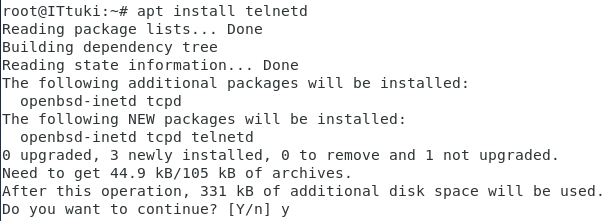
Tässä ohjeessa käydään läpi hiukan perusjuttuja Wireshark ohjelmasta, jolla katsotaan mitä eroa Telnetillä ja SSH yhteydellä on.

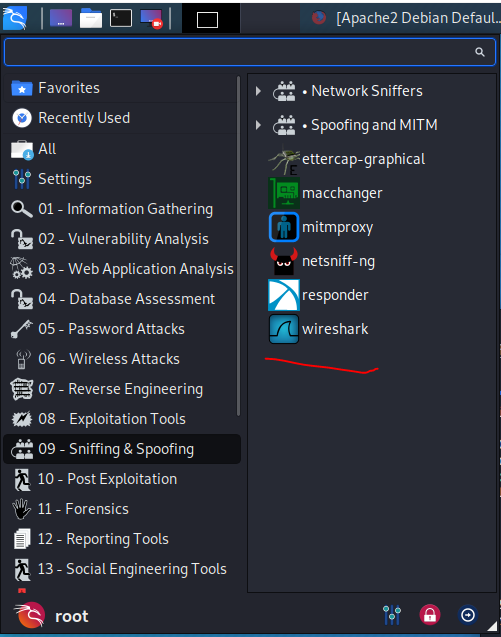
# Telnet

Ihan aluksi asenna Debian koneeseen telnet palvelin.

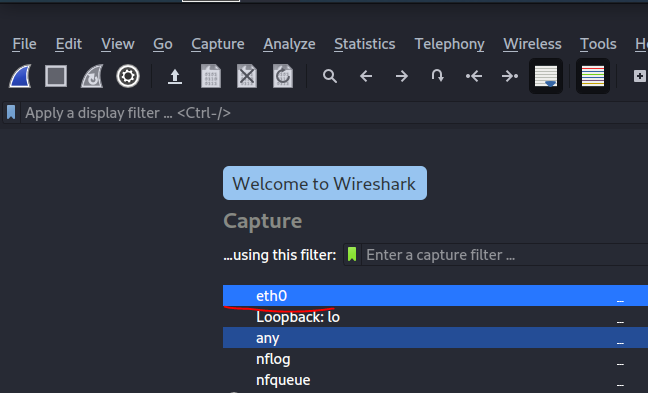


Telnettiä ei tarvitse konfiguroida mitenkään. Tässä esimerkissä telnet palvelimen IP-osoite on 192.168.0.5.

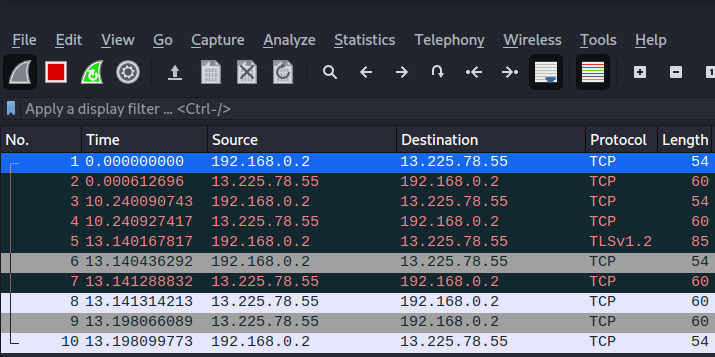
Ennen kuin palvelimeen muodostetaan telnet yhteys, käynnistä Wireshark ohjelma Kali linuxilla.



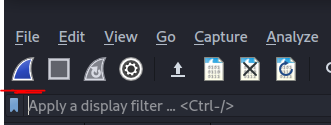
Meidän käytössämme on eth0 verkkokortti joten käytetään sitä. Saat verkkokortin selville ip a komennolla.



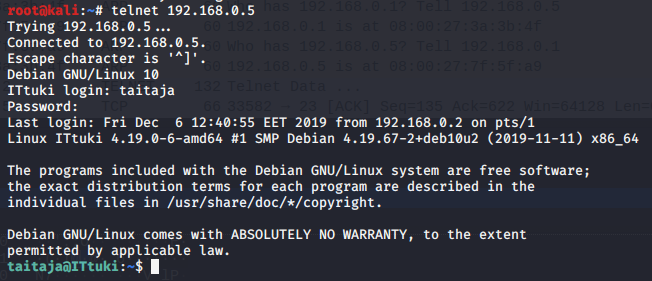
Wireshark aloittaa saman tien tietojen keräämisen.



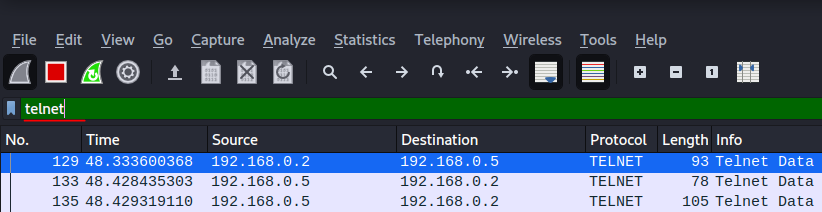
Voit myös aloittaa pakettien kaappauksen klikkaamalla hainevä kuvaketta kun se on sininen.



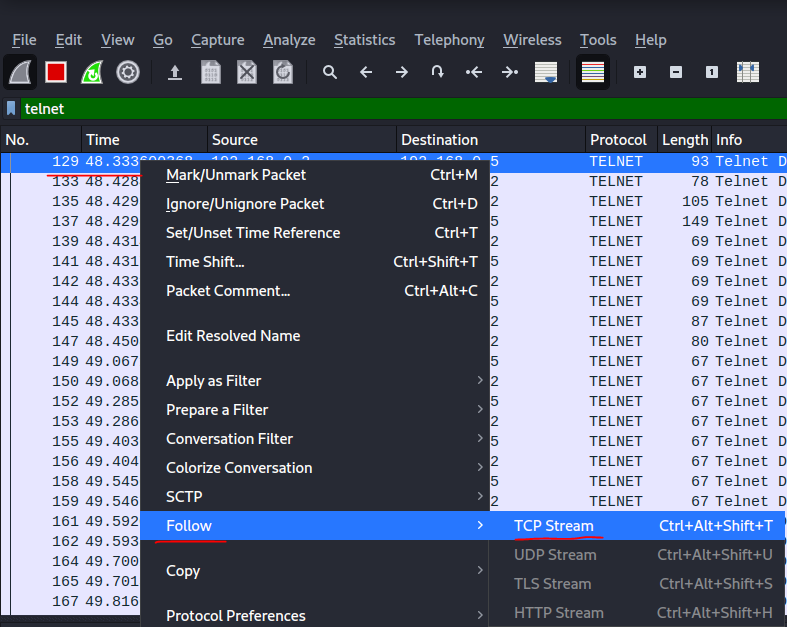
Kali koneella otetaan telnet etäyhteys Debian palvelimen.



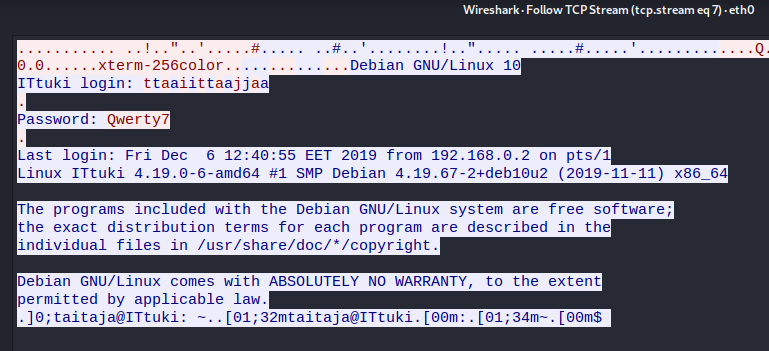
Tätä liikennettä voidaan nyt tutkia Wiresharkilla. Kirjoita Filter kenttään telnet jotta Wireshark näyttää vain telnet liittyvän liikenteen.



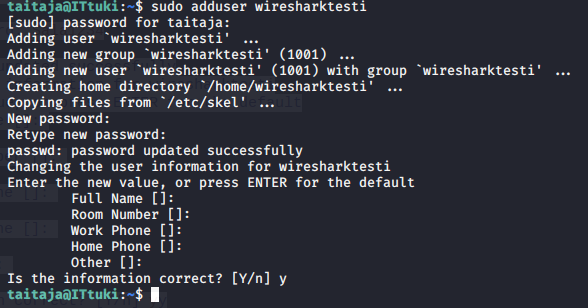
Klikkaa hiiren oikealla jotakin telnet pakettia > Follow > TCP Stream



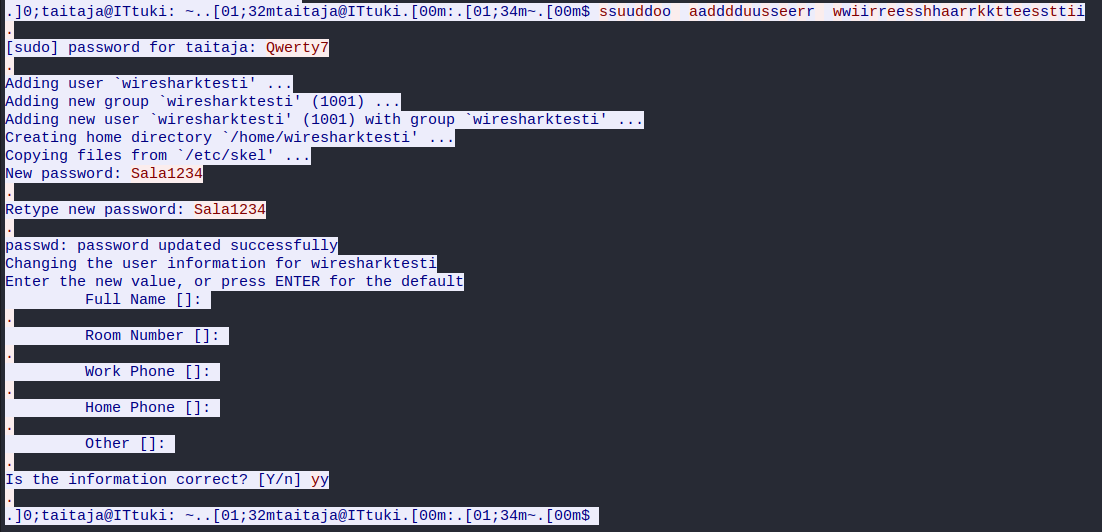
Avautuvasta ikkunasta nähdään mitä käyttäjänimeä on käytetty ja mikä sen salasana on.



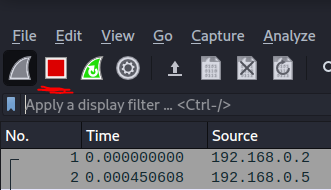
Suoritetaan nyt telnet yhteydellä muutama komento debian palvelimella. Luodaan uusi käyttäjä pyytämällä sudo oikeuksia, asetetaan uuden käyttäjän salasanaksi Sala1234



Näemme että Wireshark näkee kaiken tämän koska etäyhteys ei ole salattu millään tavalla. Olisimme siis saaneet selville rootin salasanan (koska kutsuimme sitä sudolla) ja uuden käyttäjän salasanan.



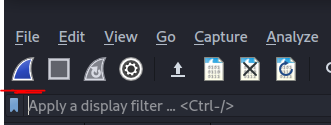
Tämän jälkeen voit lopettaa paketin kaappamisen Wiresharkissa



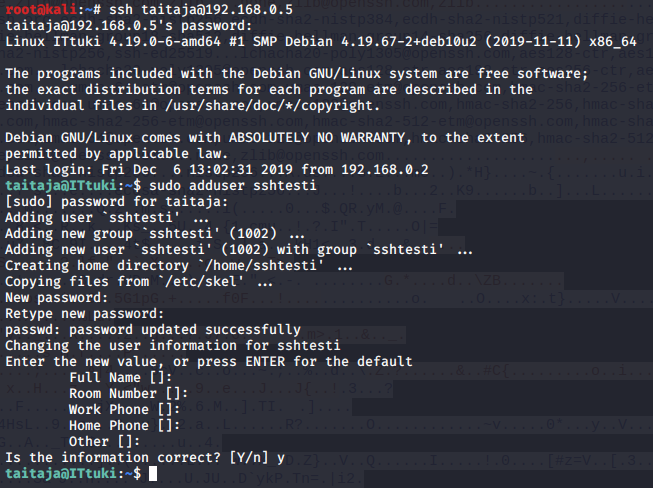
# SSH

Debianissa on jo valmiina openssh-server johon voi ottaa yhteyden.

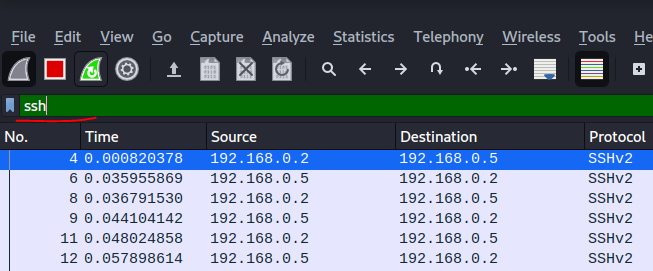
Aloita Wiresharkissa pakettien kaappaus.



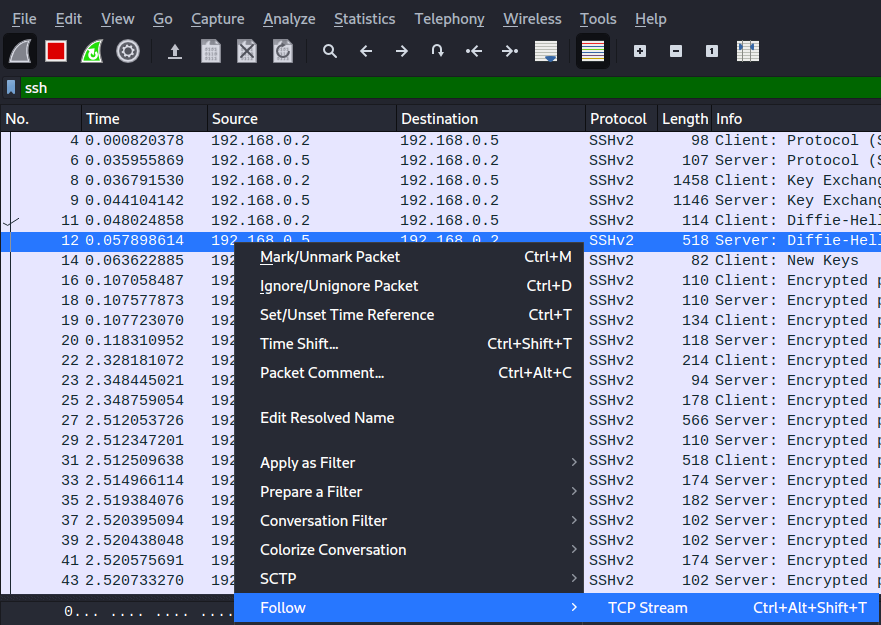
Tässä otetaan ssh yhteys samaan Debian palvelimeen ja luodaan käyttäjä kuten tehtiin Telnettiä testattaessa.



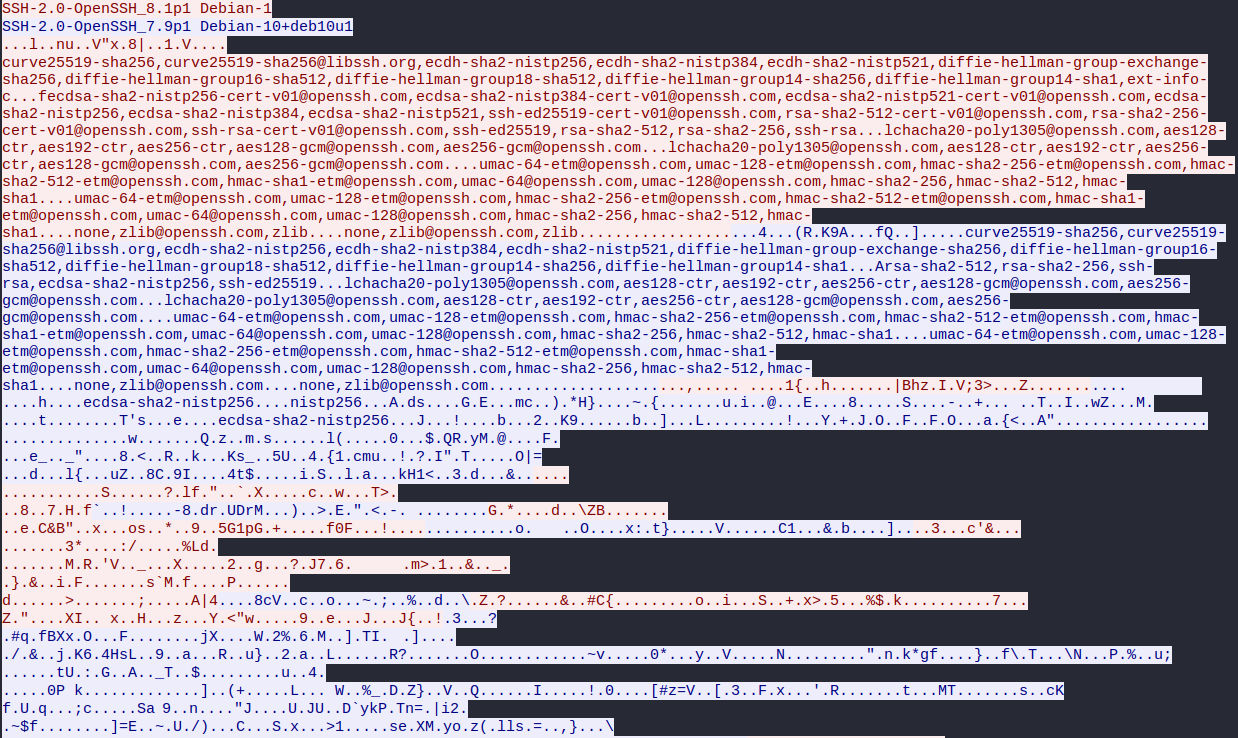
Wiresharkissa filteröi vain SSH paketit:



Seuraa striimiä:



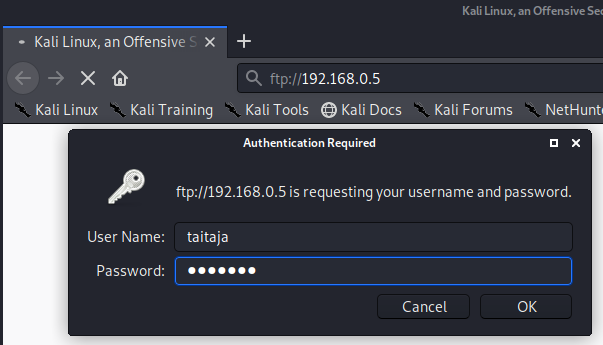
Wiresharkissa SSH yhteys näyttää tältä:

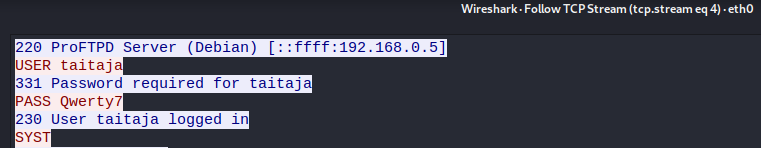


Eli siitä ei enää saa selville salasanoja tai mitä komentoja ollaan syötetty. Yhteys on siis salattua. **Tämän takia kisoissakin konfiguroidaan Linuxiin openssh-serveri ja cisco laitteissa konfiguroidaan etäyhteys SSH:lle.**

# FTP

Sama homma toimisi myös FTPlla, koska oletuksena ftp yhteys ei ole salattu. Tässä otetaan ftp yhteys debian palvelimeen jolla on asennettuna proftpd.





Tästä ongelmasta päästäisiin eroon, jos tehtäisiin FTPS palvelin, eli salattu FTP.

Sama ongelma koskee myös nettisivuja, joille pitää syöttää tärkeitä tietoja (esim. kirjautumistunnukset ja salasana). Jos tällainen sivusto olisi http sivusto, sen liikennettä voitaisiin seurata. Siksi onkin tärkeää katsoa, että sivustot joita käytät käyttävät https.