Week1- Data Collection Setup

Setting up data collection, especially for **network bandwidth usage**, is crucial to gain a clear understanding of patterns and requirements. Here's a proposed method:

Data Collection Setup for Network Bandwidth Usage:

1. **Selection of Tools:**
- Wireshark: A popular network protocol analyzer. It can capture real-time data, analyze traffic patterns, and provide detailed information about network activities.

2. **Objective Identification:**
- **Determine what specific information I need:** total bandwidth consumption, per-device consumption, specific application usage, etc.
- **Define the period for which data needs to be collected:** 24/7 monitoring, peak hours, weekends, etc.
- **Choose the Appropriate Network Interface:** For example, if I connected via Wi-Fi, choose Wi-Fi adapter; if it's Ethernet, choose that. Start the capture by double-clicking on the desired interface.

3. **Filter Packets for Specific Information (Optional):**
- **Display filters for a specific objective：** For instance, if I want to view only HTTP traffic, I can use the filter http. For HTTPS traffic, use tls.

4. **Identify Devices on the Network:**
- By default, Wireshark will capture all packets on the network interface you selected.
- To identify devices, I can look for ARP (Address Resolution Protocol) packets which help map IP addresses to MAC addresses.
- Use the filter arp in the filter bar. This will show my packets where devices are asking for the MAC address of other devices, thereby helping me identify them.

5. **Inspect Individual Packets:**
- Click on a packet to inspect its details.In the packet details pane, expand the protocol headers to see various attributes like source/destination IP, source/destination MAC address, etc.

6. **Further Analysis:**

Now, I can apply various filters, statistics, and tools provided by Wireshark to analyze the capture deeply. For example, you can go to Statistics > Conversations to see a list of all interactions between devices.