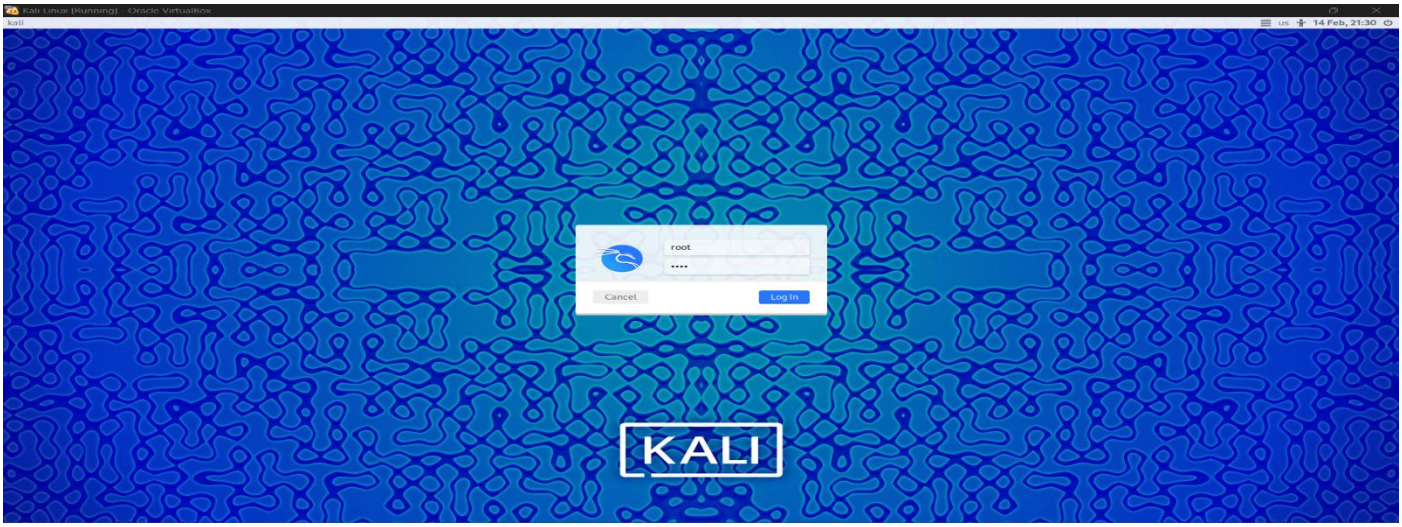
LAP1…BART2

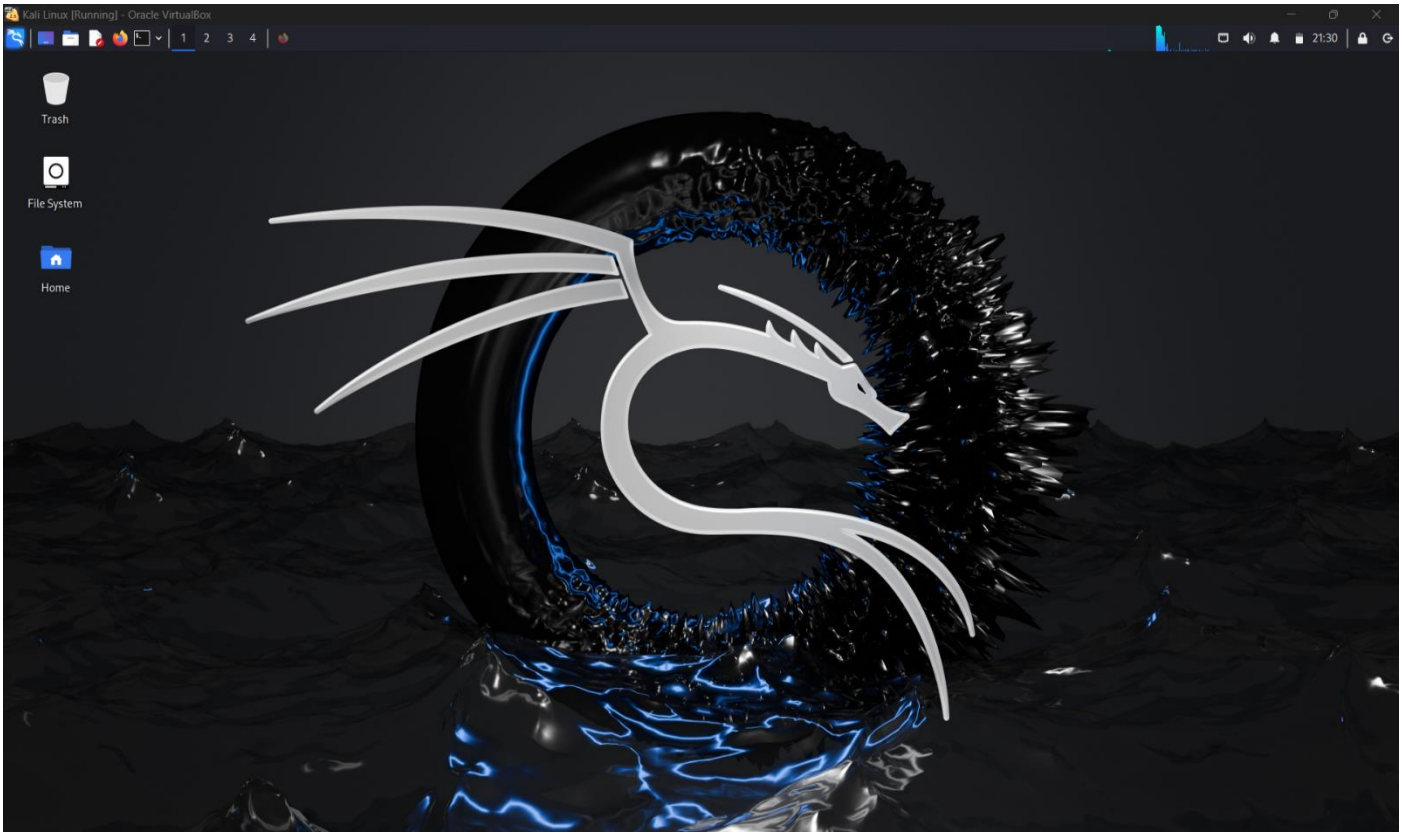
Name: Abdullah Abdulaziz Rabah Alshammari
ID: 202100569

Exercise 2: Collecting Information About a Target Website Using Firebug

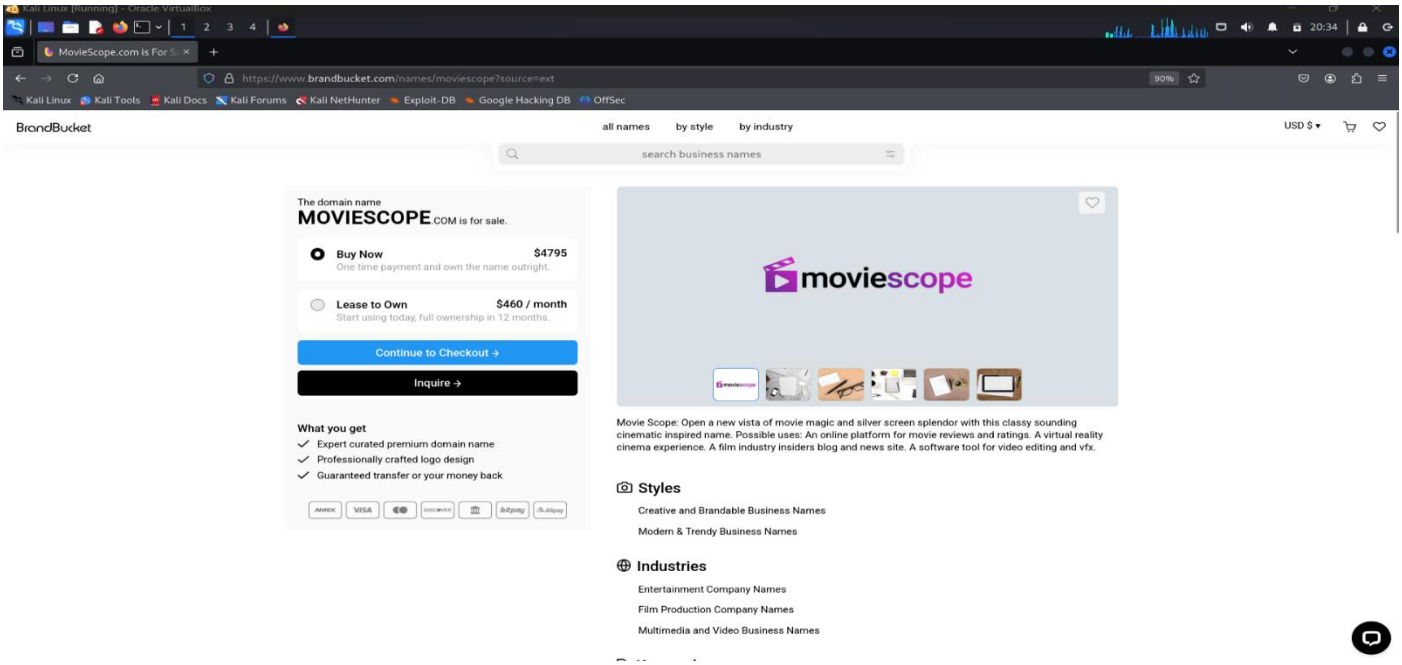
1. Click Kali Linux machine.
2. To login into the kali machine type **root** in the **Username** and click the **Next** button.
3. Next type **toor** in the **Password** field and click the **Sign In** button.



4. The Kali Linux desktop appears as shown in the screenshot. Click the **Firefox** browser icon from the favourites bar on the left-side.



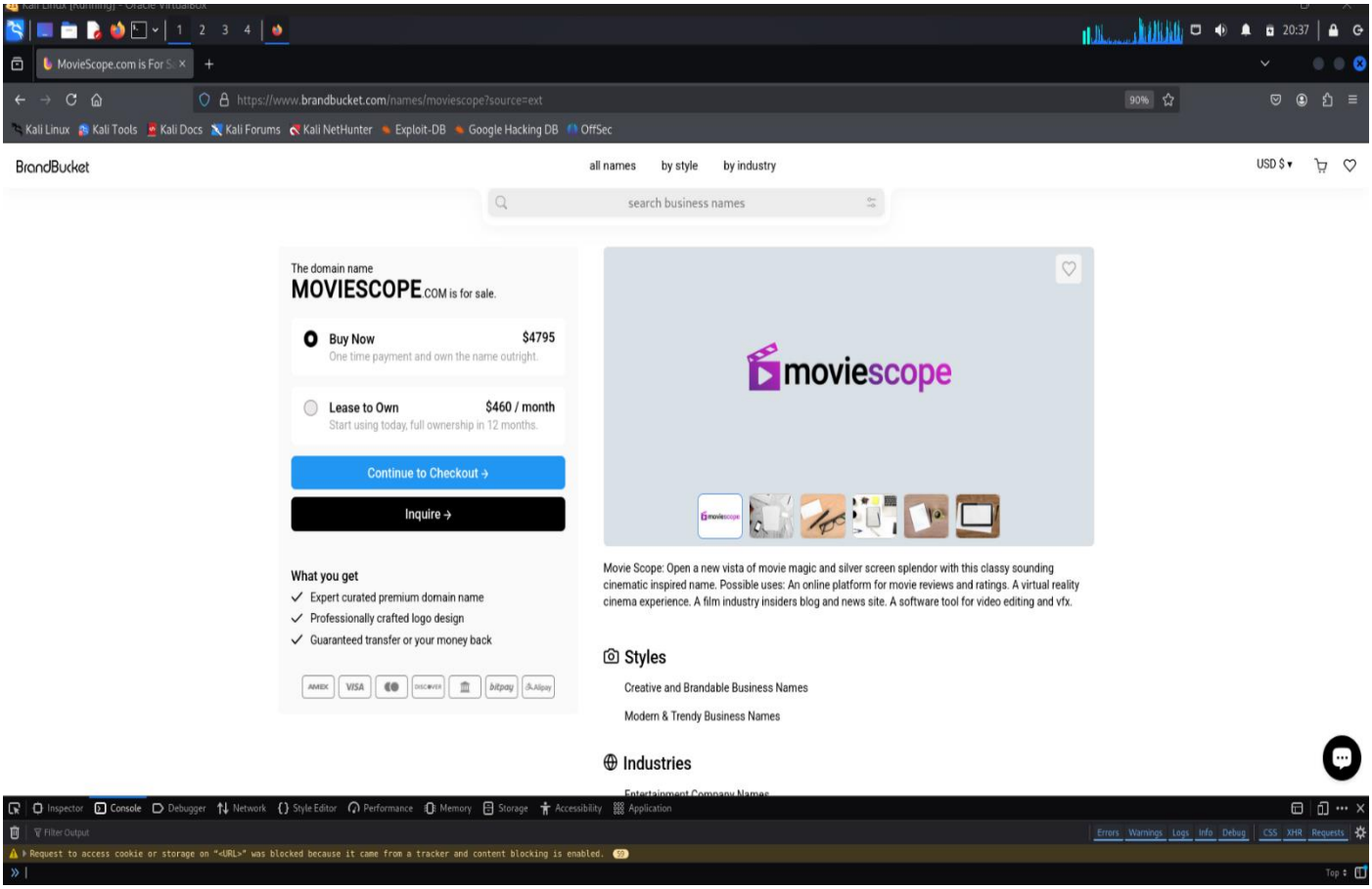
5. The firefox browser opens, type **www.moviescope.com** in the address bar and press **Enter** to browse the moviescope website.



6. Click the **Firebug** add-on on the top-right corner of the **Navigation Toolbar** to enable the **Firebug** control panel.

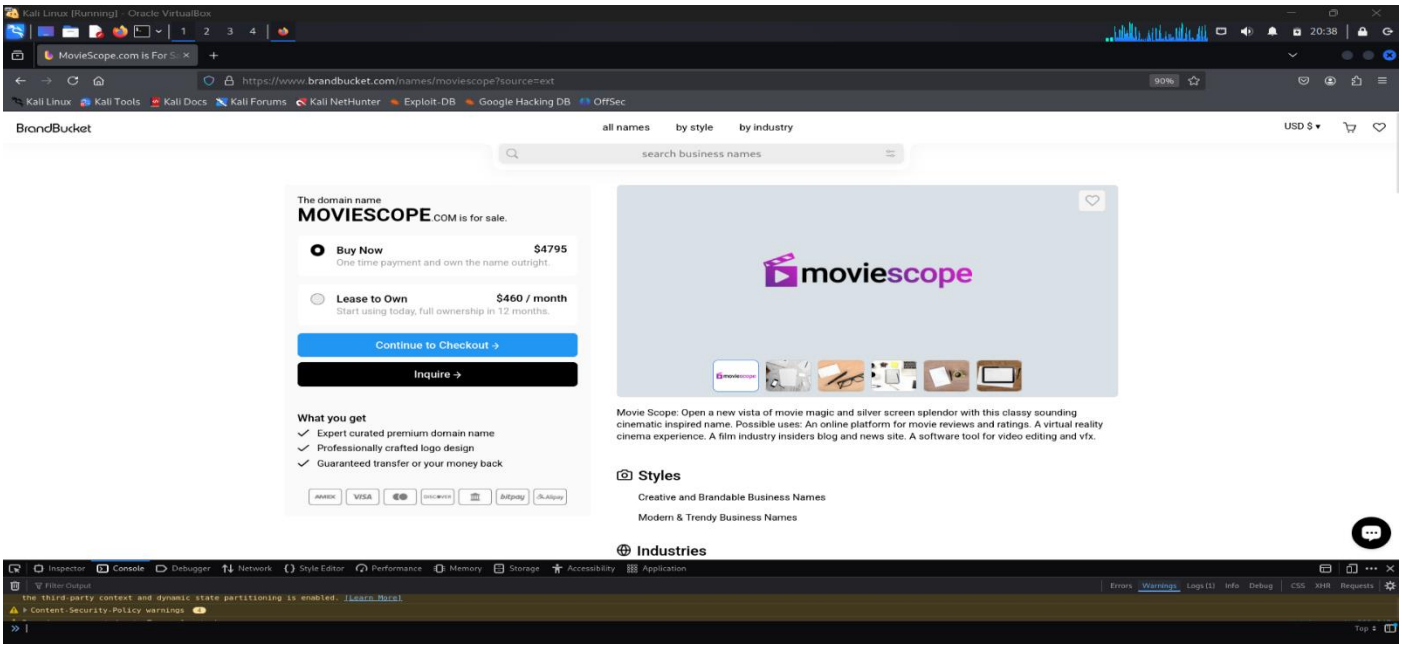
The Firebug panel appears at the lower end of the screen. By default with **Console** tab as shown in the screenshot.

If a firebug prompt appears, click **Don't show this message again.**



7. Click drop-down node from **Security** tab under **Console.** Check only the **Warnings** option.

Press **F5** on the keyboard to refresh the webpage.

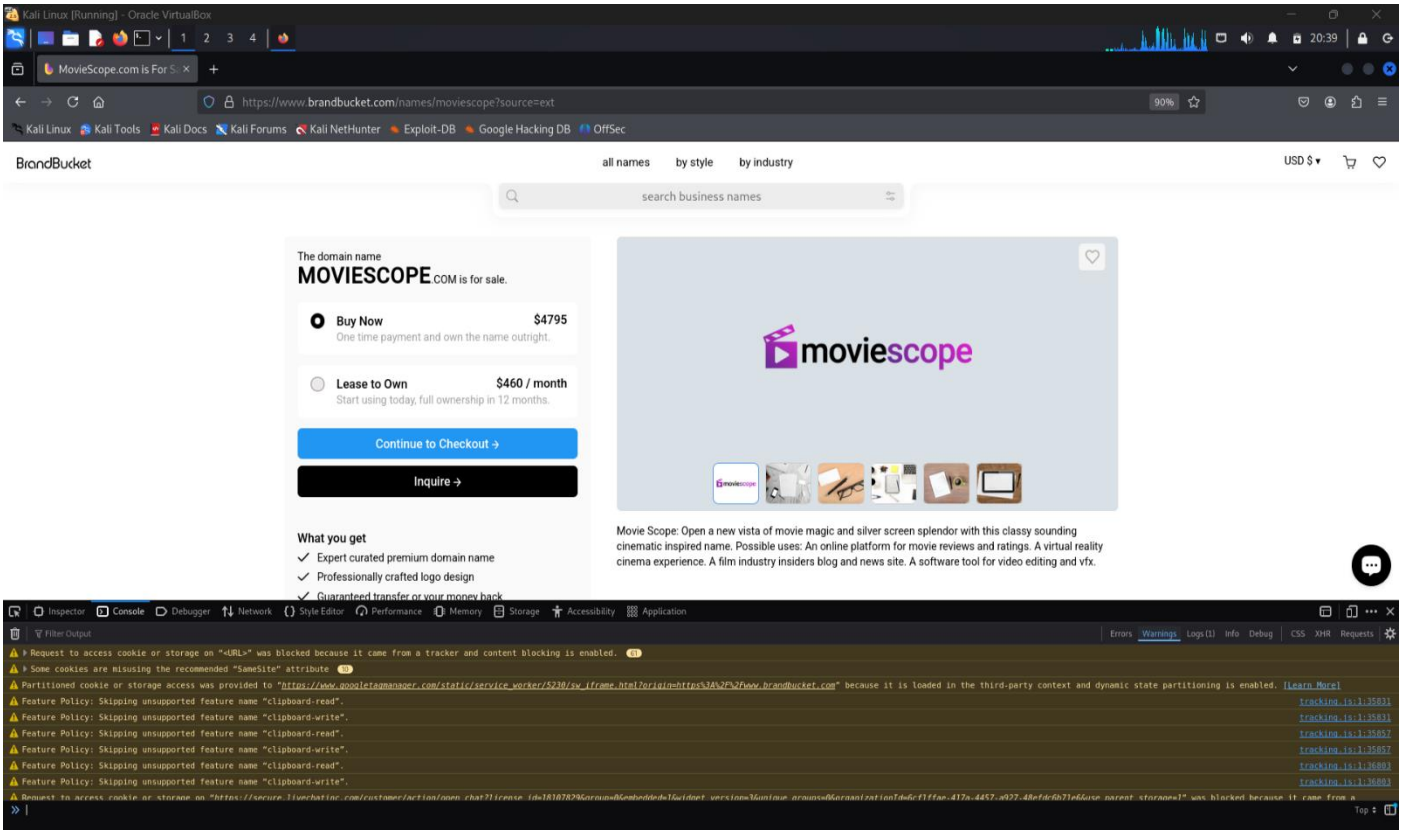


8. Examine the **Security** tab under the **Console** section. Under this tab, **Firebug** displays all the issues related to the security of the website's architecture, as shown in the screenshot.

The warning results may vary depending on the websites you access.

The warning returned in the screenshot states that the password fields are present on an insecure (http://) page.

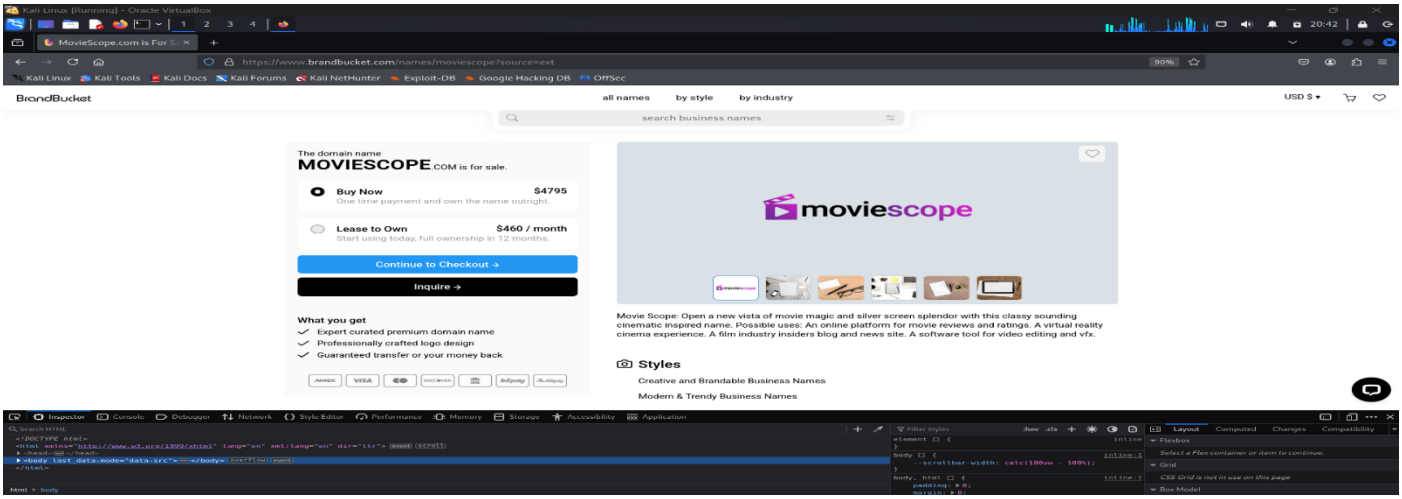
This vulnerability allows attackers to easily sniff the passwords in plain text.



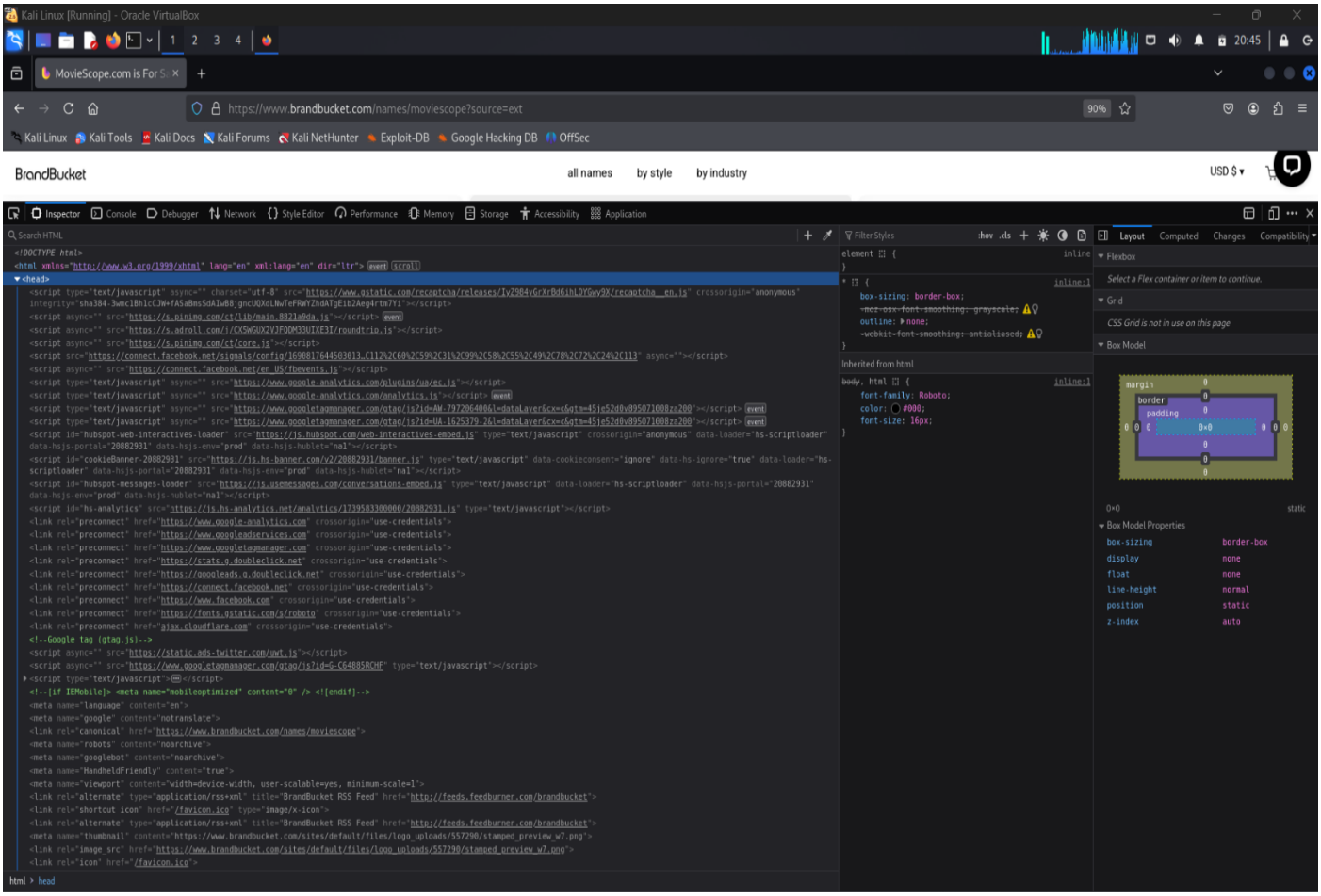
9. Click the **Inspector** tab in the **Firebug UI**. The Inspector section contains two tags: head and body, which contain scripts and text that might reveal the build of the website.

If you find this section empty, refresh the webpage.

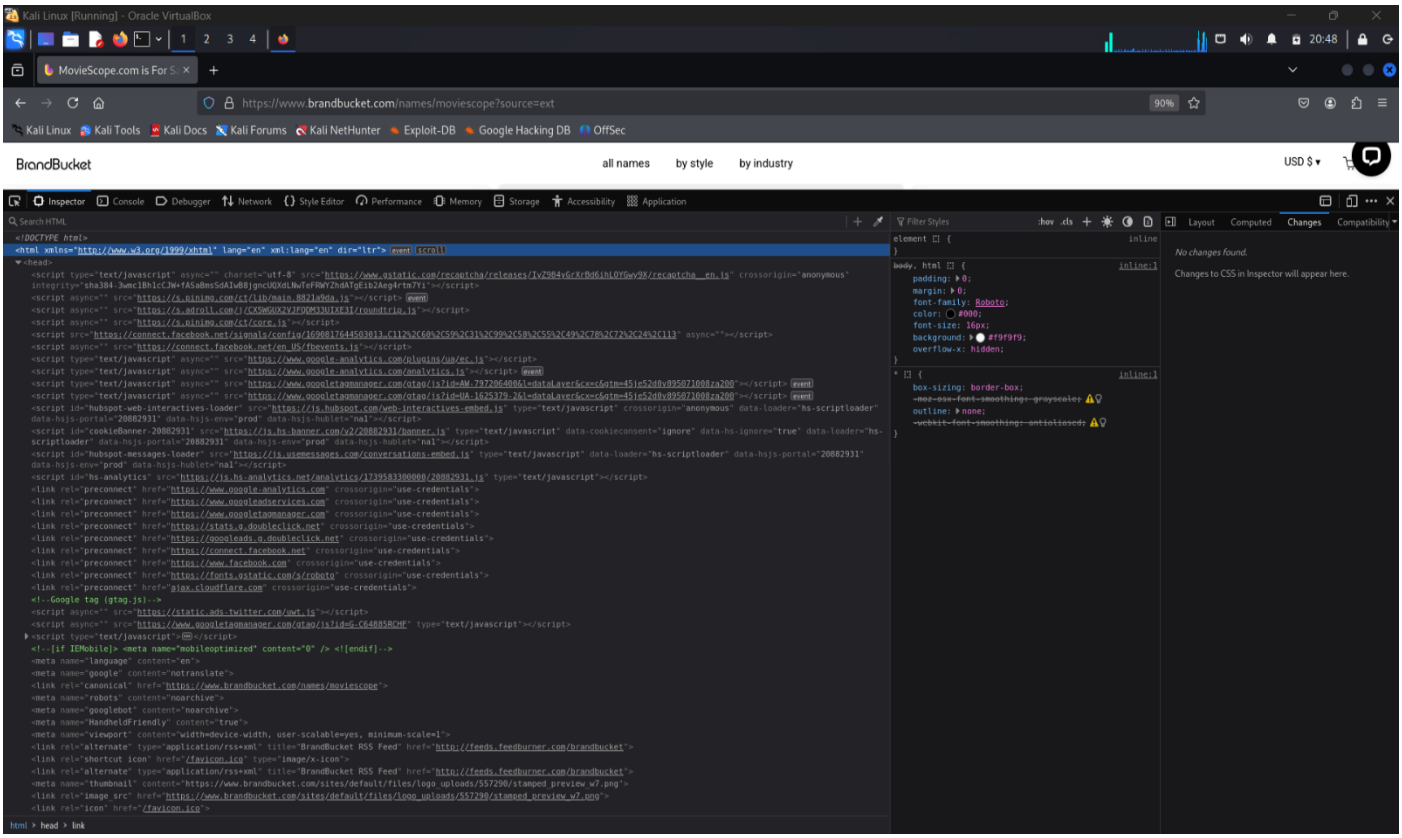
The head and body tags contain information related to the authentication of the username and password fields, such as the type of input that is to be given in the fields (numbers or characters, or combination of numbers and characters, etc.) which allows attackers to narrow down their exploitation techniques.



10. Expand these nodes and observe the script written to develop the webpage.

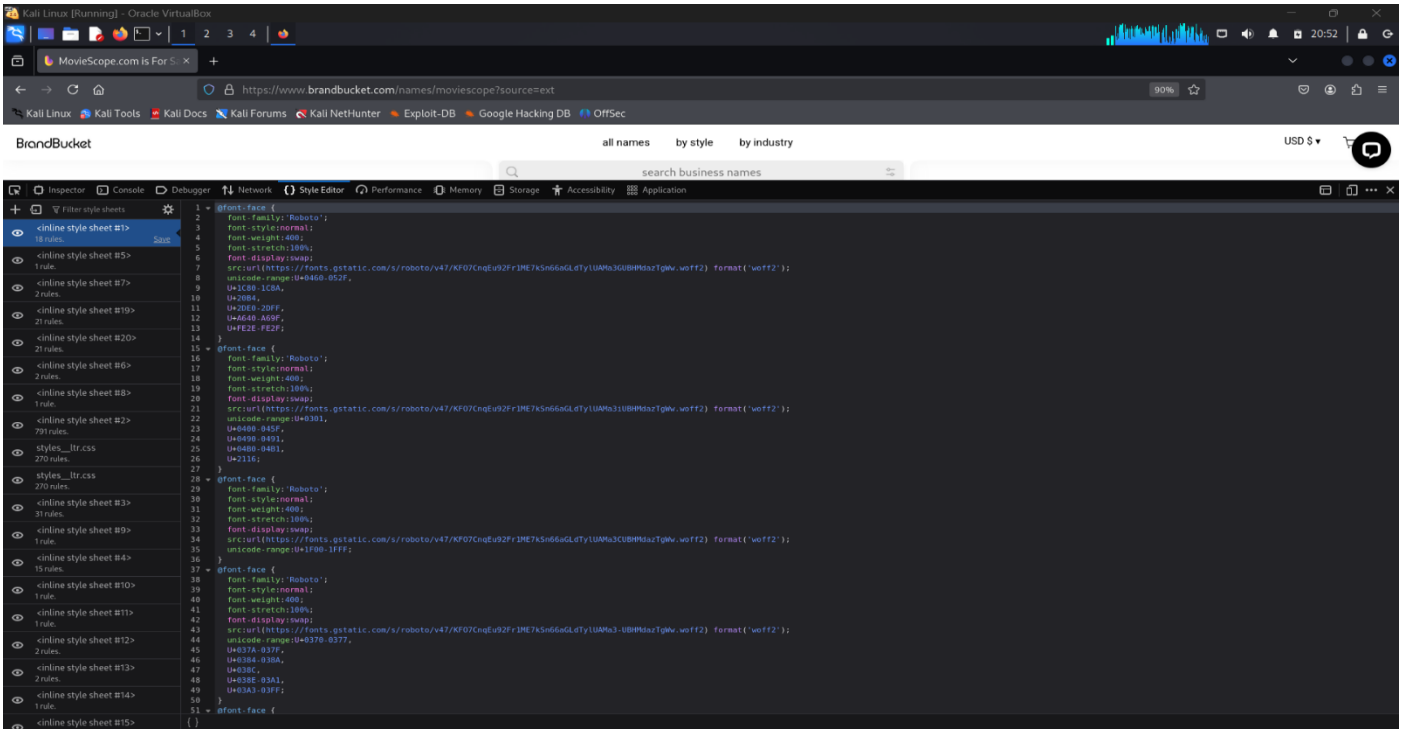


11. Refer to tabs such as **Rules, Computed, Animations** and so on in the right pane in order to observe the script used to design the webpage.



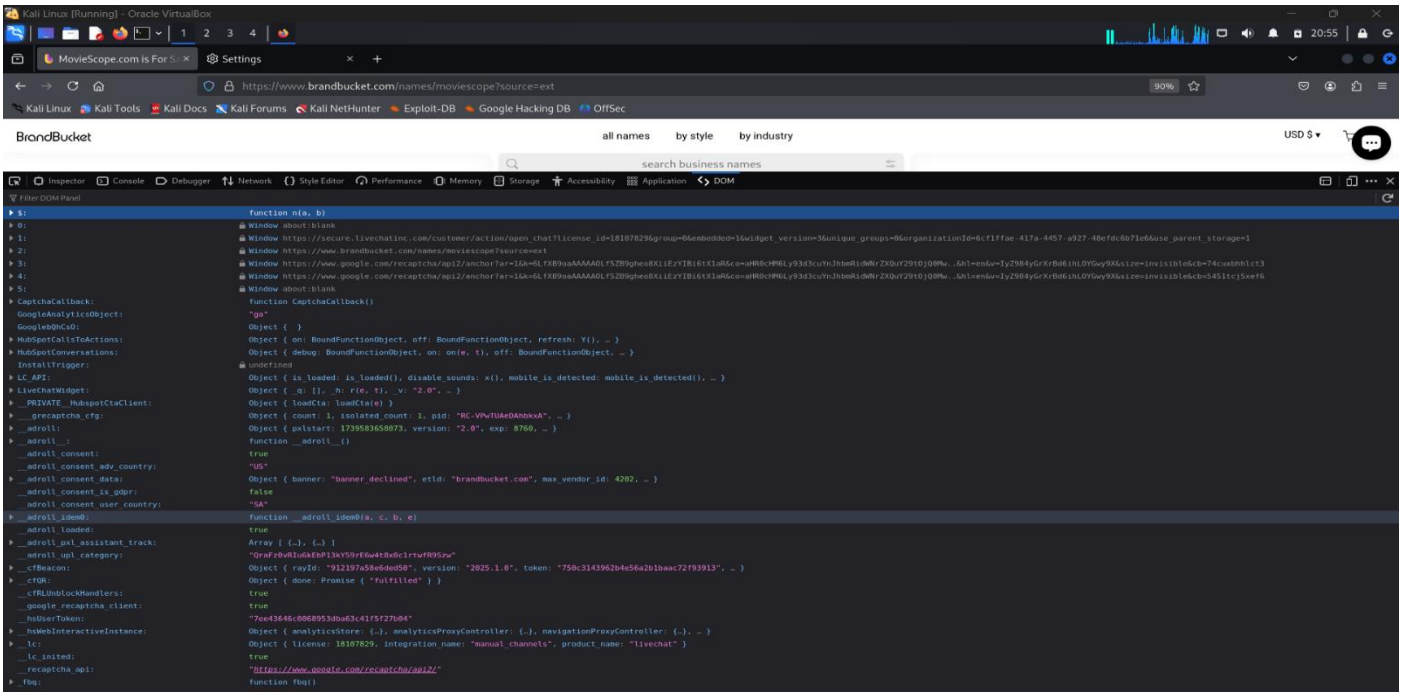
12. The **Style Editor** tab provides the information of **CSS** and **Script** of the **HTML** and **Java** scripts that were used to design the webpage.

Attackers could use these scripts to build a similar website (cloned website) which could be used to serve malicious purposes such as harvesting the data entered in specific fields.



13. Click **DOM (Document Object Model)** tab in the **Firebug** control panel.

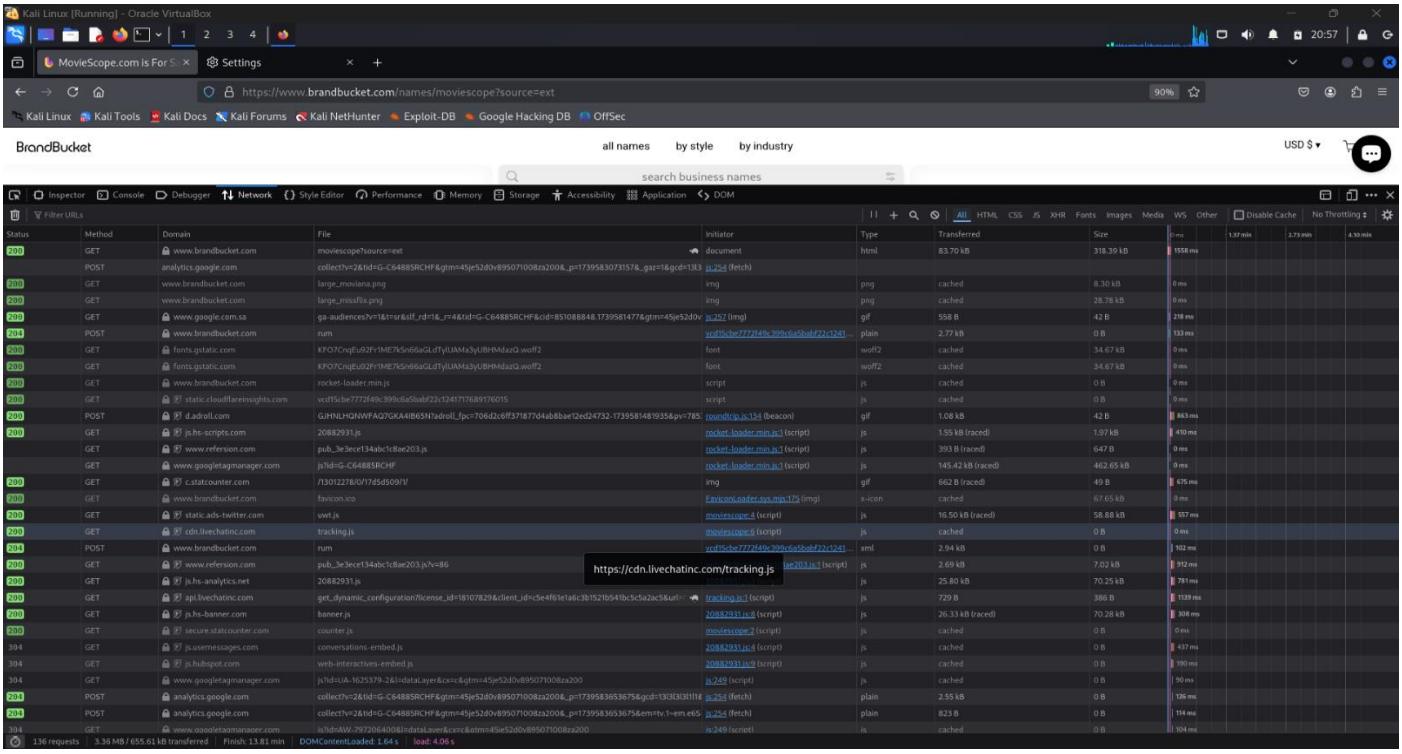
This tab contains scripts written in various web technologies such as html5, jQuery, etc. This allows attackers to perform exploitation techniques on a specific version of a web application, which leads to expose sensitive information.



14. Click the **Network** tab in the **Firebug** control panel.

By default **All** tab under this section is selected.

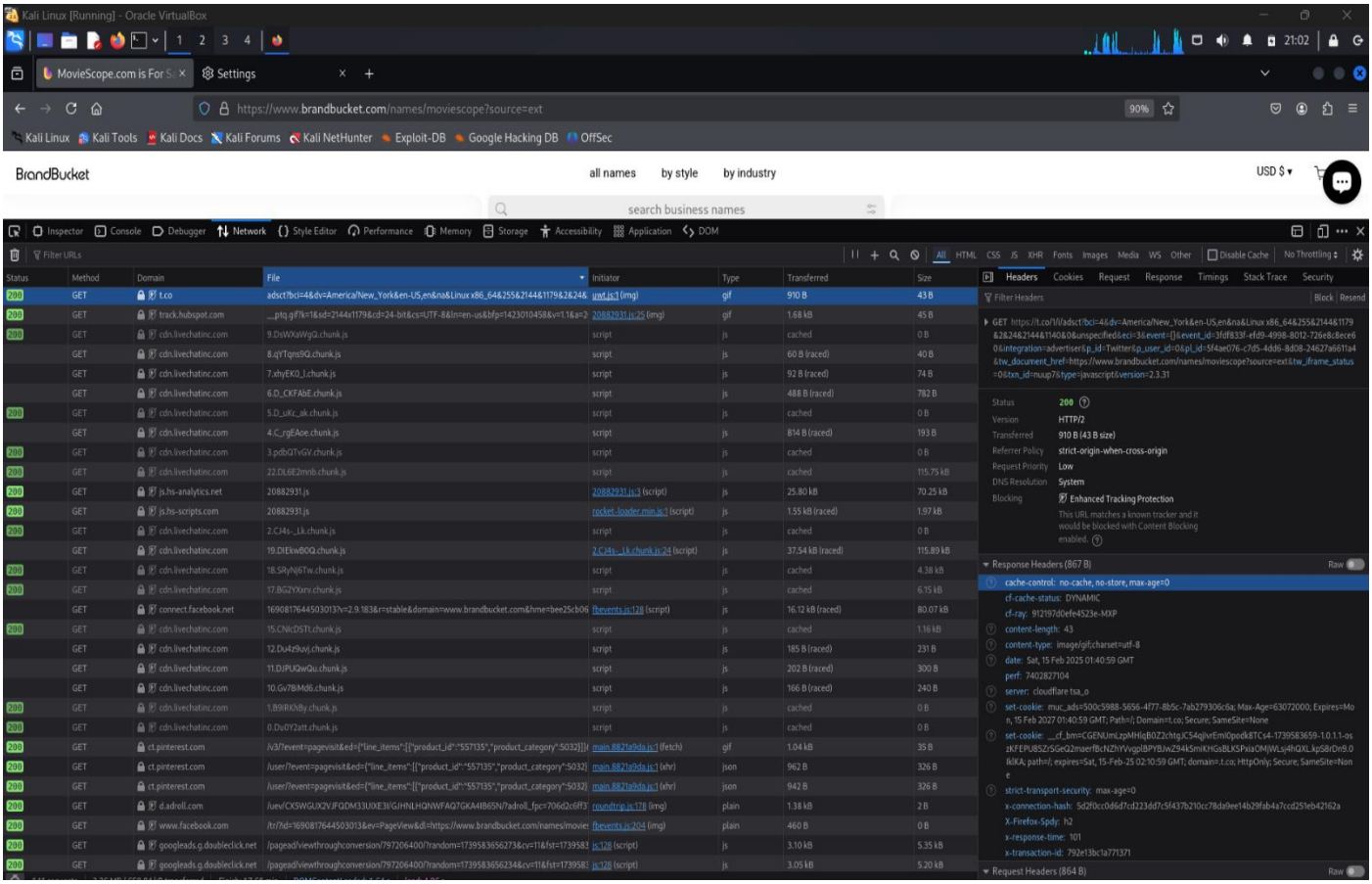
This tab displays the **GET** requests and responses for all the items in the Net section such as **HTML, CSS,** etc., along with their size, status, timeline, domain and remote IP.



15. Under the **All** tab, click a **GET** request related to moviescope.

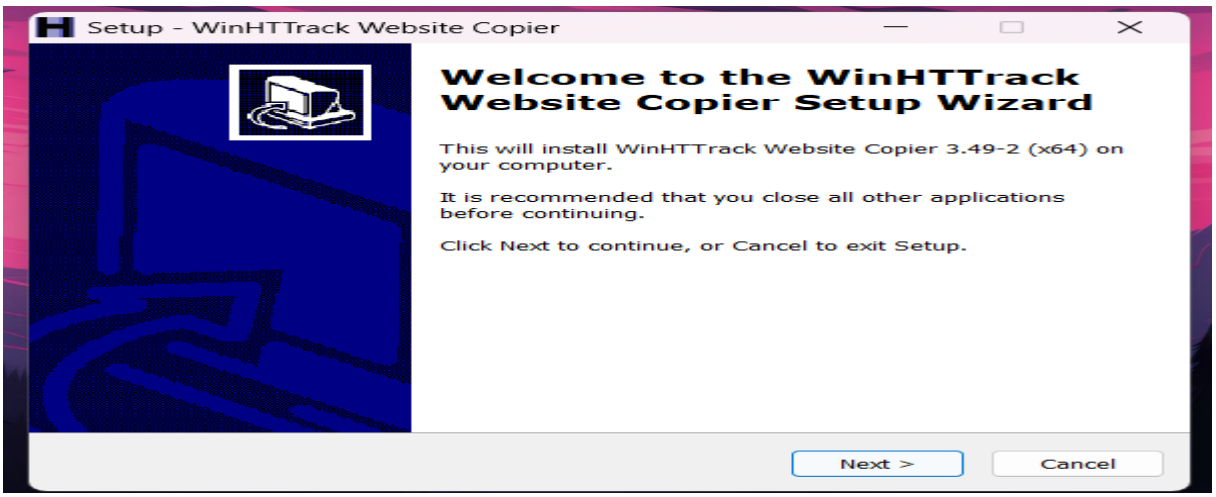
Under the **Headers** tab, expand the **Response Headers** node and observe the **Server Name (IIS)** and its version, along with the **Web Application Framework (ASP.NET)** used to develop the website and its version. By learning this, attackers can target the vulnerabilities of that specific version in an attempt to exploit the web application.

Attackers can use sniffing techniques to steal the cookies and manipulate them, thereby hijacking the session of an authenticated user without the need of entering legitimate credentials.



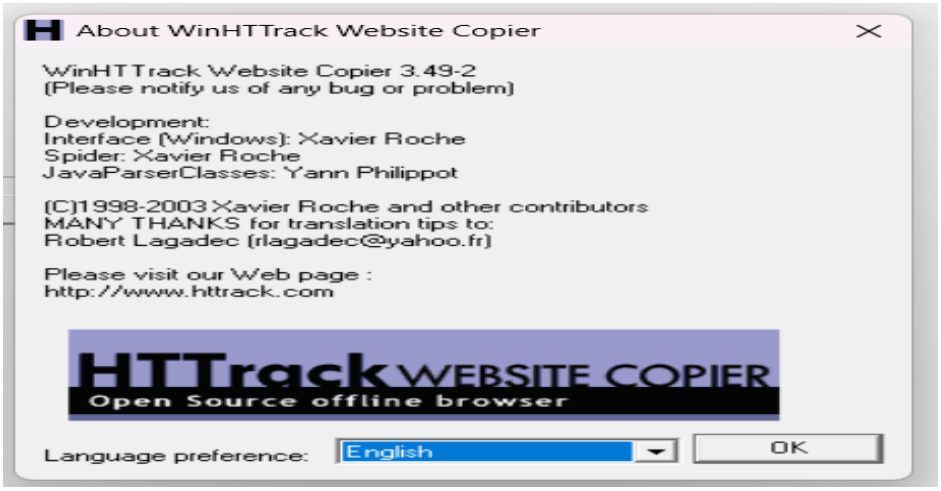
Exercise 3: **Mirroring Website Using HTTrack Web Site Copier**

1. Install https://www.httrack.com/page/2/
2. Follow the wizard steps to install **HTTrack Web Site Copier.**

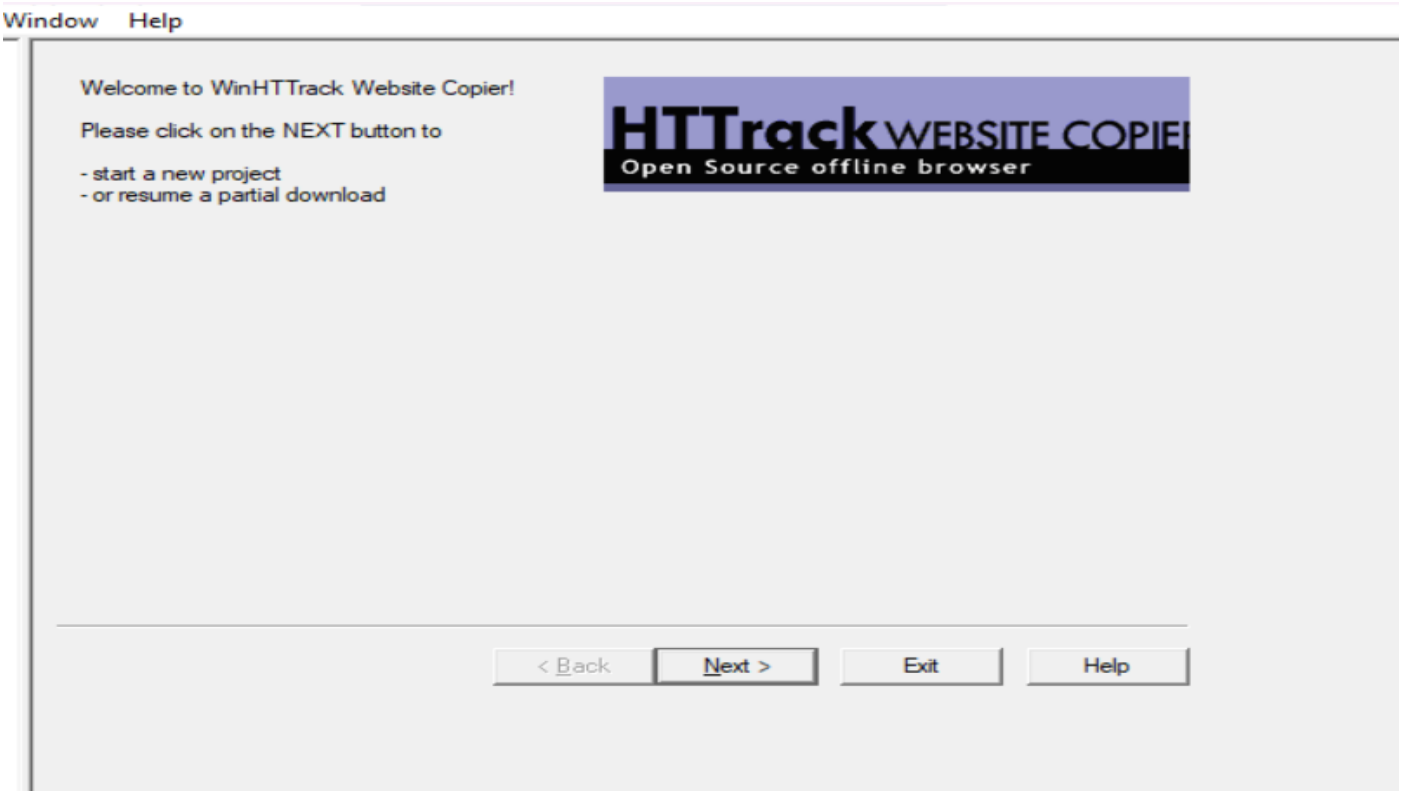


3. HTTrack application launches and the default application window appears as shown in the screenshot.

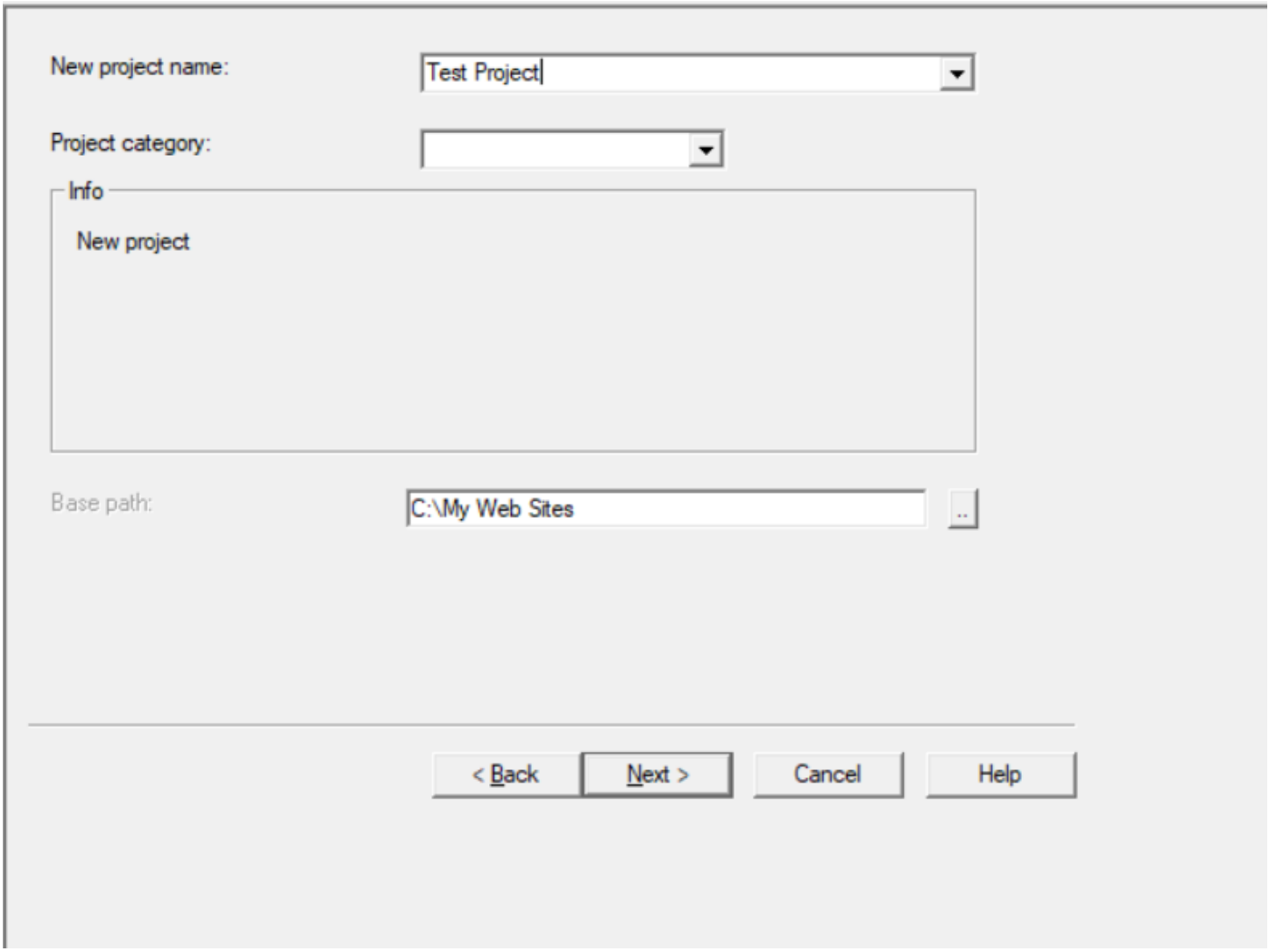
About WinHTTrack Website Copier window appears, click **OK.**



4. Click the **Next** button.

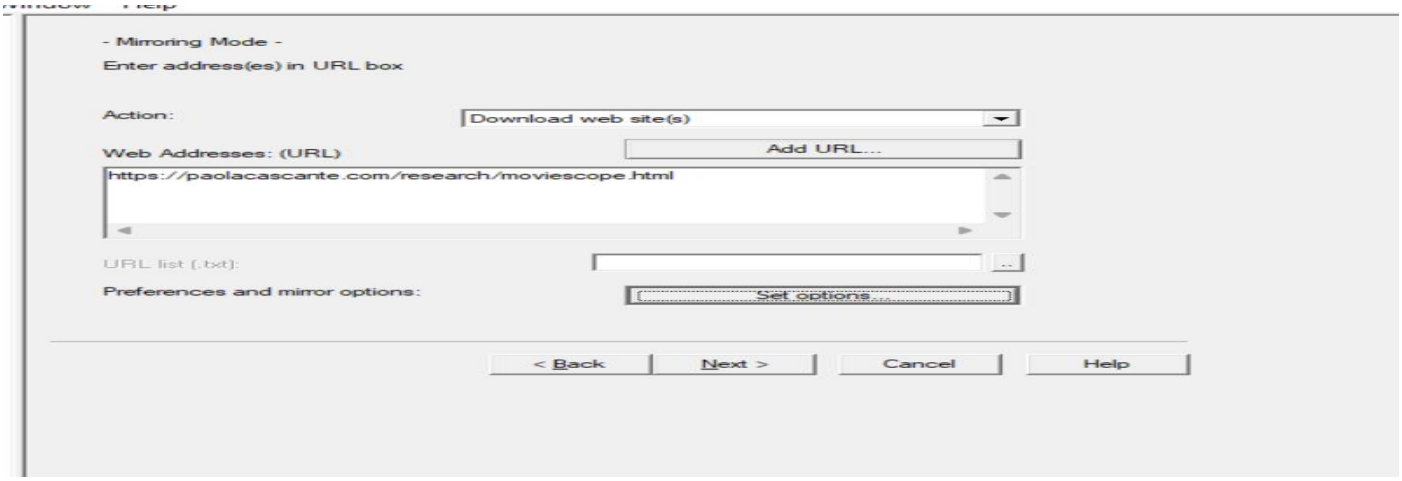


5. Type a name for your project (here **Test Project**) in the **New project name** field and verify that the **Base path** is **C:\My Web Sites**. Then click the **Next** button.

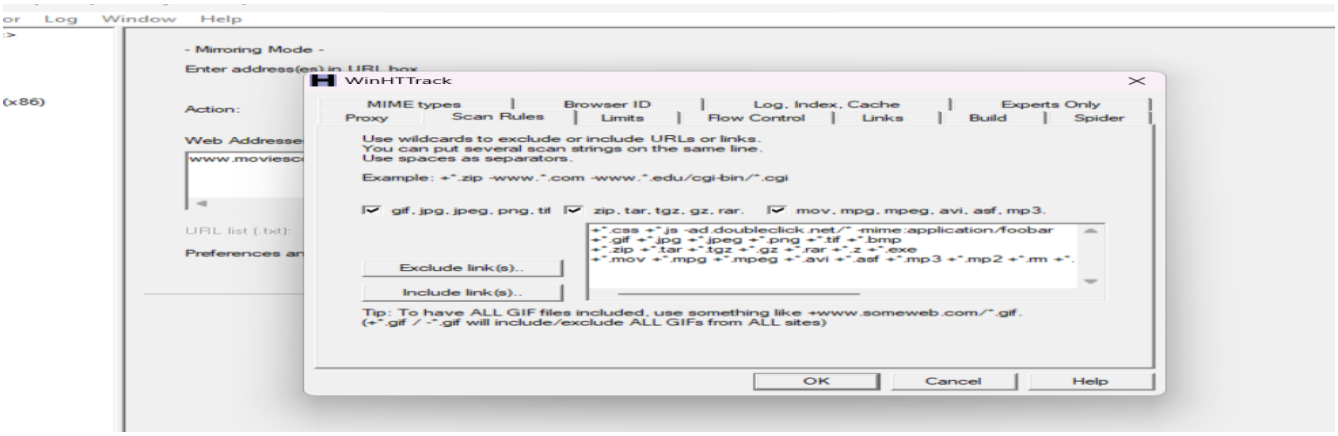


6. Type **www.moviescope.com** in the **Web Addresses: (URL)** field and click **Set options** button.

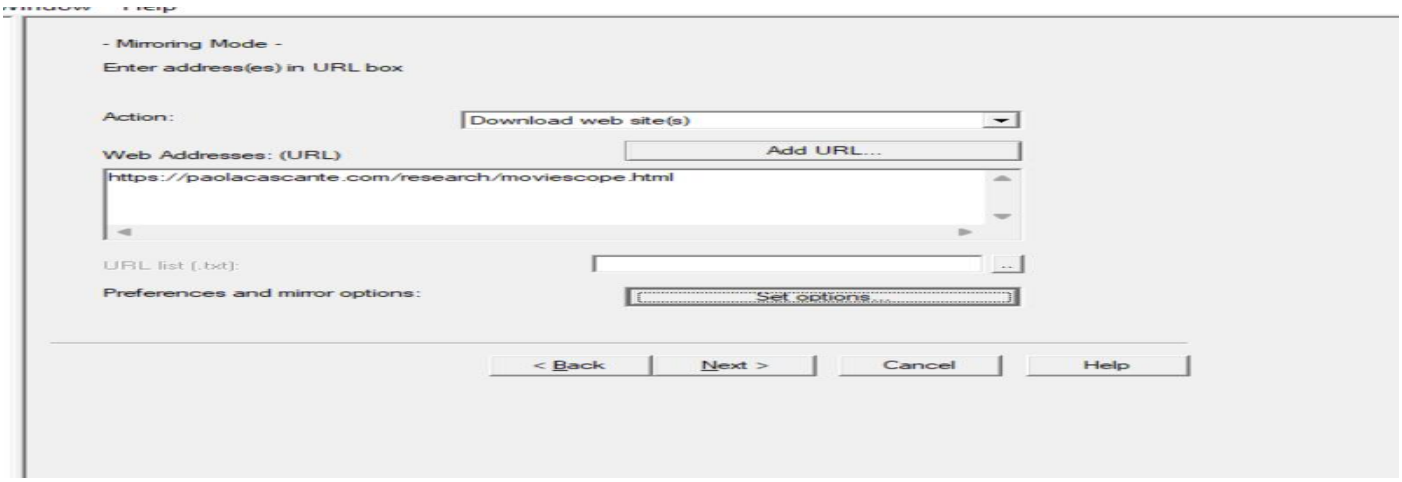
I have typed another site because www.moviescope.com didn't work so I typed https://paolacascante.com/research/moviescope.html



7. WinHTTrack window appears, click the **Scan Rules** tab and select the check boxes for the file types as shown in the screenshot, then click **OK.**

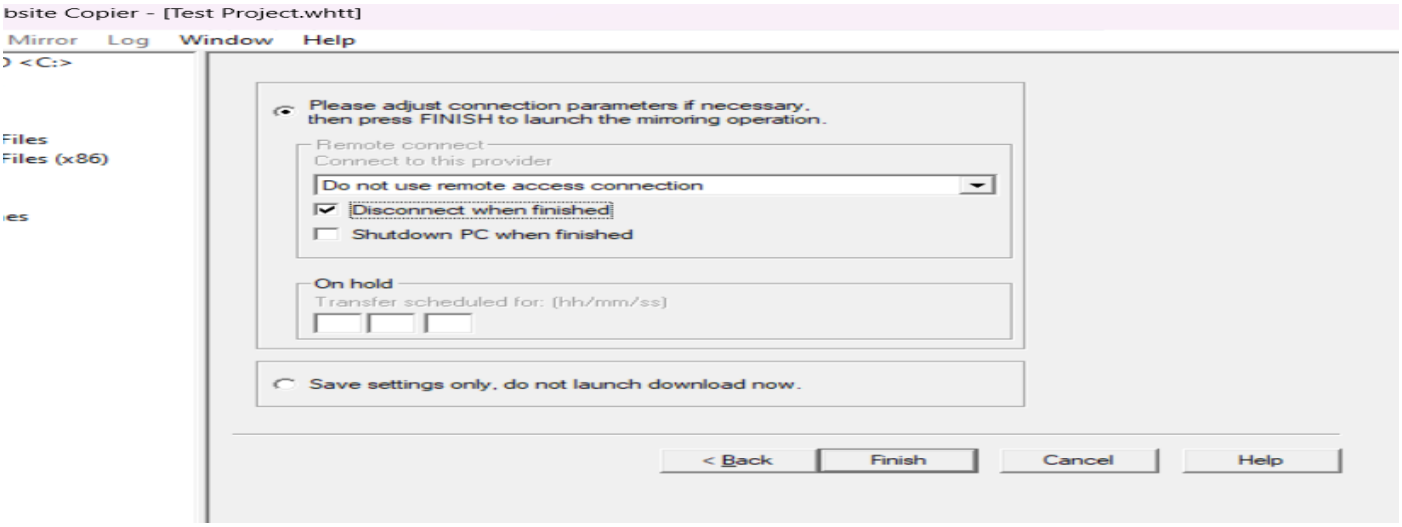


8. Click the **Next** button to procceed.

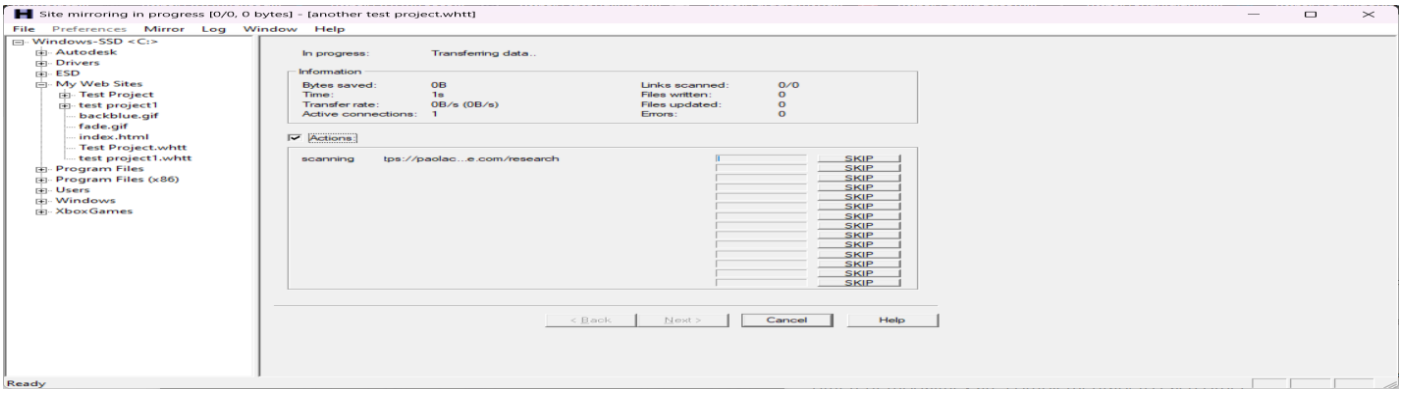


9. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation** and check **Disconnect when finished** option.

Now click **Finish** to start mirroring the website.



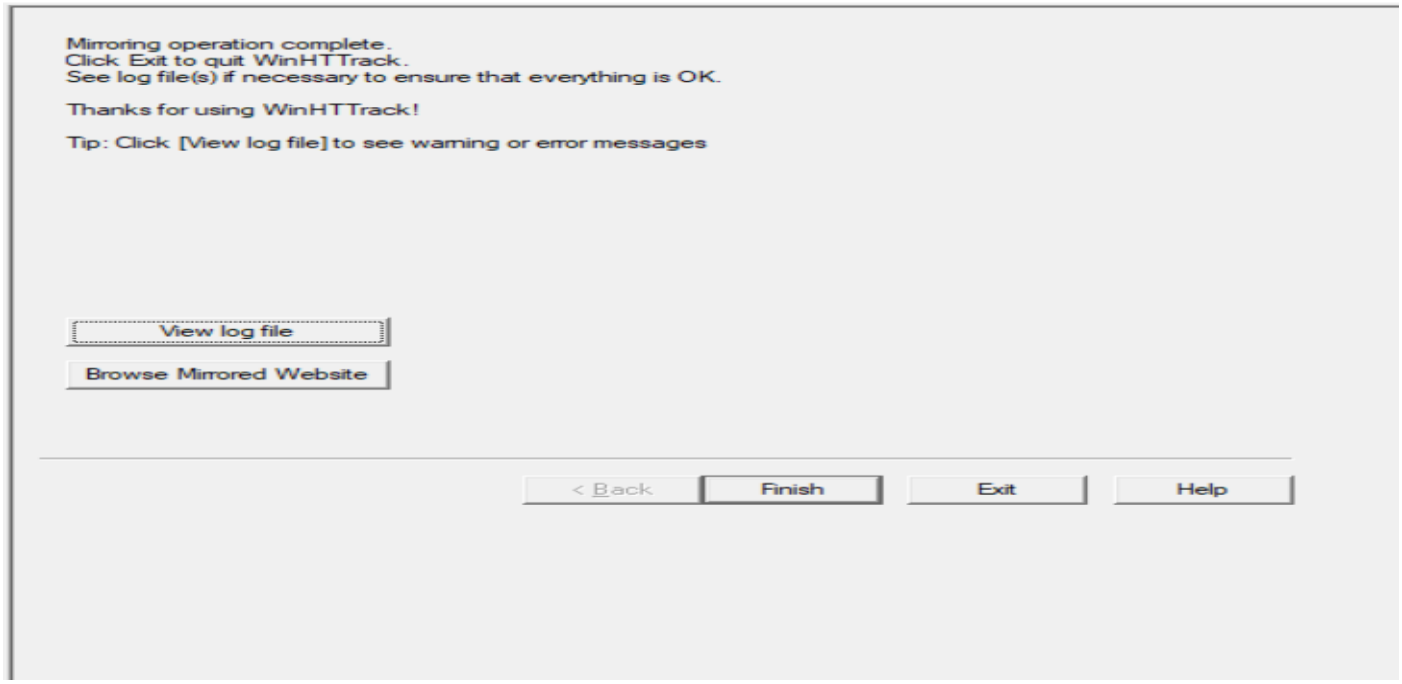
10. Site mirroring progress will be displayed as shown in the screenshot.



11. WinHTTrack displays the message **Mirroring operation complete** once the site mirroring is completed. Click **Browse Mirrored Website.**

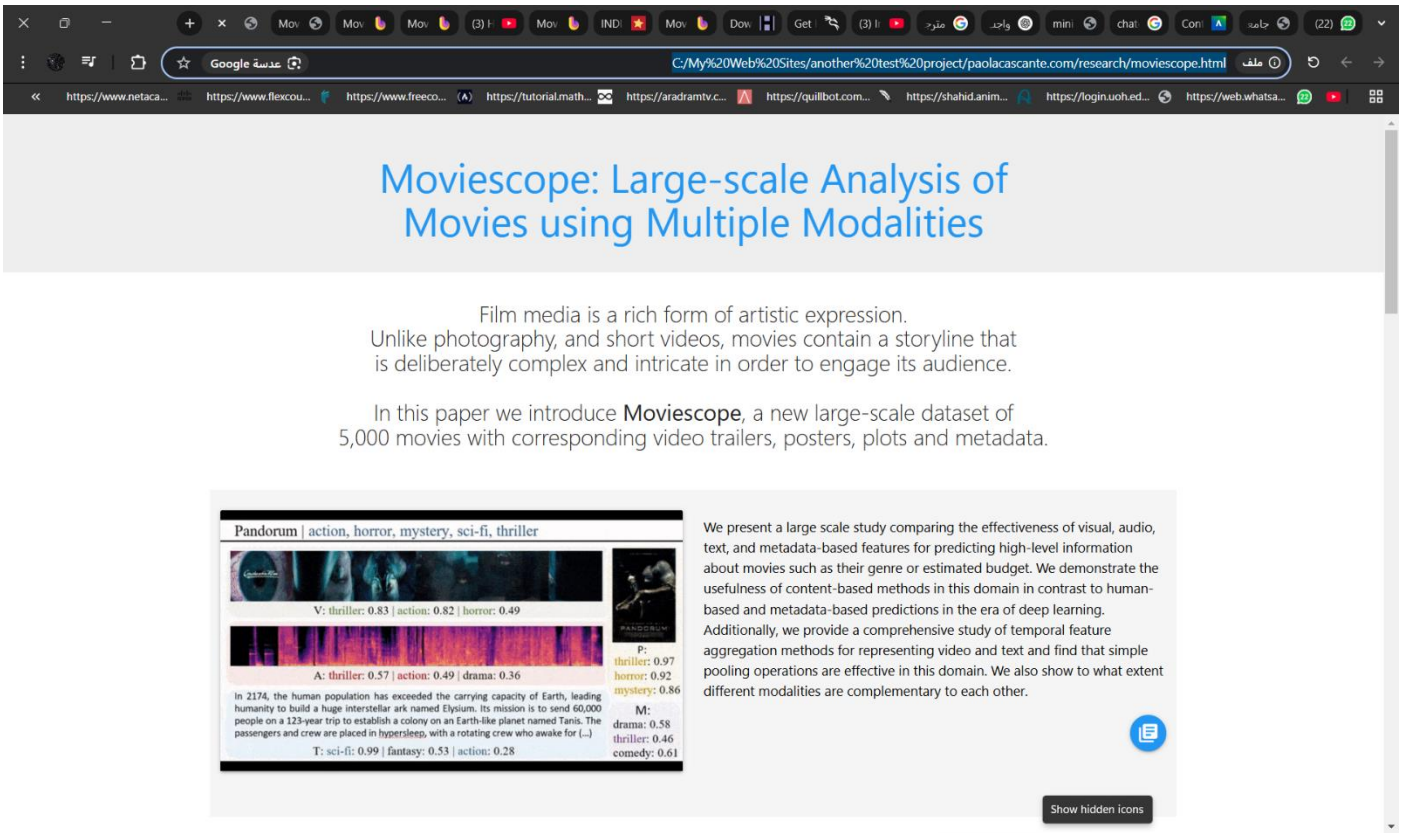
12. **How do you want to open this file?** pop-up appears, select any browser (here **Chrome)** and click **OK.**

I have google chrome in default browser already



13. The mirrored website for **www.moviescope.com** is shown in the browser. The URL displayed in the address bar indicates that the website's image is stored on the local machine.

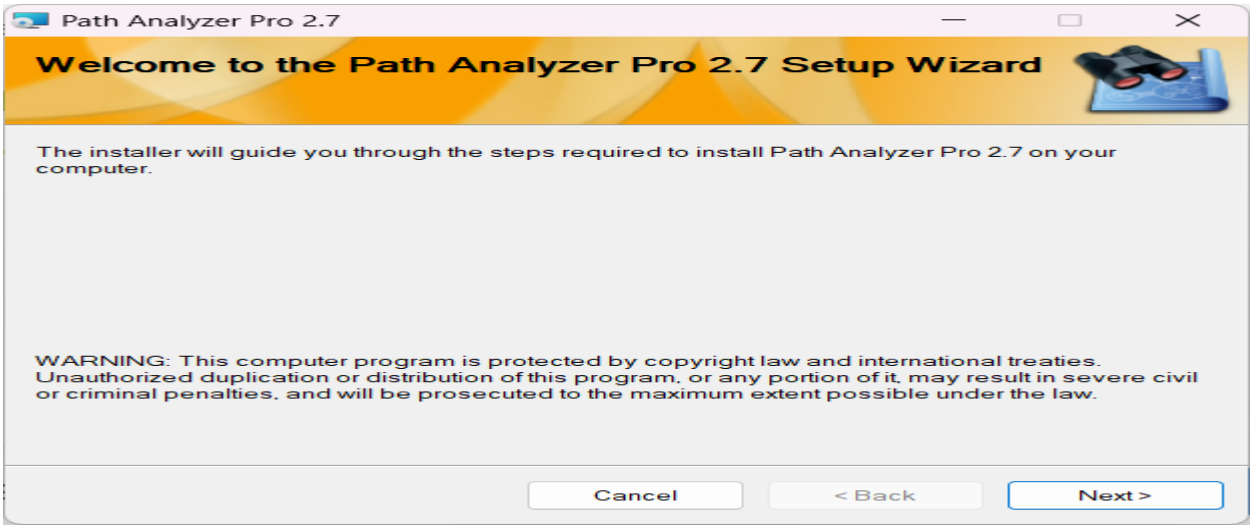
If the webpage does not open, navigate to the directory where you mirrored the website and open index.html with any browser.



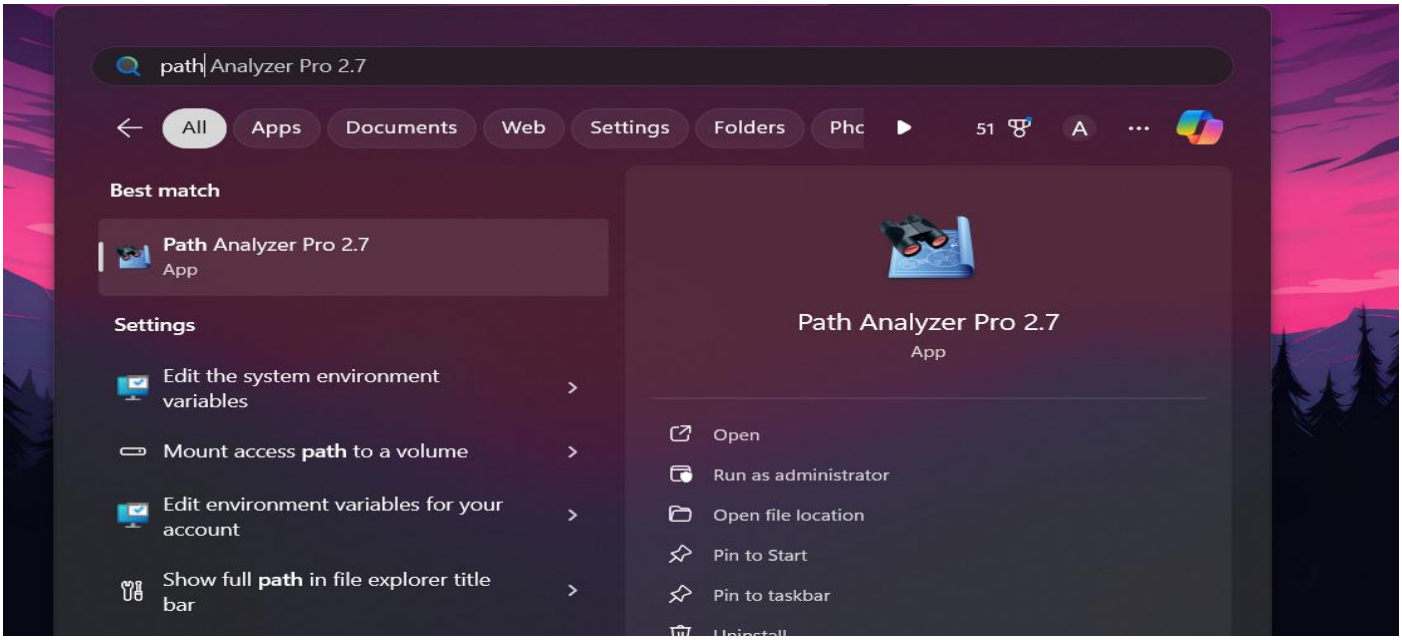
Exercise 4: **Advanced Network Route Tracing Using Path Analyzer Pro**

1. Install https://path-analyzer-pro.software.informer.com/download/#downloading
2. Follow the wizard driven installation steps (select all default options) to install Path Analyzer Pro.

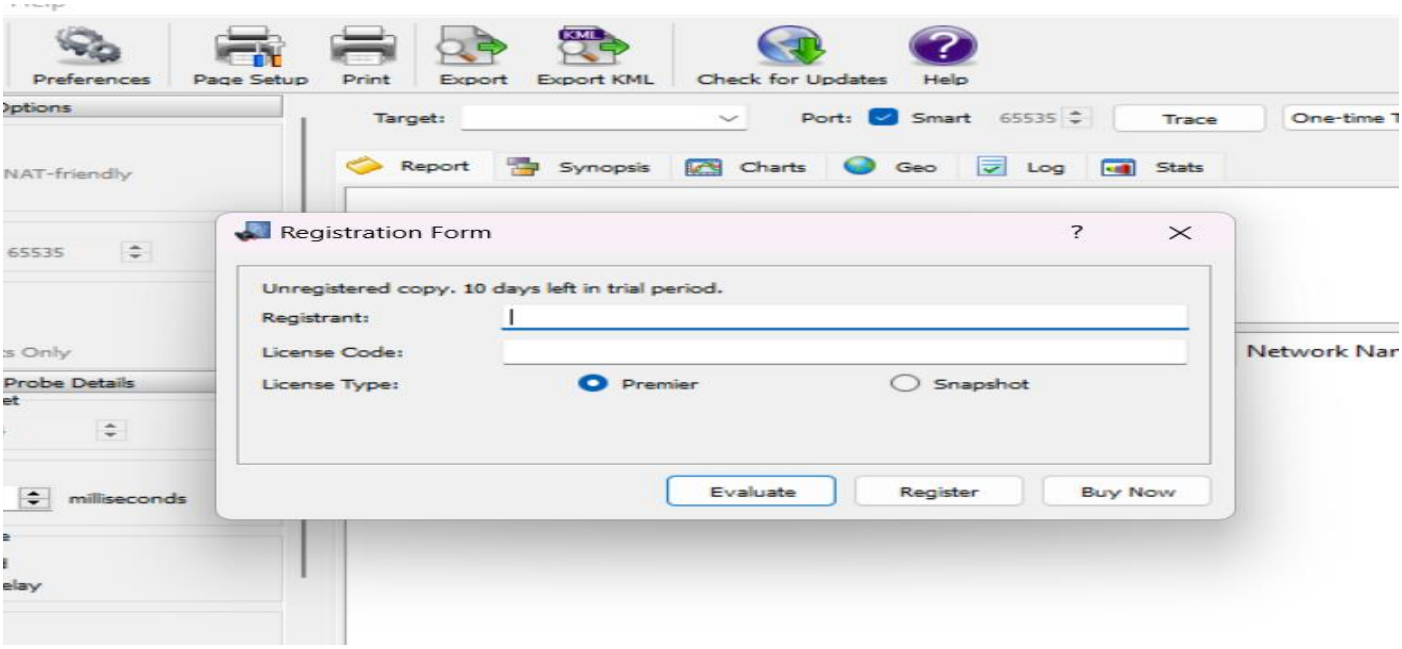
If an Open File - Security Warning pop-up appears, click Run.



3. Launch **Path Analyzer Pro** from the **Start** menu.



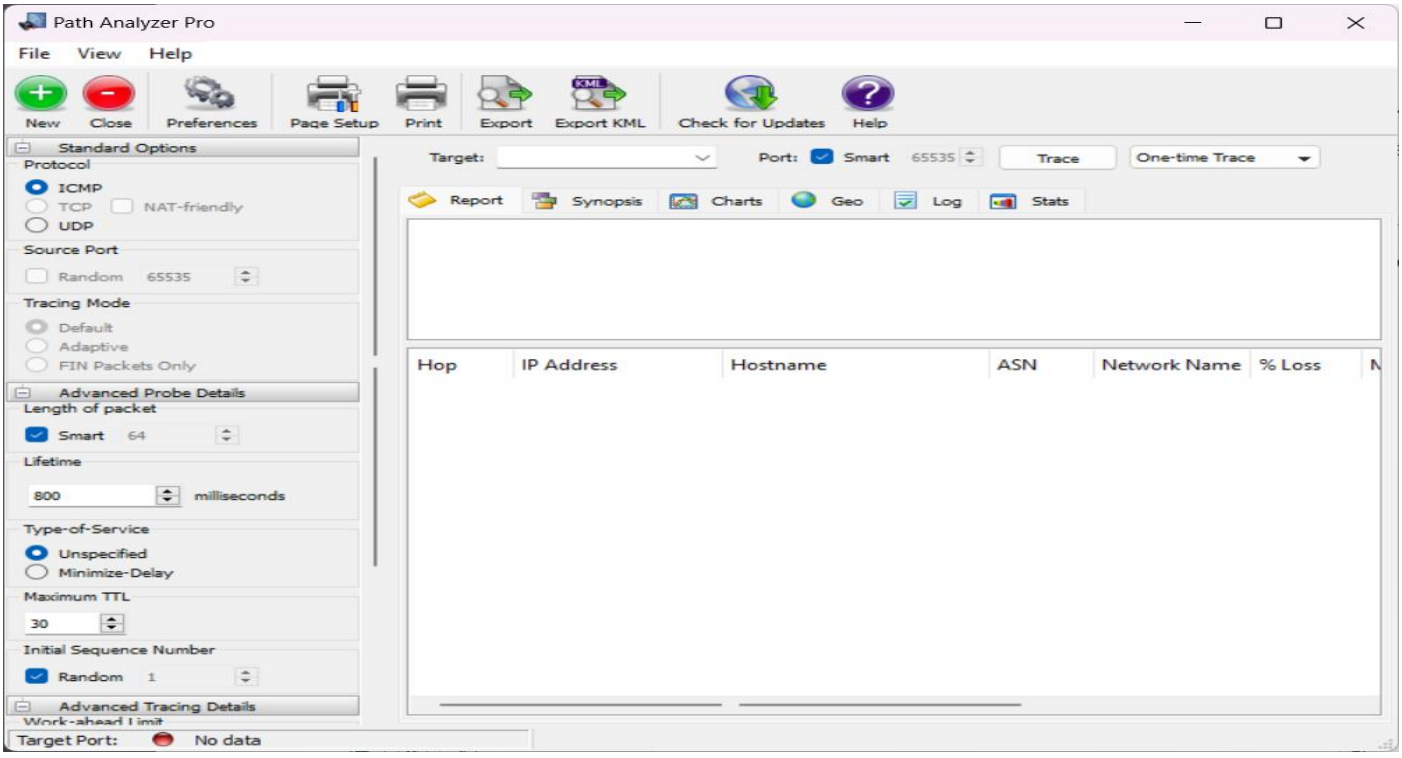
4. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up. Click **Evaluate** in the pop-up.



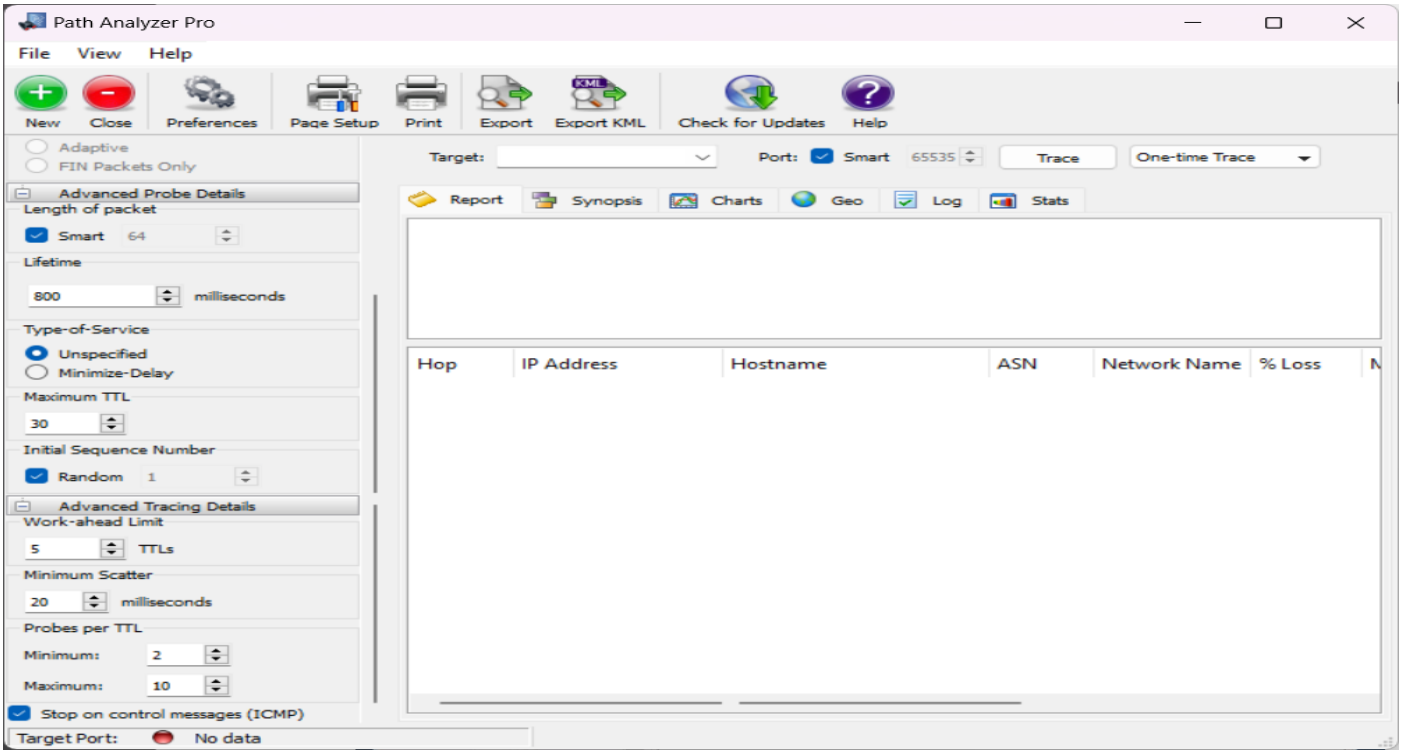
5. The main window of **Path Analyzer Pro** appears as shown in the screenshot.

In the **Standard Options** and **Advanced Probe Details** sections, a few options are set by default.

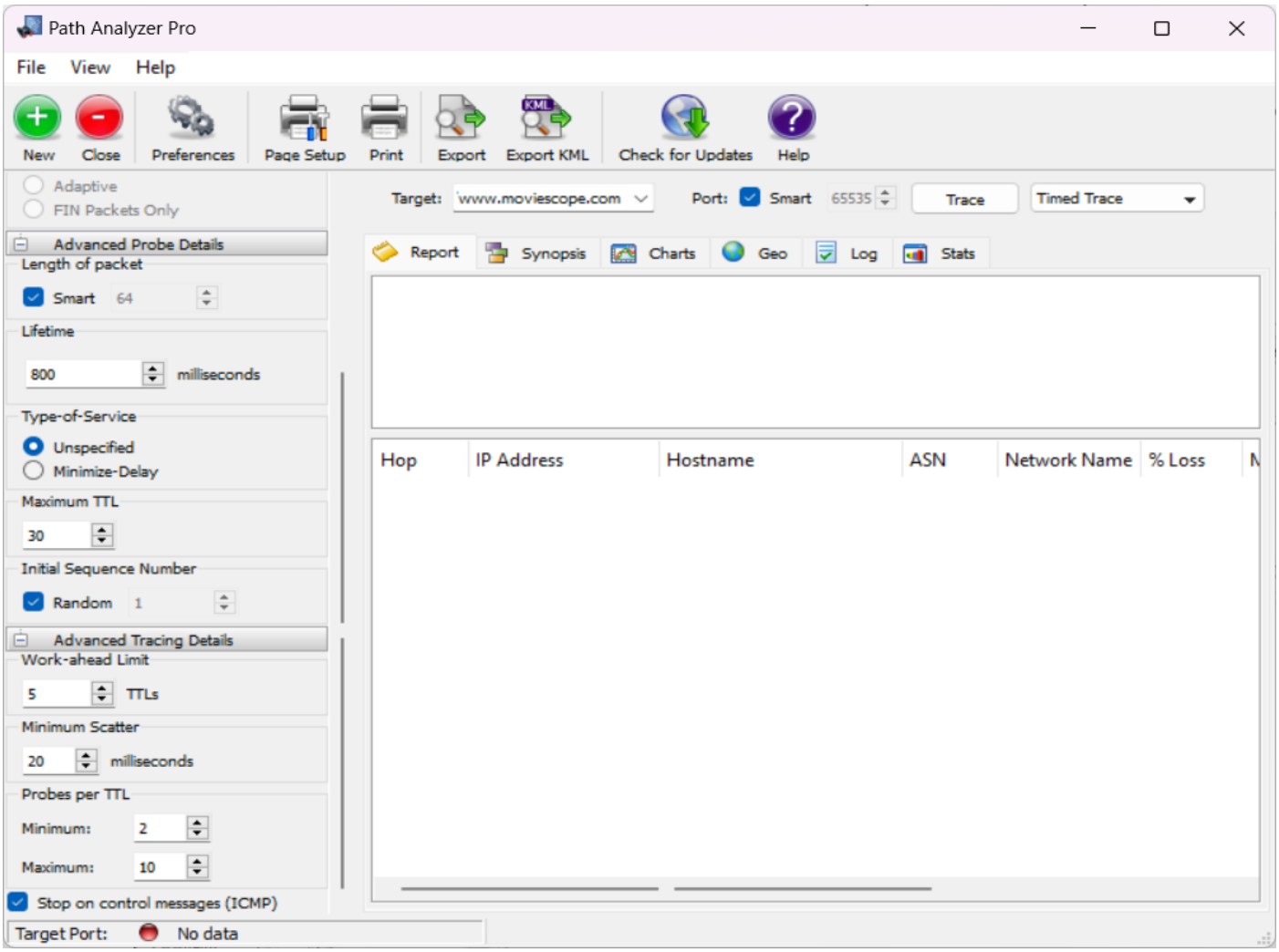
- Ensure that the **ICMP** radio button under the **Protocol** field is selected.
- In the **Advanced Probe Details** section, ensure that the **Smart** option is checked under the **Length of packet field**.



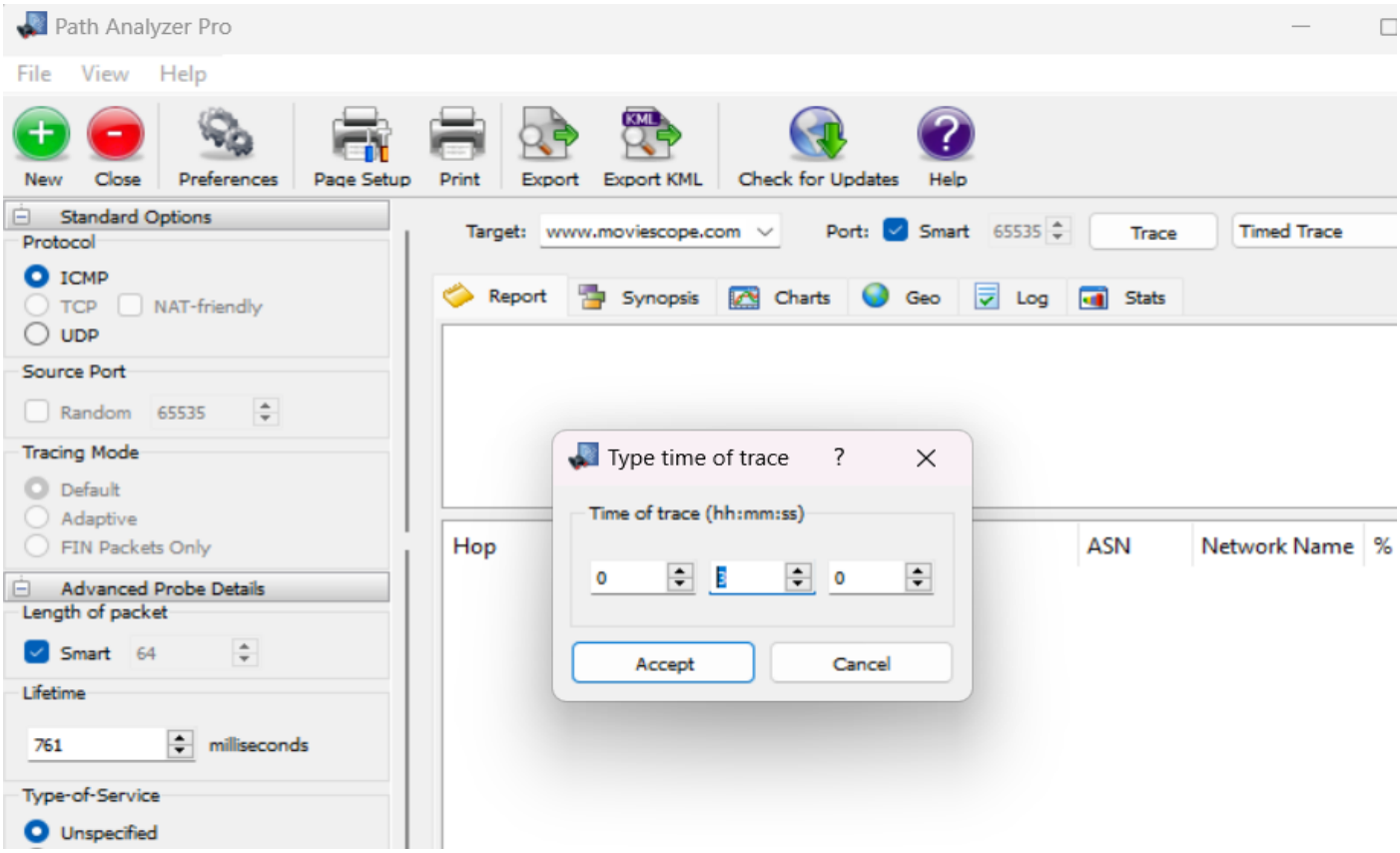
6. In the **Advanced Tracing Details** section, a few options are set to default.
   Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.



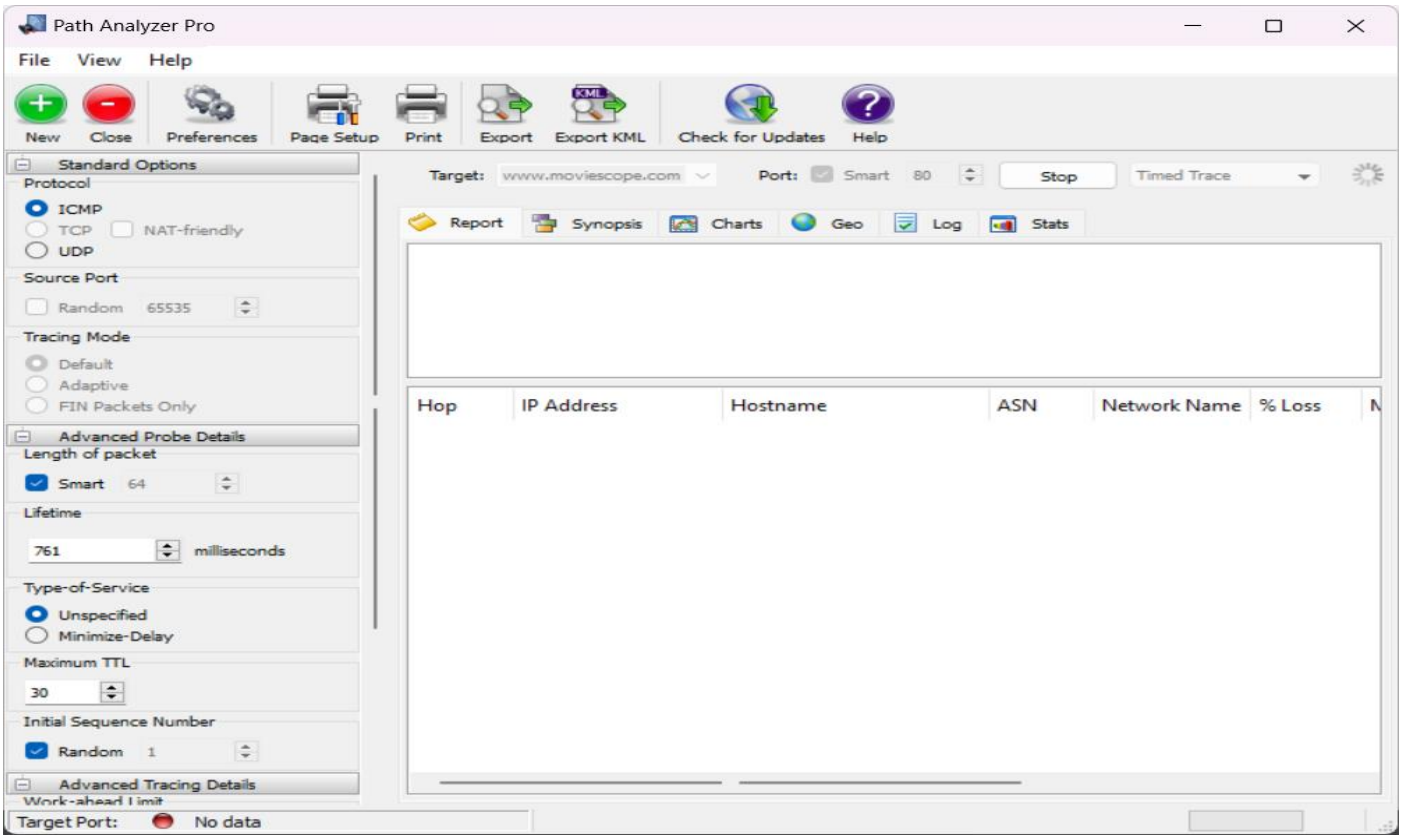
7. To perform the trace, enter the host name in the **Target** field, for instance **http://www.moviescope.com**, check **Smart** under the **Port** field as default **(65535)** and choose duration of time as **Timed Trace** from the drop-down list and click **Trace.**



8. The **Type time of trace** dialog box appears. Specify the time of trace in HH: MM: SS format and click **Accept.**



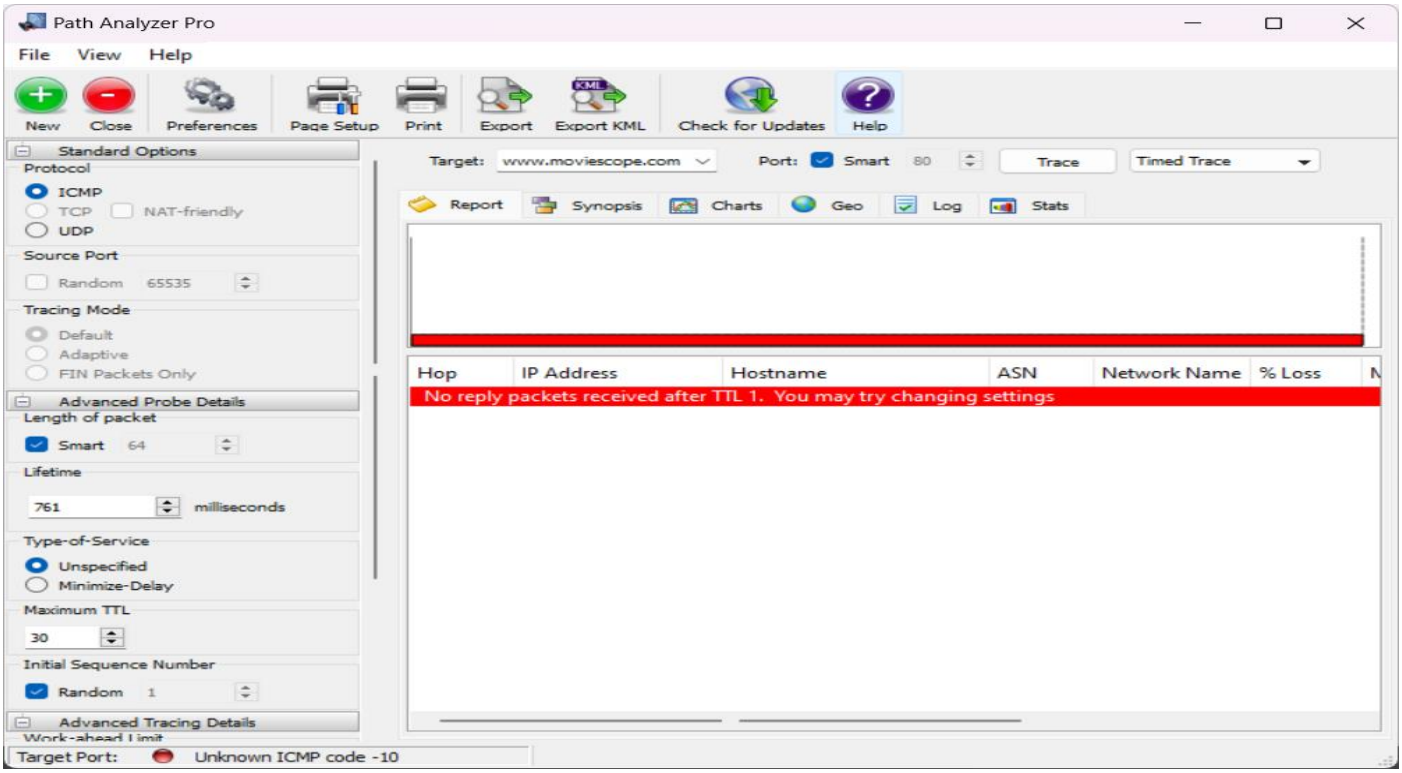
9. While Path Analyzer Pro performs this trace, the Trace tab changes automatically to **Stop.**



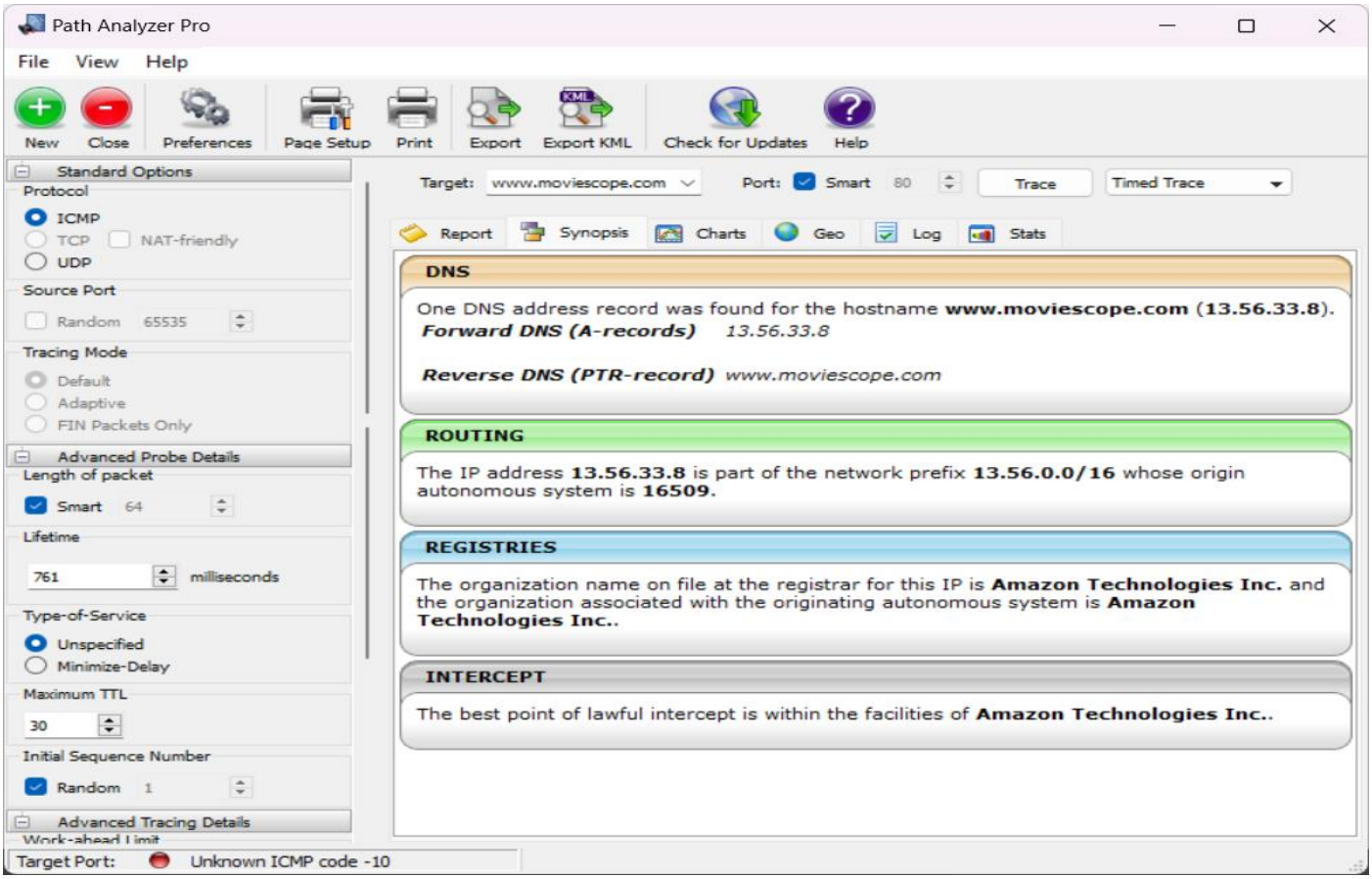
10. Click **Stop** button after **2 minutes**.

The trace results are displayed under the **Report** tab in the form of a linear chart indicating the number of hops between you and the target.

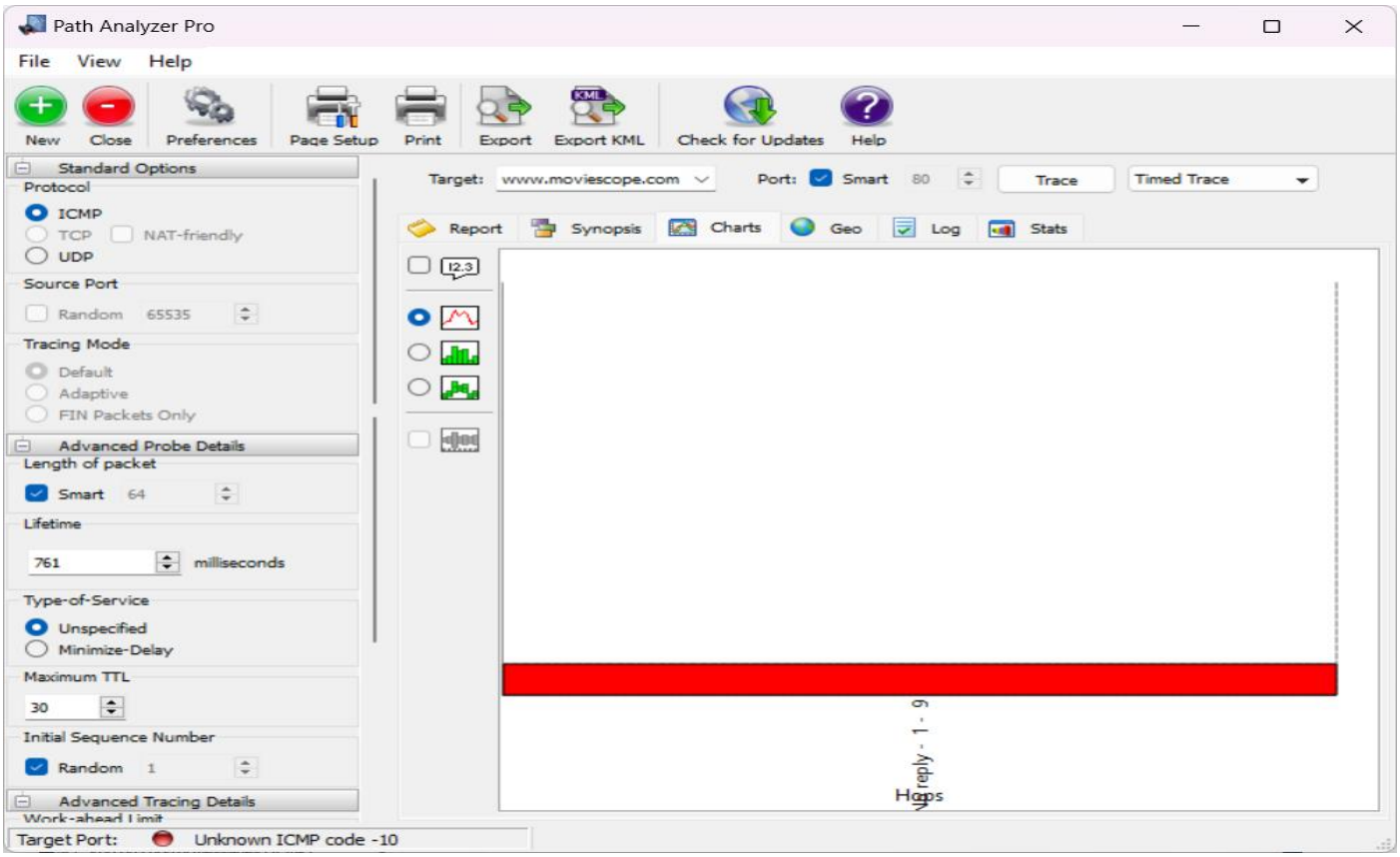
Since, this machine itself hosts the website, there won't be any hop recorded by the Path Analyzer Pro.



11. Click the **Synopsis** tab, which displays a one-page summary of trace results.

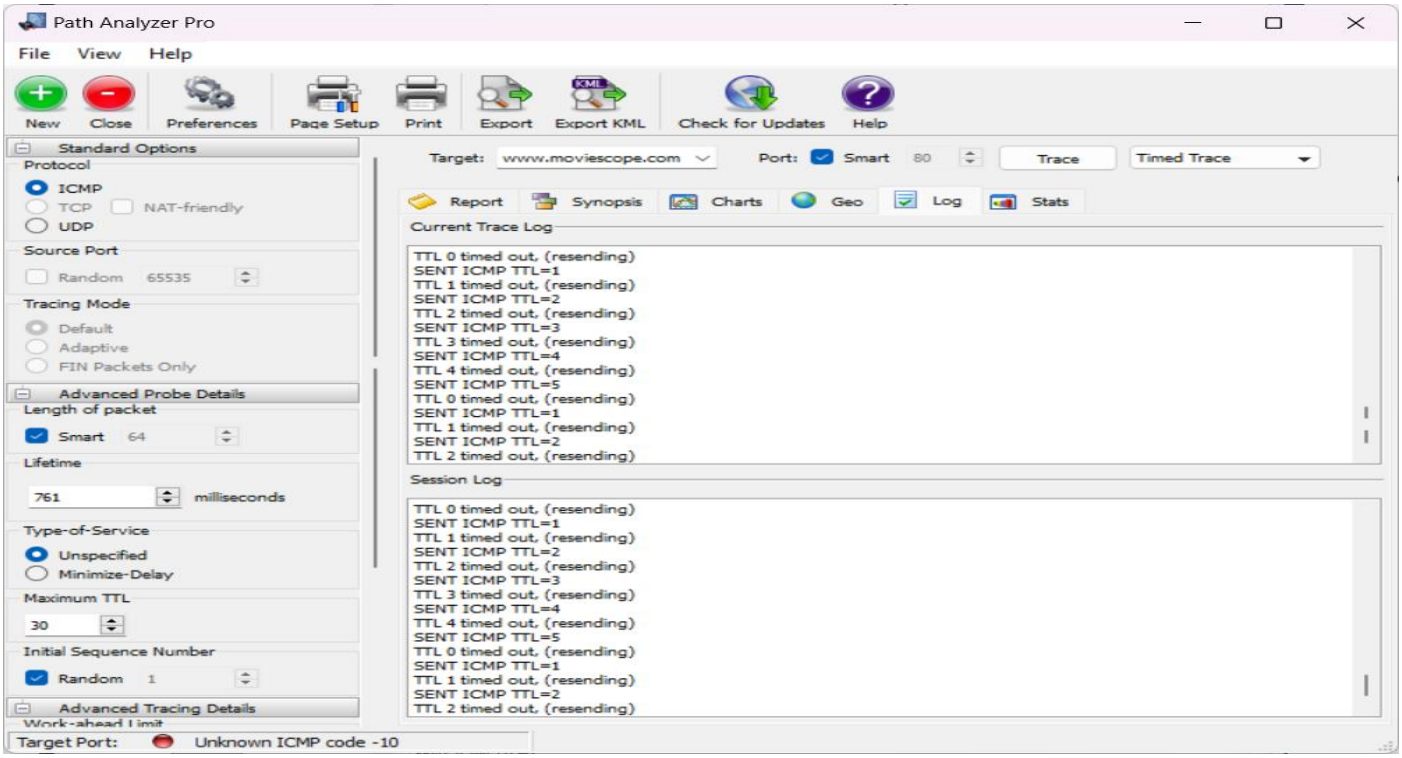


12. Click the **Charts** tab to view the results of the trace.



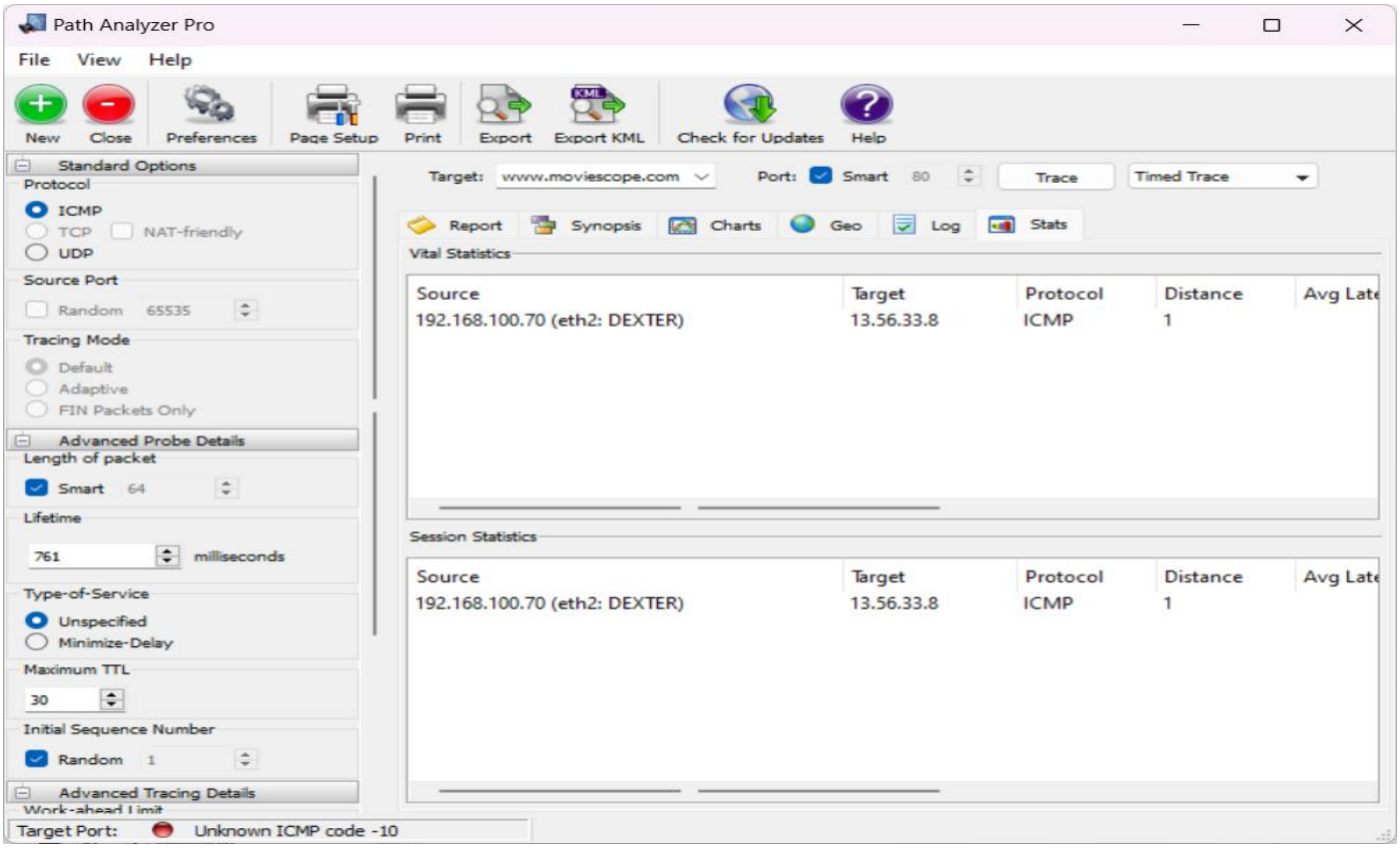
13. Click the **Log** tab to view the **Current Trace Log** and **Session Log**.

The log result might vary in your lab. At times, the Current Trace Log result might be empty.



14. Now, click the **Stats** tab, which features the **Vital Statistics** of your current trace.

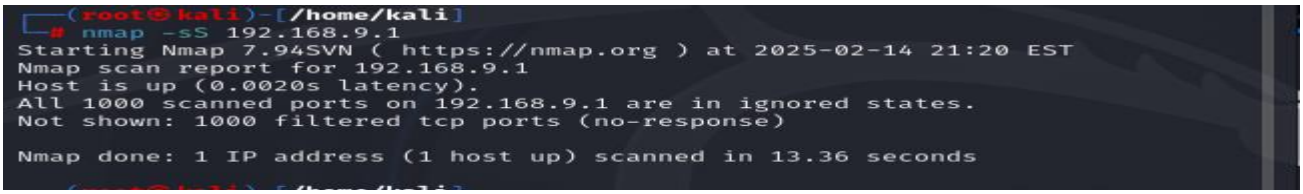
The Stats might vary in your lab.



Exercise 5: **Information Gathering and scan Using NMAP**

1- nmap -sS 192.168.9.1

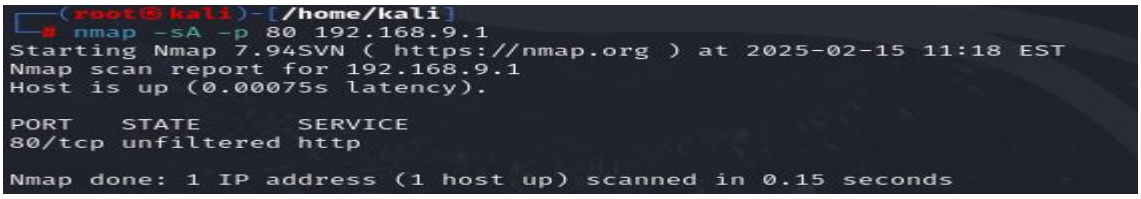
This command is usually used by everyone and it sends a SYN packet, this packet allows communication with the system and brings you the information first hand.



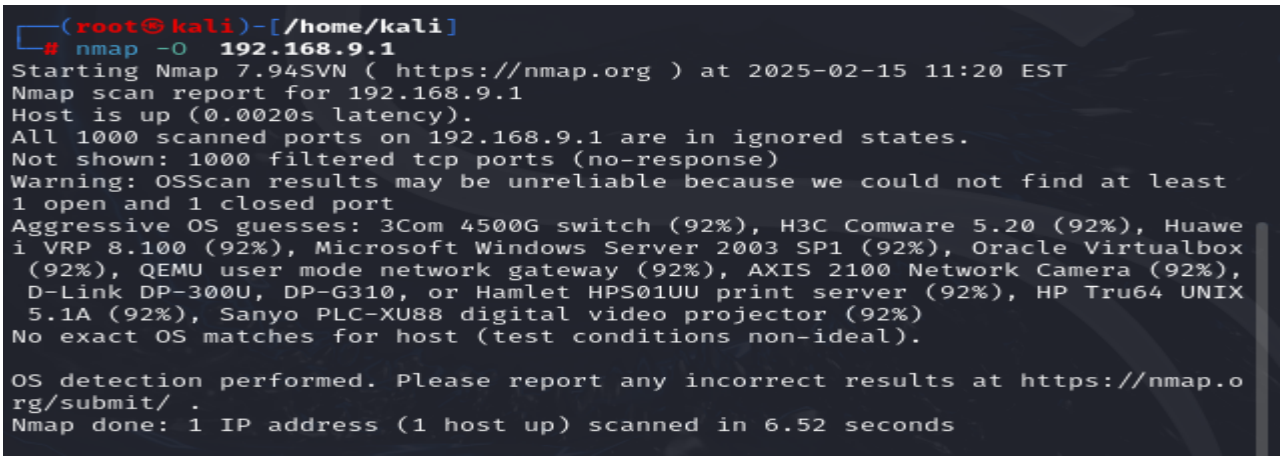
2. nmap -sU 192.168.9.1-2
   This command is to check if the ports are open or not. If they are open, it will not give a response, and if they are not open, it will send a response of an ICMP packet.

3. nmap -sA -p 80 192.168.9.1
   This is to know the strength of the firewall and this command checks the port and tells us if it is filtered or not.

   Note: Number 80 is the port that we checked and you choose any port that the victim has.



4. nmap -O 192.168.9.1
   This command is to know the type of system, whether it is Windows or Linux.



1-Install Nmap https://nmap.org/download