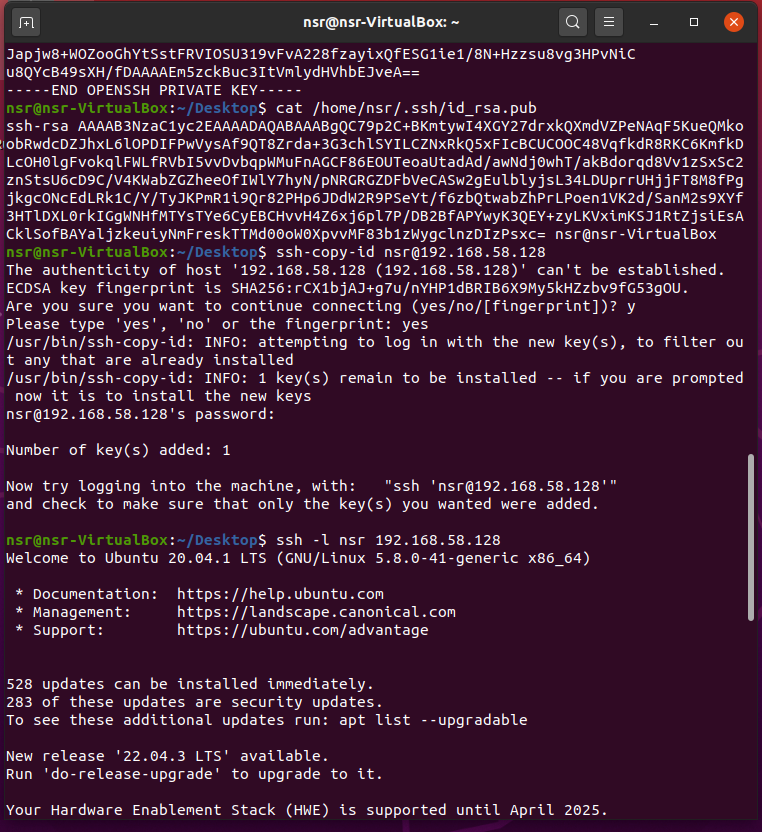
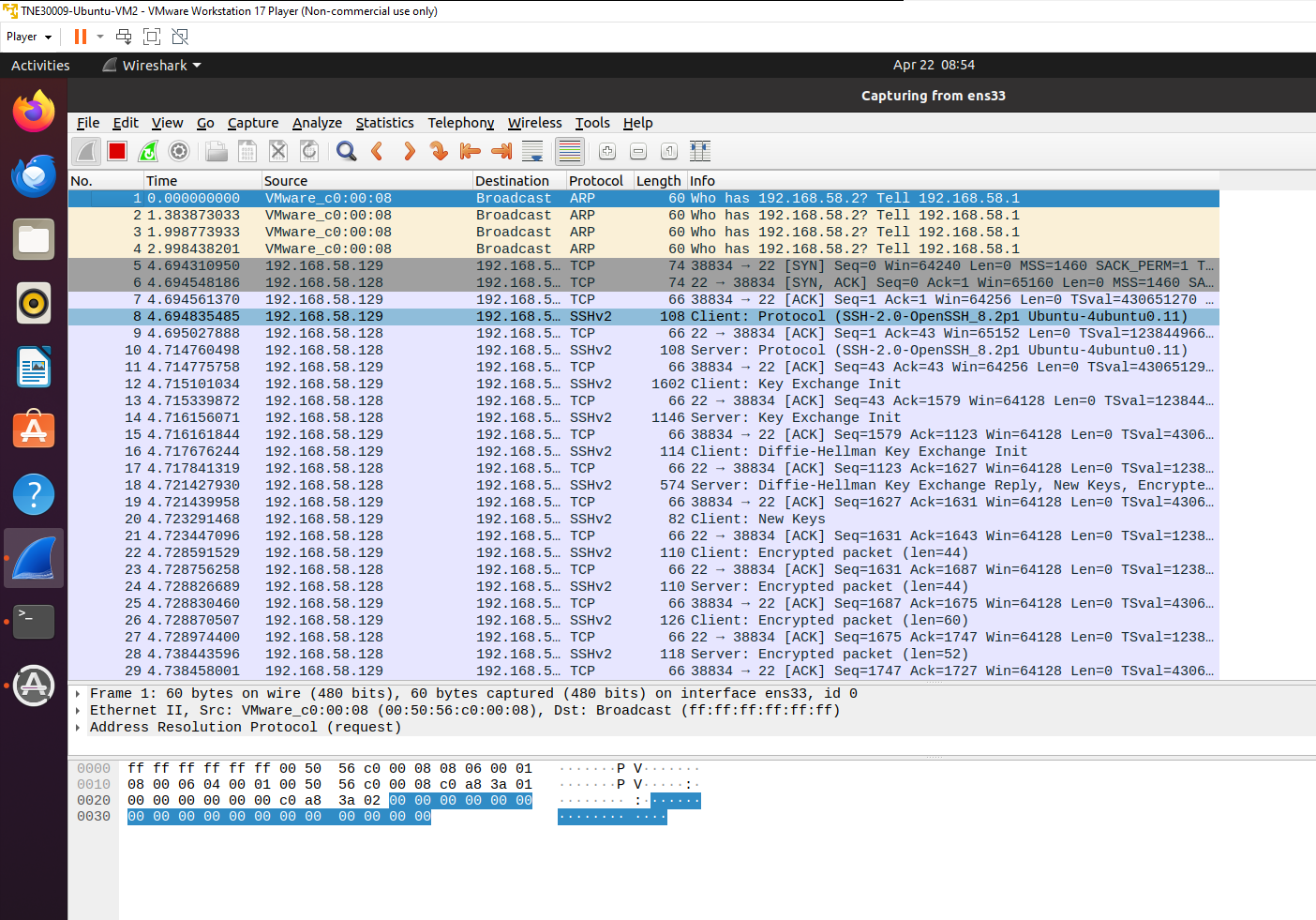
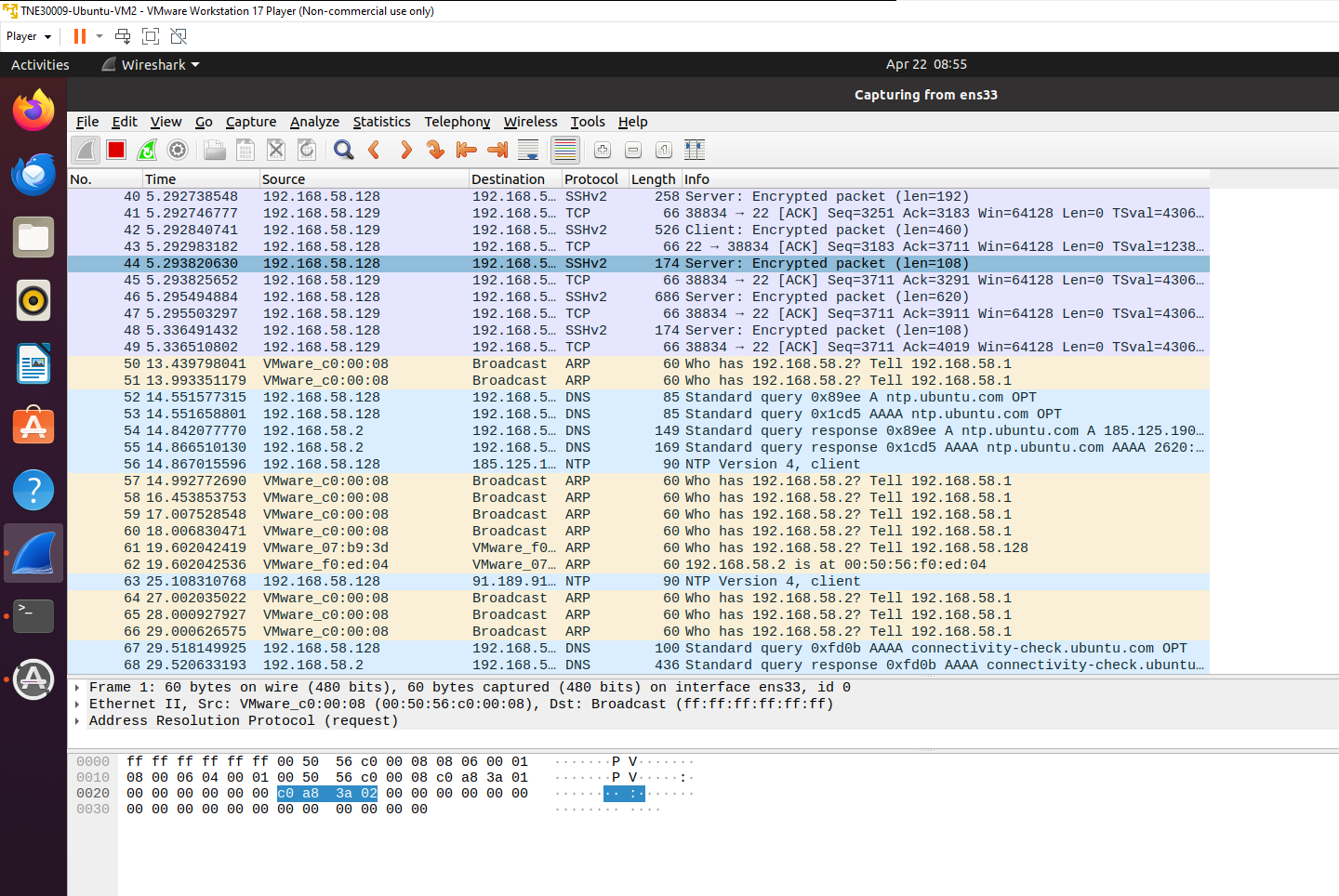
1. Screen dumps showing a successful log in using the public/private key pair. You should not be asked for a password.



1. A wireshark screen dump showing the exchange of SSH messages generated as a result of your login.

Diffie-Hellman key exchange and authentications:





1. A short explanation in very broad terms of how the log in works.

First, we generate a pair of keys – a public one and a private one. The public key is shared freely, while the private key is kept secret.

When we attempt to log in, the server sends a challenge. The user encrypts this challenge using their private key to create a response.

The server decrypts the response using the public key it has on file for that user. If the decrypted response matches the challenge, the user is authenticated.

Once authenticated, the user is granted access to the server without needing to provide a password.

In essence, the private key serves as a unique identifier for the user, and only they possess the corresponding key needed to decrypt the challenge. This method provides a secure way to authenticate users without transmitting passwords over the network.