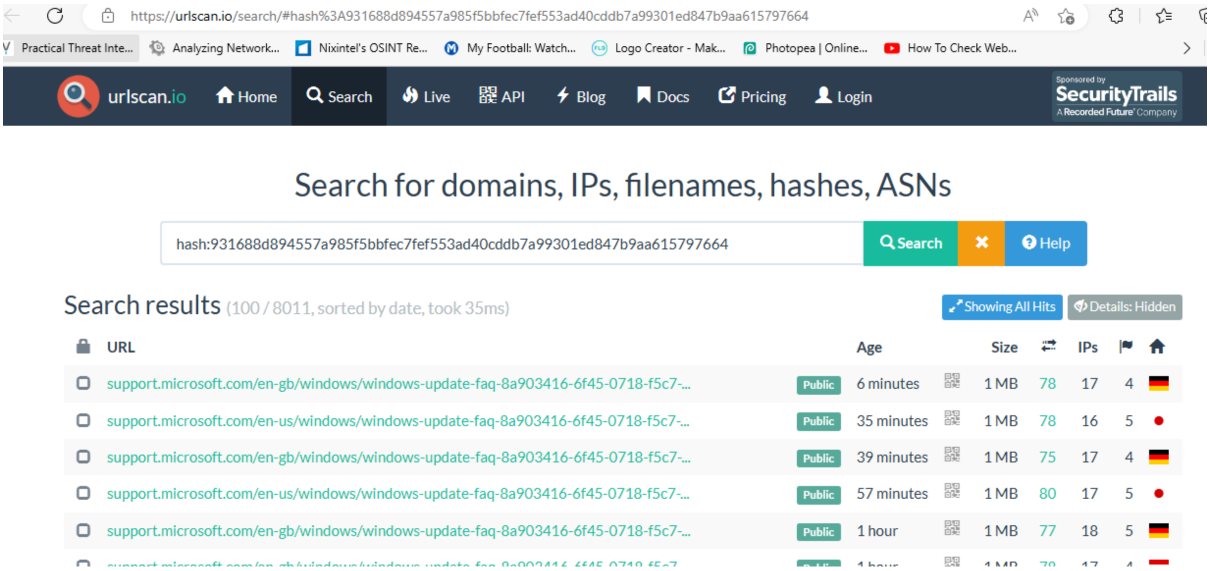
Method Protocol	Status	Resource Path	Size x-fer	Time Latency	Type MIME-Type	IP Location
GET H/1.1	200 OK	/ ctldl.windowsupdate.com/	402 B 814 B	5ms 3ms	Document text/html	2001:1900:2384:f00::1fe LEVEL3
GET H/1.1	200 OK	default.aspx fe2.update.microsoft.com/windowsupdate/v6/ Redirect Chain http://windowsupdate.microsoft.com/ http://fe2.update.microsoft.com/ http://fe2.update.microsoft.com/windowsupdate/v6/default.aspx	2 KB 1 KB	104ms 103ms	Document text/html	2603:1030:c04:3::116 MICROSOFT-CORP-MS...

General

Full URL	http://fe2.update.microsoft.com/windowsupdate/v6/default.aspx
Requested by	Host: ctldl.windowsupdate.com URL: http://ctldl.windowsupdate.com/
Protocol	HTTP/1.1
Server	2603:1030:c04:3::116 , United States, ASN8075 (MICROSOFT-CORP-MSN-AS-BLOCK, US),
Reverse DNS	
Software	Microsoft-IIS/10.0 / ASP.NET
Resource Hash	931688d894557a985f5bbfec7fef553ad40cddb7a99301ed847b9aa615797664

Figure 43 Find the connection with the domain

Over the mouse on the hash and copy the hash, click on the Search menu, and enter the query as you see in figure 42.



https://urlscan.io/search/#hash%3A931688d894557a985f5bbfec7fef553ad40cddb7a99301ed847b9aa615797664

Search for domains, IPs, filenames, hashes, ASNs

hash:931688d894557a985f5bbfec7fef553ad40cddb7a99301ed847b9aa615797664

Search results (100 / 8011, sorted by date, took 35ms)

URL		Age	Size	⇄	IPs	⚑	
support.microsoft.com/en-gb/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	6 minutes	1 MB	78	17	4	
support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	35 minutes	1 MB	78	16	5	●
support.microsoft.com/en-gb/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	39 minutes	1 MB	75	17	4	
support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	57 minutes	1 MB	80	17	5	●
support.microsoft.com/en-gb/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	1 hour	1 MB	77	18	5	

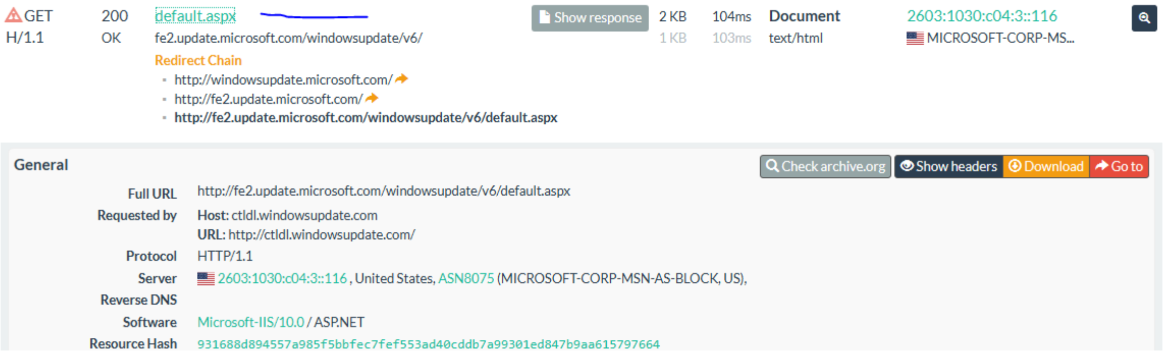
Figure 44 Search for hash in the search field

Now, we can see others websites that have used the same hash.

- **Example 4: Search for Filenames**

The same thing as we described in the previous case, the same filename can be used by the threat actor but with different domains name. We can use the same technique as we did to find the domain or website that used the filename. Be aware that the same file name does not mean that the file is the same, you need to compare the hash and also the file content to ensure that the files are the same. For instance.

From the HTTP transaction, copy the file you wish to check



GET H/1.1 | 200 OK | default.aspx | fe2.update.microsoft.com/windowsupdate/v6/ | 2 KB 1 KB | 104ms 103ms | Document text/html | 2603:1030:c04:3::116 MICROSOFT-CORP-MS...

Redirect Chain

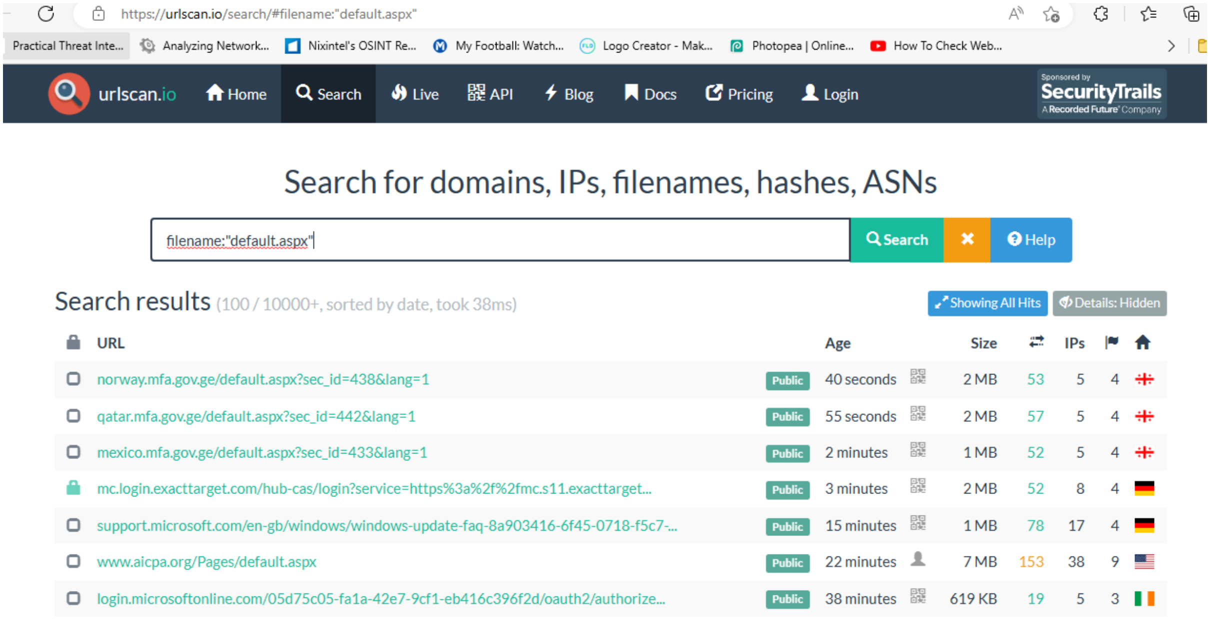
- http://windowsupdate.microsoft.com/
- http://fe2.update.microsoft.com/
- http://fe2.update.microsoft.com/windowsupdate/v6/default.aspx

General

Full URL	http://fe2.update.microsoft.com/windowsupdate/v6/default.aspx
Requested by	Host: ctldl.windowsupdate.com URL: http://ctldl.windowsupdate.com/
Protocol	HTTP/1.1
Server	2603:1030:c04:3::116 , United States, ASN8075 (MICROSOFT-CORP-MSN-AS-BLOCK, US),
Reverse DNS	
Software	Microsoft-IIS/10.0 / ASP.NET
Resource Hash	931688d894557a985f5bbfec7fef553ad40cddb7a99301ed847b9aa615797664

Figure 45 Search for hash details

Go to search, enter the query as you see in the picture below, and all the results from the search will appear.



Search for domains, IPs, filenames, hashes, ASNs

filename:"default.aspx"

Search results (100 / 10000+, sorted by date, took 38ms)

URL		Age	Size	⇄	IPs	⚑	⌂
norway.mfa.gov.ge/default.aspx?sec_id=438&lang=1	Public	40 seconds	2 MB	53	5	4	🇬🇪
qatar.mfa.gov.ge/default.aspx?sec_id=442&lang=1	Public	55 seconds	2 MB	57	5	4	🇬🇪
mexico.mfa.gov.ge/default.aspx?sec_id=433&lang=1	Public	2 minutes	1 MB	52	5	4	🇬🇪
mc.login.exacttarget.com/hub-cas/login?service=https%3a%2f%2fmc.s11.exacttarget...	Public	3 minutes	2 MB	52	8	4	🇩🇪
support.microsoft.com/en-gb/windows/windows-update-faq-8a903416-6f45-0718-f5c7-...	Public	15 minutes	1 MB	78	17	4	🇩🇪
www.aicpa.org/Pages/default.aspx	Public	22 minutes	7 MB	153	38	9	🇺🇸
login.microsoftonline.com/05d75c05-fa1a-42e7-9cf1-eb416c396f2d/oauth2/authorize...	Public	38 minutes	619 KB	19	5	3	🇮🇪

Figure 46 Search for filename details

In order to verify if the file is unique, click on the URL, and go to the HTTP transaction to compare the hash and the file content.

You can perform many types of searches using the search field. As a security guy, you should know what you are looking for before searching. The best way to learn is by practicing on a daily basis.

4 Conclusion

URLSCAN is a very amazing tool that all security guys should use to make easier their job while analyzing different information as we showed in our examples.

The tool can help you save many times as it contains many types of queries that will help you to find more information during your analysis.

If you never used it, it is time for you to start using and if you did not know the features we explained, then I suppose that you already know so enjoy.