16. Aufgabe: SSH in Wireshark

Greifen Sie mit einem geeigneten SSH-Client wie z.B. Putty oder der Kommandozeile auf den Server

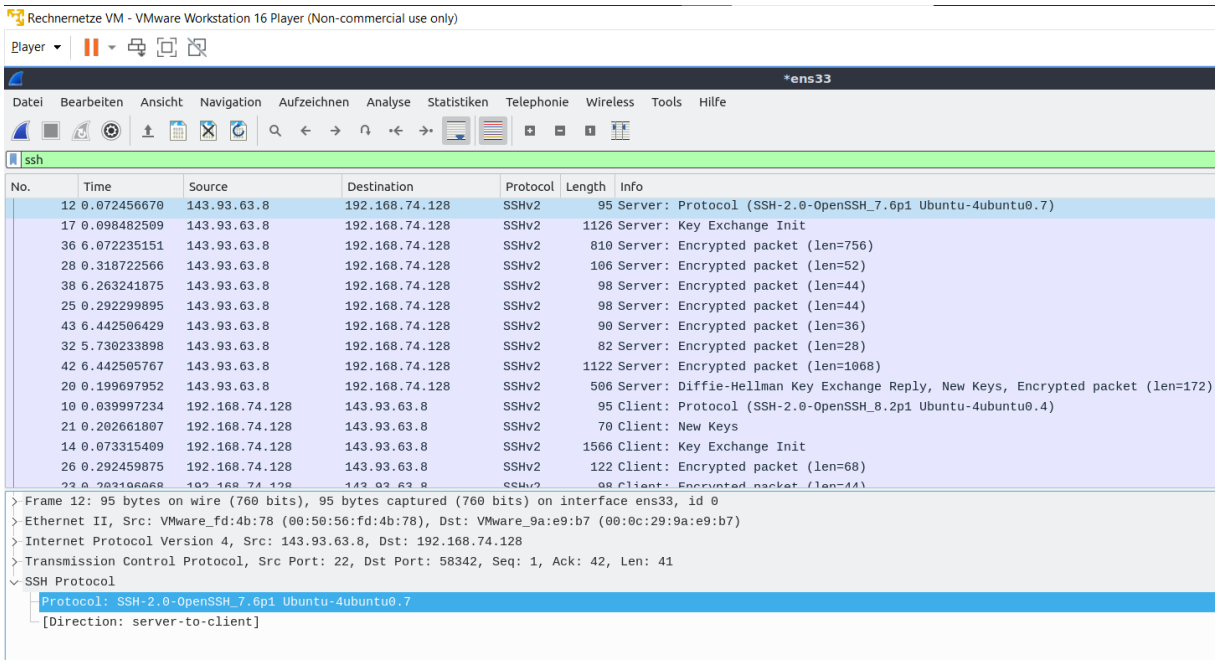
ssh.hochschule-trier.de

zu und schneiden Sie den Traffic mit Wireshark mit. Beantworten Sie dann folgende Fragen:

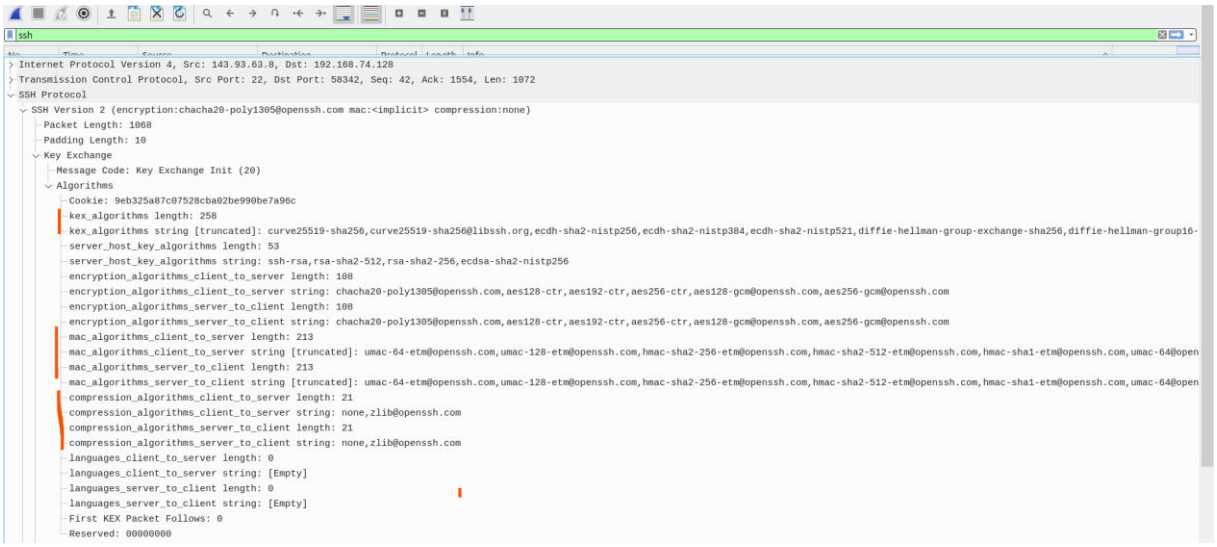
- Wie stellen Sie sicher, dass es sich tatsächlich um den SSH-Server der Hochschule handelt und Sie nicht gerade Opfer eines MITM-Angriffs werden?
- Was für ein SSH-Server wird verwendet?
- Welche Verschlüsselungs- und MAC-Algorithmen werden vorgeschlagen? Welche werden ausgewählt? Wo können Sie die Reihenfolge der Algorithmen, die von Ihrem Client vorgeschlagen werden, ändern?
- Welche Kompressionsverfahren werden vorgeschlagen? Welche werden ausgewählt?
- Wie lautet die für den Diffie-Hellman-Schlüsselaustausch verwendete Primzahl p und Primitivwurzel g bzw. die verwendete elliptische Kurve?
- Wie lauten die für den Diffie-Hellman-Schlüsselaustausch ausgetauschten Werte e und f?
- Wie lautet der für den Diffie-Hellman-Schlüsselaustausch verwendete öffentliche Schlüssel des Servers?
- Wie lautet der Wert für die Signatur von H?

-Wir müssen ja unsere Kennung und Passwort mitgeben. Die wissen ja (Im besten Fall) nur wir und der Server.

-



-Versch. Max und Komp

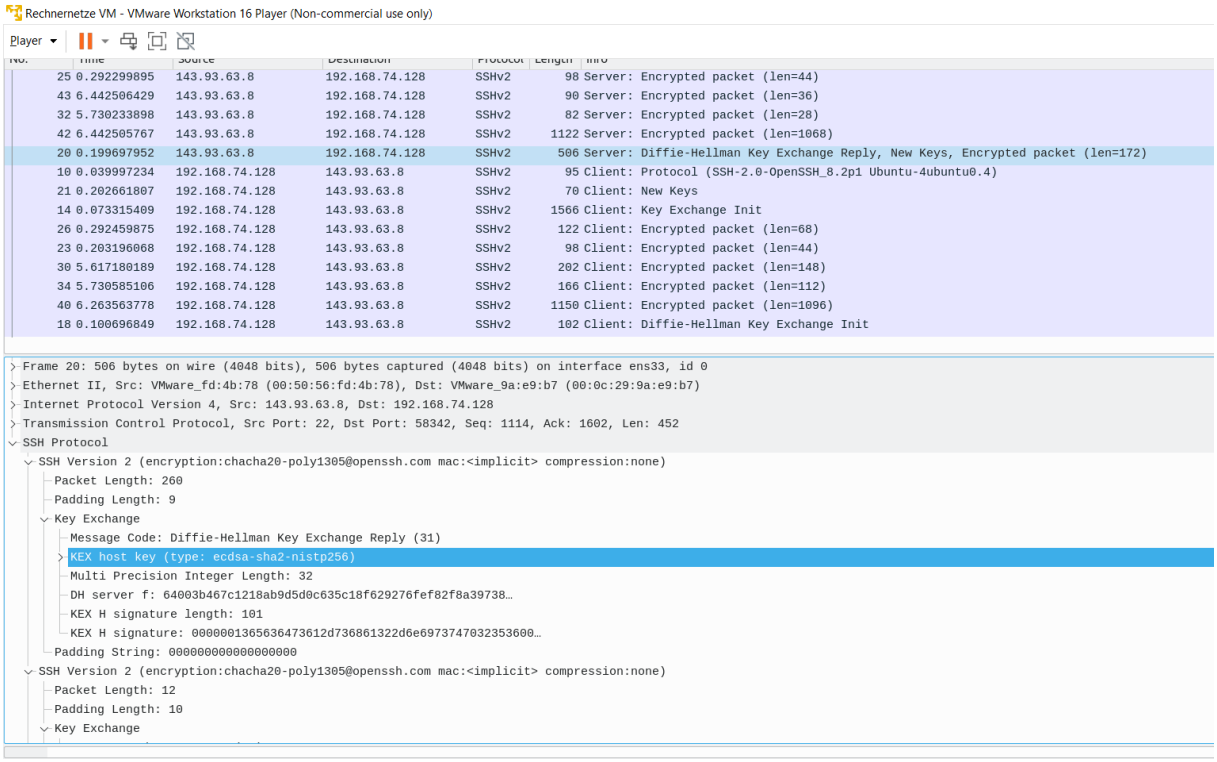


- Es wird sich auf den ersten Alg. in der Liste geeinigt.

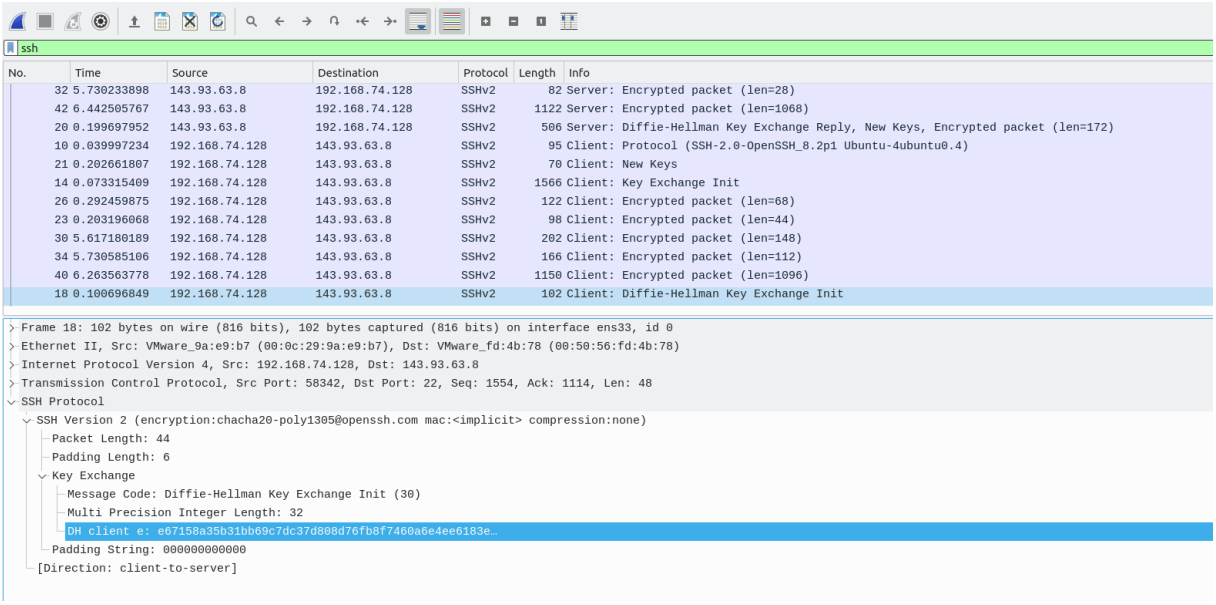
Man muss das SSH-Serverprofil bearbeiten um die Reihenfolge zu ändern

-Kompr Auswahl

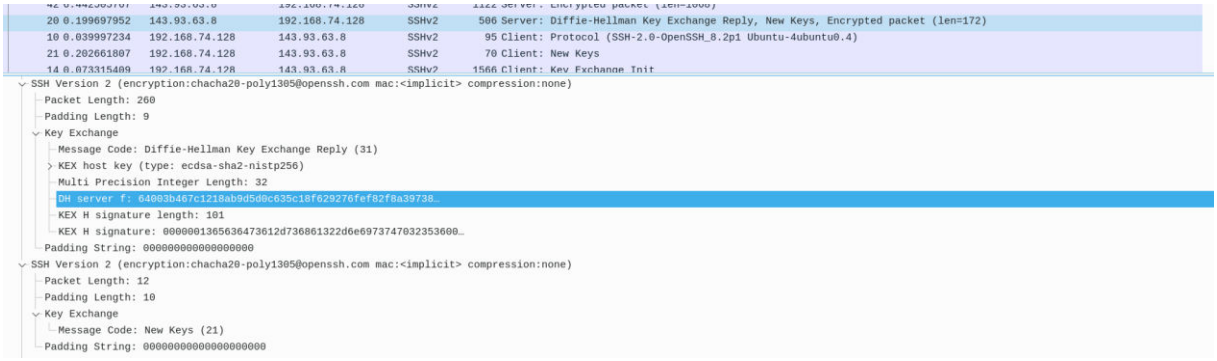
-Kurve



-e (Hoffentlich in Vorlesung sah das anders aus)



-f



Signatur