

# LAP1...BART2

Name: Abdullah Abdulaziz Rabah Alshammari  
ID: 202100569

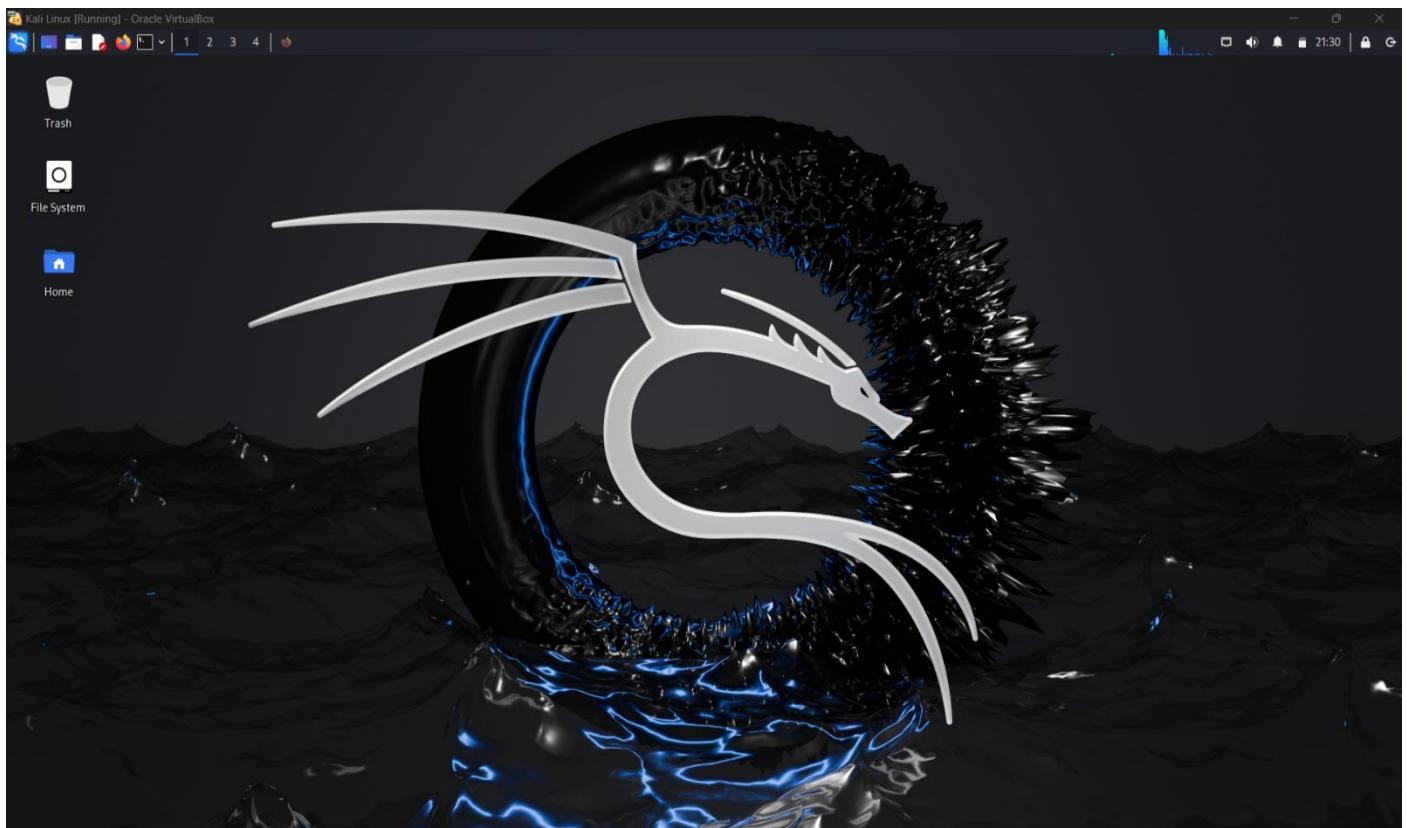
---

## Exercise 2: Collecting Information About a Target Website Using Firebug

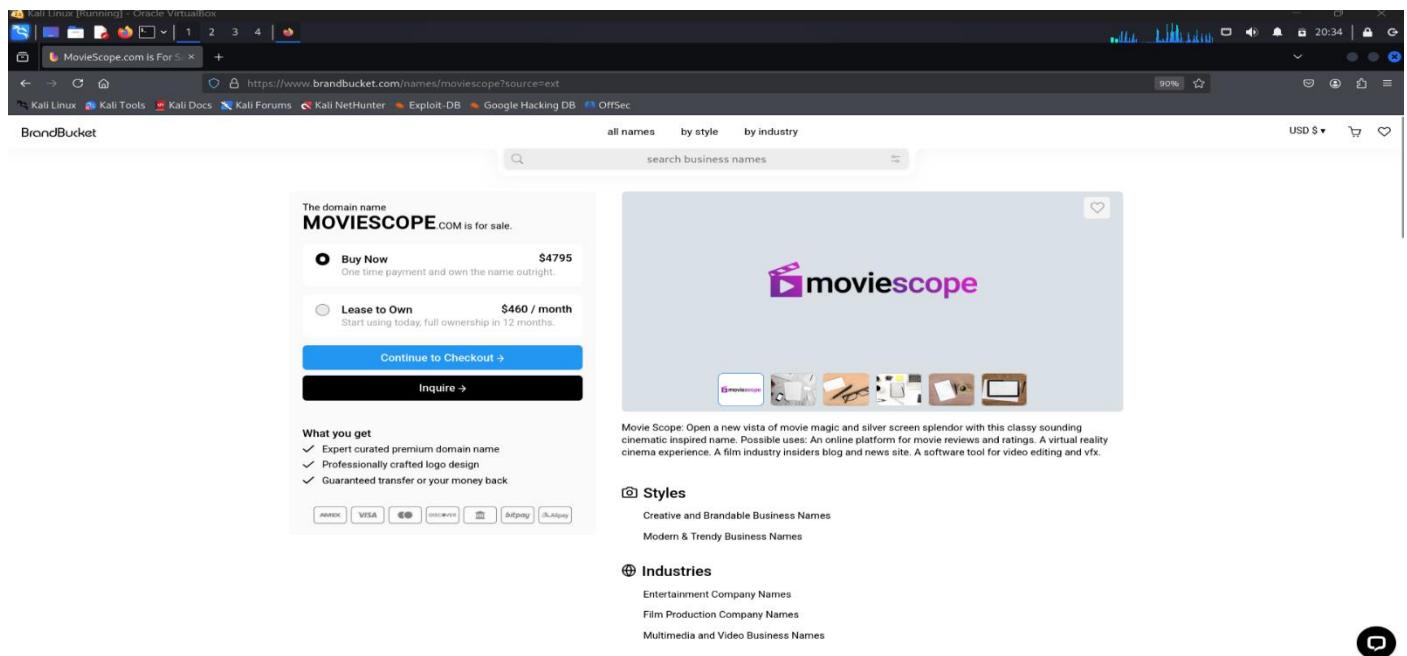
1. Click [Kali Linux](#) machine.
2. To login into the kali machine type **root** in the **Username** and click the **Next** button.
3. Next type **toor** in the **Password** field and click the **Sign In** button.



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



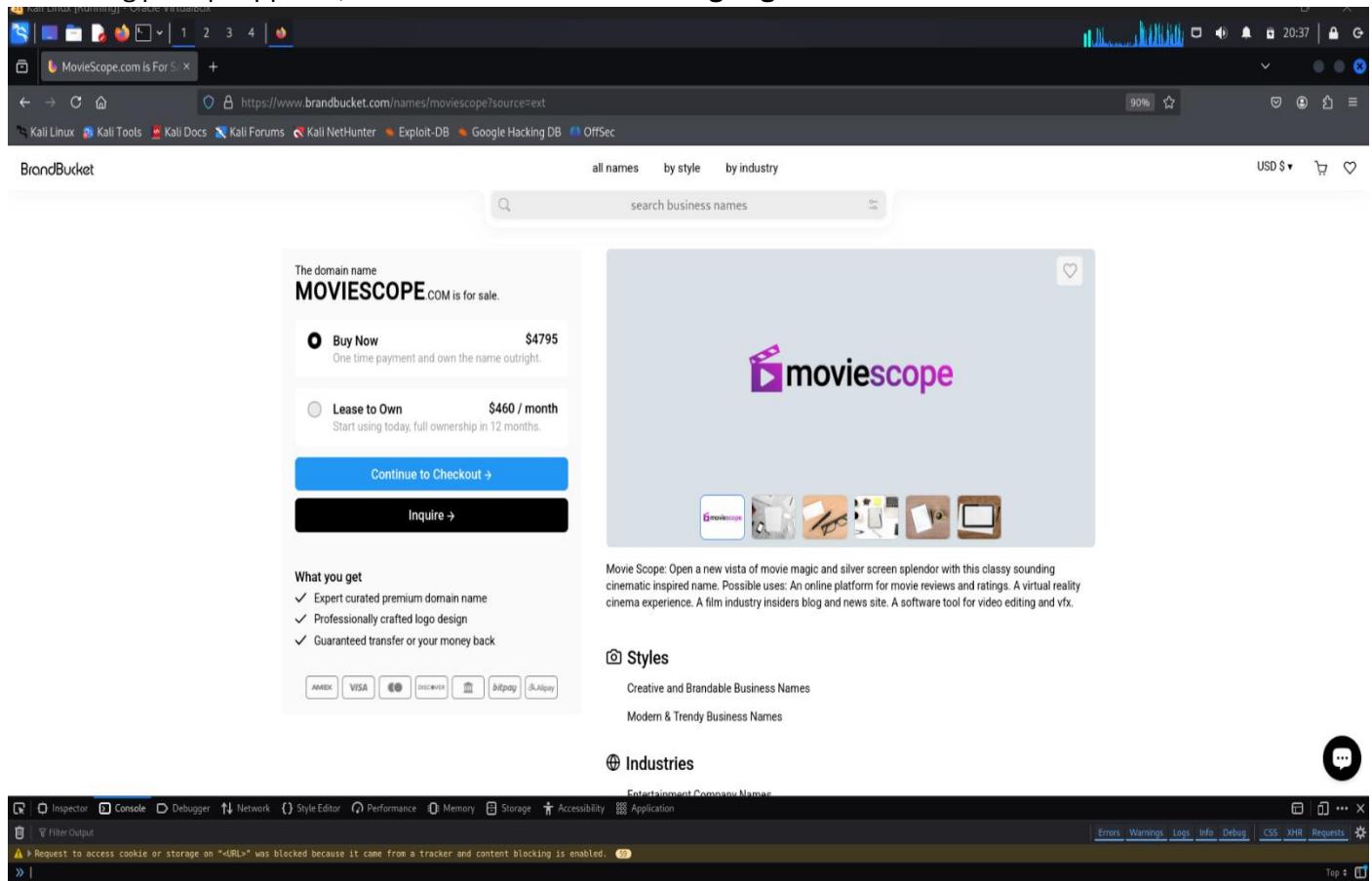
5. The firefox browser opens, type **www.moviescope.com** in the address bar and press **Enter** to browse the moviescope website.



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.

The domain name **MOVIESCOPE**.COM is for sale.

**Buy Now** \$4795  
One time payment and own the name outright.

**Lease to Own** \$460 / month  
Start using today, full ownership in 12 months.

**Continue to Checkout →** **Inquire →**

**What you get**

- ✓ Expert curated premium domain name
- ✓ Professionally crafted logo design
- ✓ Guaranteed transfer or your money back

**Styles**

Creative and Brandable Business Names  
Modern & Trendy Business Names

**Industries**

Errors Warnings Logs (1) Info Debug CSS XHR Requests

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.

The domain name **MOVIESCOPE**.COM is for sale.

**Buy Now** \$4795  
One time payment and own the name outright.

**Lease to Own** \$460 / month  
Start using today, full ownership in 12 months.

**Continue to Checkout →** **Inquire →**

**What you get**

- ✓ Expert curated premium domain name
- ✓ Professionally crafted logo design
- ✓ Guaranteed transfer or your money back

**Styles**

Creative and Brandable Business Names  
Modern & Trendy Business Names

**Industries**

Errors **Warnings** Logs (1) Info Debug CSS XHR Requests

Request to access cookie or storage on "<URL>" was blocked because it came from a tracker and content blocking is enabled. [1]

Some cookies are missing the recommended "SameSite" attribute [2]

Partitioned cookie or storage access was provided to "https://www.googleanalytics.com/static/service\_worker/5230/sw\_iframe.html?origins=https%3A%2F%2Fwww.brandbucket.com" because it is loaded in the third-party context and dynamic state partitioning is enabled. [Learn More]

Feature Policy: Skipping unsupported feature name "clipboard-read".

Feature Policy: Skipping unsupported feature name "clipboard-write".

Feature Policy: Skipping unsupported feature name "clipboard-read".

Feature Policy: Skipping unsupported feature name "clipboard-write".

Feature Policy: Skipping unsupported feature name "clipboard-read".

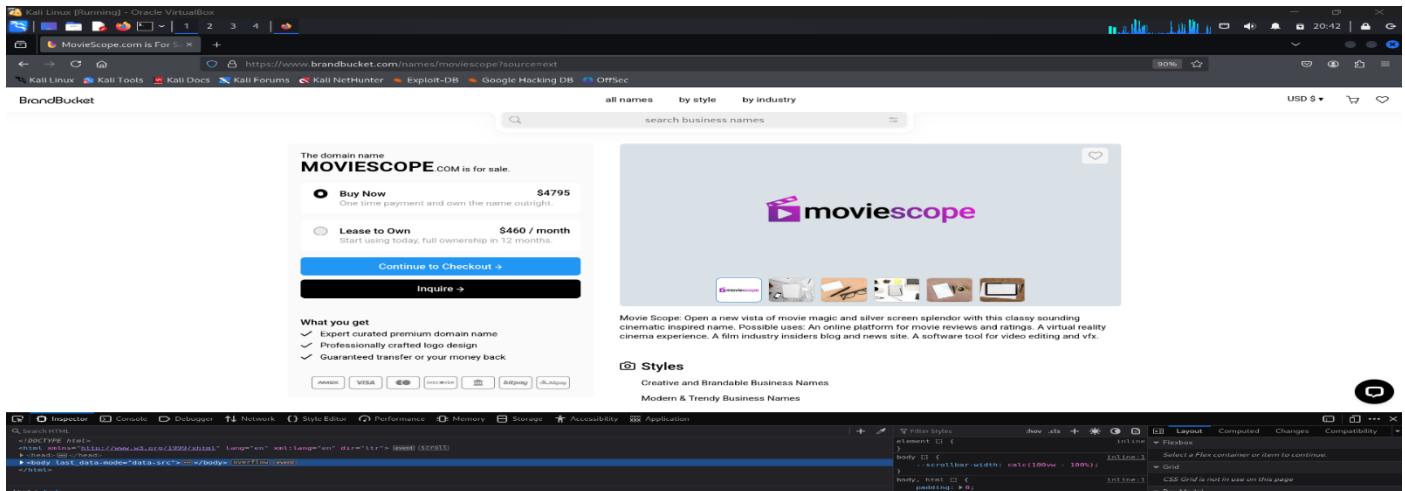
Feature Policy: Skipping unsupported feature name "clipboard-write".

Request to access cookie or storage on "https://secure.liveteaching.com/customer/account/login" was blocked because it came from a tracker and content blocking is enabled. [1]

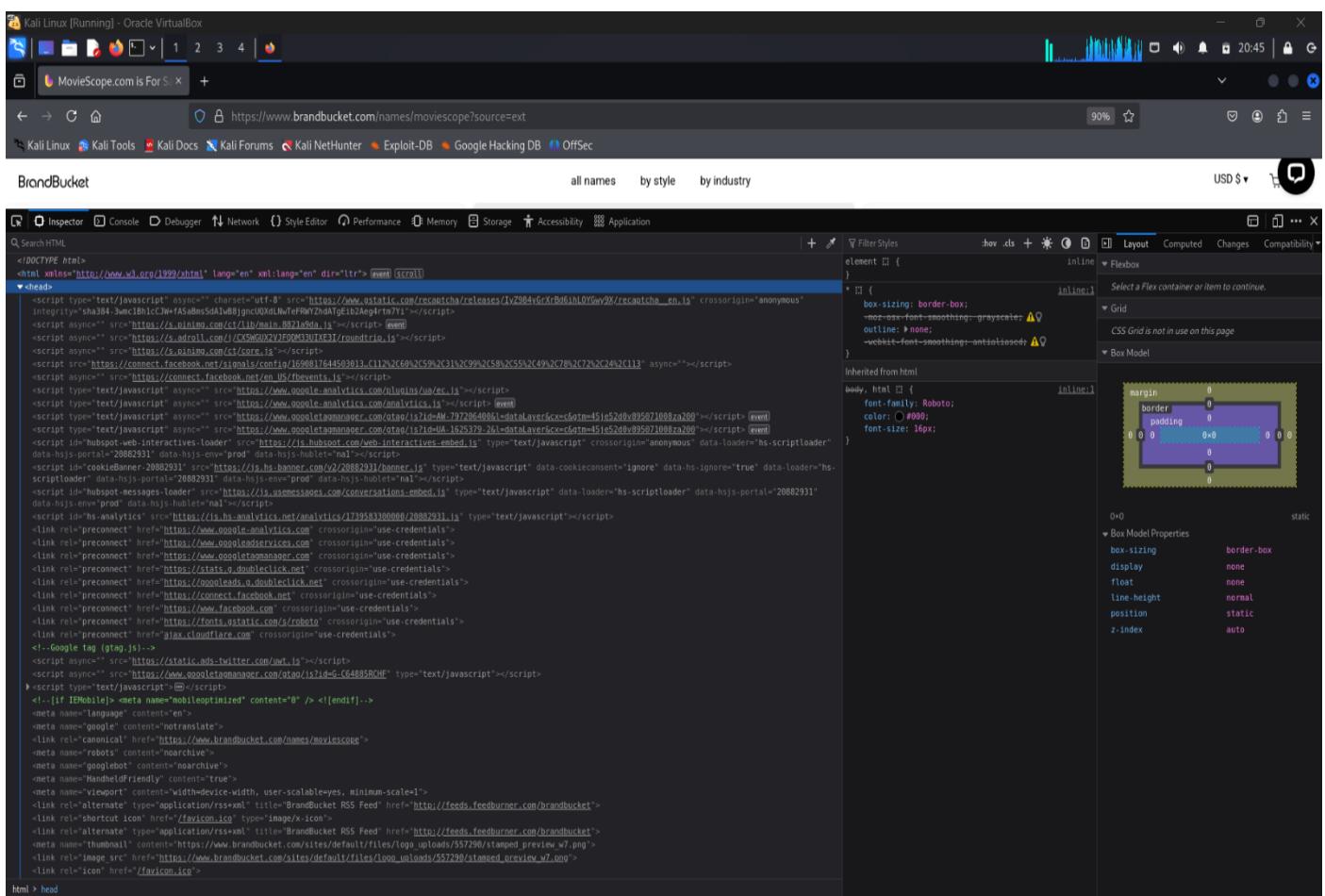
- Click the **Inspector** tab in the **Firebug UI**. The Inspector section contains two tags: head and body, which contain scripts and text that might reveal the build of the website.

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.



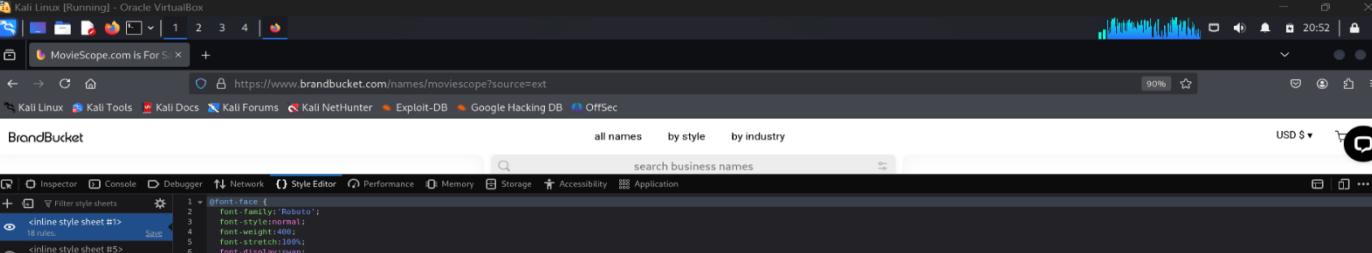
- Expand these nodes and observe the script written to develop the webpage.



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.

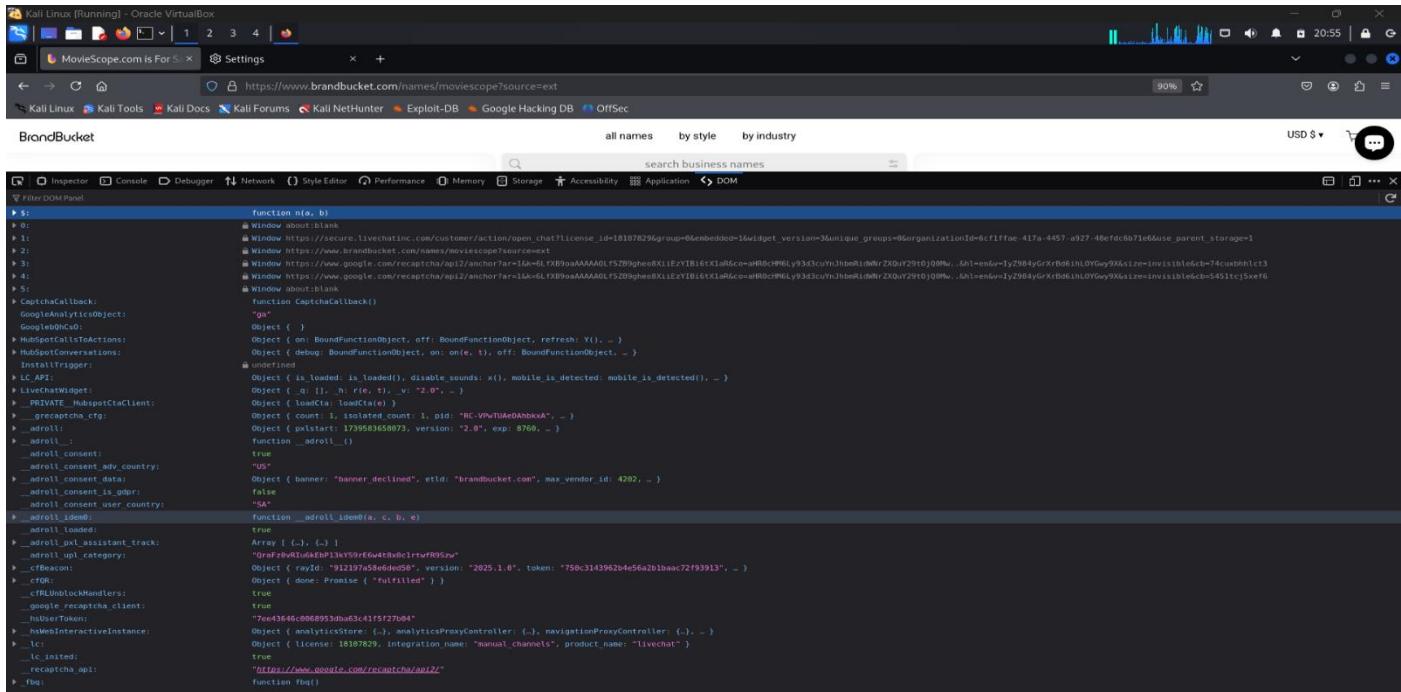


The screenshot shows a Kali Linux desktop environment with a browser window open to <https://www.brandbucket.com/names/moviescope?source=ext>. The browser's developer tools are active, specifically the Style Editor tab, displaying the CSS code for the 'moviescope' page. The code is heavily commented and includes numerous font-face declarations for various characters and ranges, such as Roboto, Arial, and specific character sets. The browser interface includes tabs for Network, Performance, Memory, Storage, Accessibility, and Application, along with a search bar for business names.

```
1 /*font-face {
2     font-family: 'Roboto';
3     font-style: normal;
4     font-weight: 400;
5     font-stretch: 100%;
6     font-display: swap;
7     src: url(https://fonts.gstatic.com/s/roboto/v47/KF07CnqEu92FrIME7kSn6GaGLdTyUWm3GUHMsazTgw.woff2) format('woff2');
8     unicode-range: U+0400-04FF,
9     U+1CB8-1CB9,
10    U+20B4,
11    U+20D0-20FF,
12    U+A640-A69F,
13    U+FE2E-FE2F;
14 }
15 */
16 /*font-face {
17     font-family: 'Roboto';
18     font-style: normal;
19     font-weight: 400;
20     font-stretch: 100%;
21     font-display: swap;
22     src: url(https://fonts.gstatic.com/s/roboto/v47/KF07CnqEu92FrIME7kSn6GaGLdTyUWm3GUHMsazTgw.woff2) format('woff2');
23     unicode-range: U+0300-03FF;
24     U+0400-049F,
25     U+0400-04B1,
26     U+2116;
27 }
28 */
29 /*font-face {
30     font-family: 'Roboto';
31     font-style: normal;
32     font-weight: 400;
33     font-stretch: 100%;
34     font-display: swap;
35     src: url(https://fonts.gstatic.com/s/roboto/v47/KF07CnqEu92FrIME7kSn6GaGLdTyUWm3GUHMsazTgw.woff2) format('woff2');
36     unicode-range: U+1F00-1FFF;
37 */
38 /*font-face {
39     font-family: 'Roboto';
40     font-style: normal;
41     font-weight: 400;
42     font-stretch: 100%;
43     font-display: swap;
44     src: url(https://fonts.gstatic.com/s/roboto/v47/KF07CnqEu92FrIME7kSn6GaGLdTyUWm3GUHMsazTgw.woff2) format('woff2');
45     U+037A-037F,
46     U+0384-038A,
47     U+038E-03A1,
48     U+03A3-03FF;
49 }
50 */
51 /*font-face {
```

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

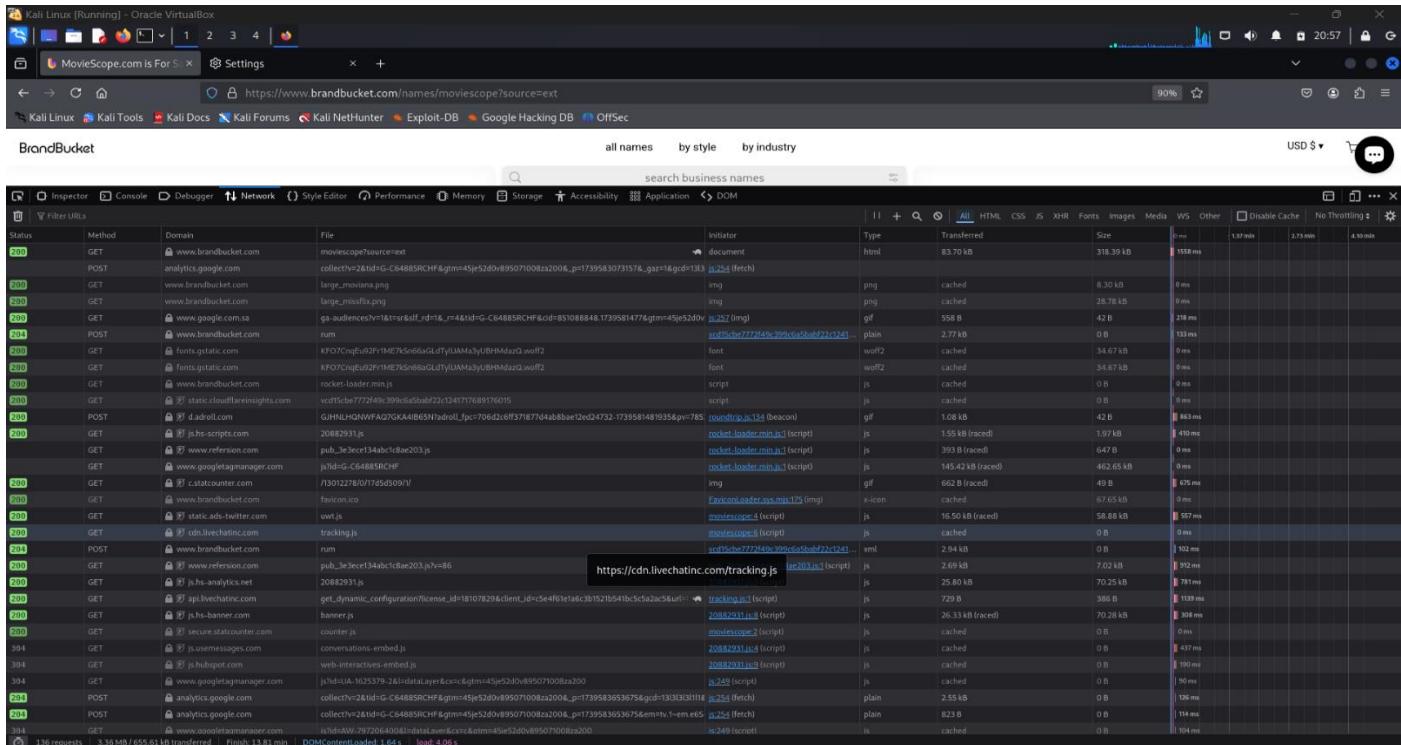
This tab contains scripts written in various web technologies such as html5, jQuery, etc. This allows attackers to perform exploitation techniques on a specific version of a web application, which leads to expose sensitive information.



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.

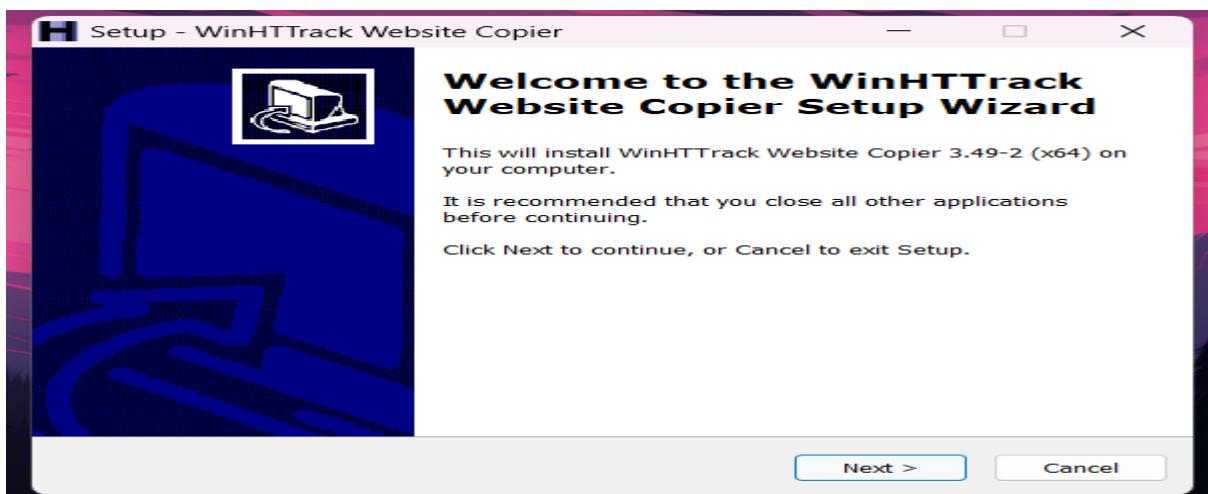
The screenshot shows the NetworkMiner tool interface. A specific GET request to <https://www.brandbucket.com/names/moviescope?source=ext> is selected. The Headers tab is active, displaying the following response headers:

Header	Value
Server	Microsoft-IIS/8.0
Date	Sat, 15 Feb 2025 01:40:59 GMT
Content-Type	image/gif; charset=turf-8
Set-Cookie	.AspNetCore.Cookies=...; .AspNetCore.Mvc.Antiforgery=...

The Response Headers section shows expanded details for the Set-Cookie header, including the cookie name (.AspNetCore.Cookies), its value, and various attributes like Max-Age, Path, and Domain.

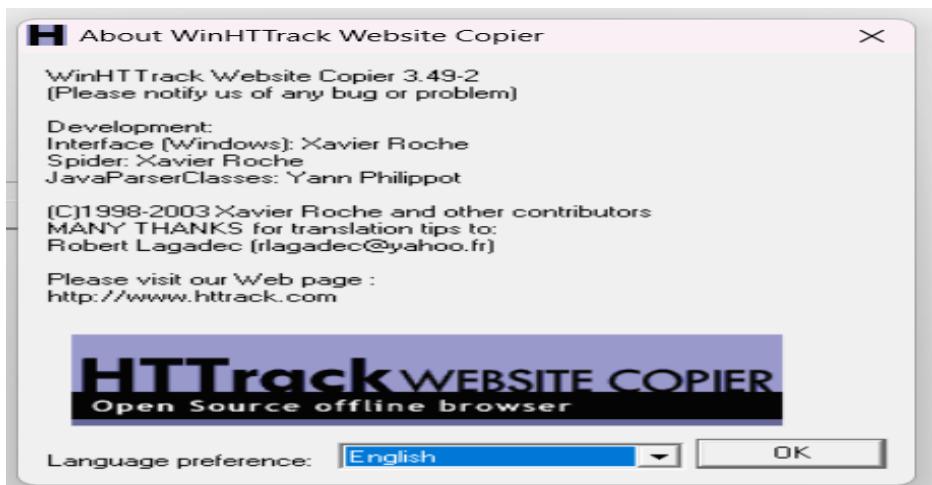
### Exercise 3: Mirroring Website Using HTTrack Web Site Copier

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.

Welcome to WinHTTrack Website Copier!

Please click on the NEXT button to

- start a new project
- or resume a partial download



< Back

Next >

Exit

Help

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.

New project name:

Test Project

Project category:

[ ]

Info

New project

Base path:

C:\My Web Sites

< Back

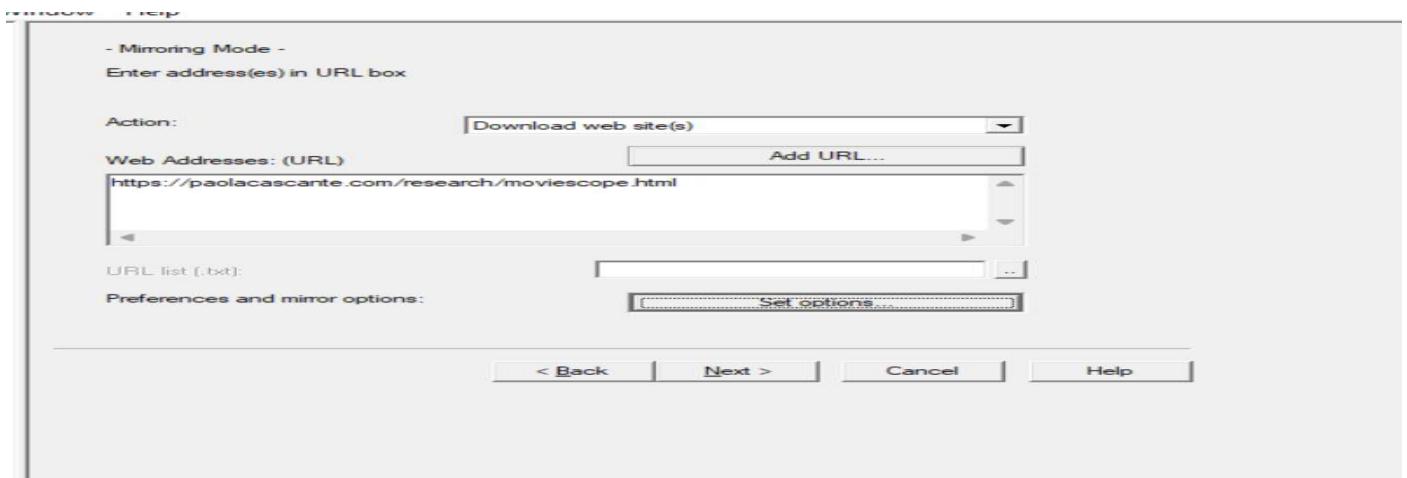
Next >

Cancel

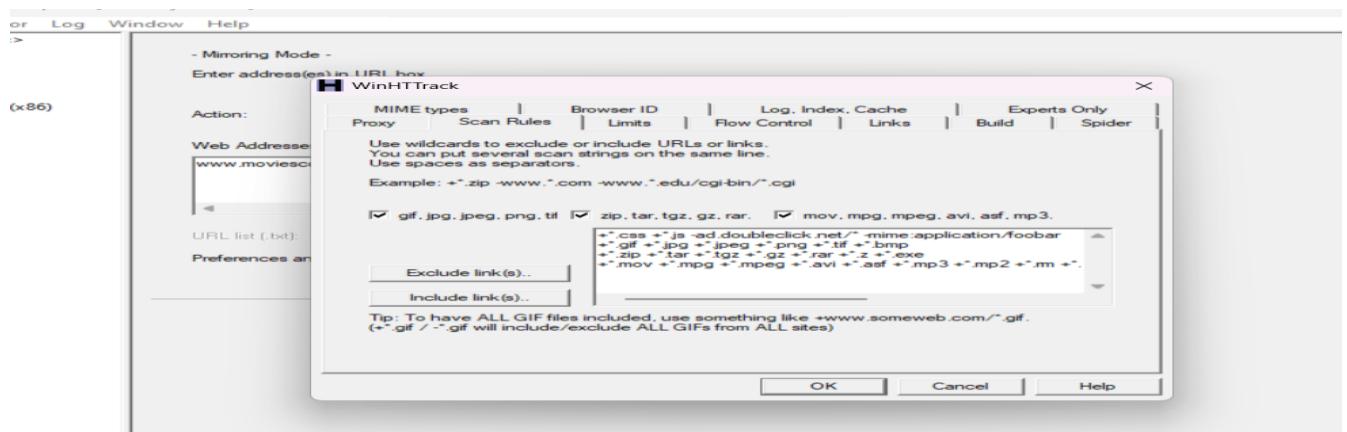
Help

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

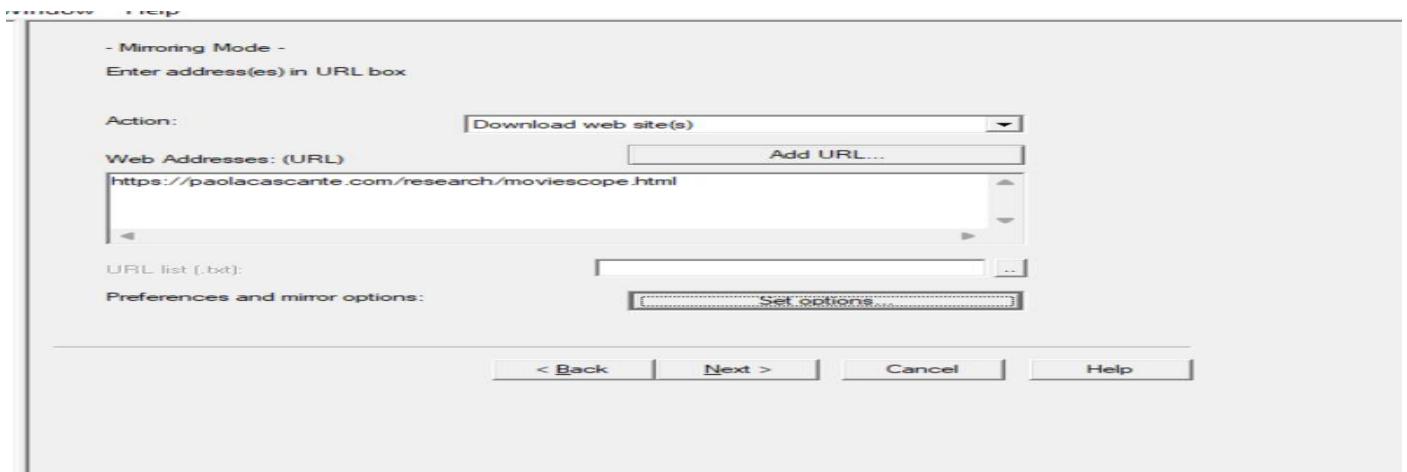
I have typed another site because [www.moviescope.com](http://www.moviescope.com) didn't work so I typed <https://paolacascante.com/research/moviescope.html>



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**.

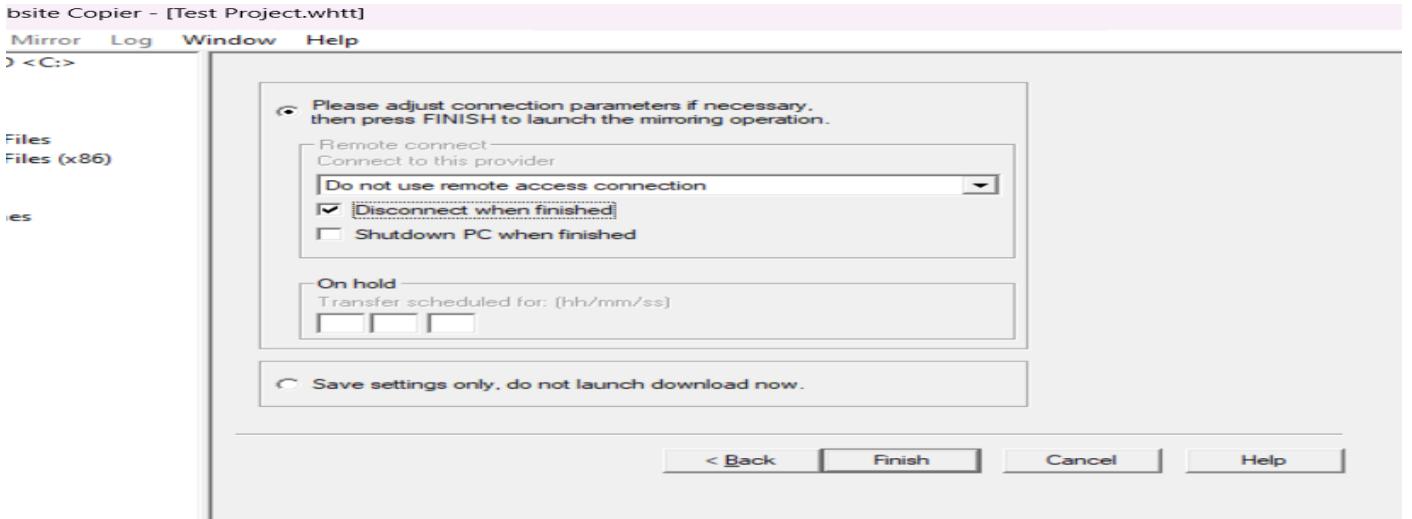


8. Click the **Next** button to proceed.

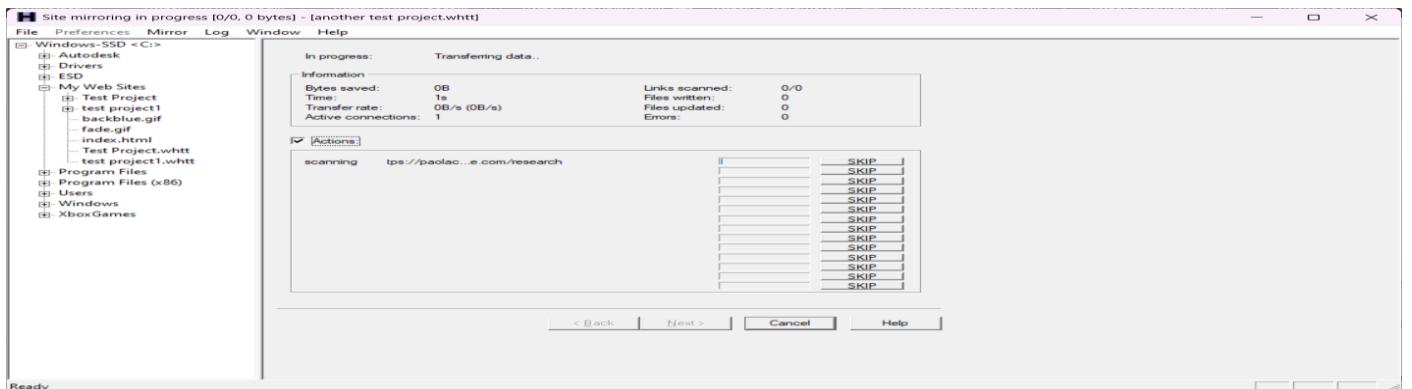


- By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation** and check **Disconnect when finished** option.

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

Mirroring operation complete.  
Click Exit to quit WinHTTrack.  
See log file(s) if necessary to ensure that everything is OK.

Thanks for using WinHTTrack!

Tip: Click [View log file] to see warning or error messages

[View log file](#)

[Browse Mirrored Website](#)

[Back](#)

[Finish](#)

[Exit](#)

[Help](#)

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.

The screenshot shows a web browser window with multiple tabs open at the top. The active tab displays the title "Moviescope: Large-scale Analysis of Movies using Multiple Modalities". Below the title, there is a paragraph about film media being a rich form of artistic expression and containing complex storylines. Another paragraph introduces the "Moviescope" dataset, which includes 5,000 movies with video trailers, posters, plots, and metadata. On the left side of the page, there is a section titled "Pandorum | action, horror, mystery, sci-fi, thriller" featuring a movie poster and some analysis. On the right side, there is a detailed technical summary of the study, mentioning visual, audio, and text features, and comparing them to human-based and metadata-based predictions. A "Show hidden icons" button is visible at the bottom right.

Film media is a rich form of artistic expression.  
Unlike photography, and short videos, movies contain a storyline that is deliberately complex and intricate in order to engage its audience.

In this paper we introduce **Moviescope**, a new large-scale dataset of 5,000 movies with corresponding video trailers, posters, plots and metadata.

Pandorum | action, horror, mystery, sci-fi, thriller

V: thriller: 0.83 | action: 0.82 | horror: 0.49

A: thriller: 0.57 | action: 0.49 | drama: 0.36

T: sci-fi: 0.99 | fantasy: 0.53 | action: 0.28

In 2174, the human population has exceeded the carrying capacity of Earth, leading humanity to build a huge interstellar ark named Elysium. Its mission is to send 60,000 people on a 123-year trip to establish a colony on an Earth-like planet named Tarsis. The passengers and crew are placed in hypersleep, with a rotating crew who awake for (...)

P: thriller: 0.97  
horror: 0.92  
mystery: 0.86

M:  
drama: 0.58  
thriller: 0.46  
comedy: 0.61

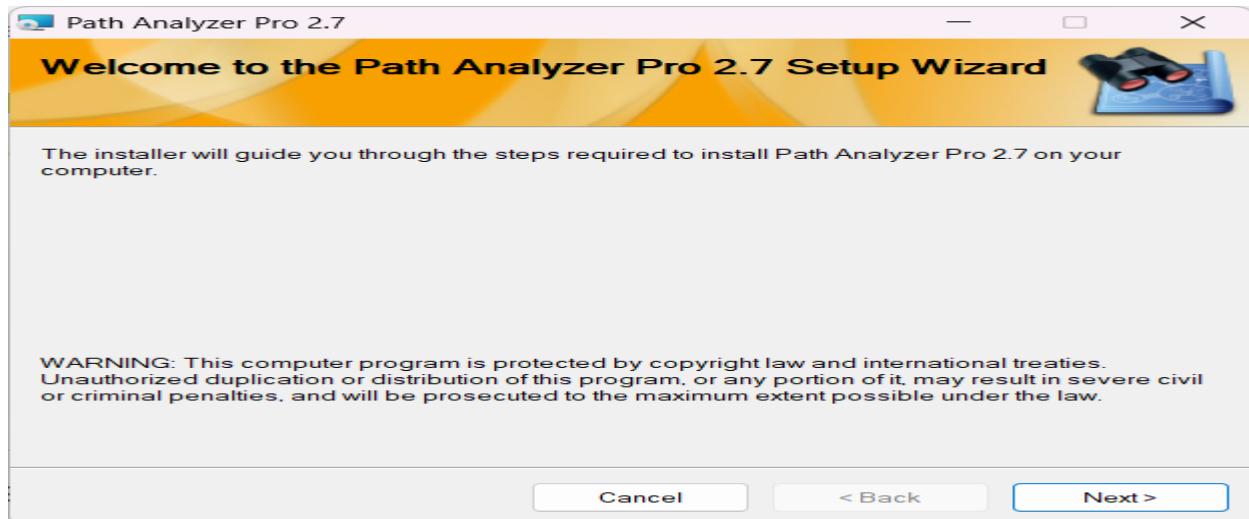
We present a large scale study comparing the effectiveness of visual, audio, text, and metadata-based features for predicting high-level information about movies such as their genre or estimated budget. We demonstrate the usefulness of content-based methods in this domain in contrast to human-based and metadata-based predictions in the era of deep learning. Additionally, we provide a comprehensive study of temporal feature aggregation methods for representing video and text and find that simple pooling operations are effective in this domain. We also show to what extent different modalities are complementary to each other.

Show hidden icons

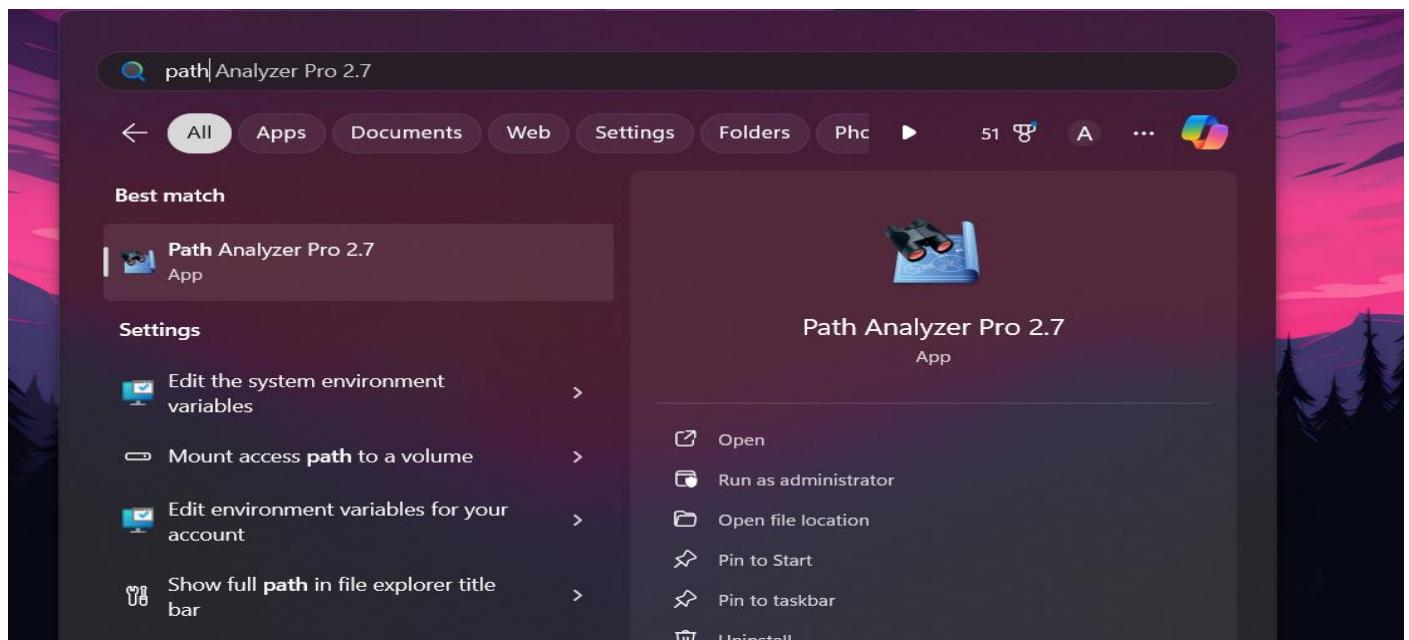
## Exercise 4: Advanced Network Route Tracing Using Path Analyzer Pro

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.

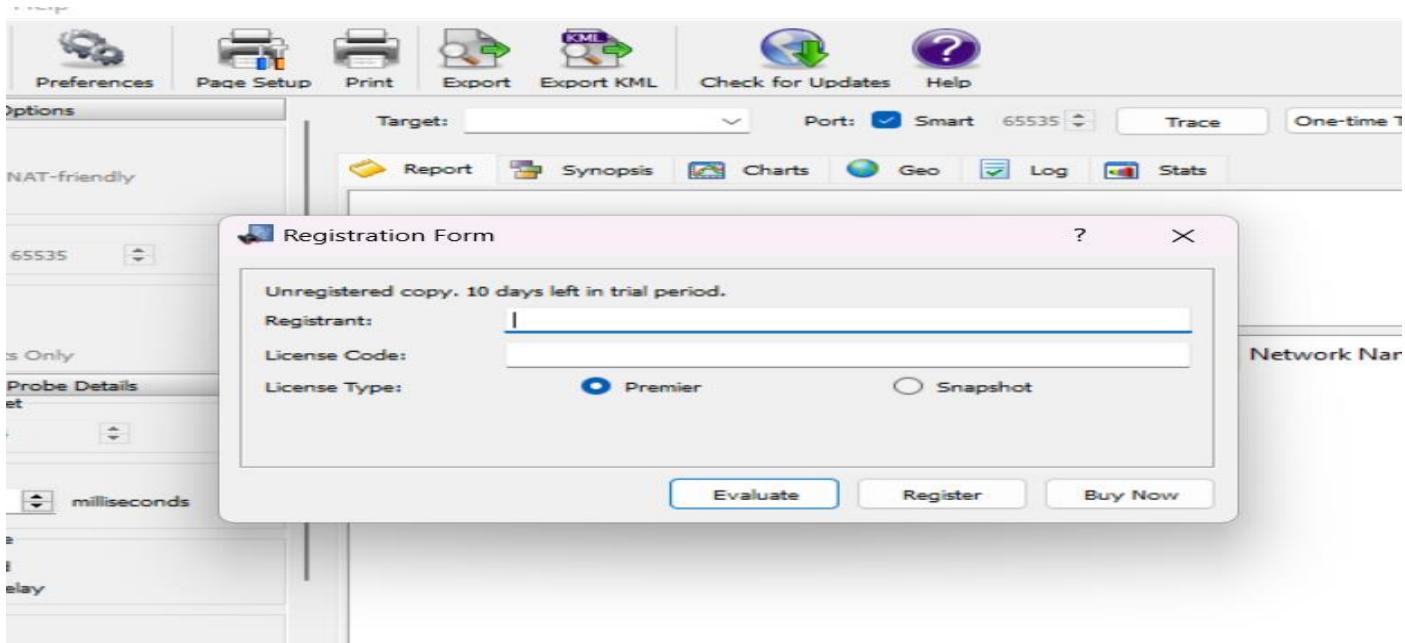
If an Open File - Security Warning pop-up appears, click Run.



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



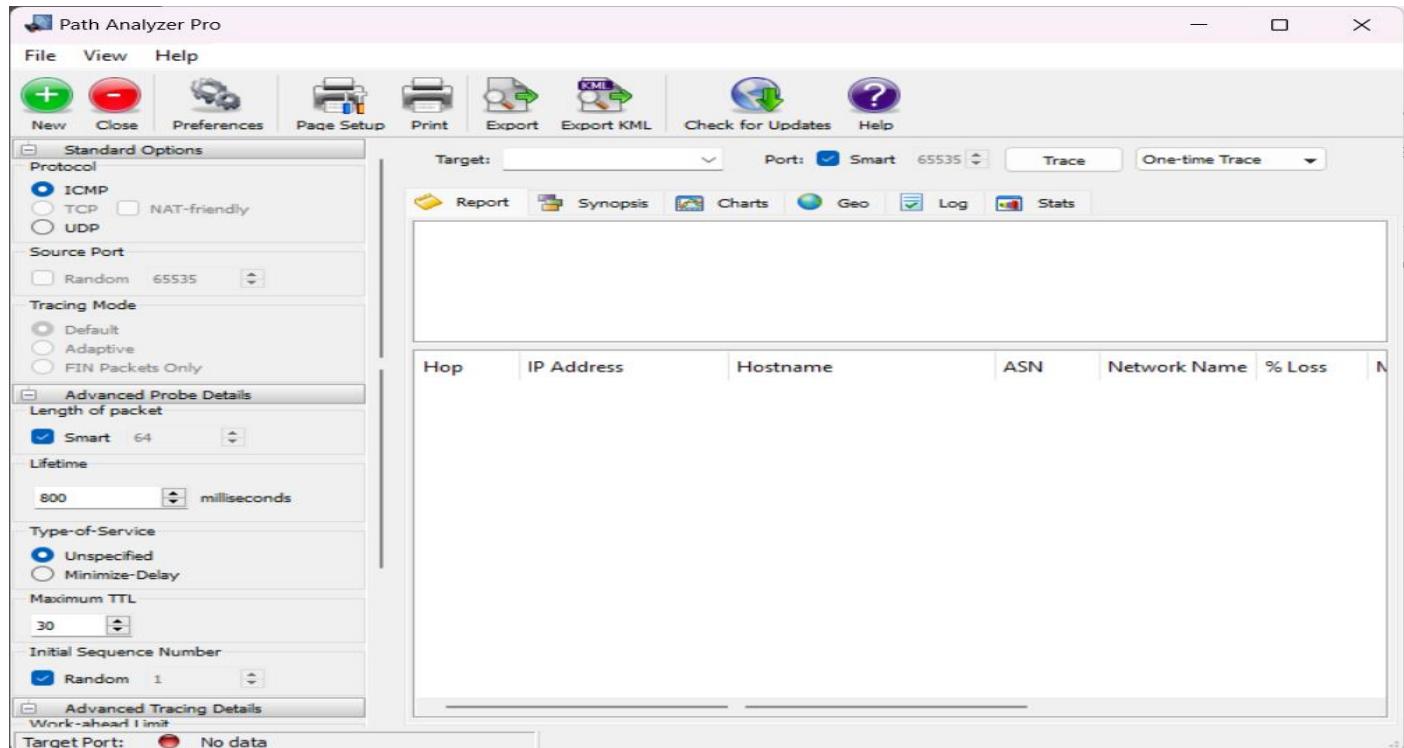
4. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up. Click **Evaluate** in the pop-up.



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

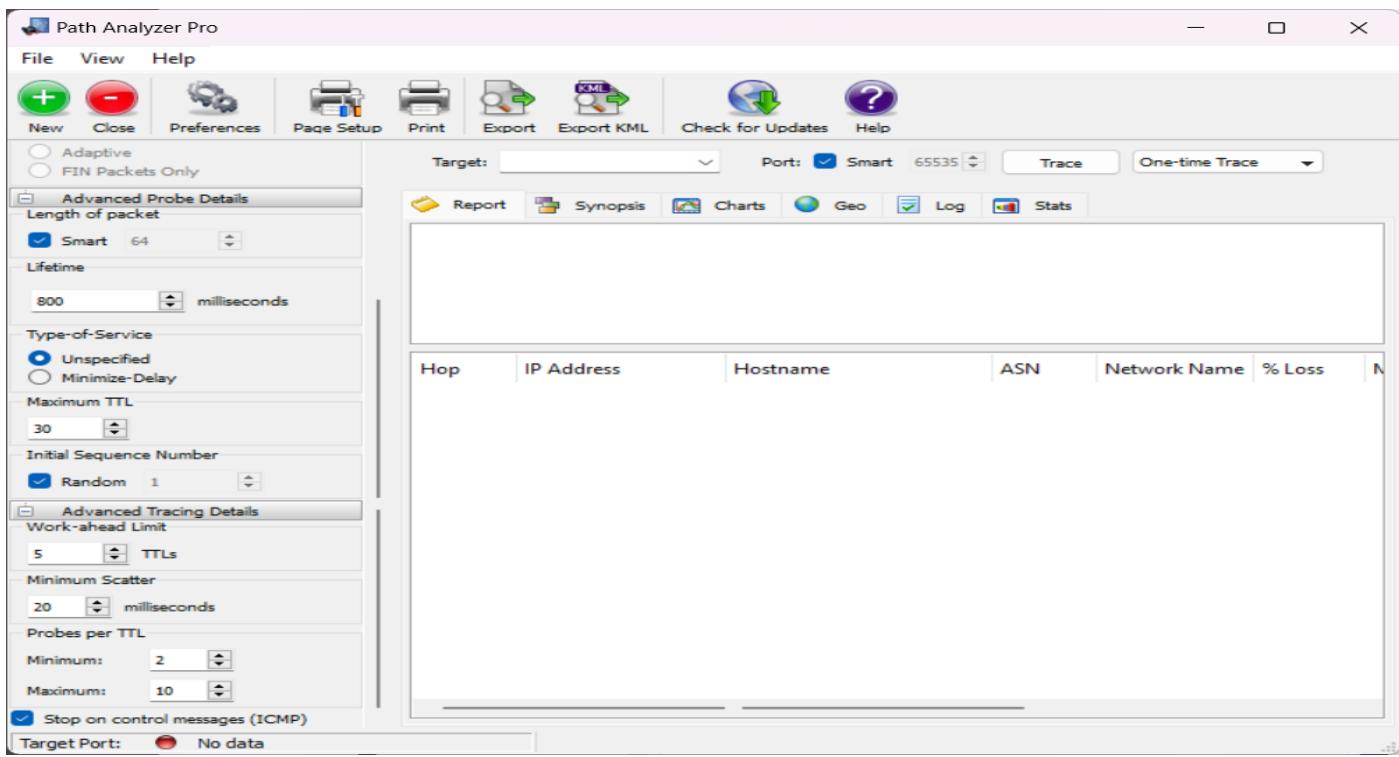
In the **Standard Options** and **Advanced Probe Details** sections, a few options are set by default.

- 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.

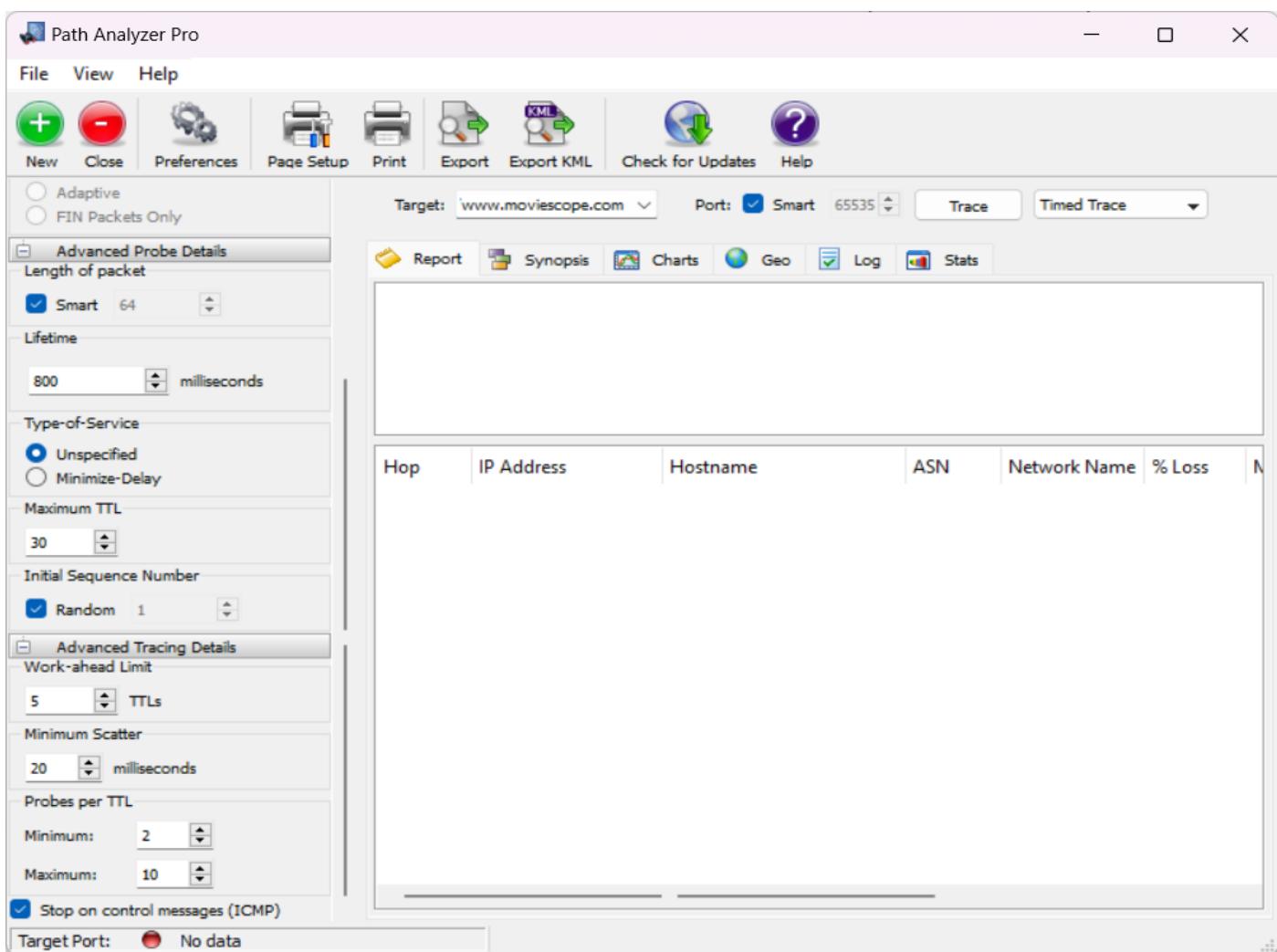


6. In the **Advanced Tracing Details** section, a few options are set to default.

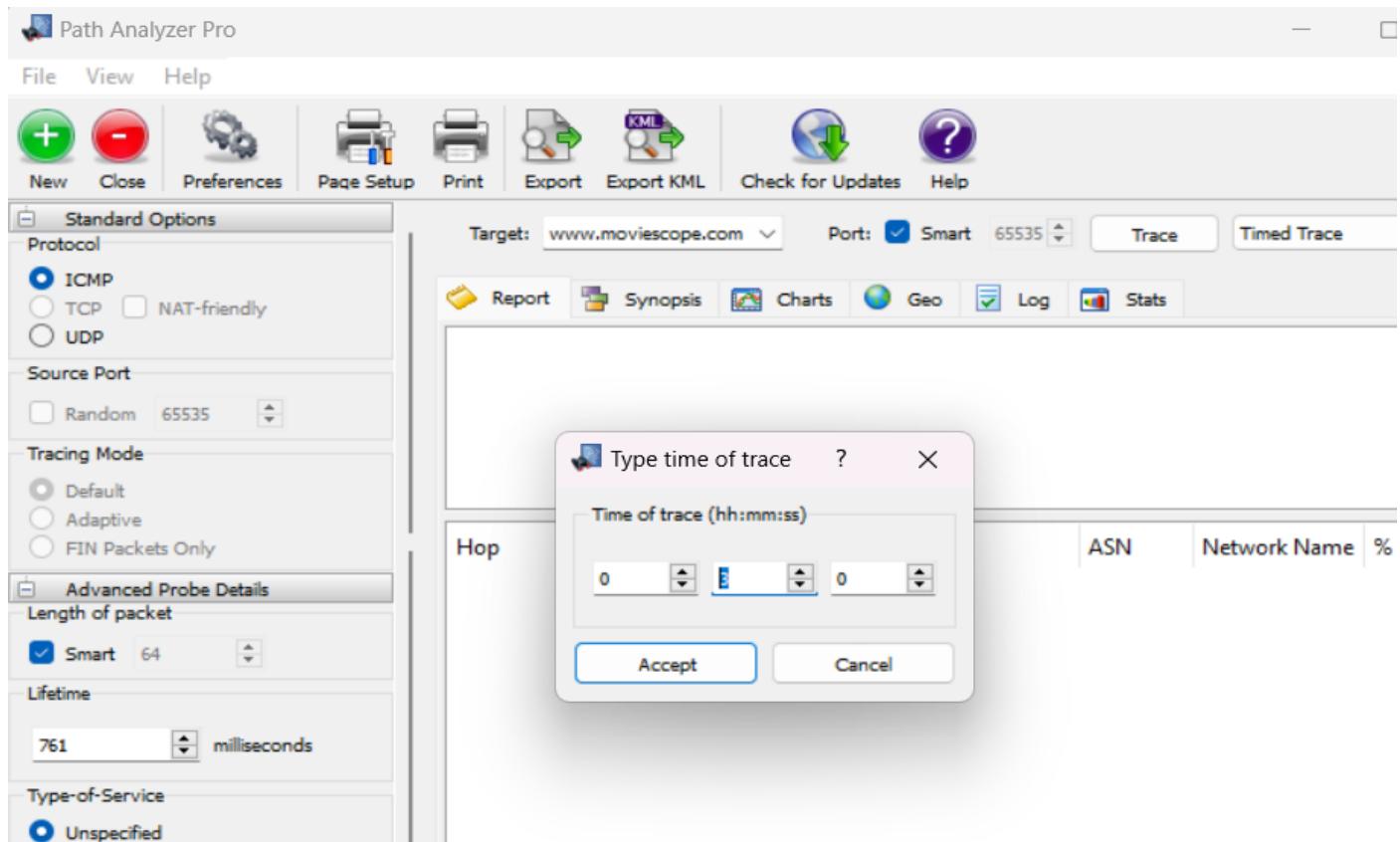
Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.



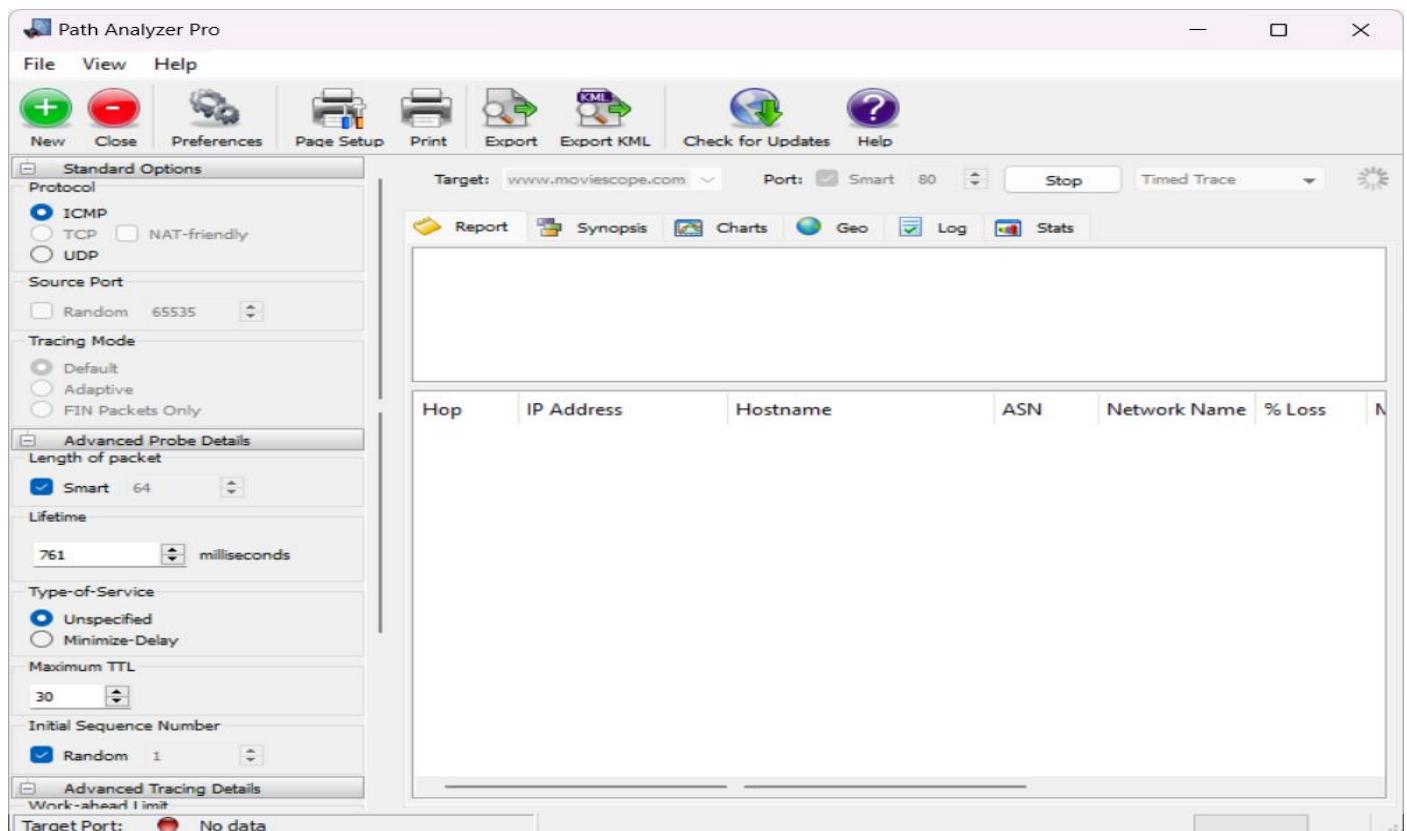
7. To perform the trace, enter the host name in the **Target** field, for instance **http://www.moviescope.com**, check **Smart** under the **Port** field as default (**65535**) and choose duration of time as **Timed Trace** from the drop-down list and click **Trace**.



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



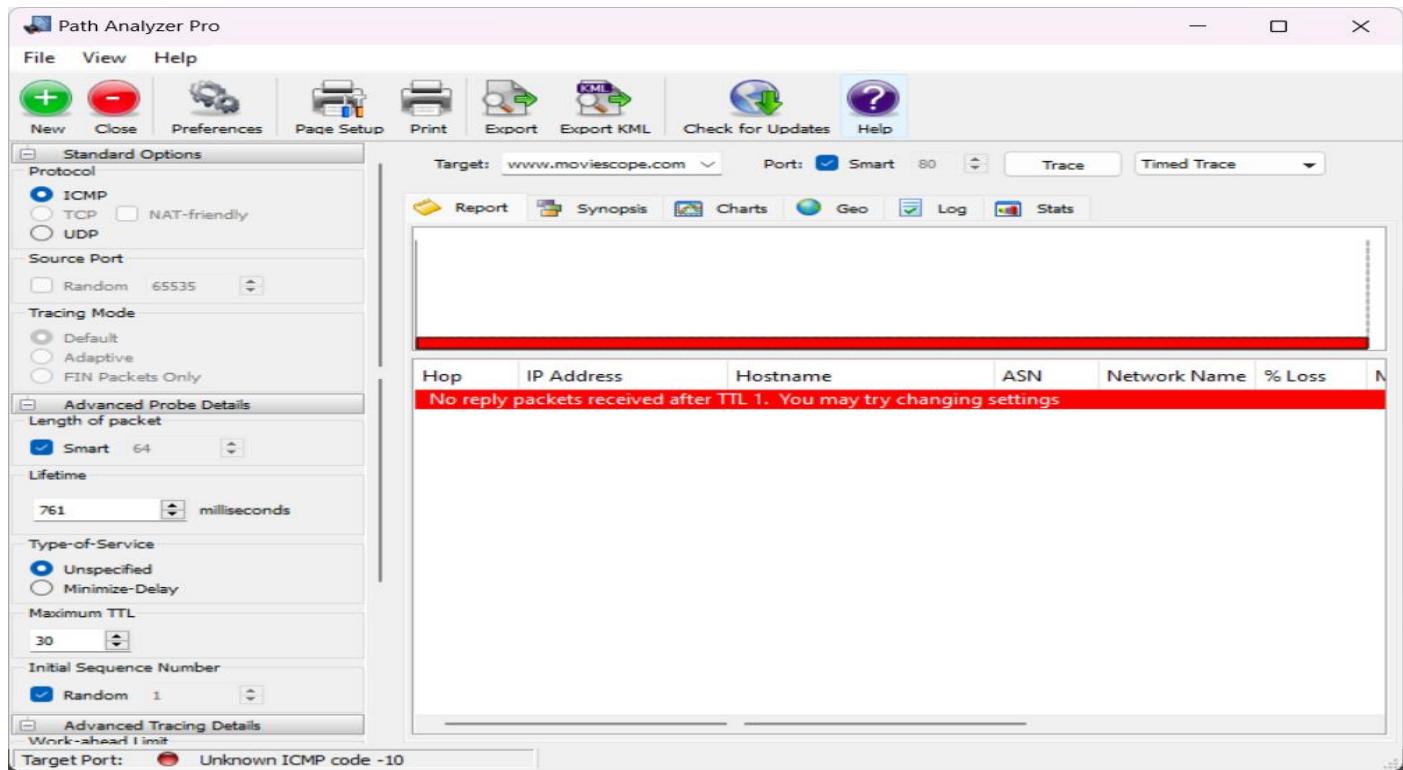
9. While Path Analyzer Pro performs this trace, the Trace tab changes automatically to **Stop**.



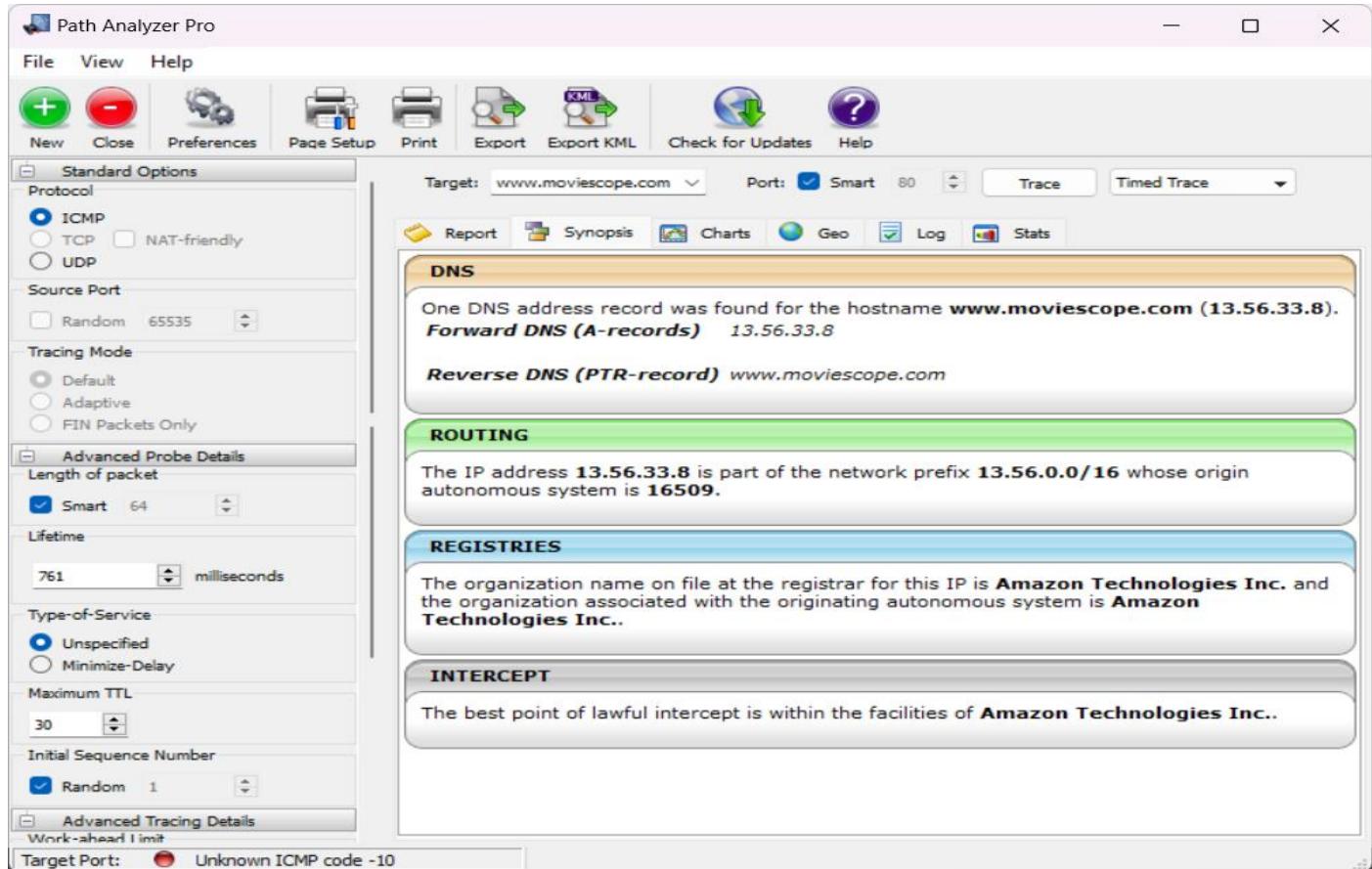
## 10. Click **Stop** button after 2 minutes.

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.

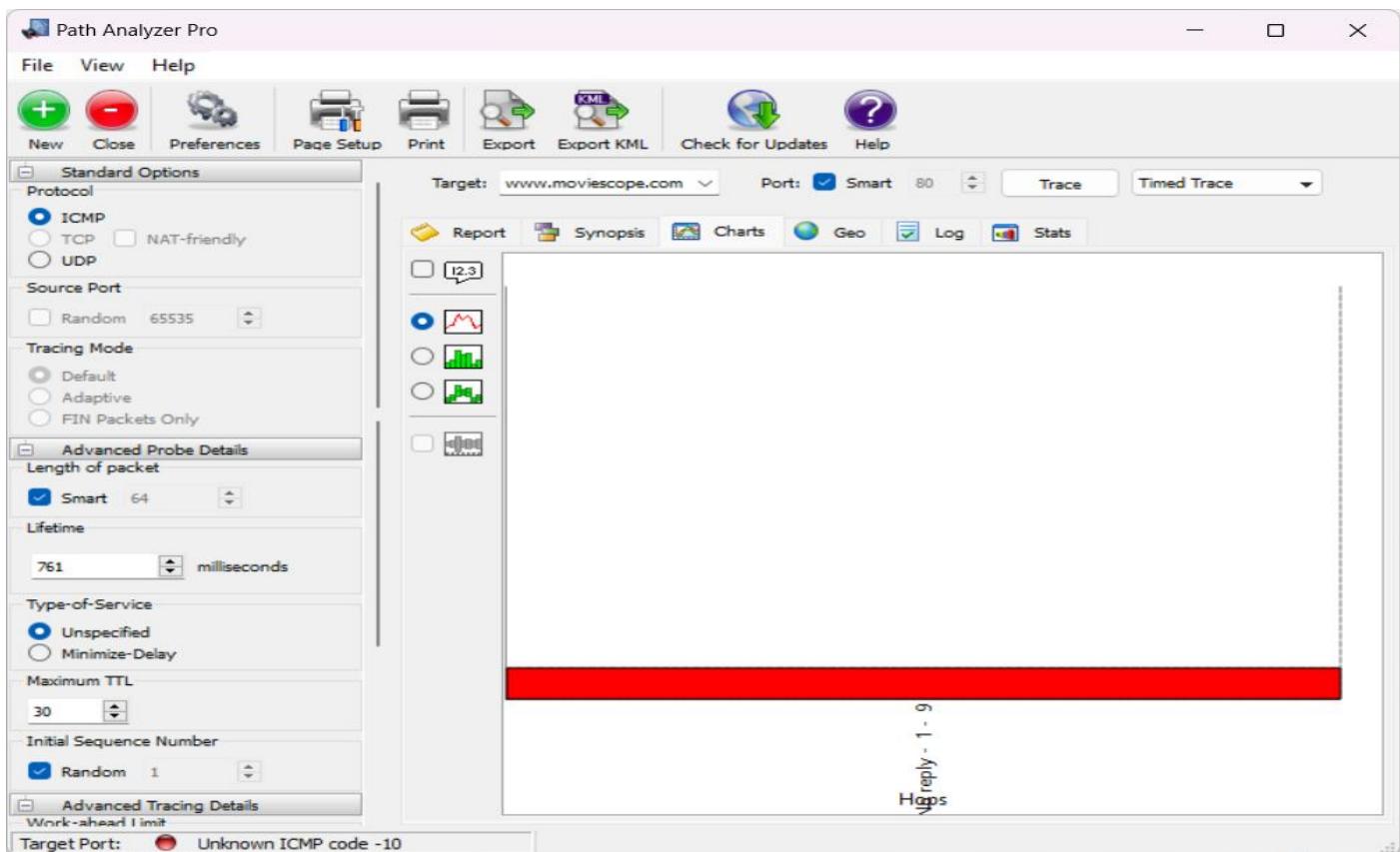
Since, this machine itself hosts the website, there won't be any hop recorded by the Path Analyzer Pro.



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

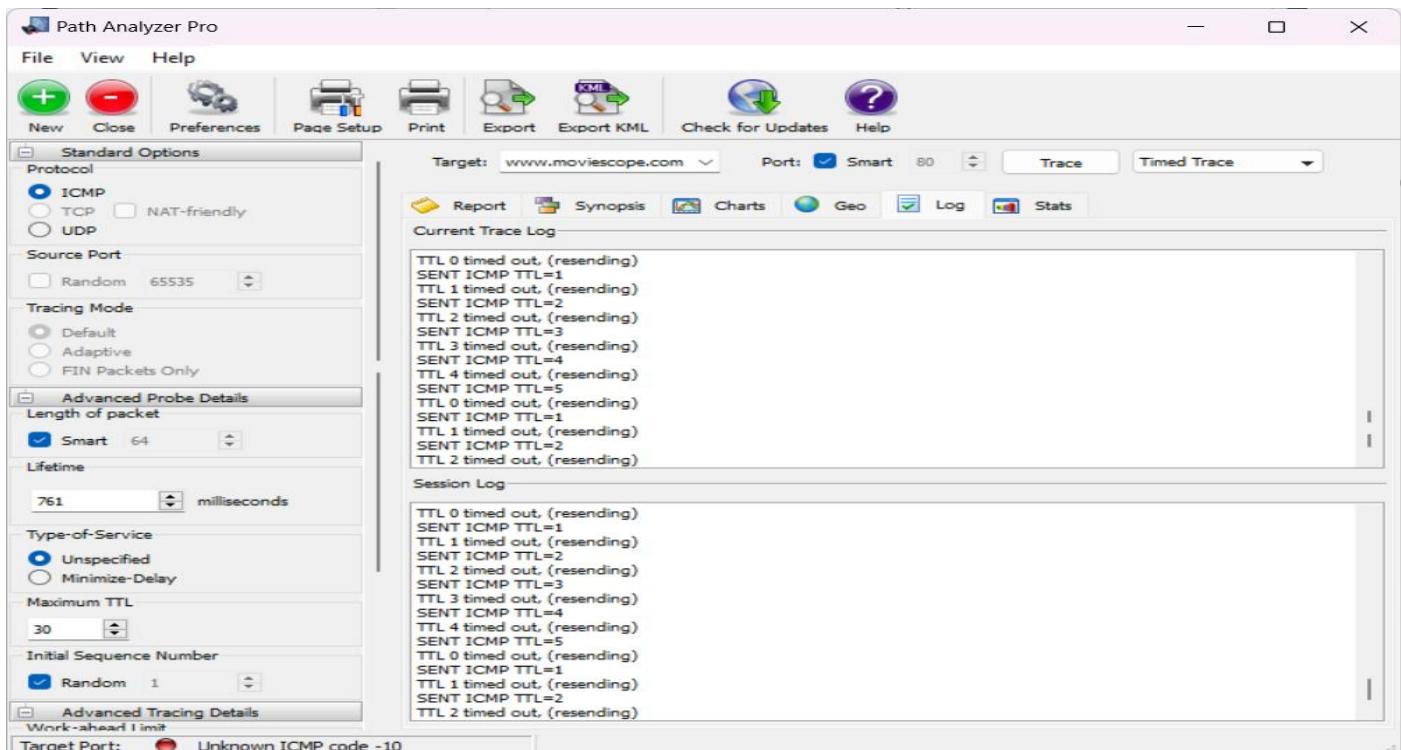


12. Click the **Charts** tab to view the results of the trace.



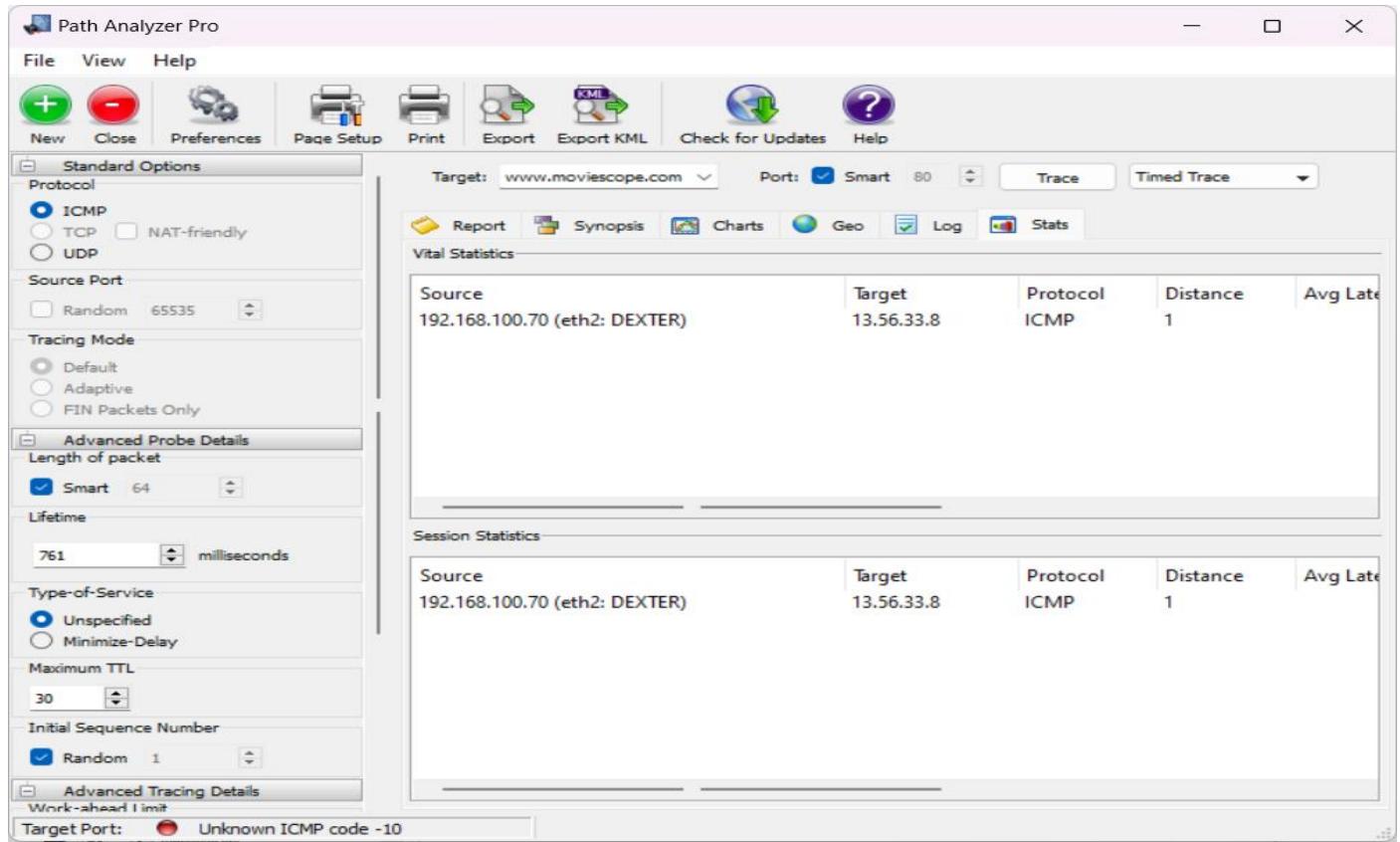
13. Click the **Log** tab to view the **Current Trace Log** and **Session Log**.

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.

```
(root㉿kali)-[~/home/kali]
# nmap -sS 192.168.9.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-14 21:20 EST
Nmap scan report for 192.168.9.1
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.9.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
```

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.

```
(root㉿kali)-[~/home/kali]
# nmap -sU 192.168.9.1-2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 13:01 EST
Nmap done: 2 IP addresses (0 hosts up) scanned in 3.10 seconds

[root@kali ~]
```

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.

```
(root㉿kali)-[~/home/kali]
# nmap -sA -p 80 192.168.9.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 11:18 EST
Nmap scan report for 192.168.9.1
Host is up (0.00075s latency).

PORT      STATE      SERVICE
80/tcp    unfiltered  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

4. nmap -O 192.168.9.1

This command is to know the type of system, whether it is Windows or Linux.

```
(root㉿kali)-[~/home/kali]
# nmap -O 192.168.9.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 11:20 EST
Nmap scan report for 192.168.9.1
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.9.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei
VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox
(92%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%),
D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX
5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

## 1-Install Nmap <https://nmap.org/download>

