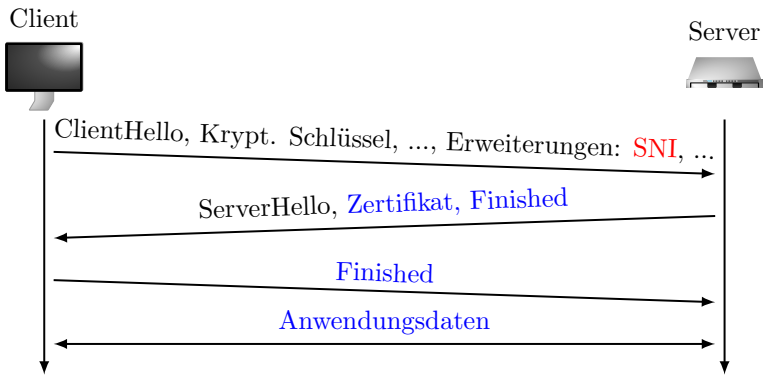
Aufgabenstellung: Eine Schulklasse soll selbstständig über HIV/AIDS im Internet recherchieren und am Ende der Stunde ihre Ergebnisse präsentieren. Die Anweisung hierbei: jeder soll sein eigenes Handy nutzen, aber ChatGPT darf unter keinen Umständen genutzt werden! Einige Schüler nehmen die Aufgabe nicht ganz ernst und scheinen stattdessen Videos auf Instagram zu schauen. Die Lehrkraft ist zwar nicht schnell genug und die Schüler wechseln immer die Website, wenn die Lehrkraft zusieht, allerdings hat die Lehrkraft ein Ass im Ärmel. Schon während der ganzen Stunde werden die Pakete, die von den Handys der Schüler aufgezeichnet werden, am WLAN-Access-Point (WLAN-Router) aufgezeichnet. Lassen sich die Schüler überführen?

Die Datei `klasse1.pcap` enthält die Pakete, die vom iPhone eines bestimmten Schülers ausgehen. Können Sie nachvollziehen, was der Schüler während der Stunde gemacht hat? Hat er ChatGPT verwendet?

Hintergrundinformationen: Pakete werden im Internet basierend auf IP-Adressen zugestellt. Damit Nutzer sich keine IP-Adressen merken müssen, werden mithilfe des Domain Name Service (DNS) Domain-Namen wie google.de zu IP-Adressen *aufgelöst*. DNS ist in der Regel unverschlüsselt und bietet somit die Möglichkeit, die aufgelösten Domain-Namen mitzulesen. Es gibt allerdings auch Technologien wie *DNS over HTTPS*, welches diese Abfragen verschlüsselt. Diese Technologien wird zum Beispiel von dem Bekannten DNS-Server von Google mit der IP-Adresse `8.8.8.8` unterstützt.

Der Großteil der Kommunikation in den Paketen läuft über HTTPS, d.h. er ist mithilfe von **TLS** verschlüsselt. TLS verschlüsselt übertragene Daten, indem sich beide Seiten (Client und Server) auf einen gemeinsamen Schlüssel einigen. Der Aufbau einer verschlüsselten Verbindung via TLS, der sogenannte *Handshake*, läuft zwischen Client (z.B. Handy) und Server wie folgt ab:



Die blauen Felder sind verschlüsselt, d.h. in den aufgezeichneten Paketen nicht lesbar. Der Client beginnt den Verbindungsaufbau und sendet kryptografisches Schlüsselmaterial, aus denen der Server einen gemeinsamen, geheimen Schlüssel ableitet. Mit diesem wird dann der Rest der Daten verschlüsselt, z.B. das Zertifikat, welches den Server identifiziert, sowie die Anwendungsdaten.

Rot markiert ist allerdings ein Feld, welches sich **SNI** (Server Name Indication) nennt. Dieses Feld ist nicht verschlüsselt und beinhaltet den Namen des Servers, mit dem die Verbindung hergestellt werden soll. Das Feld wird benötigt, falls mehrere Domain-Namen (also Namen für Websites und andere Dienste) einer IP-Adresse zugeordnet sind, um beim Verbindungsaufbau unterscheiden zu können, mit welchem Domainnamen die Verbindung hergestellt werden soll. Dies ist heutzutage fast immer der Fall.

Unter `https://teacher2.css.net.cit.tum.de/` ist ein Web-Tool verfügbar, was die Pakete aus `klasse1.pcap` darstellen kann. Oben ist eine Zeile zu finden, mit der die Pakete gefiltert werden können, es können zum Beispiel alle TLS-Pakete angezeigt werden, indem der Filter `tls` verwendet wird. Unter `https://www.wireshark.org/docs/dfref/t/tls.html` finden sich zudem die genaueren Filter für TLS.