**Report about wireless survey/phishing**

*By*

**Mehnaz Afrose**

**Question 1: what did I do?**

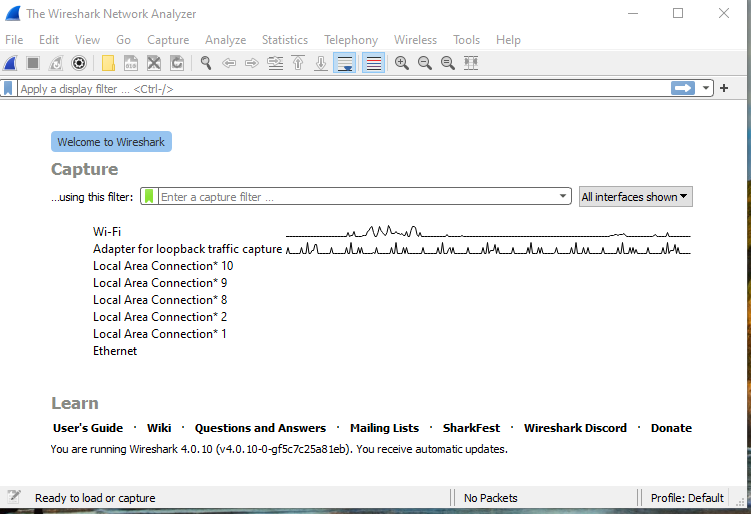
For the wireless survey, I wanted to find out whether there was any unsecured open network available in my apartment block. I accessed the Wi-Fi settings in the system tray of my windows laptop. It revealed the list of available Wi-Fi networks from the nearest apartments. After this survey, I went outside with my cellphone connected to my home network to find out how far the signal can extend outside my home. Just to be safe, I decided to analyze my own network by using Wireshark.

Before installing and using Wireshark, I did some research to know about this application, how to use it, what aspects should I know to understand the network protocol analysis, etc.

Wireshark is a free open-source network protocol analyzer, which started its journey of a project in 1998 ([About Wireshark](https://www.wireshark.org/about.html)) ([Wikipedia](https://en.wikipedia.org/wiki/Wireshark)). It can capture packets from a network connection, it is capable of slicing and dicing random live data by using filters, and it also can visualize the conversations and network stream, just like any other packet sniffer ([What is Wireshark and How Is It Used?](https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it)). To understand network communications, analyze the communication, and for troubleshooting any issues in communication that arise within network communication protocol, Wireshark can be incredibly beneficial ([How to Use Wireshark: Comprehensive Tutorial + Tips](https://www.varonis.com/blog/how-to-use-wireshark)).

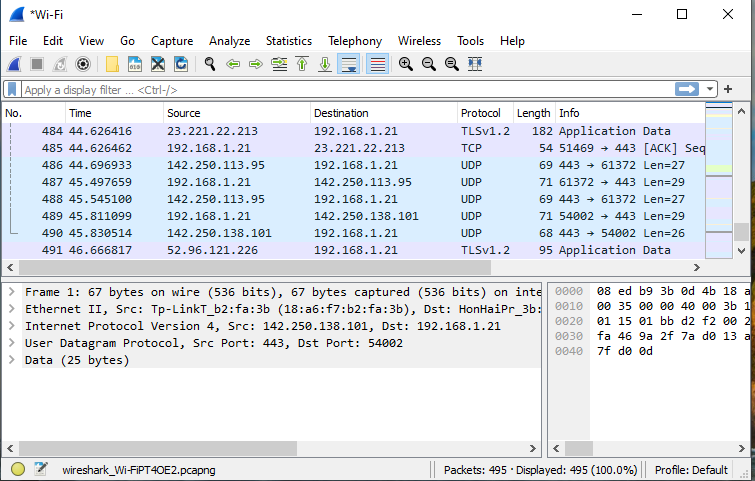
After going through the whereabouts of Wireshark, I successfully installed the application on my computer. Then I delved into the process about [how to use Wireshark for protocol analysis](https://www.youtube.com/watch?v=95WbK95D0Xo). Watched more videos: [Wireshark - Malware traffic Analysis,](https://www.youtube.com/watch?v=3t1BNAavrlQ) [What Is Wireshark And How It Works?,](https://chat.openai.com/c/5994031e-6fb9-4cdb-88a6-44402869588d) [Finding Open Ports with Wireshark,](https://www.youtube.com/watch?v=AWqVuFGqlFI&t=89s) [Identifying Open Ports in Wireshark,](https://www.youtube.com/watch?v=Zi1aaEJg5YI) [Scanning Networks For Open Ports To Access, and so on.](https://www.youtube.com/watch?v=TyUtnOb-kS0&t=266s)

I installed the free version of Wireshark. When I launched the application on my computer, it was showing eight types of network connection: Wi-Fi, Adapter for loopback traffic capture, Local Are Connection\*10, Local Are Connection\*9, Local Are Connection\*8, Local Are Connection\*2, Local Are Connection\*1, and Ethernet. These were the connections connected to my computer network then. The difference between the graphs represented the traffic on the network that was present. For further analysis about what was going on the network, I selected Wi-Fi network on my computer.



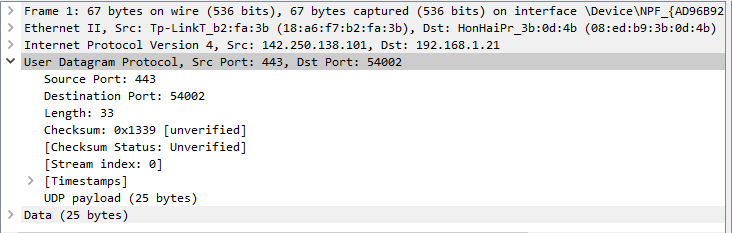
*Figure 1: Wireshark presenting traffic of networks*

The application captured the packets for about 10 or 20 seconds and picked up 67packets. It represented some packet settings presented in figure 2. These were the packet transactions that had been made on my network through the internet.



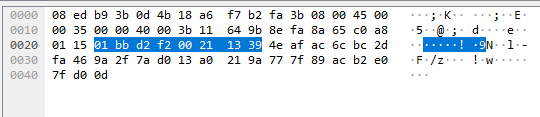
*Figure 2: Packet settings presented by Wireshark*

The bottom left of the page represented the various detailed information about the transaction. We can see this in figure 3.



*Figure 3: Detail information about the transactions*

The bottom right part represented some binary values which users do not use most often. So, I also ignored that part.

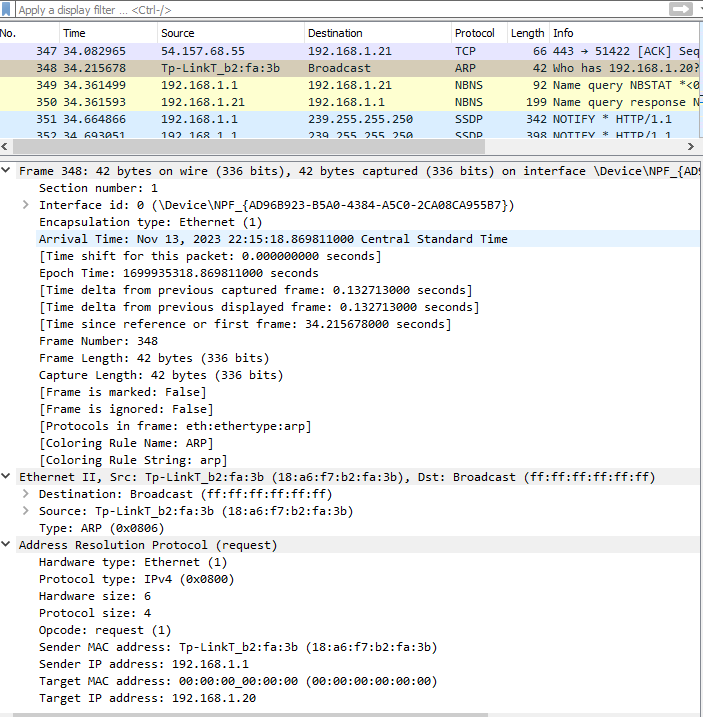


*Figure 4: Binary values represented by Wireshark*

There was another exercise about phishing. A phishing attack is a fraudulent cyber-attack where fake emails or websites are used by attackers to steal people's personal information ([What Is Phishing?](https://www.phishing.org/what-is-phishing)). For this exercise I took part in [SONICWALL PHISHING QUIZ](https://www.sonicwall.com/phishing-iq-test/). And another [PHISHING QUIZ](https://www.opendns.com/phishing-quiz/) from OpenDNS.

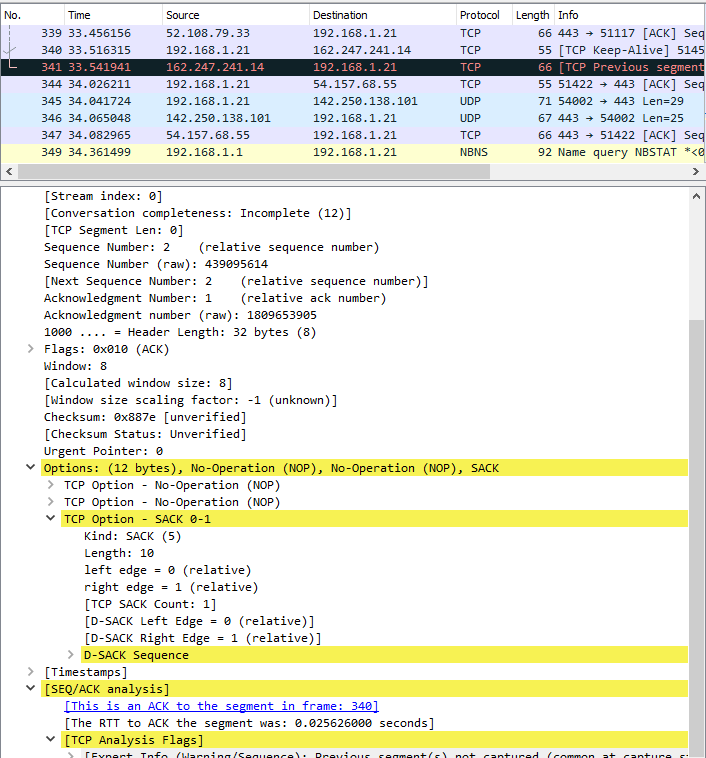
**Question 2: What were the results?**

To analyze the network packets, I randomly selected frame 348, which is an ARP protocol. ARP, which stands for Address Resolution Protocol, is used to map an IP address to a MAC address ([What is Address Resolution Protocol (ARP)?](https://chat.openai.com/c/5994031e-6fb9-4cdb-88a6-44402869588d)). By clicking the interface id, I was able to know when it was picked up, how big it is, etc. By clicking Ethernet II, I was able to know the destination and source of the MAC address. By going deeper by clicking Address Resolution Protocol, I could see the information carried by an ARP.



*Figure 5: Information from an ARP protocol*

To check whether there has been any DHCP traffic going on, I added the filter ‘bootp.’ There was no DHCP traffic going on at that time of capture. DHCP or Dynamic Host Configuration Protocol is used to assign IP address and network configuration information to devices on a network automatically ([What is DHCP and why is it important?](https://efficientip.com/glossary/what-is-dhcp-and-why-is-it-important/)). Then I looked for “HTTP” traffic, and there was no such traffic captured by the Wireshark application. This stands for Hypertext Transfer Protocol and this one is an application layer protocol that provides the transfer of hypertext including text, images, videos, and other multimedia resources, between users and servers ([What is HTTP?](https://www.cloudflare.com/en-in/learning/ddos/glossary/hypertext-transfer-protocol-http/)). Just to be safe, I filtered out all the traffic using my own IP address.

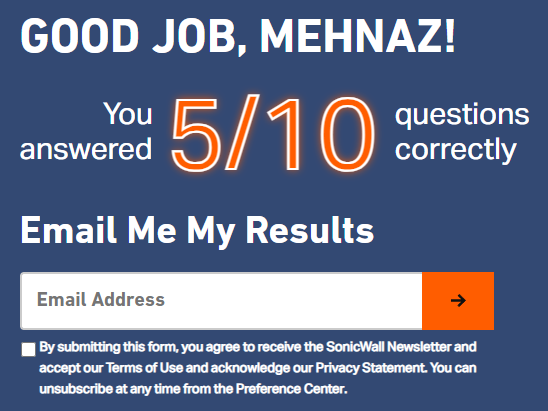


*Figure 6: Frame 341 information*

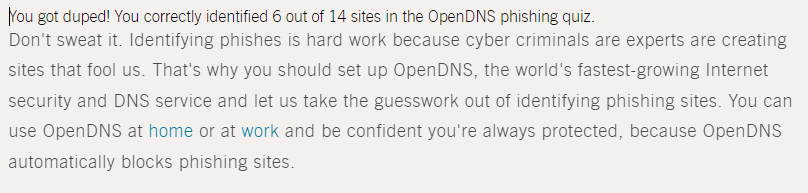
The frame number 341, which was a TCP protocol, showed that this packet was not carrying out any specific function or action. TCP protocol stands for Transmission Control Protocol and operates at the transport layer of the TCP/IP model and is responsible for establishing and maintaining connections, segmenting data into packets, ensuring reliable delivery, and managing flow control ([What is Transmission Control Protocol TCP/IP?](https://www.fortinet.com/resources/cyberglossary/tcp-ip)).

I accessed the Wi-Fi settings in the system tray of my windows laptop. It revealed the list of available Wi-Fi networks from the nearest apartments. Among all those available networks, no network was showing the absence of a lock icon. That means every network was password protected. After this survey, I went outside with my cellphone connected with my home network to find out how far the signal can extend outside my home. I found out that around three blocks of my apartment my network system was visible, that means, anyone who is within this area can get access to my router using my provided password.

In the first phishing quiz, the result was not satisfactory. I was able to identify five phishing/legitimate emails out of ten emails. For the second quiz, this one was not satisfactory either. In the second quiz, I provided six correct answers out of fourteen sites.



*Figure 7: Scores of Phishing quiz 1*



*Figure 8: Result of Phishing quiz 2*

**Question 3: what did I learn?**

By knowing about Wireshark, I came to understand that this application can be significantly useful in protecting my network. With this application, I can look closer at the data flowing through my network system. I can spot odd behaviors, like strange traffic or unknown devices, which might signal a problem. By analyzing the traffic, I might catch signs of attacks, unauthorized access attempts, or even malware. But Wireshark is not the ultimate solution for the protection of the network. Along with this we also need the combination of firewalls, antivirus software, and strong passwords for better protection.

After taking part in the phishing quizzes, I realized how weak my cybersecurity knowledge in identifying phishing emails. I should gather more information and knowledge in this area.

Reference:

1. [About Wireshark](https://www.wireshark.org/about.html)
2. [Wikipedia](https://en.wikipedia.org/wiki/Wireshark)
3. [What is Wireshark and How Is It Used?](https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it)
4. [How to Use Wireshark: Comprehensive Tutorial + Tips](https://www.varonis.com/blog/how-to-use-wireshark)
5. [How to use Wireshark for protocol analysis](https://www.youtube.com/watch?v=95WbK95D0Xo)
6. [Wireshark - Malware traffic Analysis](https://www.youtube.com/watch?v=3t1BNAavrlQ)
7. [What Is Wireshark And How It Works?](https://chat.openai.com/c/5994031e-6fb9-4cdb-88a6-44402869588d)
8. [Finding Open Ports with Wireshark](https://www.youtube.com/watch?v=AWqVuFGqlFI&t=89s)
9. [Identifying Open Ports in Wireshark](https://www.youtube.com/watch?v=Zi1aaEJg5YI)
10. [Scanning Networks For Open Ports To Access](https://www.youtube.com/watch?v=TyUtnOb-kS0&t=266s)
11. [What Is Phishing?](https://www.phishing.org/what-is-phishing)
12. [What is Address Resolution Protocol (ARP)?](https://chat.openai.com/c/5994031e-6fb9-4cdb-88a6-44402869588d)
13. [What is DHCP and why is it important?](https://efficientip.com/glossary/what-is-dhcp-and-why-is-it-important/)
14. [What is HTTP?](https://www.cloudflare.com/en-in/learning/ddos/glossary/hypertext-transfer-protocol-http/)
15. [What is Transmission Control Protocol TCP/IP?](https://www.fortinet.com/resources/cyberglossary/tcp-ip)