Auftrag

Vorbereitende Aufgaben:

1) Installiere Wireshark auf deinem Linux-System:

   ```
   $ sudo apt-get install wireshark
   ```

2) Starte den Chatserver, den Chat-Reader sowie den Chat-Writer auf deinem Computer und verwende die IP-Adresse 127.0.0.1, um mit dem chatserver auf der lokalen Maschine über das loopback-Interface zu kommunizieren.

3) Starte wireshark und beginne, auf dem Interface lo den Traffic mitzuschneiden:

   ```
   $ sudo wireshark
   ```

4) Schreibe ein paar Chat-Nachrichten und beende anschliessend die Chat-Session. Stoppe anschliessend die Live-Capture in Wireshark und schau dir den Mitschnitt des Datenverkehrs an.

Aufgaben:

1. Betrachte das erste Paket, das vom Chat-Writer an den Server gesendet wurde. Von welchem Ort und welcher IP-Adresse an welchen Port und welche IP-Adresse ging es? Warum?
2. Schau dir das 2. Paket an. Was sind Quelle und Ziel? Weshalb?
3. Schau dir Pakete Nummer 3 und 4 an: Quelle und Ziel? Erklärung?
4. Betrachte die Grösse des 1. Pakets. Wie gross ist es? Wieviel davon sind Nutzdaten für das Chat-Protokoll, wieviel sind andere Daten?
5. Jedes Paket transportiert Daten für mehrere Schichten, Angefangen vom Frame über Ethernet II, Internet Protocol Version 4 und User Datagram Protocol bis zu “Data”. Kannst du dir darauf einen Reim machen? Schau dir die Daten in den einzelnen Schichten an und versuche herauszufinden, was es eventuell damit auf sich hat.
6. Wenn du soweit bist, mach eine Gruppe mit 2 anderen Leuten. Startet auf einem Computer den chatserver und verbindet euch auf zwei anderen Computern damit. Lasst auf allen Computern wireshark auf dem Interface eth0 mitlaufen und vergleicht dann den Datenverkehr mit dem vorherigen. Findet ihr die Chat-Pakete? Was hat sich an ihnen geändert?