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 foot printing 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:

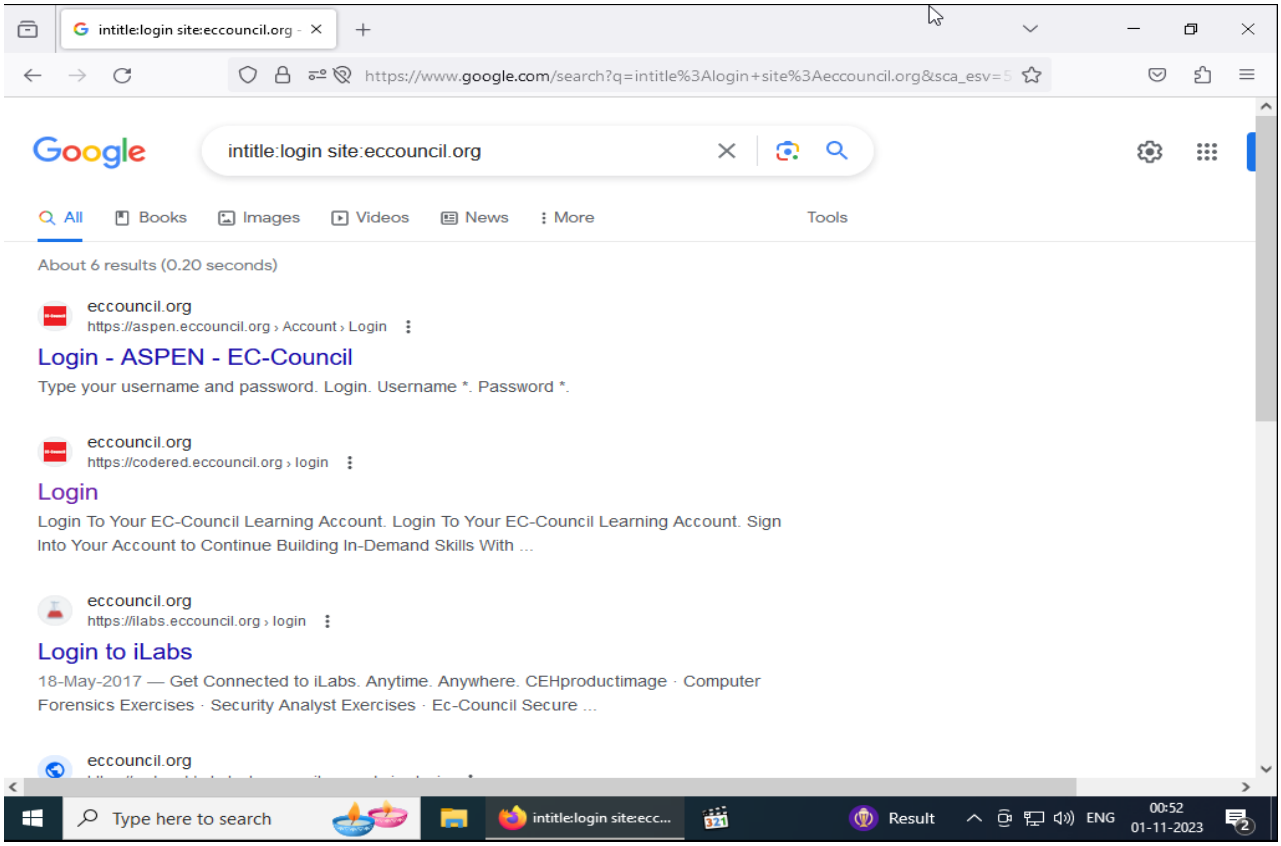
- Gather information using advanced Google hacking techniques
- Gather information from video search engines
- Gather information from FTP search engines
- Gather information from IoT search engines

It is the first assignment of the assignment 1

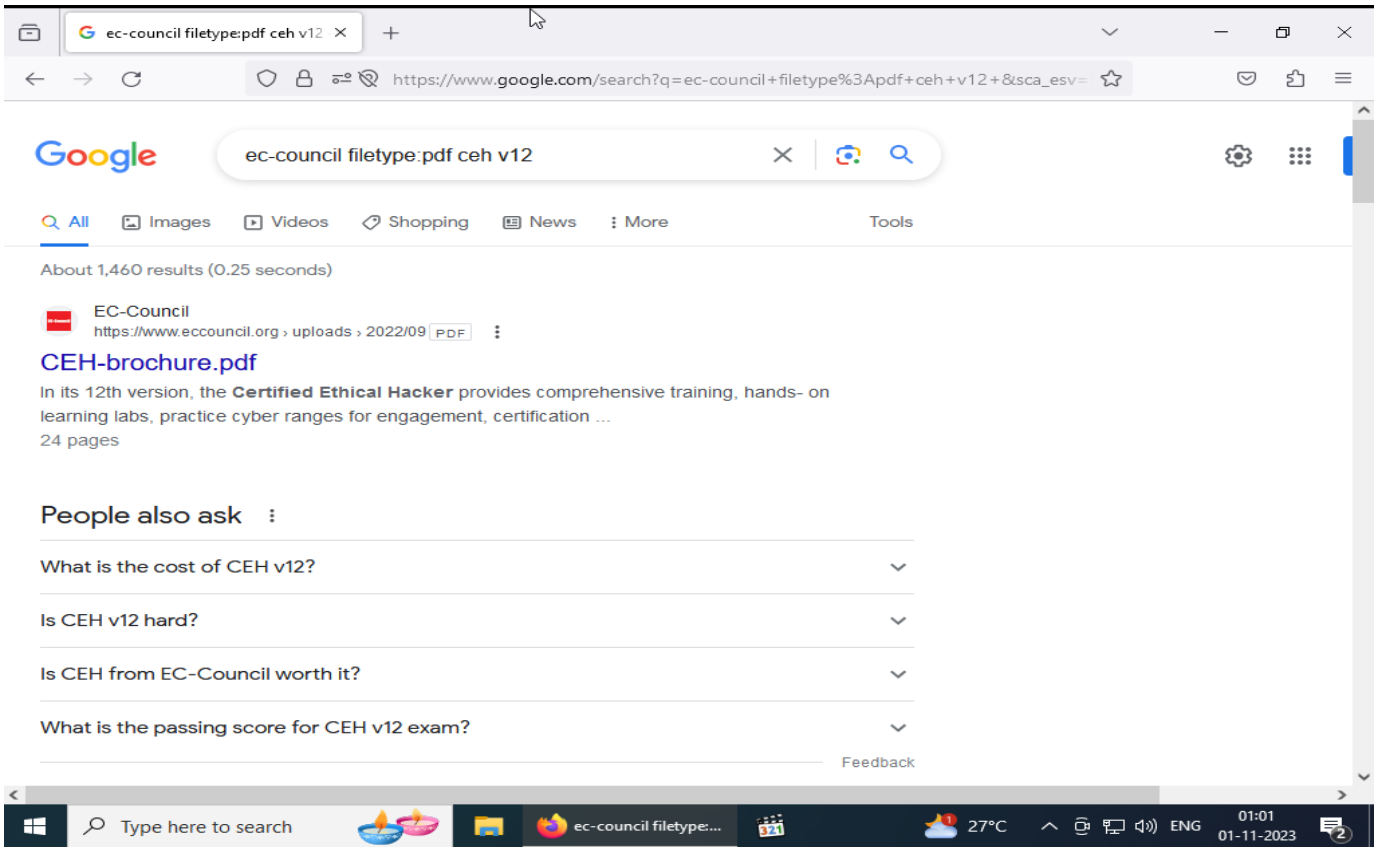
• Gather information using advanced Google hacking techniques

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**

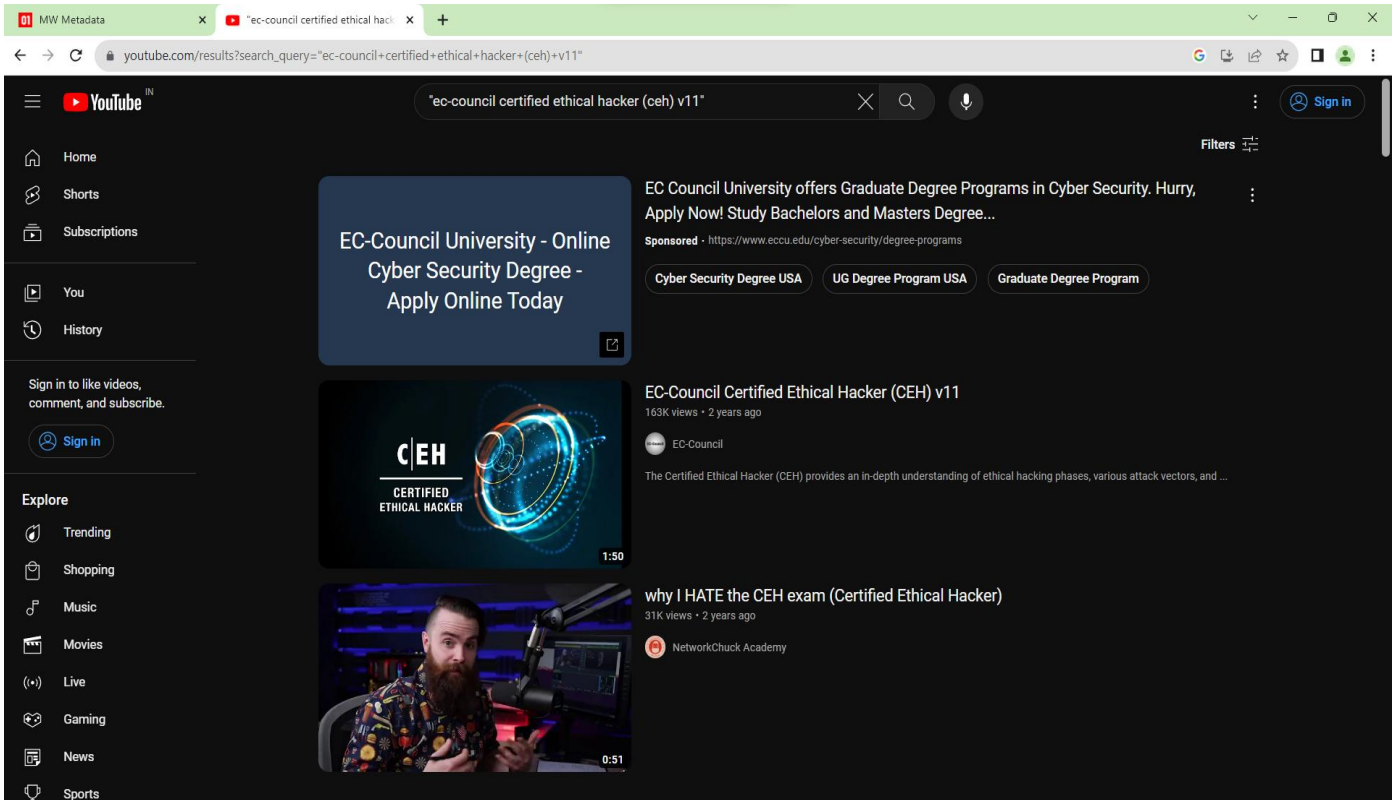


Gather information from video search engines

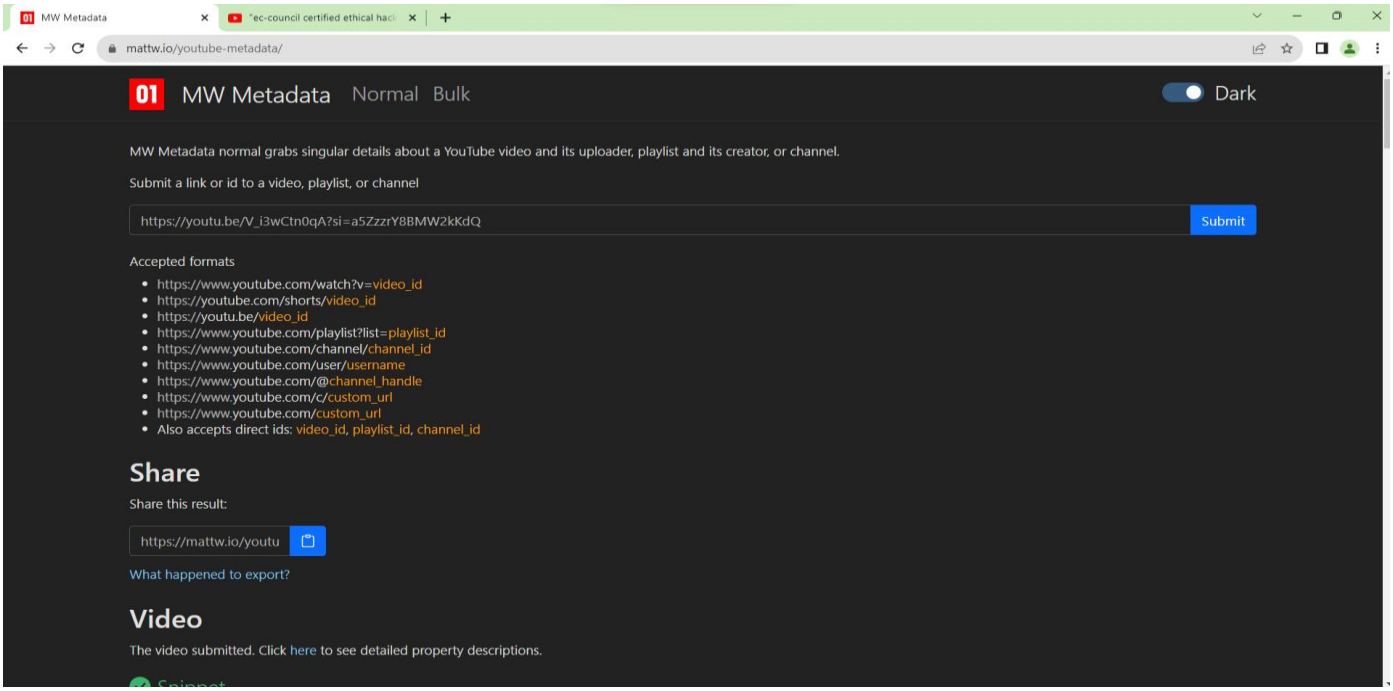
for video search engine I should two website

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

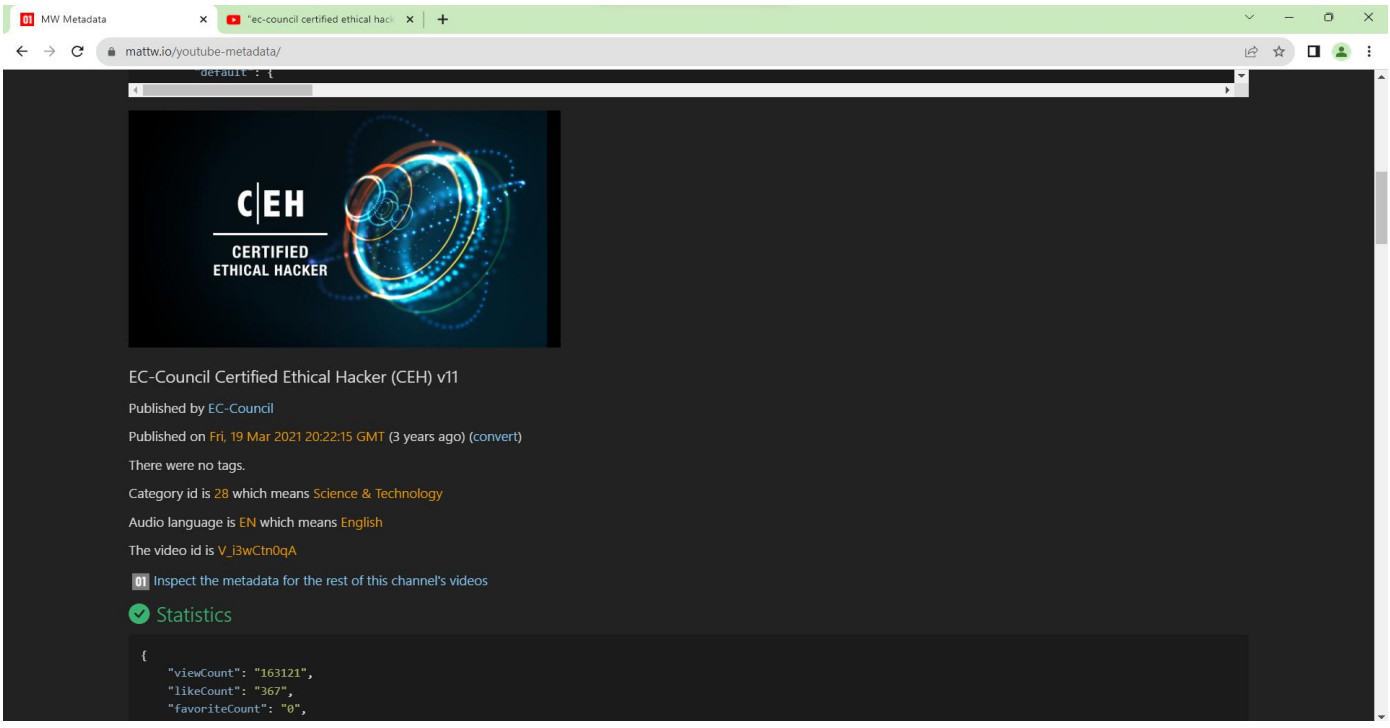
   https://mattw.io/youtube-metadata/?url=https%3A%2F%2Fyoutu.be%2FV_i3wCtn0qA%3Fsi%3Da5ZzzrY8BMW2kKdQ&submit=true
3. In youtube search **“ec-council certificate ethical hacker (CEH)v11”**



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

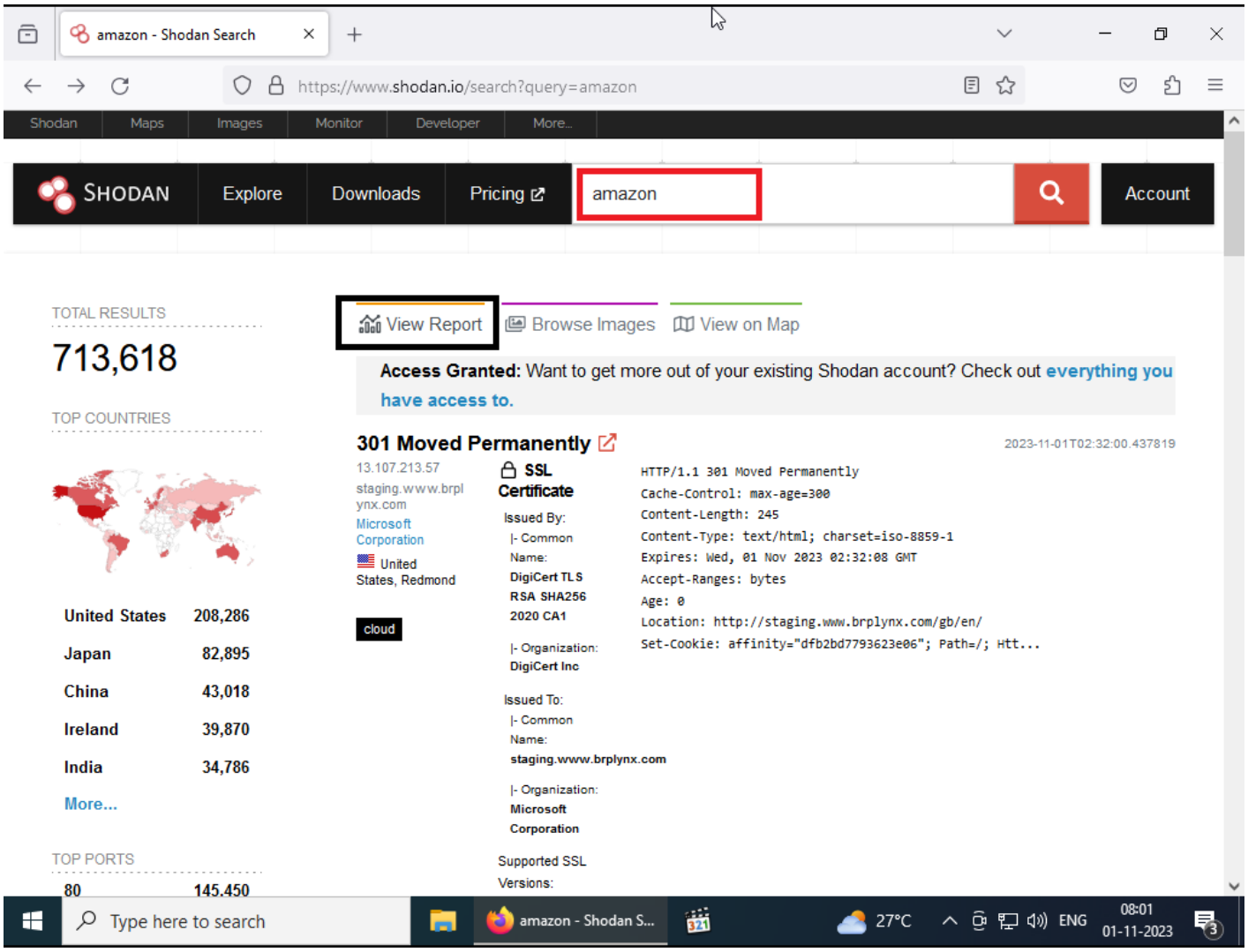


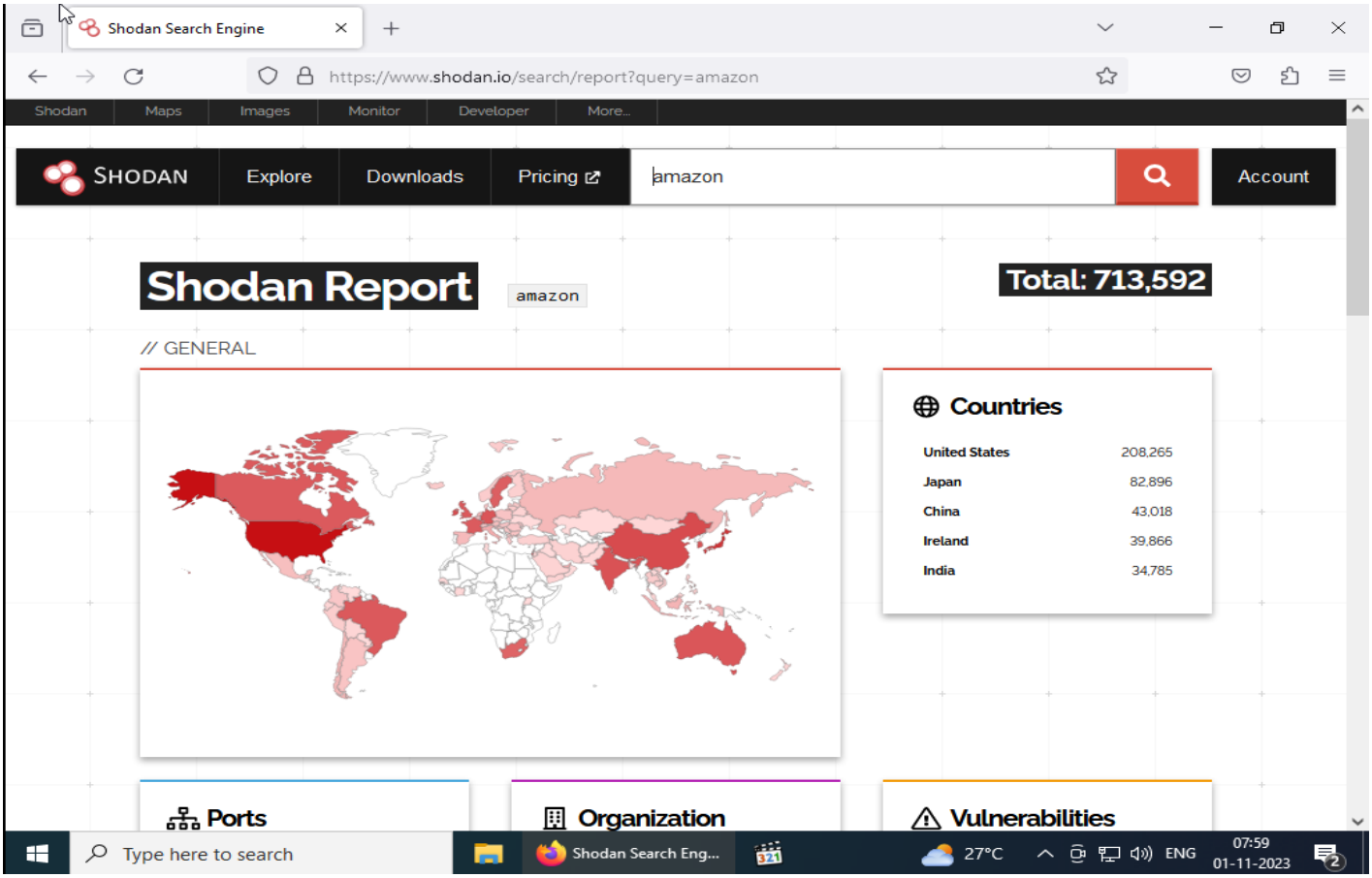
3. In this website show full information of any video like video id , uploading date , organization details and many more.

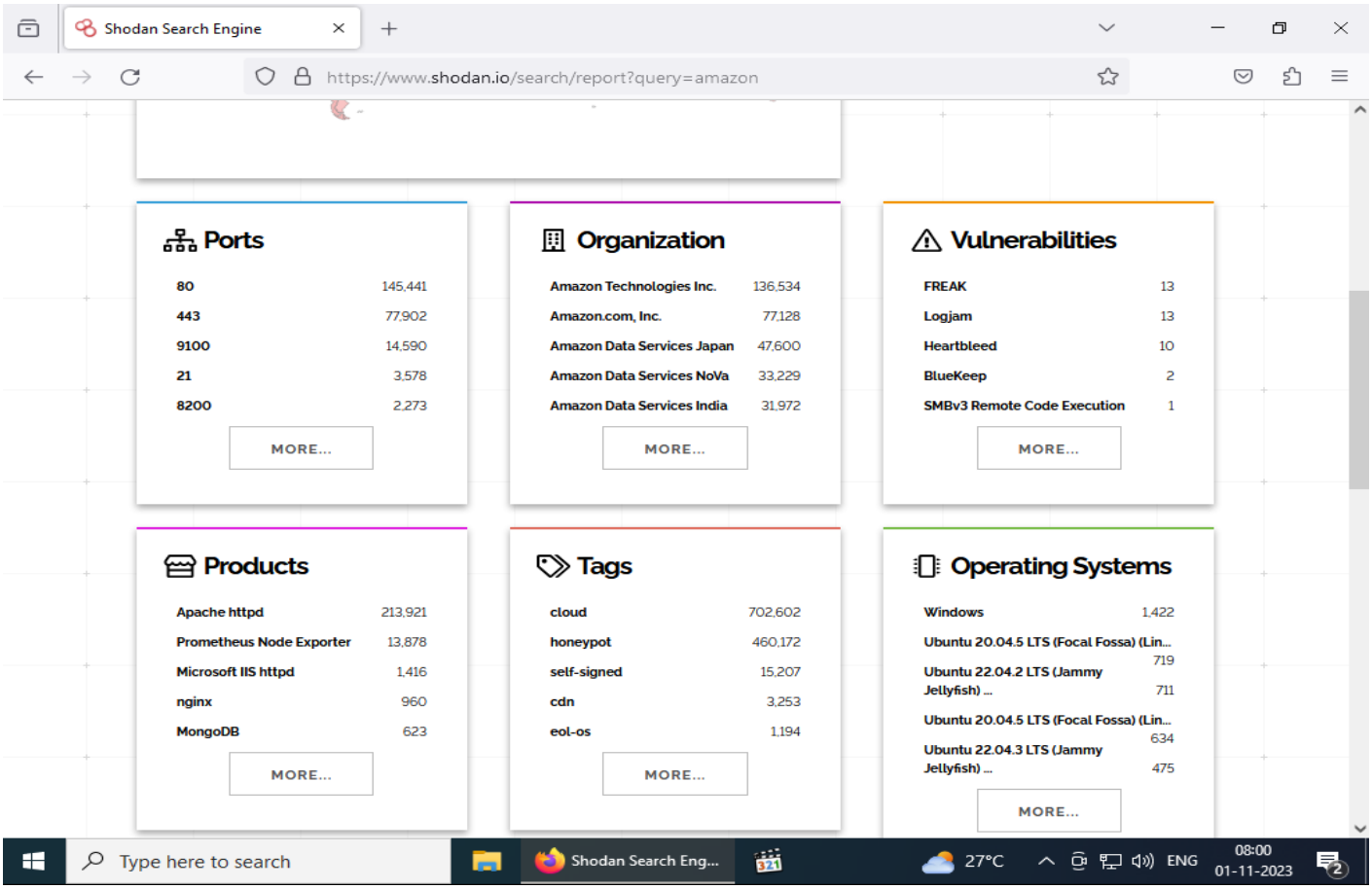


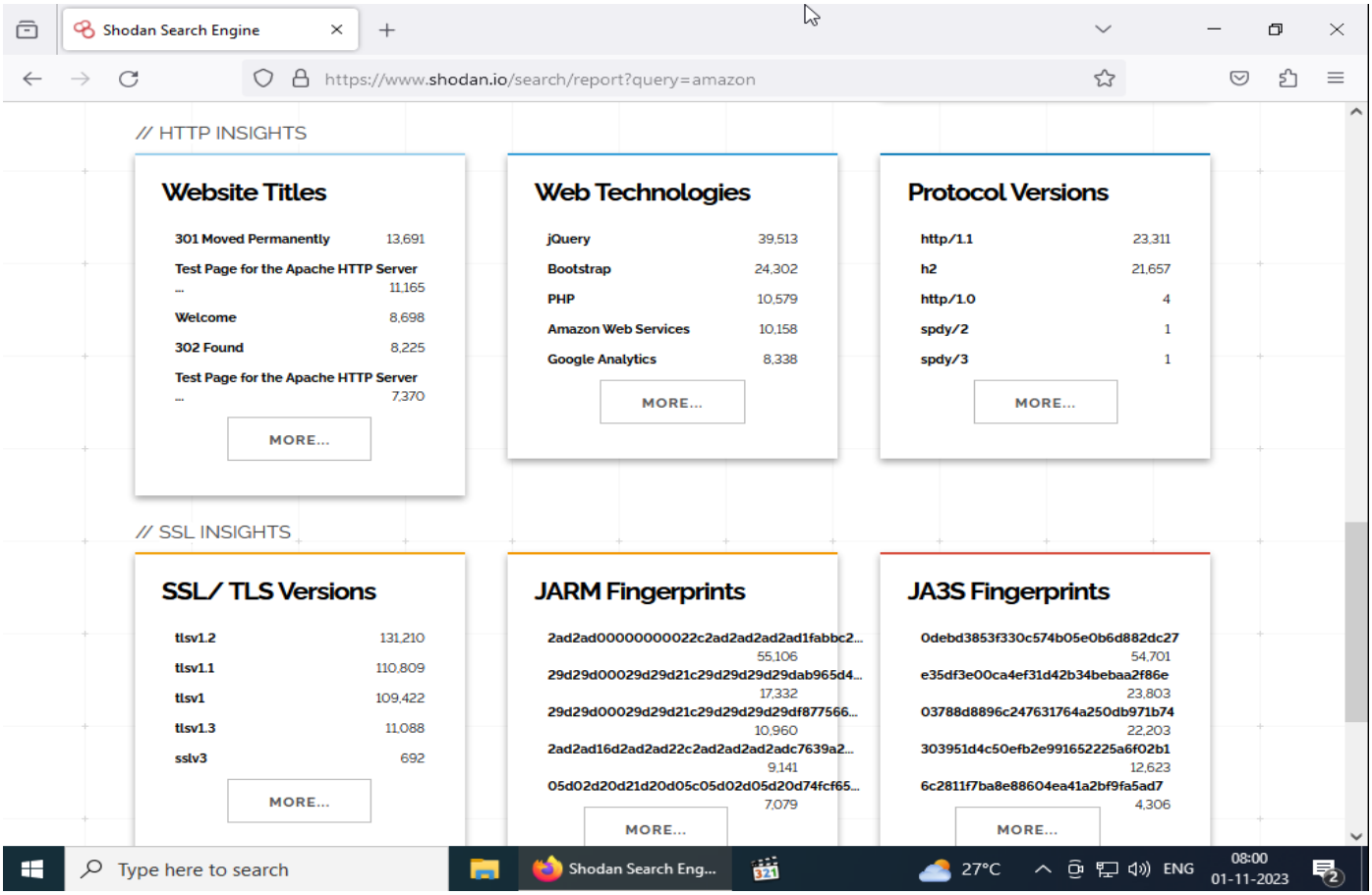
- **Gather information from IoT search engines**

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



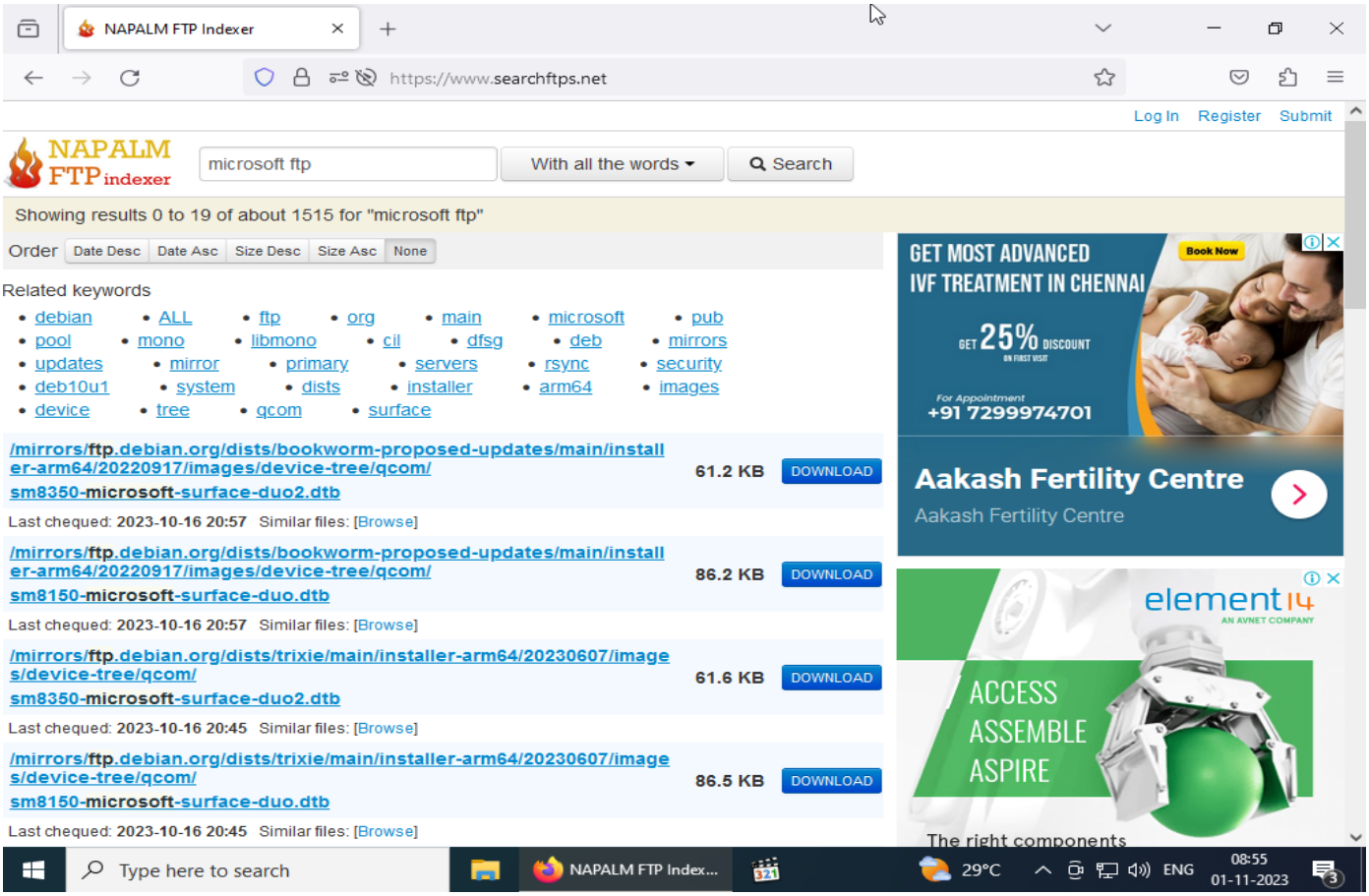

Shodan Search Engine
https://www.shodan.io/search/report?query=amazon
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
amazon
Account
Shodan Report
amazon
Total: 713,592
// GENERAL
Countries
United States 208,265
Japan 82,896
China 43,018
Ireland 39,866
India 34,785
Ports
Organization
Vulnerabilities
Type here to search
Shodan Search Eng...
27°C
ENG
07:59
01-11-2023

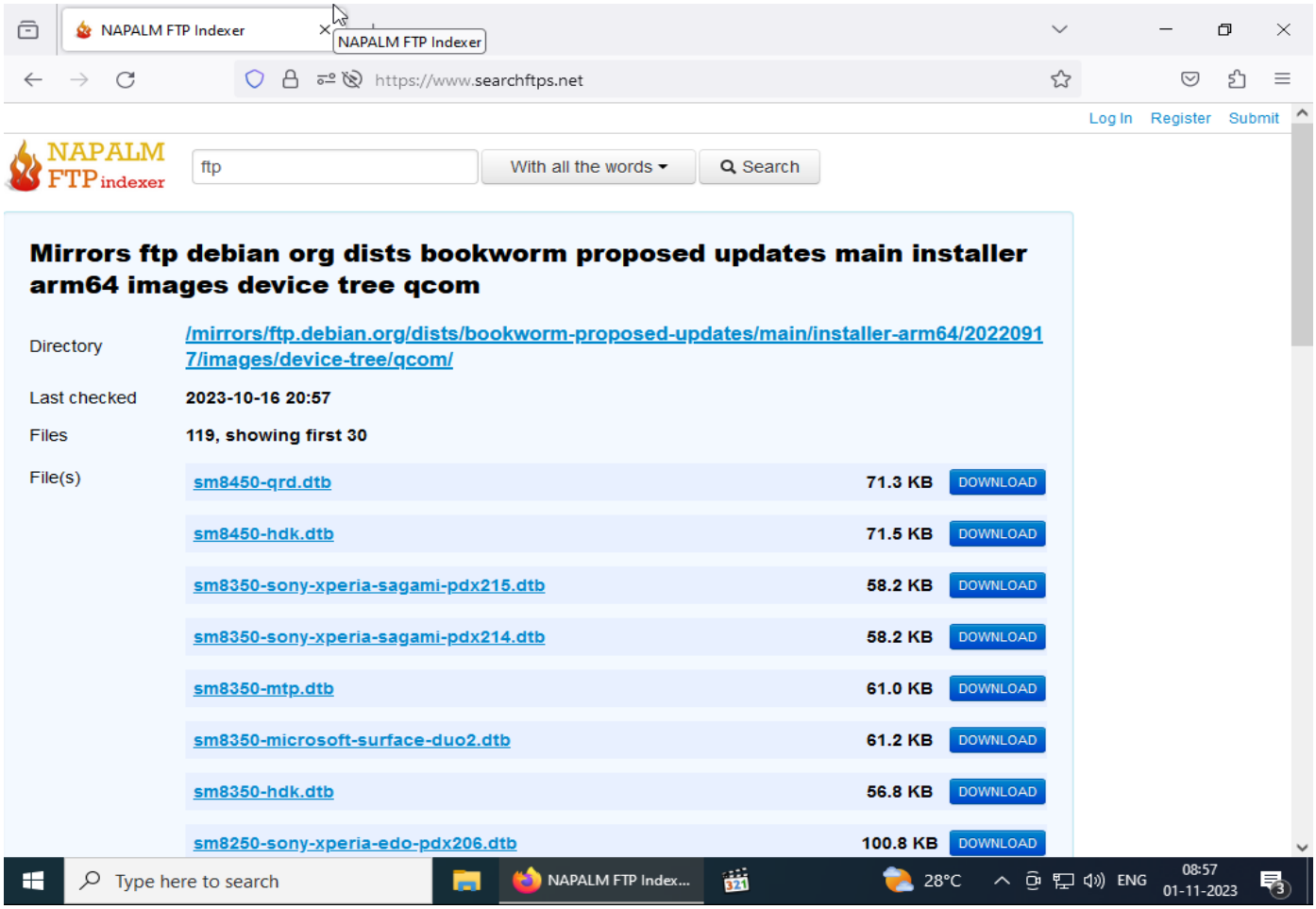

Shodan Search Engine
https://www.shodan.io/search/report?query=amazon
Ports
80 145,441
443 77,902
9100 14,590
21 3,578
8200 2,273
MORE...
Organization
Amazon Technologies Inc. 136,534
Amazon.com, Inc. 77,128
Amazon Data Services Japan 47,600
Amazon Data Services NoVa 33,229
Amazon Data Services India 31,972
MORE...
Vulnerabilities
FREAK 13
Logjam 13
Heartbleed 10
BlueKeep 2
SMBv3 Remote Code Execution 1
MORE...
Products
Apache httpd 213,921
Prometheus Node Exporter 13,878
Microsoft IIS httpd 1,416
nginx 960
MongoDB 623
MORE...
Tags
cloud 702,602
honeypot 460,172
self-signed 15,207
cdn 3,253
eol-os 1,194
MORE...
Operating Systems
Windows 1,422
Ubuntu 20.04.5 LTS (Focal Fossa) (Lin... 719
Ubuntu 22.04.2 LTS (Jammy Jellyfish) ... 711
Ubuntu 20.04.5 LTS (Focal Fossa) (Lin... 634
Ubuntu 22.04.3 LTS (Jammy Jellyfish) ... 475
MORE...
Type here to search
Shodan Search Eng...
27°C
ENG
08:00
01-11-2023


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
2ad2ad00000000022c2ad2ad2ad2ad1fabbc2... 55,106
29d29d00029d29d21c29d29d29d29dab965d4... 17,332
29d29d00029d29d21c29d29d29d29df877566... 10,960
2ad2ad16d2ad2ad22c2ad2ad2ad2adc7639a2... 9,141
05d02d20d21d20d05c05d02d05d20d74fcf65... 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
ENG
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




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