**What did you do?**

For this assignment, I obtained permission from the Canyon Public Library to conduct network analysis and packet capturing using Wireshark on their Wi-Fi network. Before starting the process, I ensured that I had the necessary authorization to monitor and analyze their network traffic.

The following steps were involved in the process: **Network and Protocol Identification**:

I started by launching Wireshark and selecting the appropriate network interface to monitor. In the case of the Canyon Public Library, I chose the Wi-Fi network interface. Wireshark's wireless scanning feature allowed me to identify all the available Wi-Fi networks in the vicinity, including their names, MAC addresses, and signal strengths. From the scan results, I focused on the library's Wi-Fi network for further analysis. **Packet Capturing**: The network scan using Wireshark revealed 15 devices connected to the library's Wi-Fi network during the 5 minutes capture period. During this time, I observed the network traffic, both transmitted and received by devices connected to the Wi-Fi network. Additionally, I conducted a loopback packet capture on one of the library's computers to understand local communications and potential security issues within the device itself. **Analysis of Captured Packets:** Wireshark provided a comprehensive view of the captured packets, displaying various protocols and data transmitted over the network. I analyzed the captured packets to understand the types of traffic present on the network, including HTTP for web browsing, DNS for domain resolution, and TCP for data transfer. I also examined loopback packets to gain insights into the communication between processes on the library's computer.

**What are the results?**

In the results section, I observed the following: **Networks and Protocols Identified**: The network scan revealed 15 devices connected to the library's Wi-Fi network during the 5 minutes capture period. I identified the MAC addresses of these devices and the access points they were connected to. Common Wi-Fi protocols, such as Beacon frames, Probe Request/Response, and Data frames, were observed during the scan. **Packet Analysis:** The captured packets provided valuable insights into the network's activities. I observed various protocols being used for legitimate purposes, and there were no signs of any packets reflecting a cyber attack during the capture period. The loopback analysis on the library's computer also did not show any suspicious communications. **Attack Surface Assessment:** The presence of 15 connected devices on the Wi-Fi network indicates a potential attack surface for unauthorized devices. While no cyber attack evidence was found in the captured packets, it is essential for the organization to regularly monitor the network for any anomalies and unauthorized access attempts to minimize the attack surface.

**What did you learn?**

From this assignment, I learned the following: **Understanding Digital Networks and Packets:** Wireshark is a powerful tool for network analysis that allows us to monitor and capture packets to gain insights into network activities. It helps in identifying connected devices, network protocols, and data transmissions, enabling better network security and troubleshooting. **Assessing Attack Surface:** Analyzing the captured packets and network activities helped me understand the concept of attack surface. The attack surface represents all the potential points of entry for cyber attackers and includes connected devices, open ports, protocols, and system vulnerabilities. Regular monitoring and security measures are necessary to reduce the attack surface and mitigate potential risks. **Value to the Organization:** Wireshark and network analysis play a crucial role in enhancing cybersecurity for organizations. By identifying potential threats and vulnerabilities, organizations can take proactive measures to secure their networks, protect sensitive data, and ensure smooth operations. Additionally, loopback packet analysis can be valuable for detecting security issues within individual devices.

**Future Use and Recommendations:** In the future, I can leverage the knowledge gained from this assignment to perform more in-depth network analysis and packet captures for various organizations. As an organization, implementing regular network monitoring and packet analysis can significantly improve network security and reduce the risk of cyber attacks. It is essential to stay up to date with the latest cybersecurity practices and tools to ensure a safe digital environment.

This assignment provided hands-on experience in network analysis, packet capturing, and understanding the attack surface presented by a Wi-Fi network. I gained valuable insights into the functioning of digital networks, the significance of analyzing network traffic, and the importance of securing data and devices from potential cyber threats.