

CEH Module 2: Assignment 1

Lab Scenario As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks

Lab Objectives:

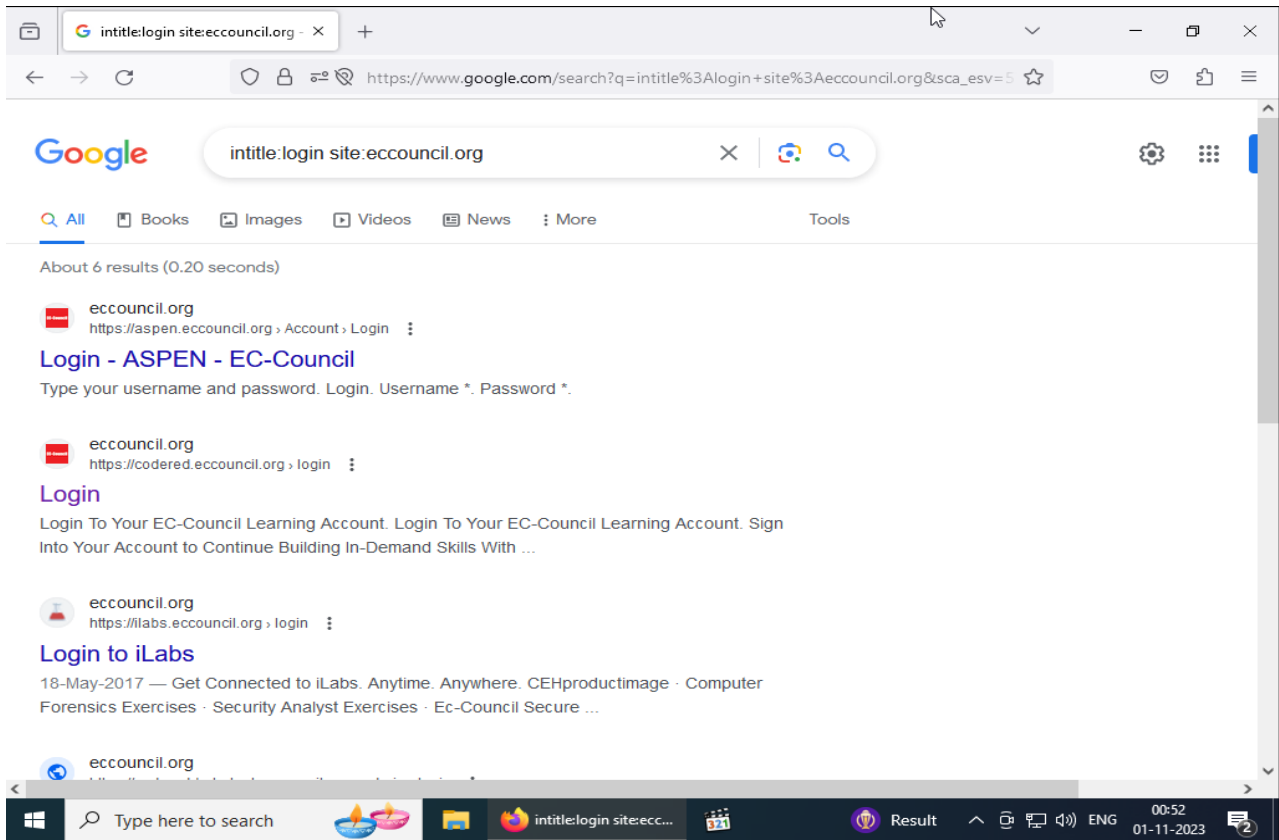
- Gather information using advanced Google hacking techniques
- Gather information from video search engines
- Gather information from FTP search engines
- Gather information from IoT search engines

It is the first assignment of the assignment 1

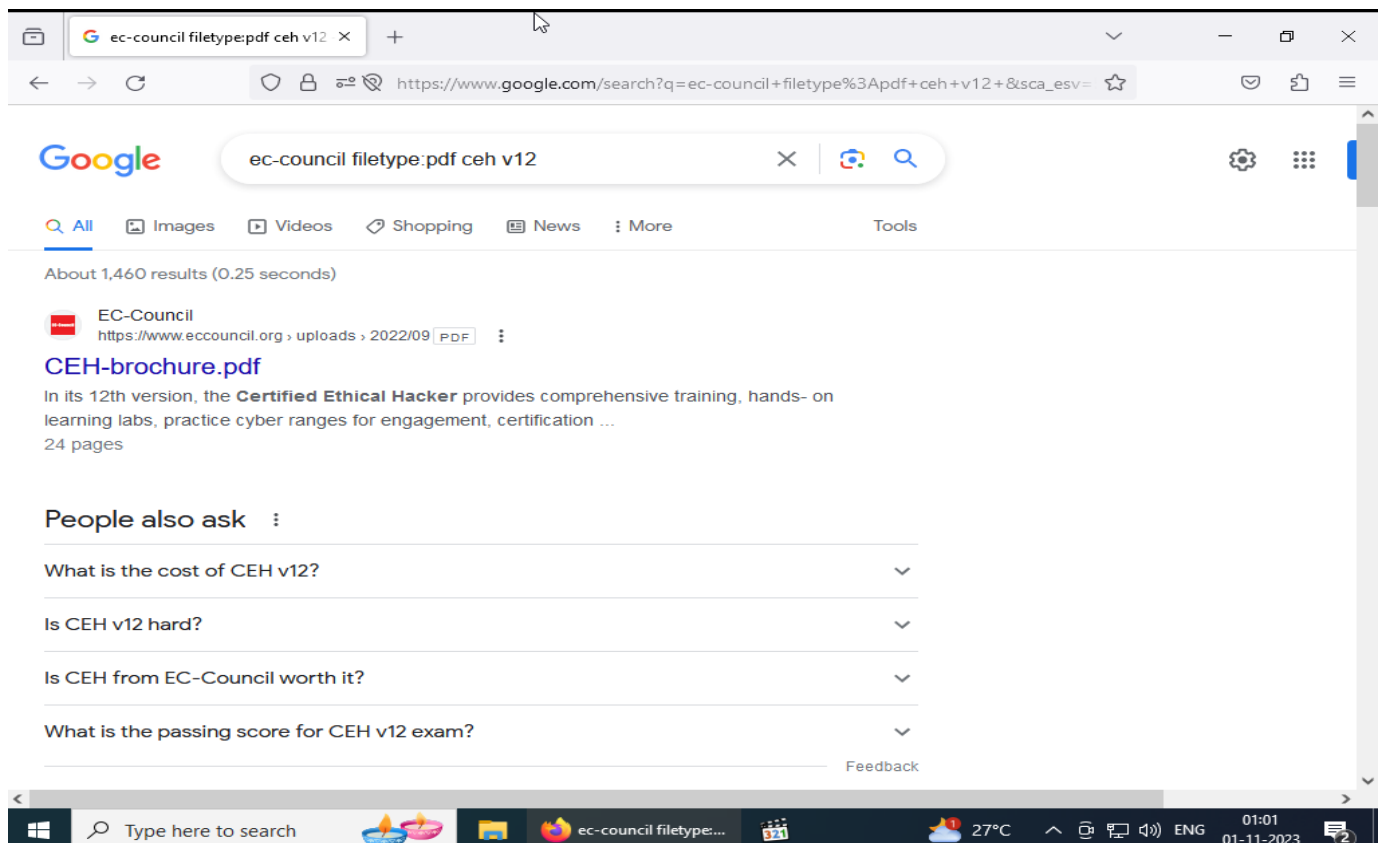
• Gather information using advanced Google hacking techniques

For the assignment I should consider a lab Environment **Windows 10 virtual machine**

1. Website name EC-Council.org
2. I found the login pages using google dorks *intitle:login site:eccouncil.org*
3. I got only 6 result



2. I Found some pdf using google dorks **ec-council filetype:pdf ceh v12**



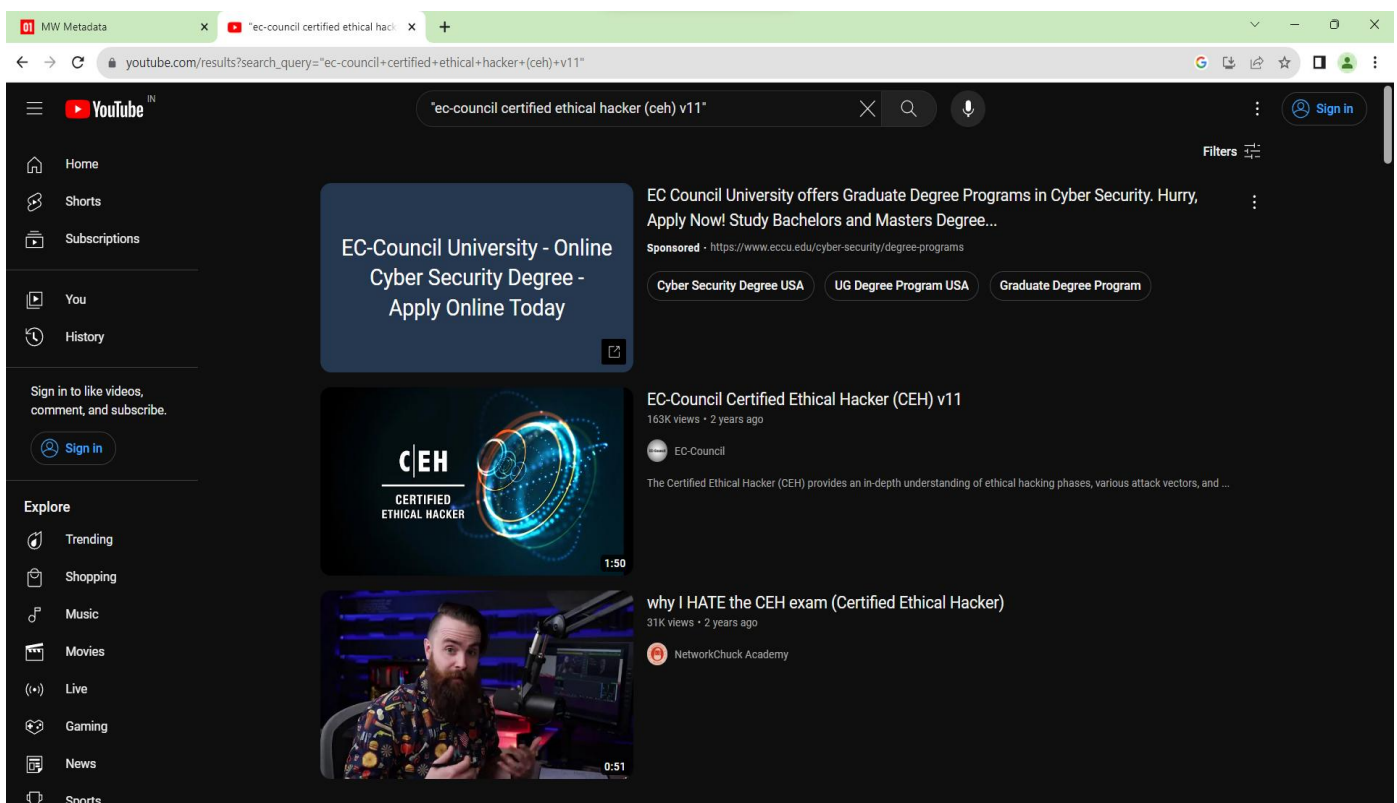
Gather information from video search engines

for video search engine I should two website

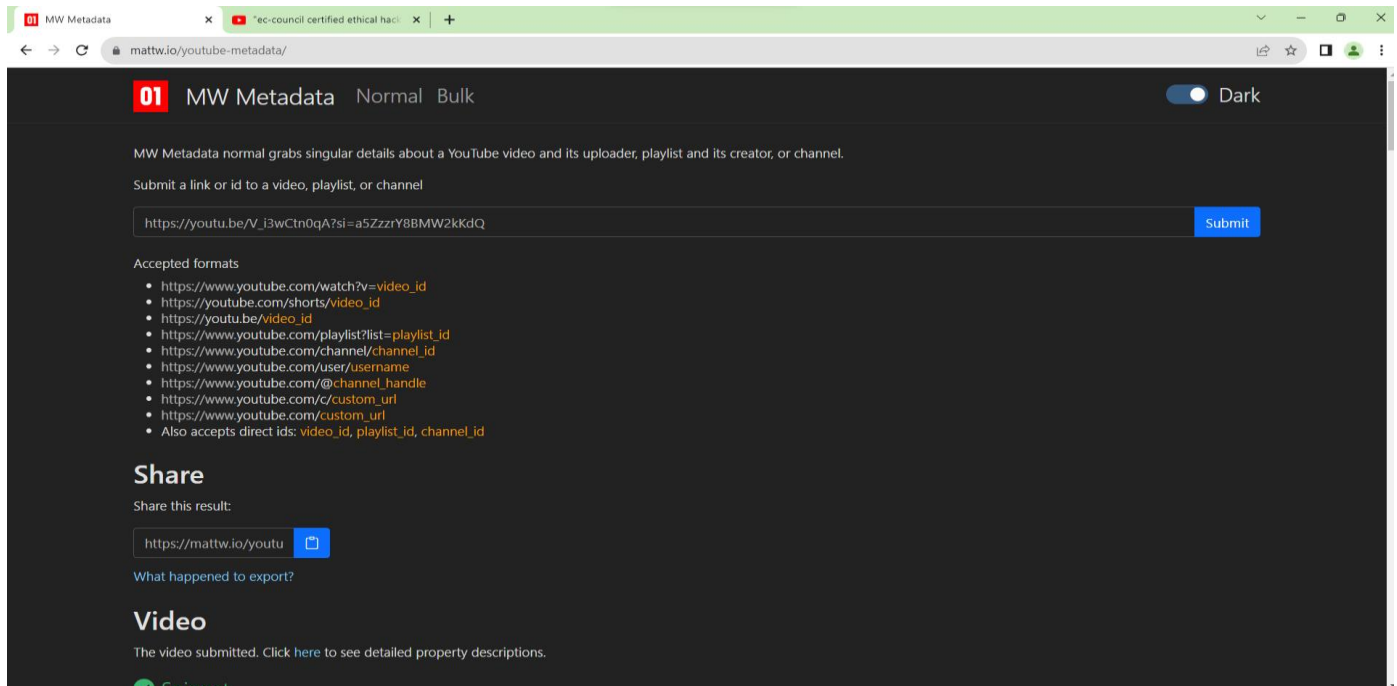
1. youtube.com
2. <https://mattw.io/youtube-metadata>

https://mattw.io/youtube-metadata/?url=https%3A%2F%2Fyoutu.be%2FV_i3wCtn0qA%3Fsi%3Da5ZzzrY8BMW2kKdQ&submit=true

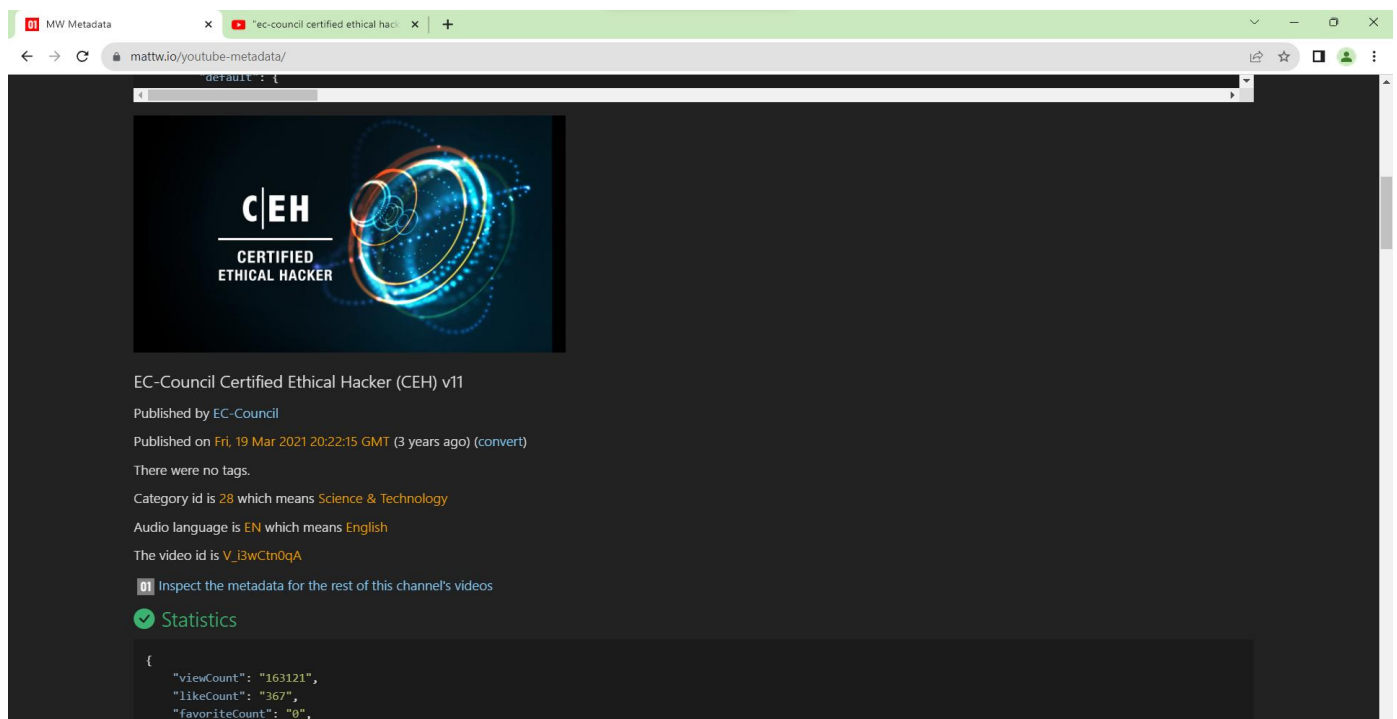
3. In youtube search “**ec-council certificate ethical hacker (CEH)v11**”



1. Copy the link of the 2nd video
2. Go to the <https://mattw.io/youtube-metadata>



3. In this website show full information of any video like video id , uploading date , organization details and many more.



- **Gather information from IoT search engines**

1. For IOT search engines I consider **shodan** website
2. Shodan one of the biggest website for gathering information of any website
3. Search amazon goto the **view report**

The screenshot displays the Shodan search engine interface. The browser's address bar shows the URL `https://www.shodan.io/search?query=amazon`. The search bar contains the text "amazon". The page shows a total of 713,618 results. On the left, there is a section for "TOP COUNTRIES" with a world map and a list of countries: United States (208,286), Japan (82,895), China (43,018), Ireland (39,870), and India (34,786). Below this is a "TOP PORTS" section showing port 80 with 145,450 results. The main content area displays a search result for "301 Moved Permanently" from the IP address 13.107.213.57, which belongs to staging.www.brplynx.com. The result includes an SSL certificate issued by DigiCert TLS RSA SHA256 2020 CA1. The certificate details show it was issued to staging.www.brplynx.com and is valid until November 1, 2023. The result also shows the HTTP status "301 Moved Permanently" and the location `http://staging.www.brplynx.com/gb/en/`. The Windows taskbar at the bottom shows the time as 08:01 on 01-11-2023.

TOTAL RESULTS
713,618

TOP COUNTRIES

United States 208,286
Japan 82,895
China 43,018
Ireland 39,870
India 34,786
[More...](#)

TOP PORTS
80 145,450

301 Moved Permanently

13.107.213.57
staging.www.brplynx.com
Microsoft Corporation
United States, Redmond

SSL Certificate

Issued By:
|- Common
Name:
DigiCert TLS
RSA SHA256
2020 CA1

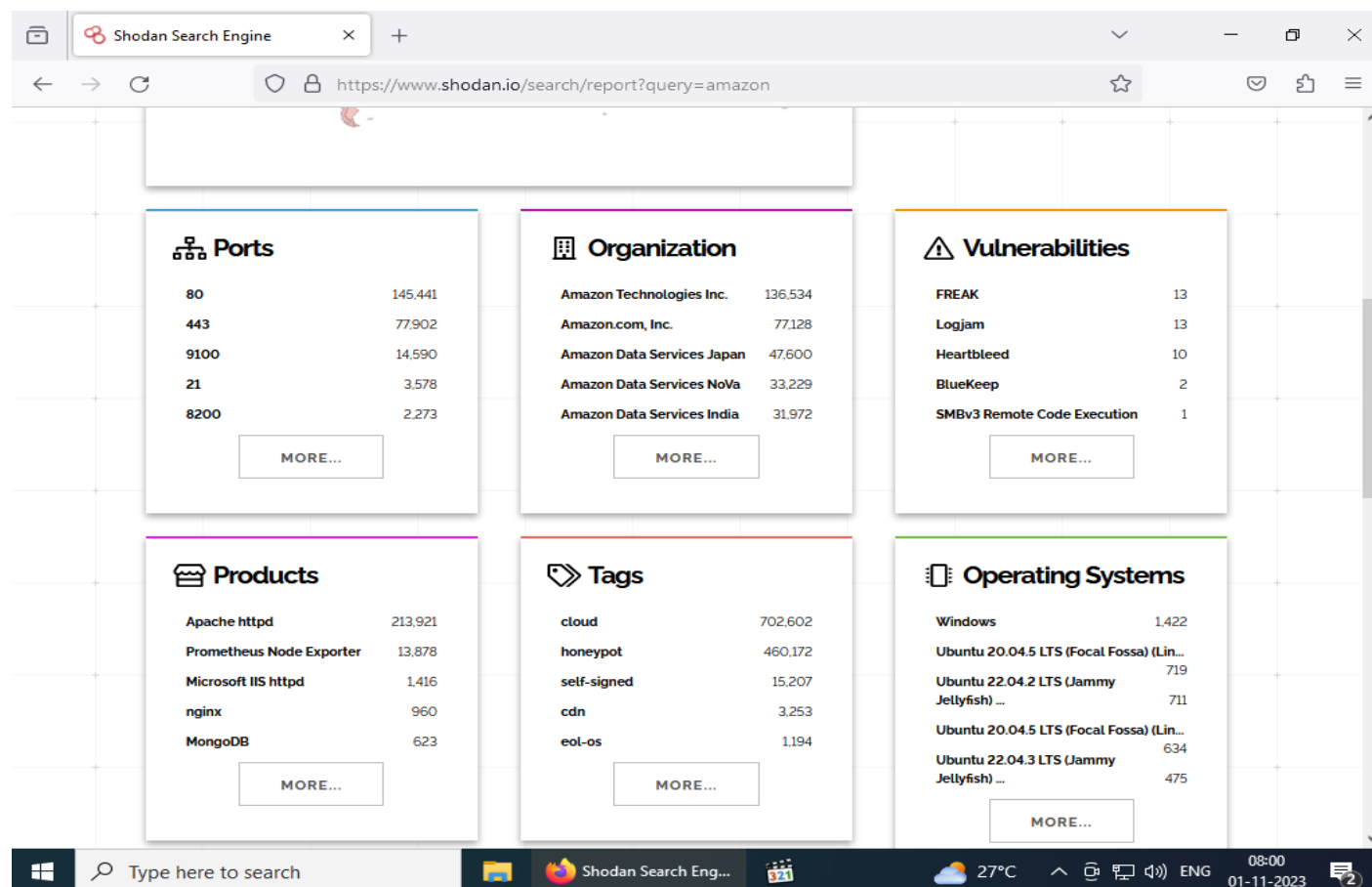
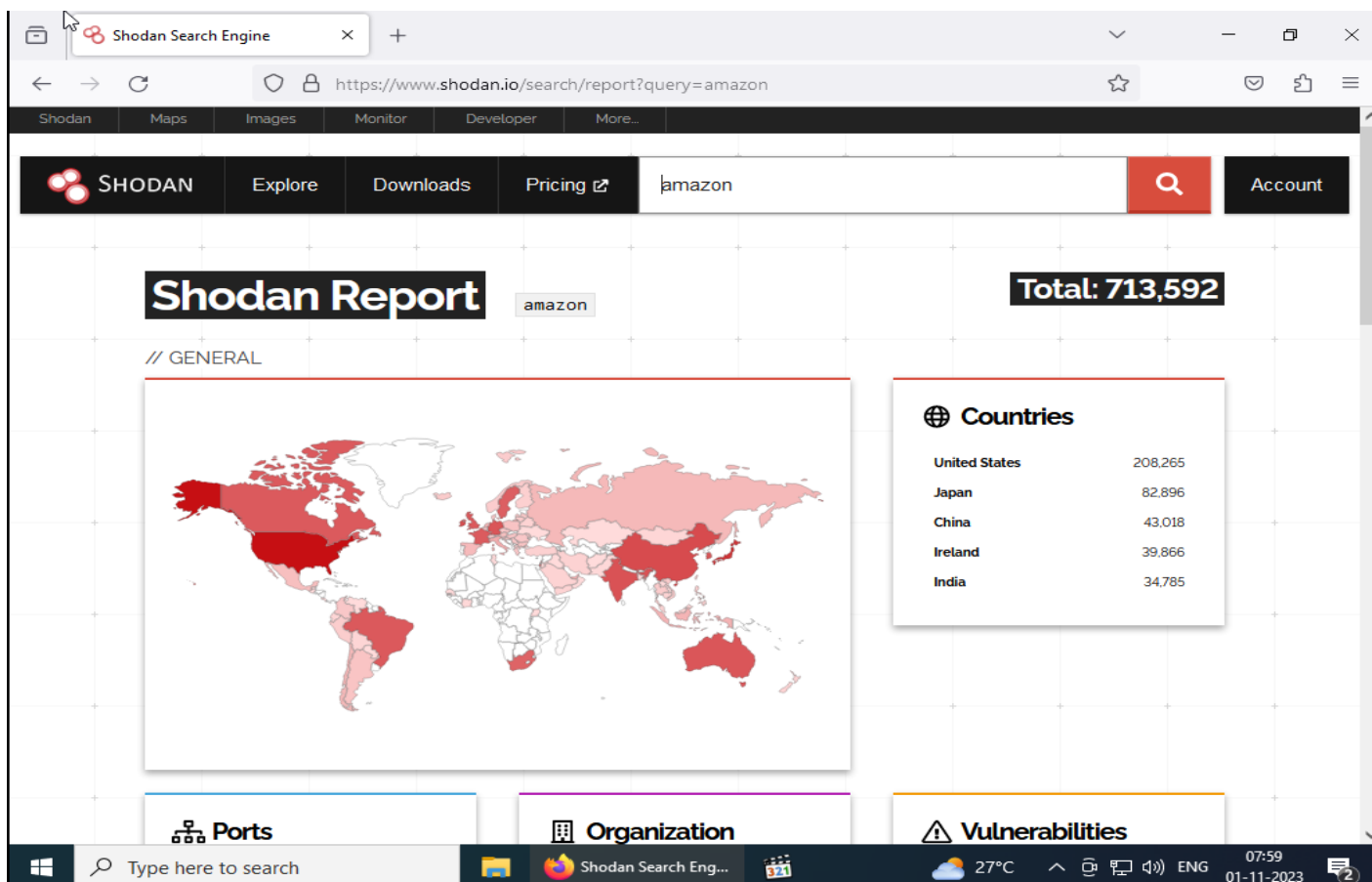
Issued To:
|- Common
Name:
staging.www.brplynx.com

|- Organization:
Microsoft Corporation

Supported SSL Versions:

HTTP/1.1 301 Moved Permanently
Cache-Control: max-age=300
Content-Length: 245
Content-Type: text/html; charset=iso-8859-1
Expires: Wed, 01 Nov 2023 02:32:08 GMT
Accept-Ranges: bytes
Age: 0
Location: http://staging.www.brplynx.com/gb/en/
Set-Cookie: affinity="dfb2bd7793623e06"; Path=/; Htt...

2023-11-01T02:32:00.437819



Shodan Search Engine

https://www.shodan.io/search/report?query=amazon

// HTTP INSIGHTS

Website Titles

301 Moved Permanently	13,691
Test Page for the Apache HTTP Server	11,165
...	...
Welcome	8,698
302 Found	8,225
Test Page for the Apache HTTP Server	7,370
...	...

MORE...

Web Technologies

jQuery	39,513
Bootstrap	24,302
PHP	10,579
Amazon Web Services	10,158
Google Analytics	8,338

MORE...

Protocol Versions

http/1.1	23,311
h2	21,657
http/1.0	4
spdy/2	1
spdy/3	1

MORE...

// SSL INSIGHTS

SSL/ TLS Versions

tlsv1.2	131,210
tlsv1.1	110,809
tlsv1	109,422
tlsv1.3	11,088
sslv3	692

MORE...

JARM Fingerprints

2ad2ad0000000022c2ad2ad2ad1fabbc2...	55,106
29d29d00029d29d21c29d29d29dab965d4...	17,332
29d29d00029d29d21c29d29d29df877566...	10,960
2ad2ad16d2ad2ad22c2ad2ad2adc7639a2...	9,141
05d02d20d21d20d05c05d02d05d20d74cf65...	7,079

MORE...

JA3S Fingerprints

0debd3853f330c574b05e0b6d882dc27	54,701
e35df3e00ca4ef31d42b34bebaa2f86e	23,803
03788d8896c247631764a250db971b74	22,203
303951d4c50efb2e991652225a6f02b1	12,623
6c2811f7ba8e88604ea41a2bf9fa5ad7	4,306

MORE...

Type here to search

Shodan Search Eng...

27°C

08:00

01-11-2023

• Gather information from FTP search engines

1. For FTP search engine. Go to ftp website <https://www.searchftps.net/>
2. Here I am using **firefox search engine** website name **NAPALM FTP indexer**
3. Now I am going to search ftp service of Microsoft

The screenshot shows a web browser window with the NAPALM FTP Indexer search engine. The search query is "microsoft ftp". The results show four files, each with a download button and a "Last checked" timestamp. The files are:

- </mirrors/ftp.debian.org/dists/bookworm-proposed-updates/main/installer-arm64/20220917/images/device-tree/qcom/sm8350-microsoft-surface-duo2.dtb> (61.2 KB)
- </mirrors/ftp.debian.org/dists/bookworm-proposed-updates/main/installer-arm64/20220917/images/device-tree/qcom/sm8150-microsoft-surface-duo.dtb> (86.2 KB)
- </mirrors/ftp.debian.org/dists/trixie/main/installer-arm64/20230607/images/device-tree/qcom/sm8350-microsoft-surface-duo2.dtb> (61.6 KB)
- </mirrors/ftp.debian.org/dists/trixie/main/installer-arm64/20230607/images/device-tree/qcom/sm8150-microsoft-surface-duo.dtb> (86.5 KB)

Related keywords include: debian, pool, updates, deb10u1, device, ALL, mono, mirror, system, tree, ftp, libmono, primary, dists, qcom, org, cil, servers, installer, surface, microsoft, deb, rsync, arm64, pub, mirrors, security, images.

On the right side of the page, there are two advertisements. The top one is for "Aakash Fertility Centre" with a 25% discount on IVF treatment. The bottom one is for "element14" with the text "ACCESS ASSEMBLE ASPIRE".

NAPALM FTP Indexer

https://www.searchftps.net

Log In Register Submit

NAPALM FTP indexer

ftp With all the words Search

Mirrors ftp debian org dists bookworm proposed updates main installer arm64 images device tree qcom

Directory </mirrors/ftp.debian.org/dists/bookworm-proposed-updates/main/installer-arm64/20220917/images/device-tree/qcom/>

Last checked **2023-10-16 20:57**

Files **119, showing first 30**

File(s)			
sm8450-qrd.dtb	71.3 KB	DOWNLOAD	
sm8450-hdk.dtb	71.5 KB	DOWNLOAD	
sm8350-sony-xperia-sagami-pdx215.dtb	58.2 KB	DOWNLOAD	
sm8350-sony-xperia-sagami-pdx214.dtb	58.2 KB	DOWNLOAD	
sm8350-mtp.dtb	61.0 KB	DOWNLOAD	
sm8350-microsoft-surface-duo2.dtb	61.2 KB	DOWNLOAD	
sm8350-hdk.dtb	56.8 KB	DOWNLOAD	
sm8250-sony-xperia-edo-pdx206.dtb	100.8 KB	DOWNLOAD	

Type here to search

NAPALM FTP Index...

28°C

ENG

08:57

01-11-2023