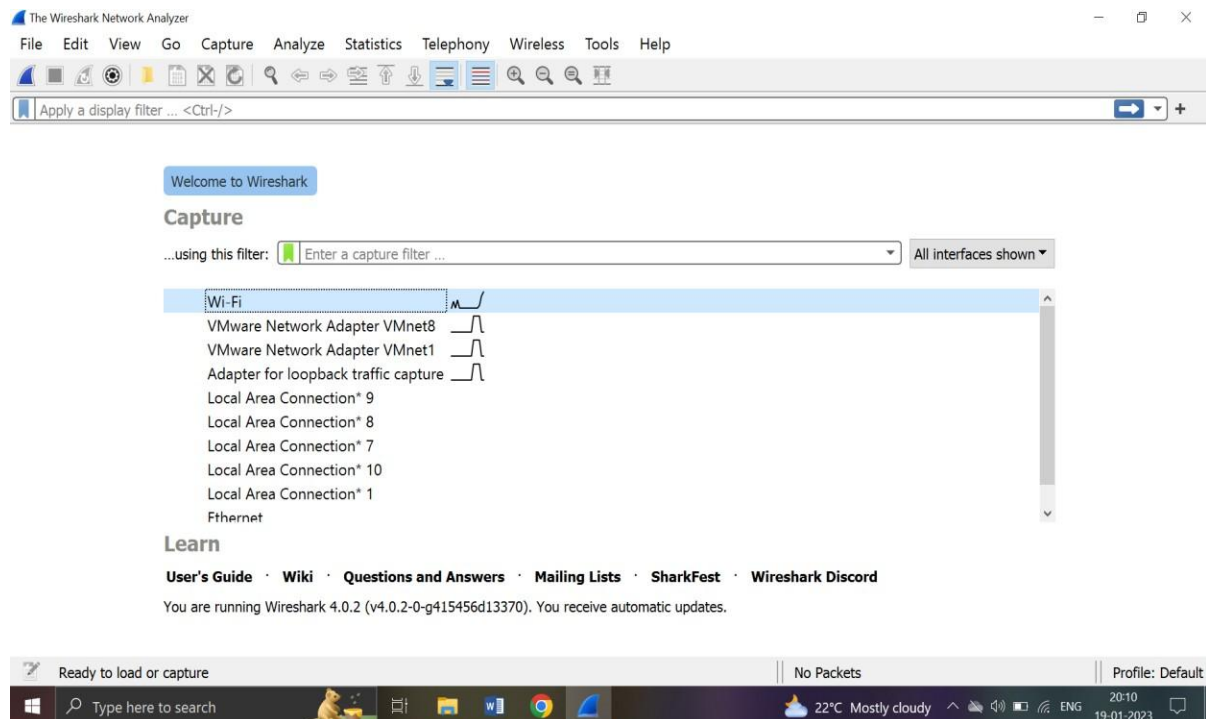
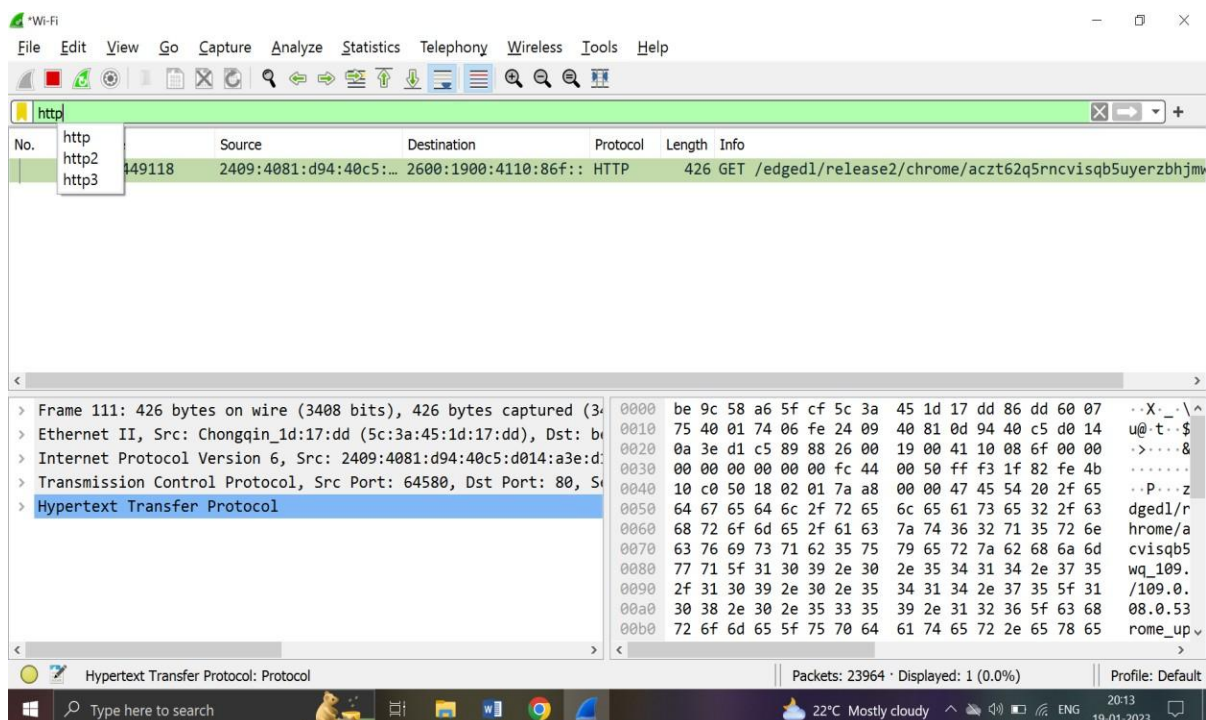


Title: Analyze the packets and solve the questions using Wireshark.

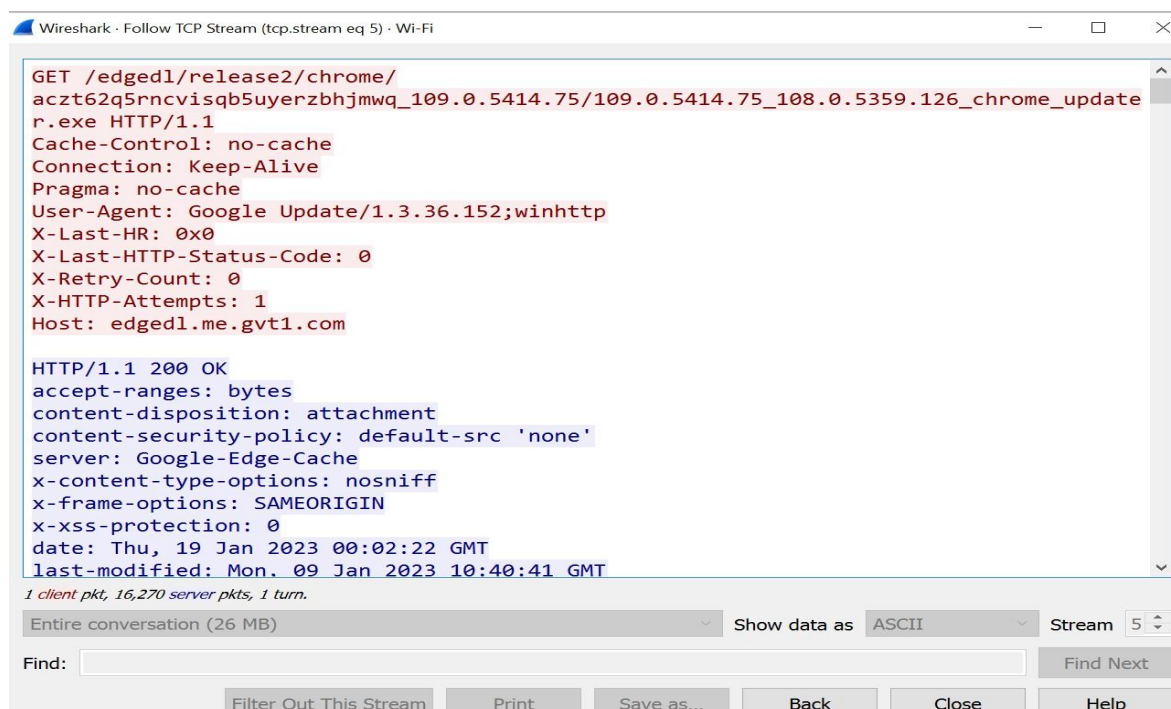
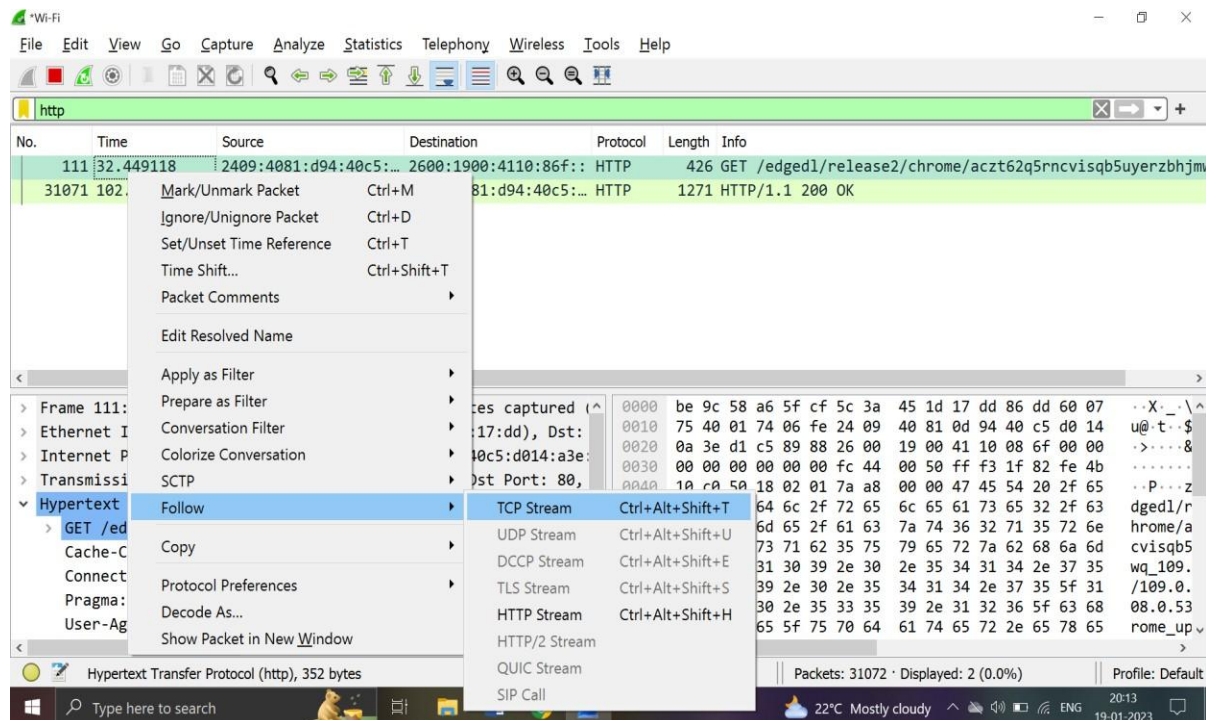
Step 1: Open Wireshark and Select your Network Connection.



Step 2: Identifying the GET/HTTP used by snopes.com



Step 3: Follow the TCP Stream to find out Server.



Step 4: Go to www.zero.webappsecurity.com and Login.

Zero Bank

Log in to ZeroBank

Login

Password

Keep me signed in ☐

[Sign in](#)

[Forgot your password ?](#)

Step 5: Look for the POST SIGN-IN method. It will have your Username and Password captured.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
72898	338.274780	64:ff9b::3652:16d6	2409:4081:d94:40c5::...	HTTP	759	HTTP/1.1 200 OK (text/html)
74155	342.482582	2409:4081:d94:40c5::...	64:ff9b::3652:16d6	HTTP	614	GET /online-banking.html HTTP/1.1
74289	342.825733	64:ff9b::3652:16d6	2409:4081:d94:40c5::...	HTTP	990	HTTP/1.1 200 OK (text/html)
74924	344.434166	2409:4081:d94:40c5::...	64:ff9b::3652:16d6	HTTP	587	GET / HTTP/1.1
75123	345.123772	64:ff9b::3652:16d6	2409:4081:d94:40c5::...	HTTP	759	HTTP/1.1 200 OK (text/html)
81278	369.459666	2409:4081:d94:40c5::...	64:ff9b::3652:16d6	HTTP	597	GET /login.html HTTP/1.1
81321	370.132481	64:ff9b::3652:16d6	2409:4081:d94:40c5::...	HTTP	981	HTTP/1.1 200 OK (text/html)
81439	396.780790	2409:4081:d94:40c5::...	64:ff9b::3652:16d6	HTTP	881	POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
81444	397.143045	64:ff9b::3652:16d6	2409:4081:d94:40c5::...	HTTP	395	HTTP/1.1 302 Found

[Full request URI: http://zero.webappsecurity.com/signin.html]
[HTTP request 1/2]
[Response in frame: 81444]
[Next request in frame: 81445]

File Data: 128 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "user_login" = "carnage7demon@gmail.com"
- Form item: "user_password" = "ChessMan@10"
- Form item: "submit" = "Sign in"
- Form item: "user_token" = "21060997-d8ca-45c9-b38a-34f662fc60370"

Text item (text), 38 bytes

Packets: 166300 · Displayed: 187 (0.1%) Profile: Default

22°C Mostly cloudy 20:26 19-01-2023

Step 6: If you follow stream TCP you can see both Username and Password captured in highlighted part.

