EXPERIMENT 7B

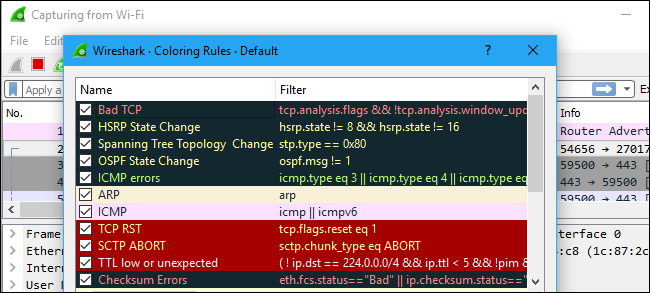
**Aim:** Traffic Analysis Using Wireshark

**1) Explain wiershark coloring rules:**

A very useful mechanism available in Wireshark is packet colorization. You can set up Wireshark so that it will colorize packets according to a display filter. This allows you to emphasize the packets you might be interested in. Wire shark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

There are two types of coloring rules in Wireshark: temporary rules that are only in effect until you quit the program, and permanent rules that are saved in a preference file so that they are available the next time you run Wireshark.

To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



**2) Difference HTTP and HTTPS**

|  |  |
| --- | --- |
| HTTP | HTTPS |
| HTTP URL in your browser’s address bar is http:// | HTTP URL in your browser’s address bar is https:// |
| HTTP is unsecured | HTTPS is secured |
| HTTP sends data over port 80 | HTTPS sends data 443. |
| HTTP operates at application layer | HTTPS operates at transport layer. |
| No SSL certificates are required for HTTP | HTTPS it is required that you have an SSL certificate and it is signed by a CA. |
| HTTP doesn’t require domain validation | HTTPS requires at least domain validation and certain certificates even require legal document validation. |
| No encryption in HTTP | HTTPS the data is encrypted before sending |
| It is less secure as the data can be vulnerable to hackers. | It is designed to prevent hackers from accessing critical information. It is secure against such attacks. |

3) **Difference between Get and Post.**

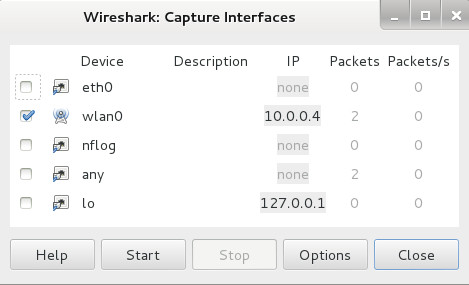
|  |  |  |
| --- | --- | --- |
| PARAMETERS | GET | POST |
| HISTORY | Parameters remain in browser history because they are part of the URL | Parameters are not saved in browser history. |
| BOOKMARKED | Can be bookmarked. | Cannot be bookmarked. |
| BACK button/resubmit behaviour | GET requests are re-executed but may not be re-submitted to server if the HTML is stored in the browser cache. | The browser usually alerts the user that [data](https://www.diffen.com/difference/Data_vs_Information) will need to be re-submitted. |
| Encoding Type | application/x-www-form-urlencoded | multipart/form-data or application/x-www-form-urlencoded Use multipart encoding for binary data. |
| Parameters | can send but the parameter data is limited to what we can stuff into the request line (URL). Safest to use less than 2K of parameters, some servers handle up to 64K | Can send parameters, including uploading files, to the server |
| Hacked | Easier to hack for script kiddies | More difficult to hack |
| Restrictions on datatype | Yes, only ASCII characters allowed. | No restrictions. Binary data is also allowed. |
| Security | GET is less secure compared to POST because data sent is part of the URL. So it's saved in browser history and server logs in plaintext. | POST is a little safer than GET because the parameters are not stored in browser history or in [web server](https://www.diffen.com/difference/Application_Server_vs_Web_Server) logs |
| Usability | GET method should not be used when sending passwords or other sensitive information. | POST method used when sending passwords or other sensitive information. |
| Visibility | GET method is visible to everyone (it will be displayed in the browser's address bar) and has limits on the amount of information to send. | POST method variables are not displayed in the URL |
| Cached | Can be cached | Not cached |

4) **How do you use wireshark to find password in any network?**

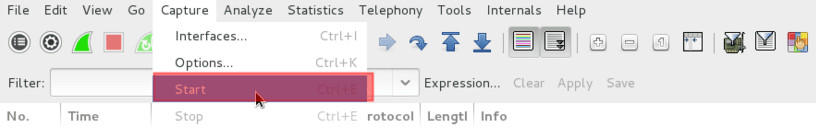
Step 1: Start Wireshark and capture traffic

In Kali Linux you can start Wireshark by going to Application > Kali Linux > Top 10 Security Tools > Wireshark

In Wireshark go to Capture > Interface and tick the interface that applies to you. In my case, I am using a Wireless USB card, so I’ve selected wlan0.



Ideally you could just press Start button here and wire shark will start capturing traffic. In case you missed this, you can always capture traffic by going back to Capture > Interface > Start



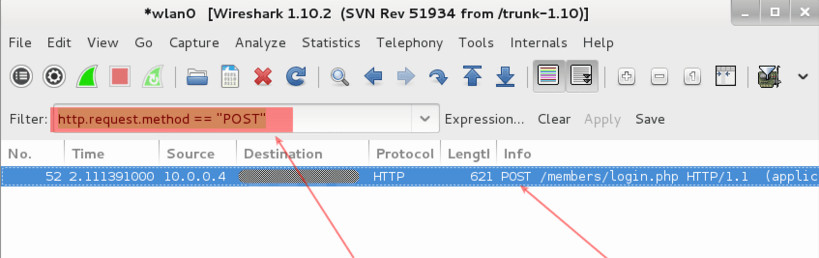
Step 2: Filter captured traffic for POST data

At this point Wire shark is listening to all network traffic and capturing them. I opened a browser and signed in a website using my username and password. When the authentication process was complete and I was logged in, I went back and stopped the capture in Wire shark. When we type in your username, password and press the Login button, it generates a POST method (in short – you’re sending data to the remote server).

To filter all traffic and locate POST data, type in the following in the filter section

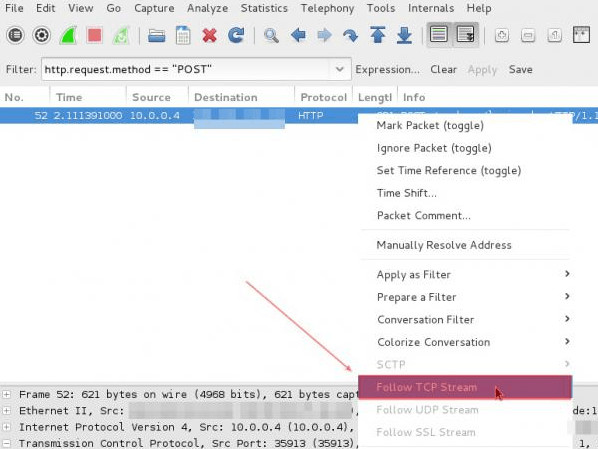
http.request.method == “POST”

See screenshot below. It is showing 1 POST event.

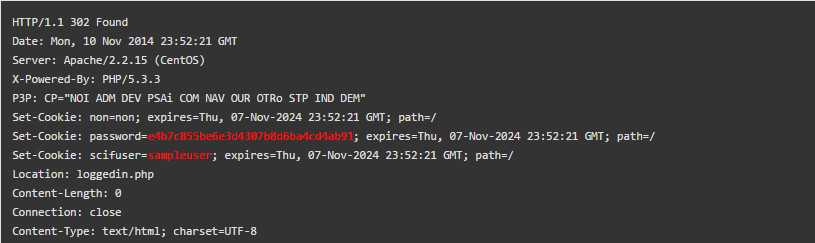


Step 3: Analyze POST data for username and password

Now right click on that line and select Follow TCP Steam



This will open a new Window that contains something like this :



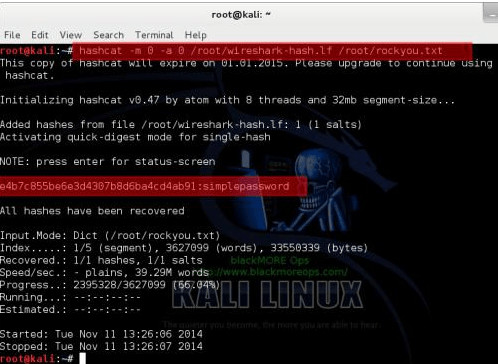
So in this case,

Username : sampleuser

Password : e4b7c855be6e3d4307b8d6ba4cd4ab91

But hold on, e4b7c855be6e3d4307b8d6ba4cd4ab91 can’t be a real password. It must be a hash value.

To crack this password its simple just open new terminal window and type this :



**5) Which filter is used to check all incomingand outgoing packets in a network?**

HTTP web servers use TCP port 80. Incoming requests to the web server would have the destination port number as 80. If you want to measure the number of connections rather than the amount of data, you can limit the capture or display filters to one side of the communication. So the filter used is tcp.dstport==80.

Outgoing packets would contain the IP address of the system as it’s source address. So assuming that the IP address of the system is 192.168.1.2, the filter would be ip .src==192.168.1.2

**CONCLUSION:**

From this Experiment we learnt about a Software called Wireshark.We Looked through the interface of wireshark and saw the traffic analysis.Wireshark is a widely used network protocol analyzer.Various color rules are used in displaying the packets.We also learnt the differencce beteween HTTP and HTTPS and Difference between Get and Post in Networking.