Lab 1: Perform Footprinting Through Search Engines

**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

**Overview of Search Engines**

Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

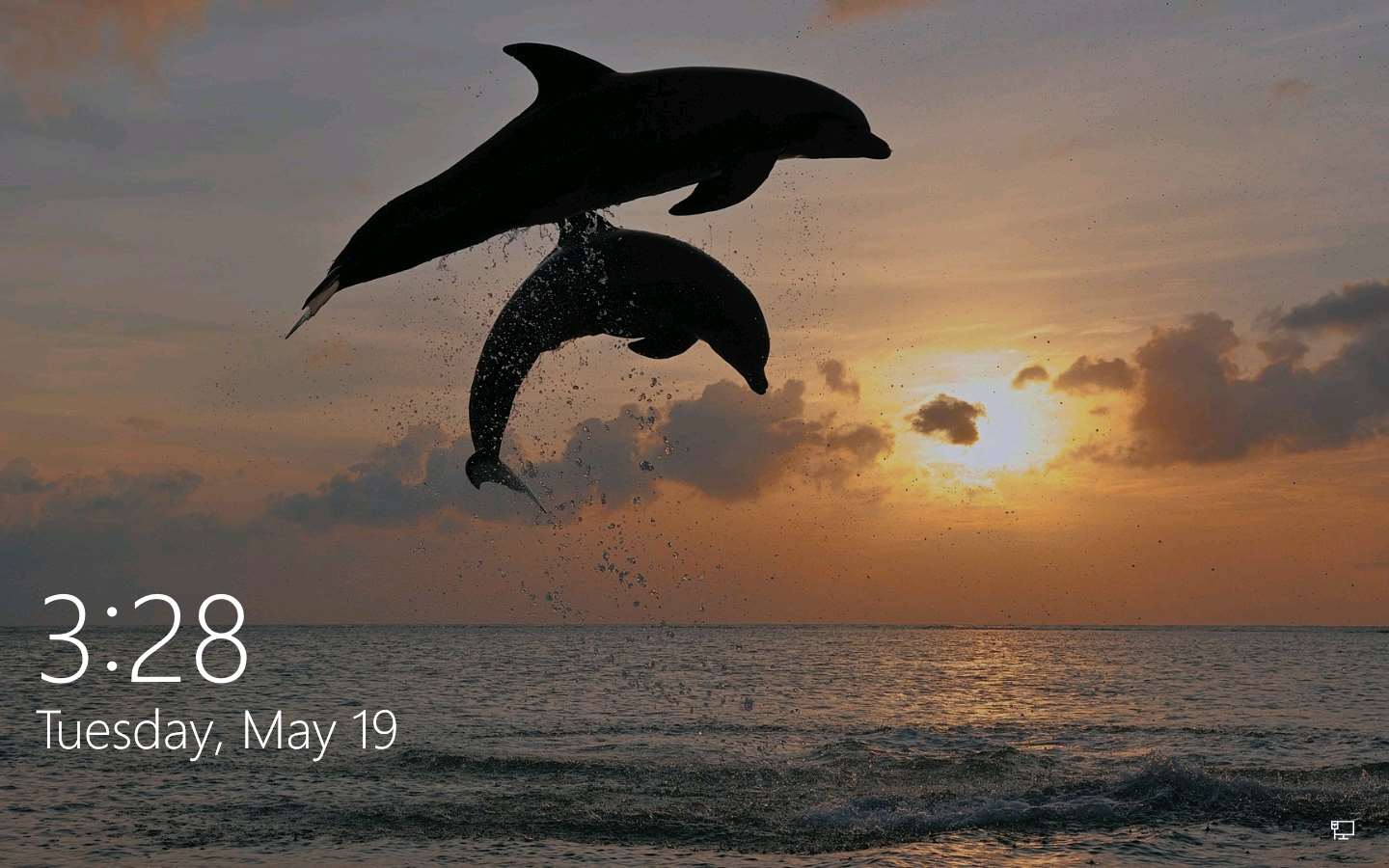
Task 1: Gather Information using Advanced Google Hacking Techniques

Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation.

Here, we will consider **EC-Council** as a target organization.

1. By default **Windows 10** machine selected, click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10).

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

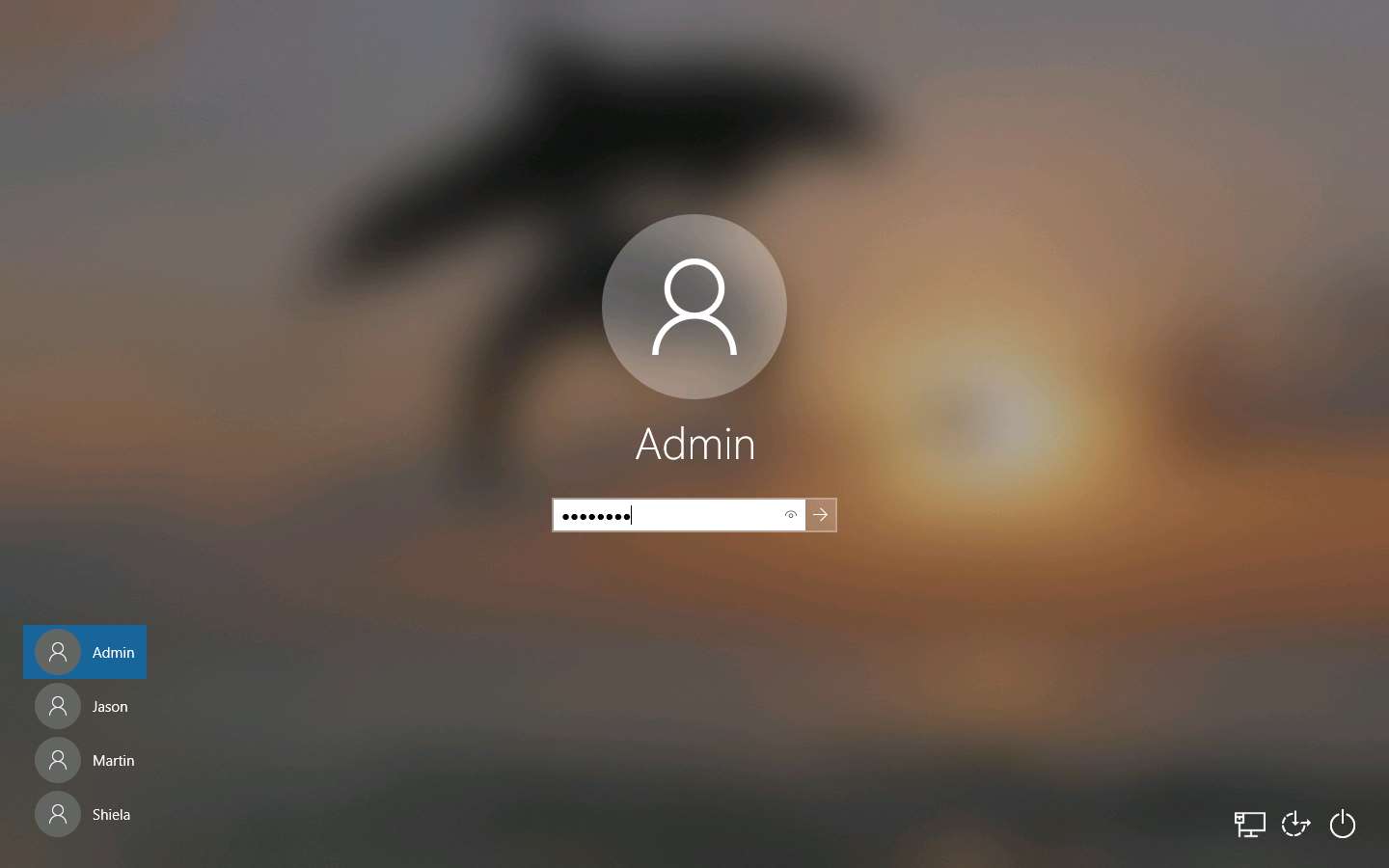


1. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

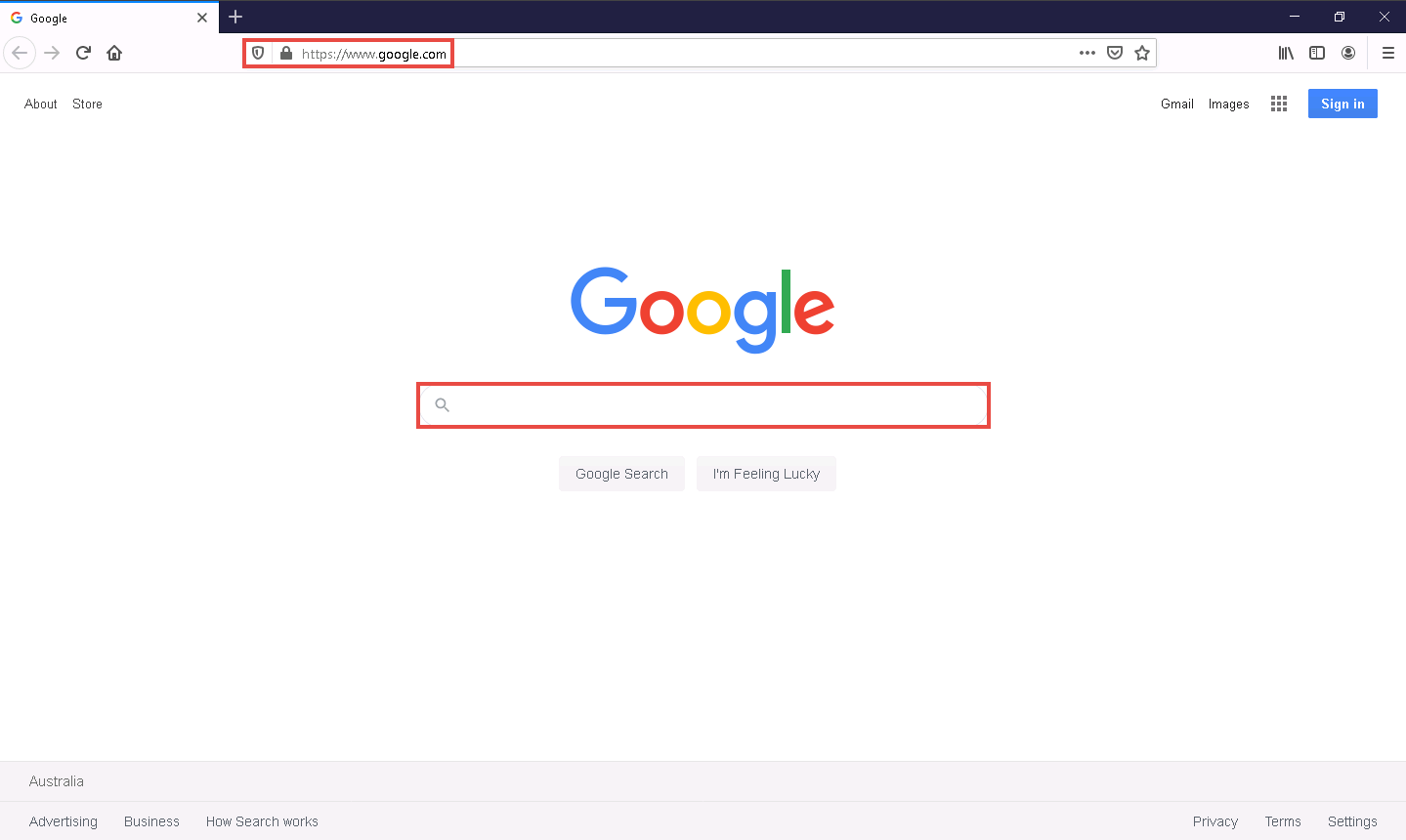
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



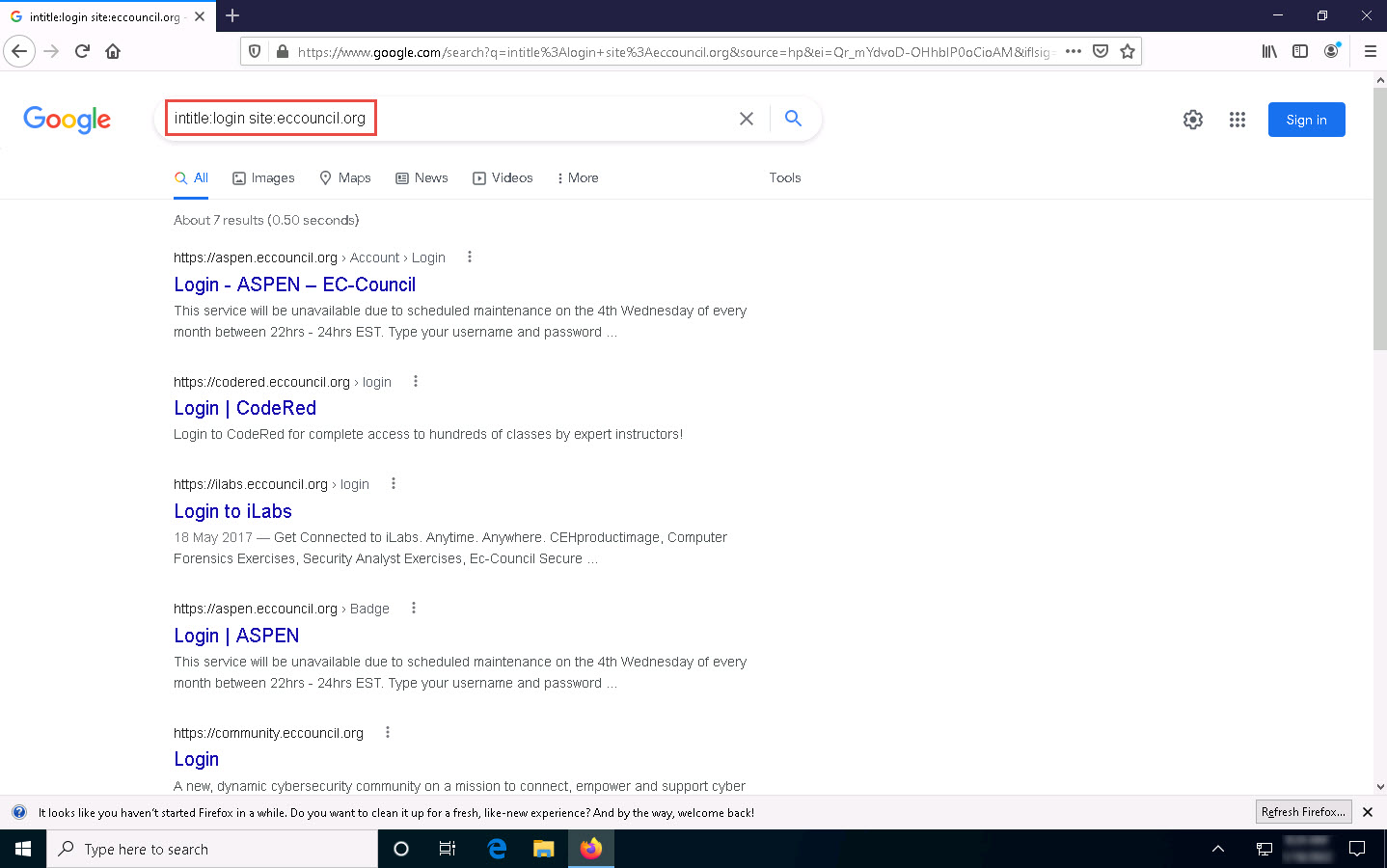
1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.google.com and press **Enter**.
   * If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
   * If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.
2. Once the **Google** search engine appears, you should see a search bar.

If any pop-up window appears at the top-right corner, click **No, thanks**.

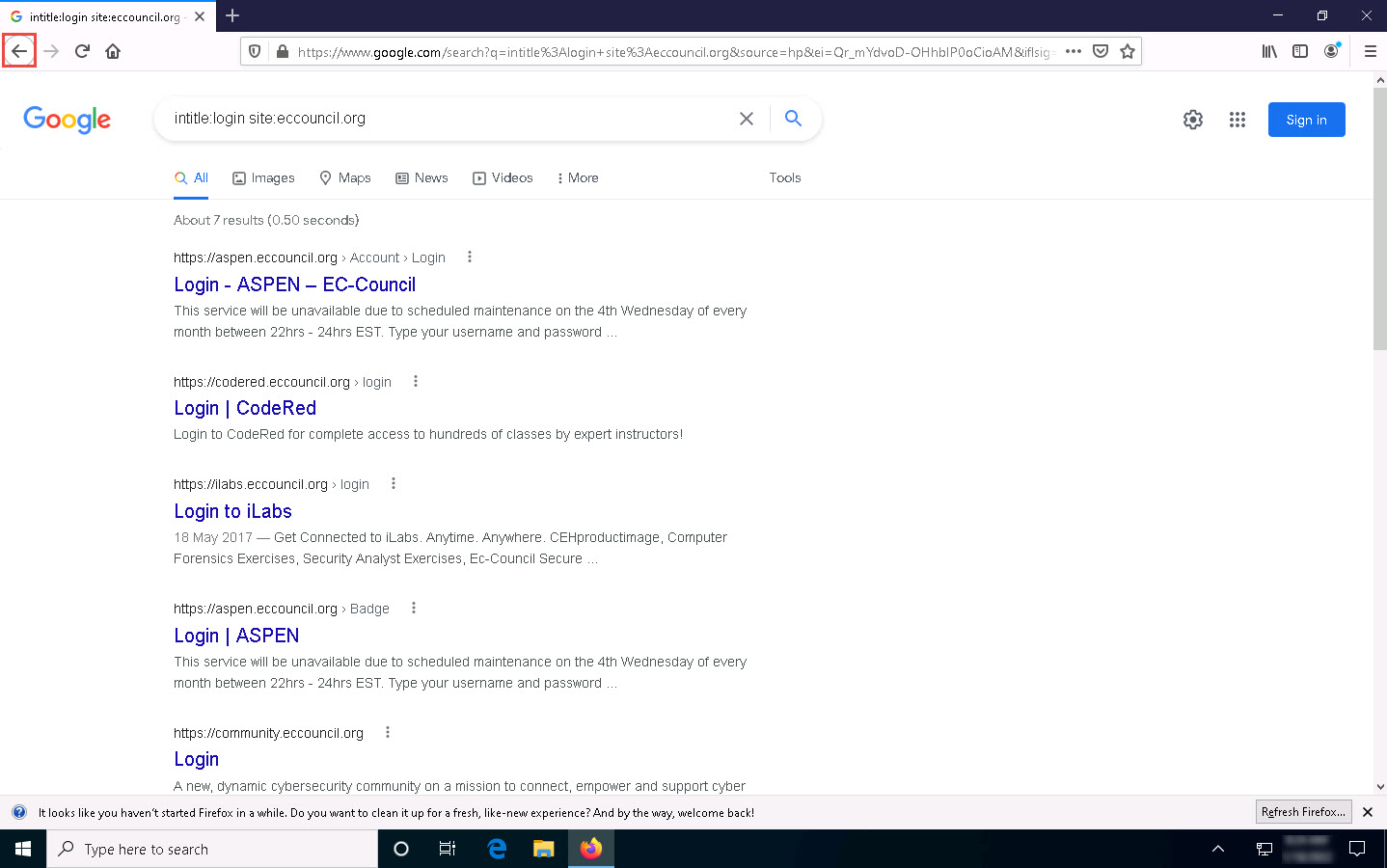


1. Type **intitle:login site:eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **eccouncil.org** website that contain the **login** pages. An example is shown in the screenshot below.

Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential bruteforcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.



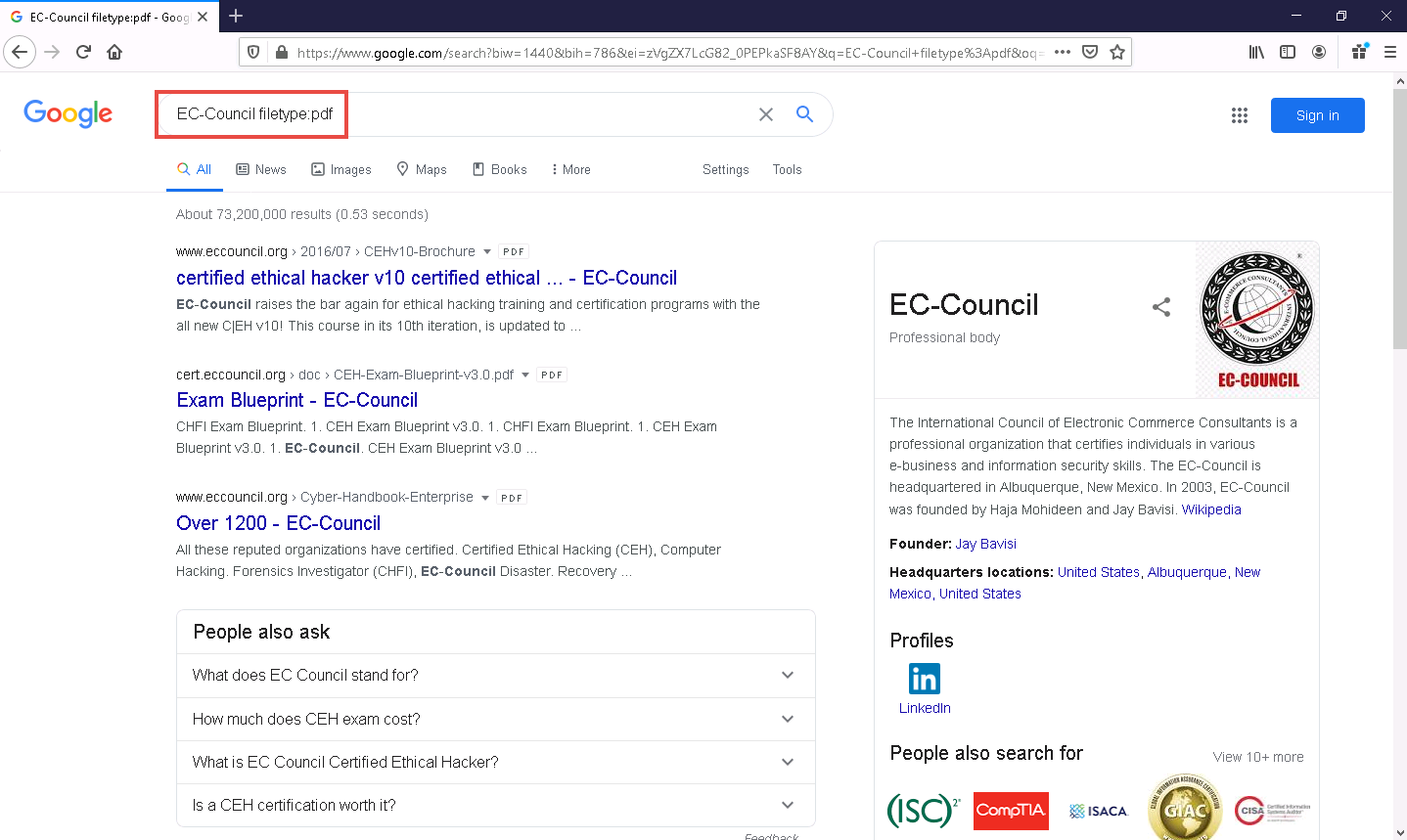
1. Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.



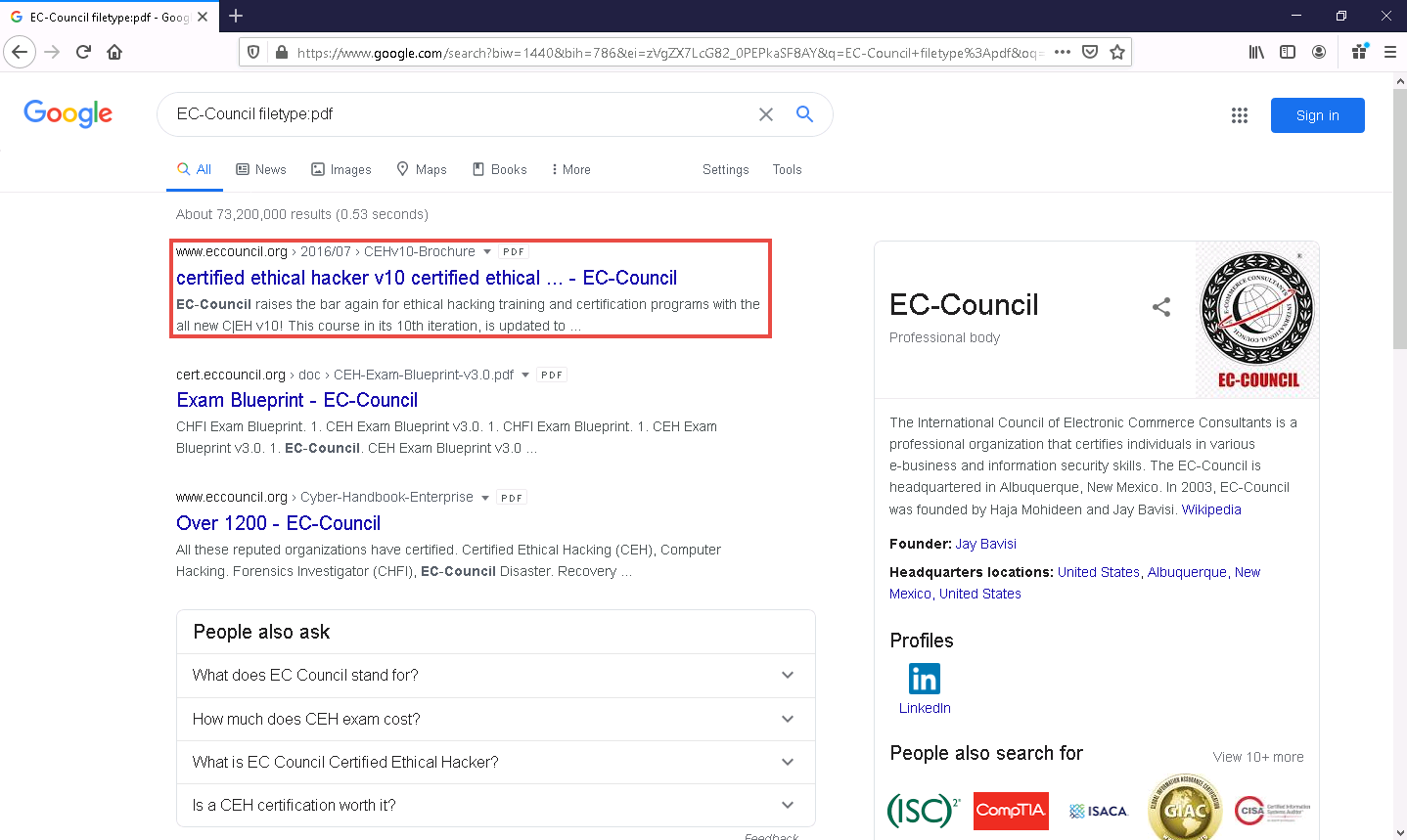
1. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.

The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target. Pen testers also look for these files to assess the target organisation's security posture.



1. Now, click on any link from the results (here, first link) to view the pdf file.



1. The page appears displaying the PDF file, as shown in the screenshot.



1. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.
   * **cache**: This operator allows you to view cached version of the web page. [cache:www.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org
   * **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL. [allinurl: EC-Council career]—Query returns only pages containing the words “EC-Council” and “career” in the URL
   * **inurl**: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.eccouncil.org]—Query returns only pages in EC-Council site in which the URL has the word “copy”
   * **allintitle**: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words “detect” and “malware” in the title
   * **inanchor**: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word “Norton” and the page containing the word “Anti-virus”
   * **allinanchor**: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words “best,” “cloud,” “service,” and “provider”
   * **link**: This operator searches websites or pages that contain links to the specified website or page. [link:www.eccouncil.org]—Finds pages that point to EC-Council’s home page
   * **related**: This operator displays websites that are similar or related to the URL specified. [related:www.eccouncil.org]—Query provides the Google search engine results page with websites similar to eccouncil.org
   * **info**: This operator finds information for the specified web page. [info:eccouncil.org]—Query provides information about the www.eccouncil.org home page
   * **location**: This operator finds information for a specific location. [location: EC-Council]—Query give you results based around the term EC-Council
2. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
3. Close all open windows and document all the acquired information.

Task 2: Gather Information from Video Search Engines

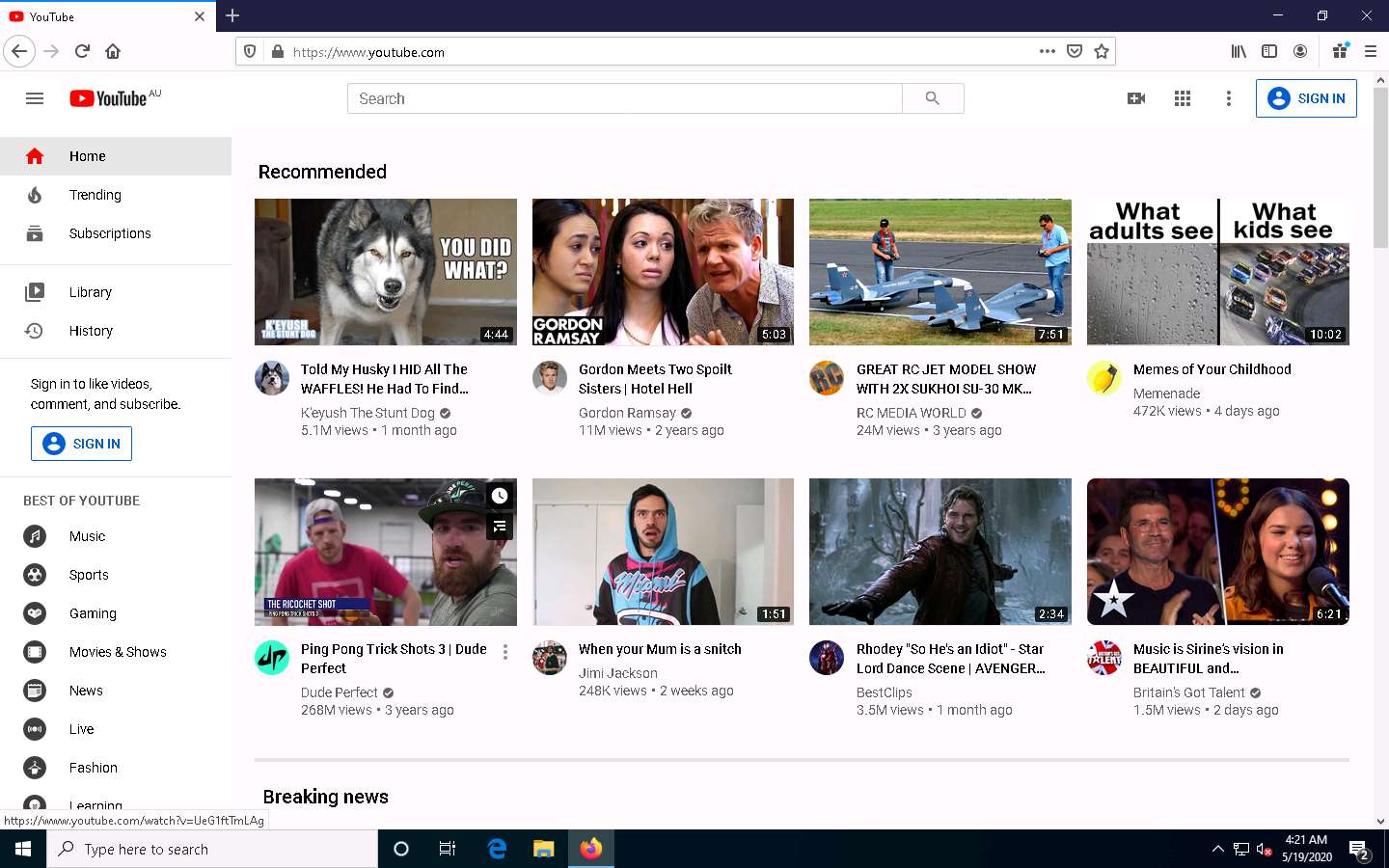
Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

Here, we will perform an advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.

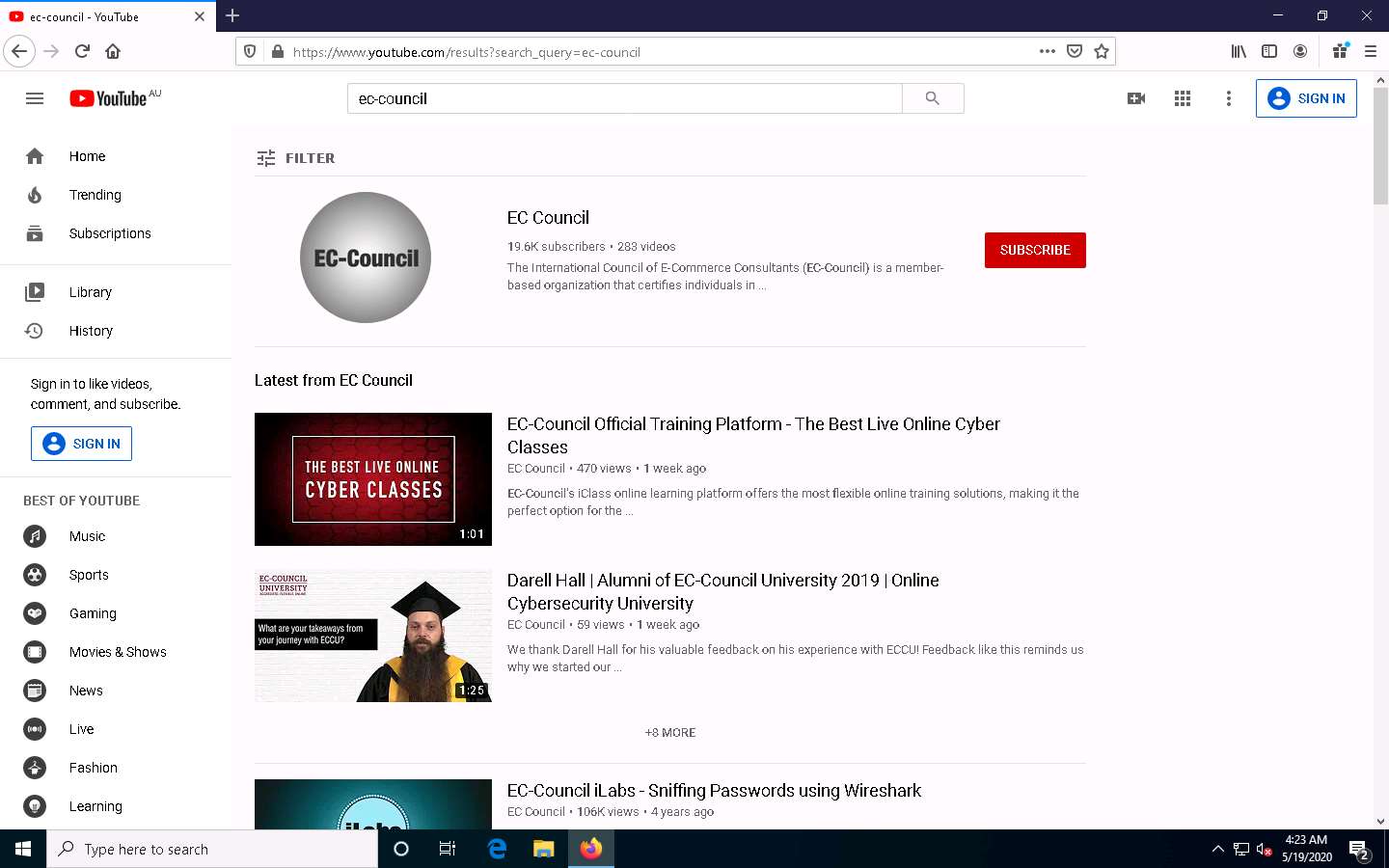
Here, we will consider **EC-Council** as a target organization.

1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.youtube.com and press **Enter**. YouTube page appears as shown in the screenshot.

If you choose to use another web browser, the screenshots will differ.

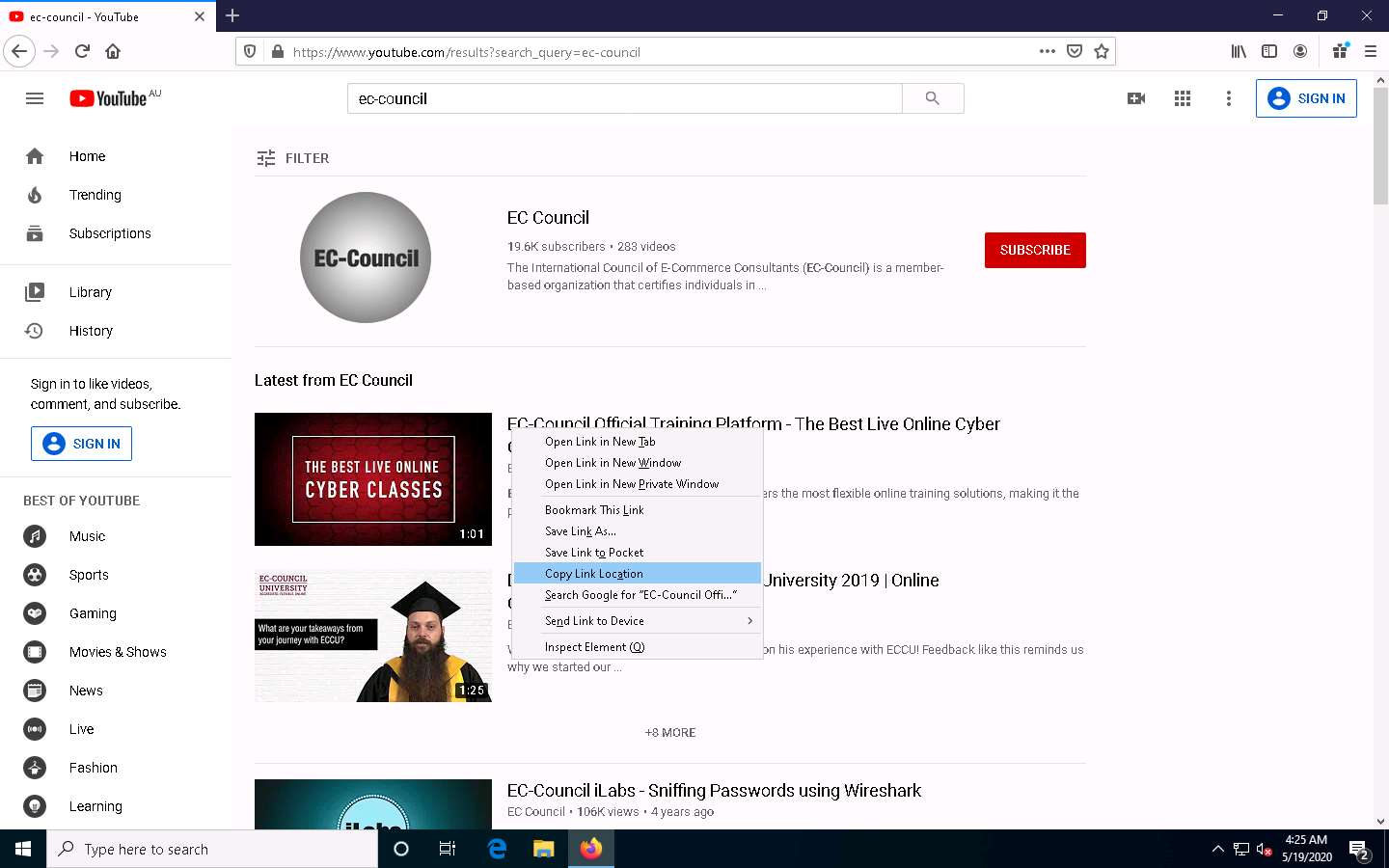


1. In the search field, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.

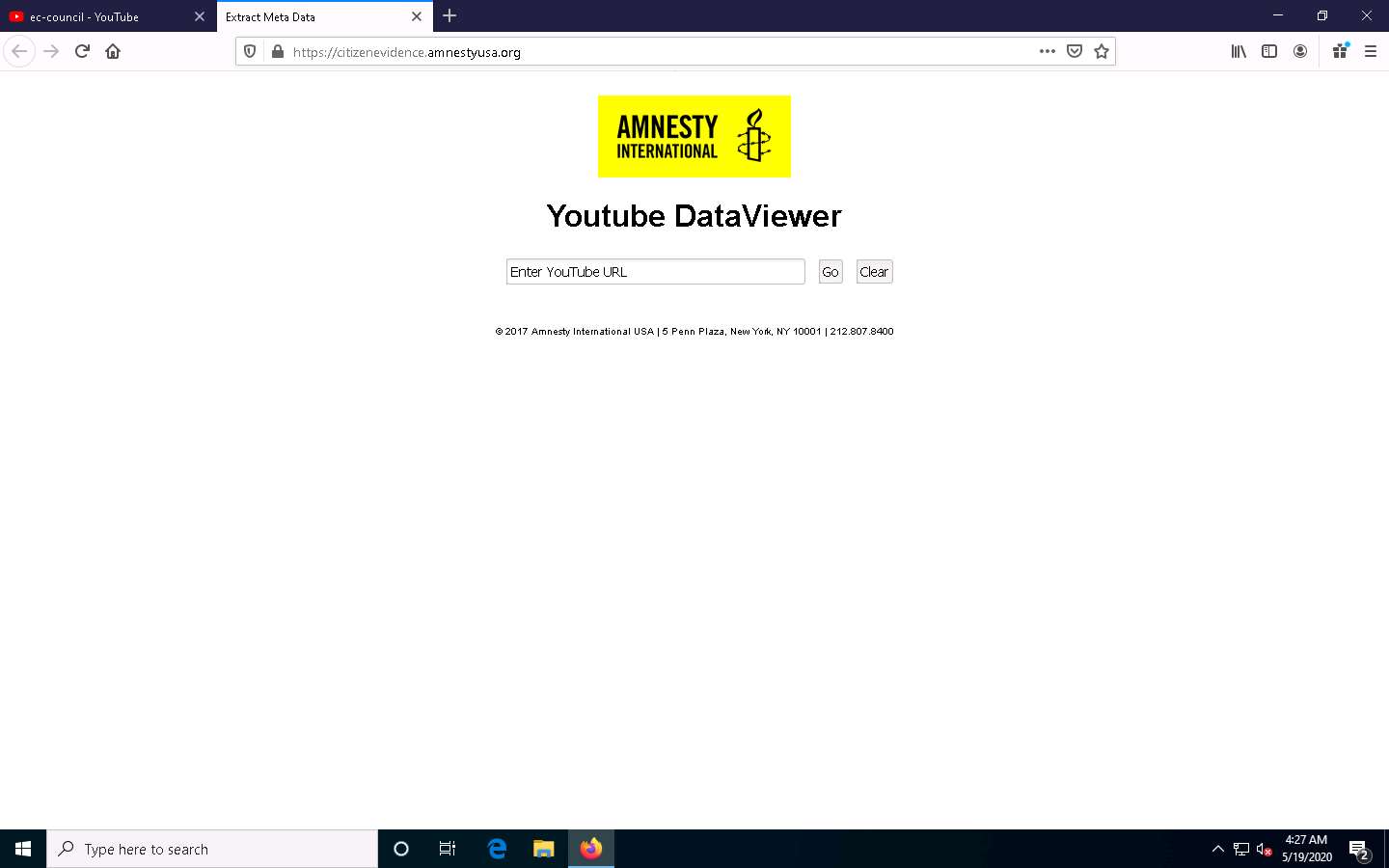


1. Select any video of your choice, right-click on the video title, and click **Copy Link Location**.

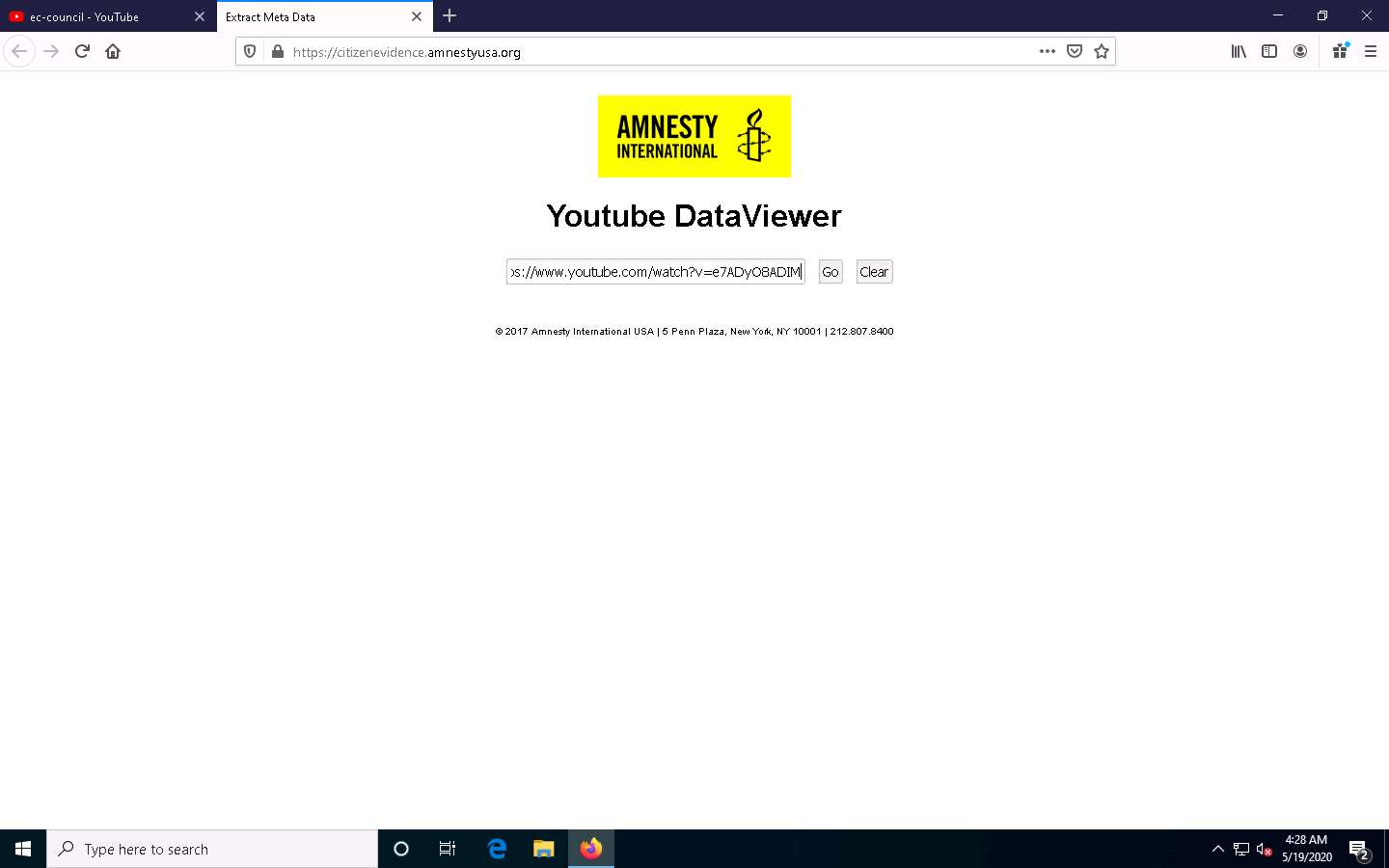
If you are using a newer or updated version of Firefox then you must select **Copy Link** option.



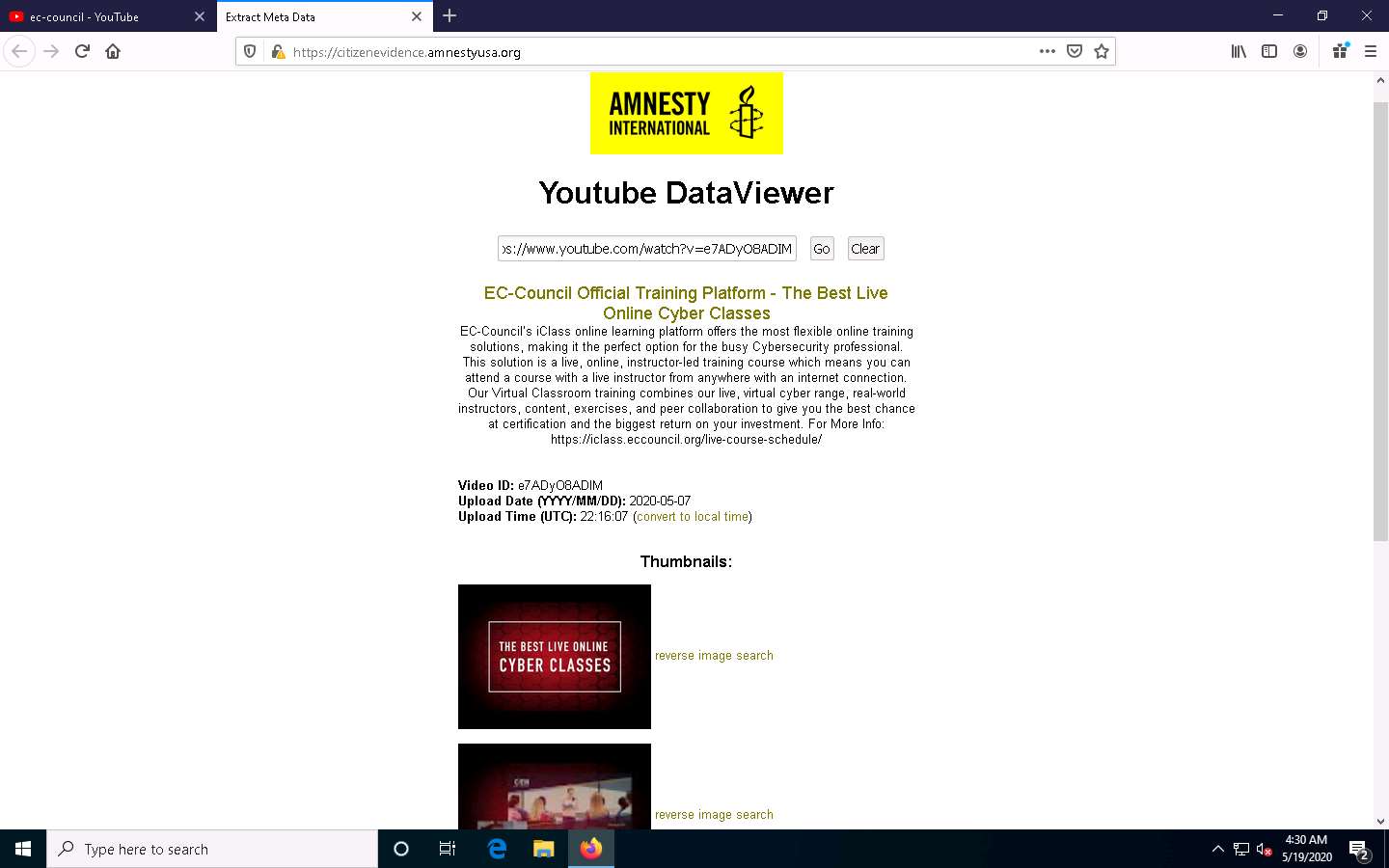
1. After the video link is copied, open a new tab in **Mozilla Firefox**, place your mouse cursor in the address bar and click https://citizenevidence.amnestyusa.org/ and press **Enter**.



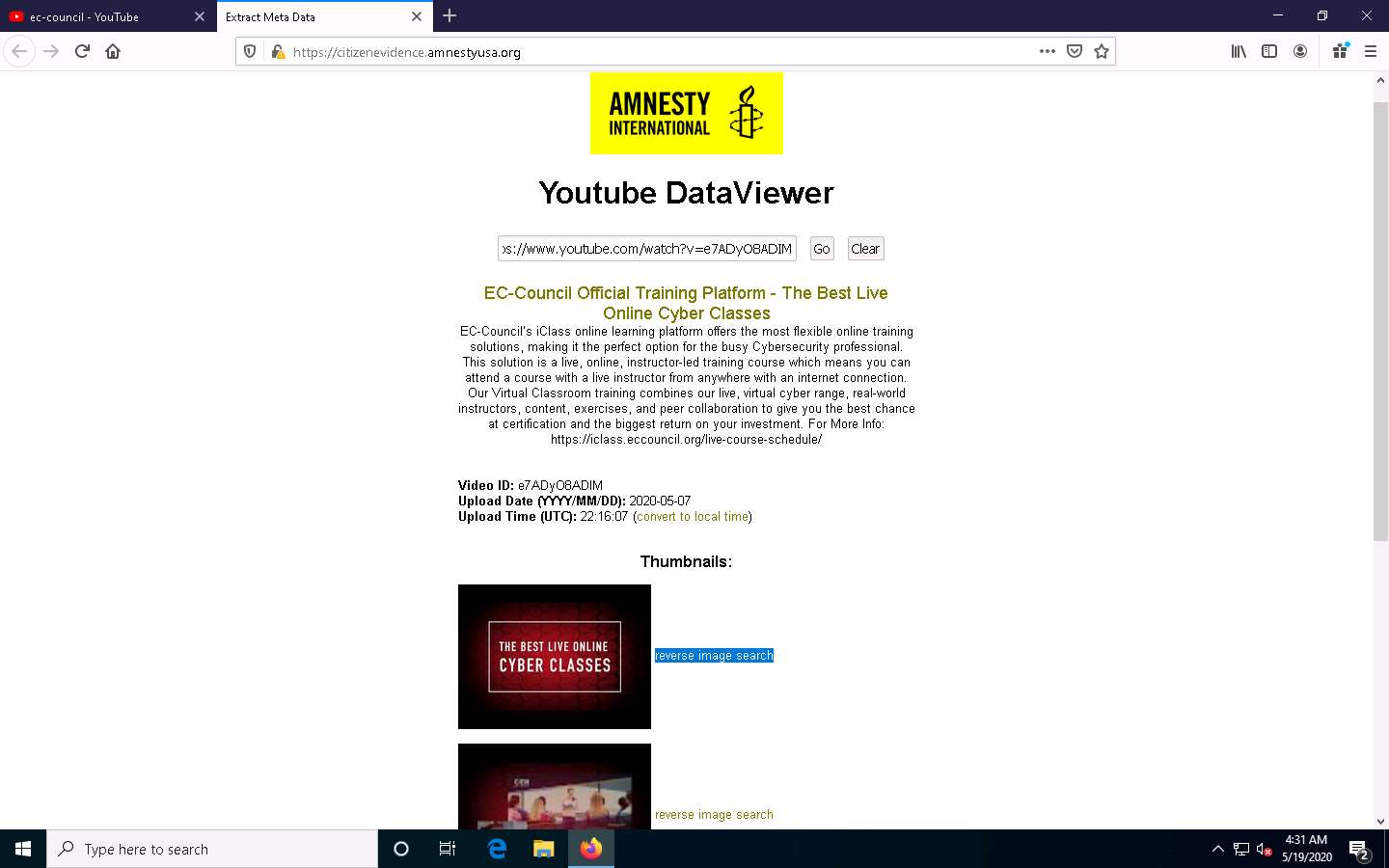
1. Extract Meta Data page appears, in the **Enter YouTube URL** search field, paste the copied YouTube video location and click **Go**.



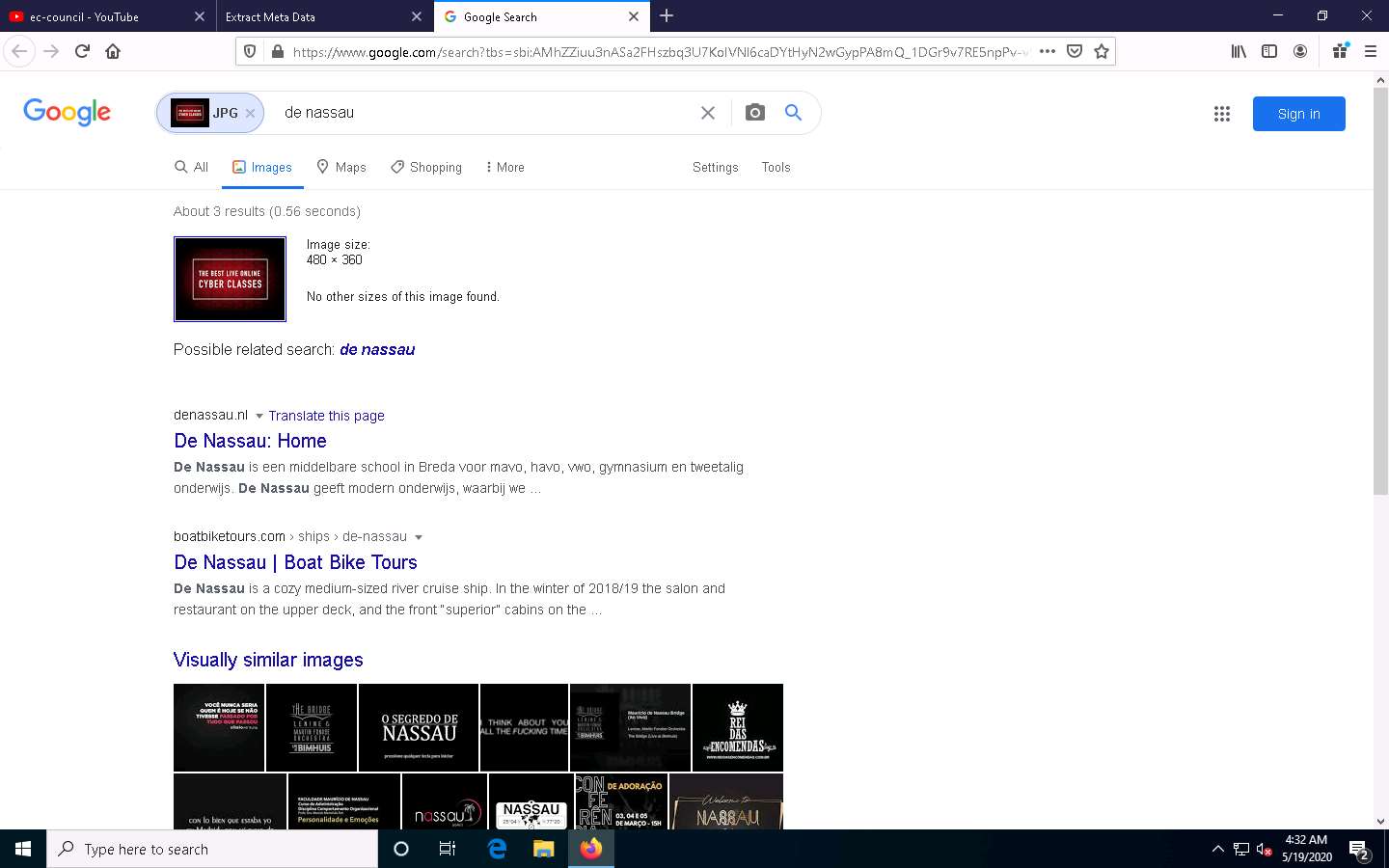
1. In the search result, you can observe the details related to the video such as **Video ID**, **Upload Date**, **Upload Time**, etc. You can also find **Thumbnails** to perform a **reverse image search**.



1. Now, click on the **reverse image search** option for any thumbnail.



1. A new tab in Google appears, and the results for the reverse image search are displayed.



1. This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.
2. You can use other video search engines such as **Google videos** (https://video.google.com), **Yahoo videos** (https://video.search.yahoo.com), etc.; video analysis tools such as **EZGif** (https://ezgif.com), **VideoReverser.com**, etc.; and reverse image search tools such as **TinEye Reverse Image Search** (https://tineye.com), **Yahoo Image Search** (https://images.search.yahoo.com), etc. to gather crucial information about the target organization.
3. Close all open windows and document all acquired information.

Task 3: Gather Information from FTP Search Engines

File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that are shared among their employees. FTP search engines provide information about critical files and directories, including valuable information such as business strategies, tax documents, employee’s personal records, financial records, licensed software, and other confidential information.

Here, we will use the NAPALM FTP indexer FTP search engine to extract critical FTP information about the target organization.

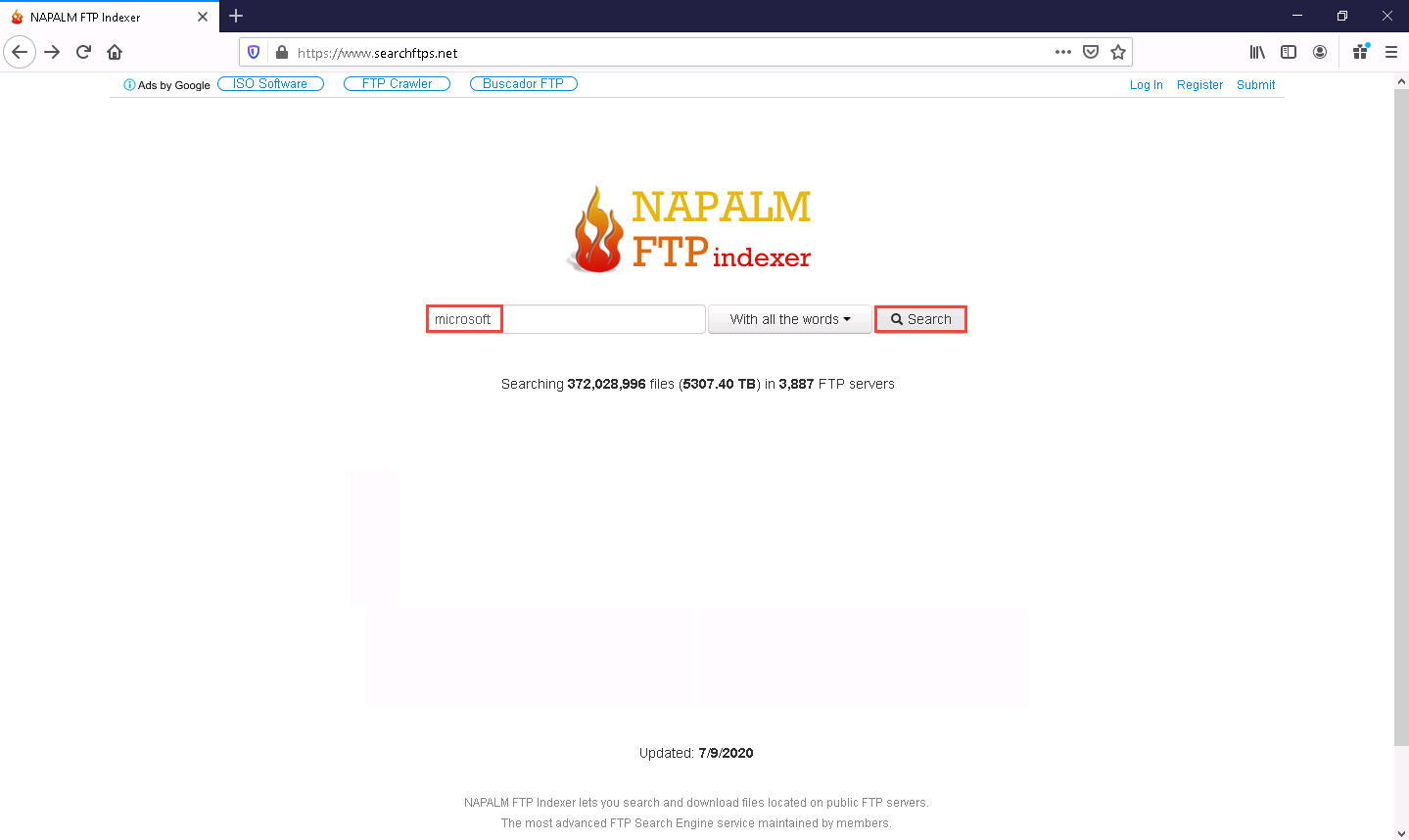
1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.searchftps.net/ and press **Enter**.

If you choose to use another web browser, the screenshots will differ.

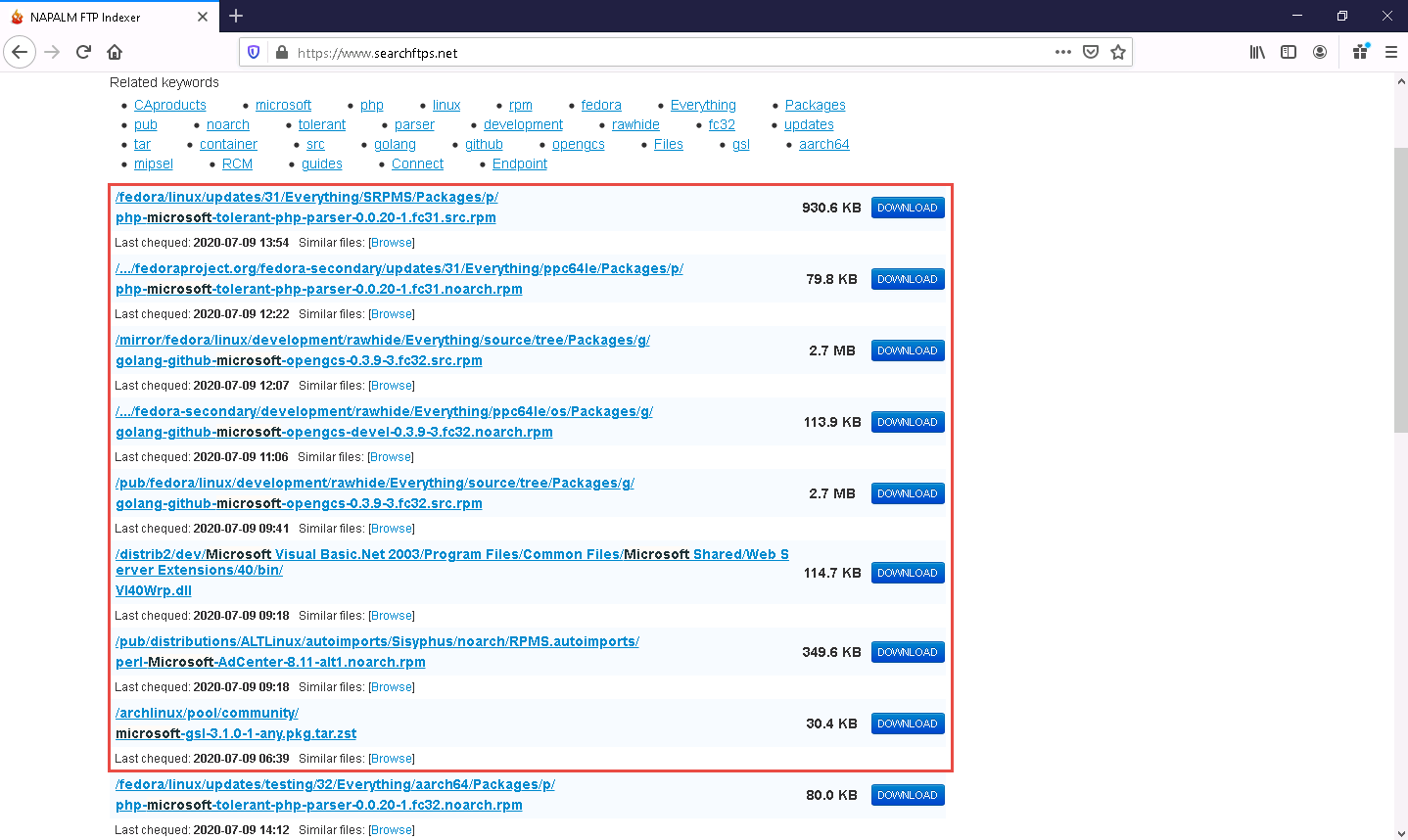
1. NAPALM FTP indexer website appears, as shown in the screenshot.



1. In the search bar, type **microsoft** and click **Search**.



1. You will get the search results with the details of the FTP in the target organization, as shown in the screenshot.



1. This concludes the demonstration of gathering information from the FTP search engine.
2. You can also use FTP search engines such as **Global FTP Search Engine** (https://globalfilesearch.com), **FreewareWeb FTP File Search** (http://www.freewareweb.com), etc. to gather crucial FTP information about the target organization.
3. Close all open windows and document all the acquired information.

Task 4: Gather Information from IoT Search Engines

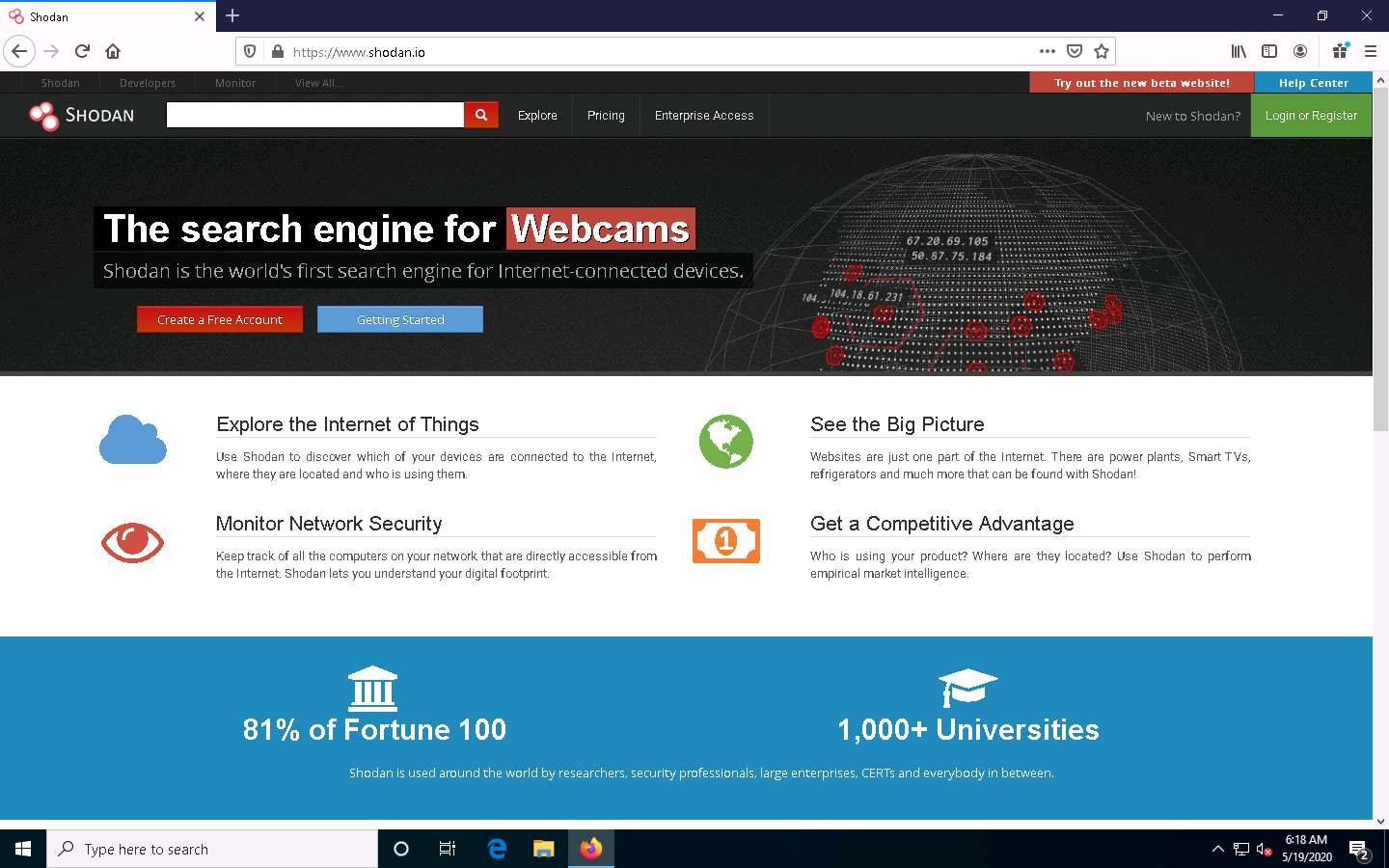
IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc.

Here, we will search for information about any vulnerable IoT device in the target organization using the Shodan IoT search engine.

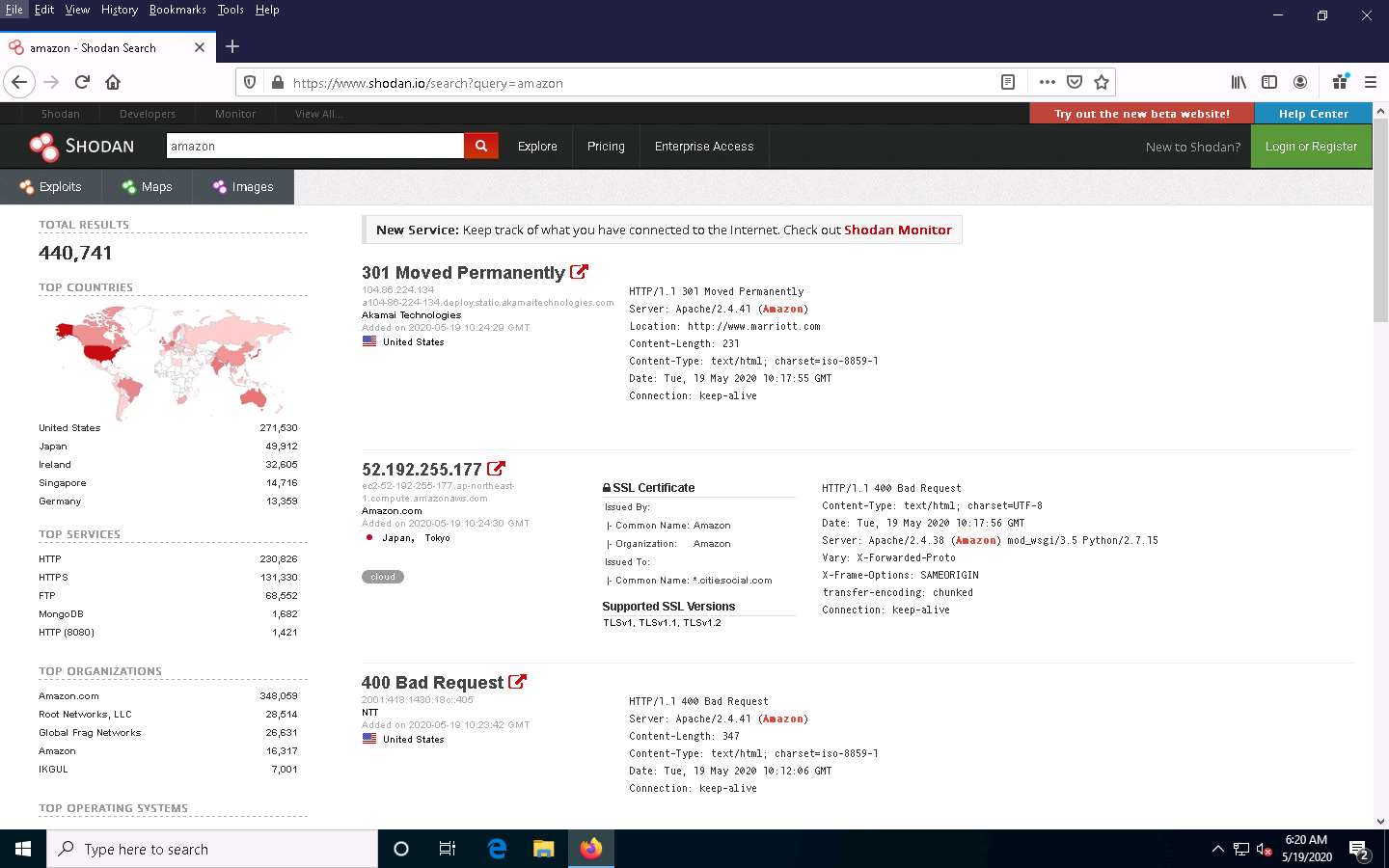
1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.shodan.io/ and press **Enter**.

If you choose to use another web browser, the screenshots will differ.

1. **Shodan** page appears, as shown in the screenshot.



1. In the search bar, type **amazon** and press **Enter**.
2. You will obtain the search results with the details of all the vulnerable IoT devices related to amazon in various countries, as shown in the screenshot.



1. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
2. You can also use **Censys** (https://censys.io), **Thingful** (https://www.thingful.net), etc., which are IoT search engines, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.
3. Close all open windows and document all the acquired information.