Welcome to Wireshark MeetUp #3

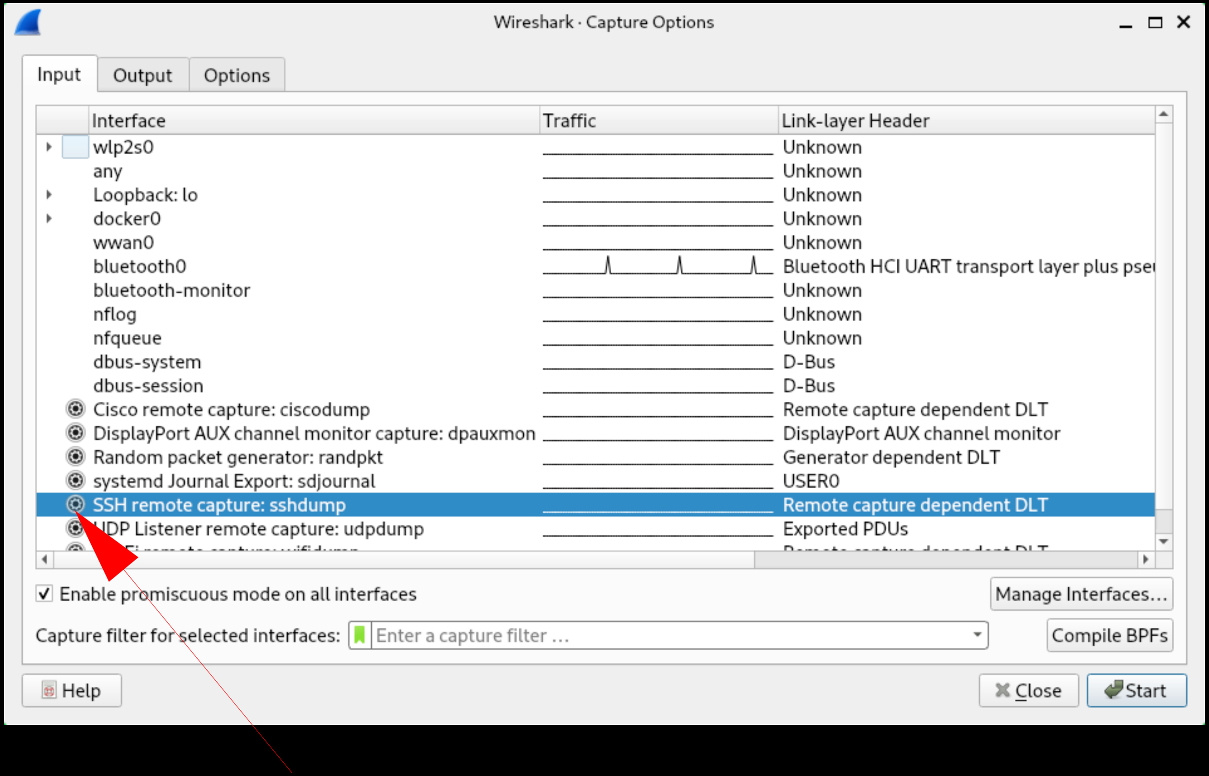
27-2-2024

Sshdump & Ciscodump

By Eduard Kooijmans

Sshdump

User needs sudo rights

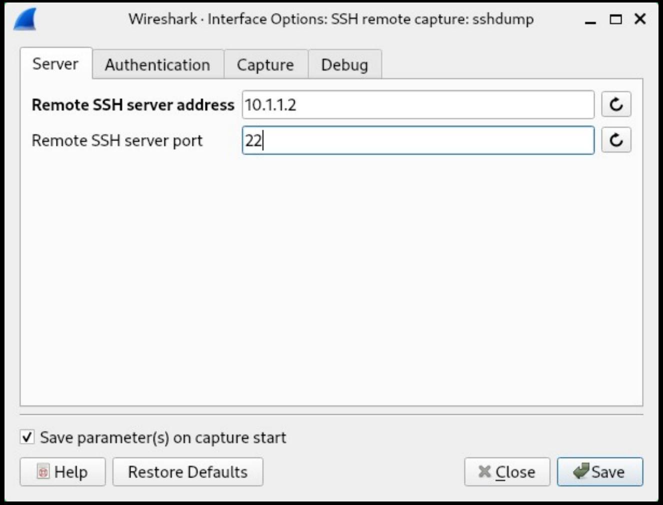


Interface	Traffic	Link-layer Header
wlp2s0		Unknown
any		Unknown
Loopback: lo		Unknown
docker0		Unknown
wwan0		Unknown
bluetooth0		Bluetooth HCI UART transport layer plus pse
bluetooth-monitor		Unknown
nflog		Unknown
nfqueue		Unknown
dbus-system		D-Bus
dbus-session		D-Bus
Cisco remote capture: ciscodump		Remote capture dependent DLT
DisplayPort AUX channel monitor capture: dpauxmon		DisplayPort AUX channel monitor
Random packet generator: randpkt		Generator dependent DLT
systemd Journal Export: sdjournal		USER0
SSH remote capture: sshdump		Remote capture dependent DLT
UDP Listener remote capture: udpdump		Exported PDUs
Wi-Fi remote capture: wifidump		Remote capture dependent DLT

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Click on

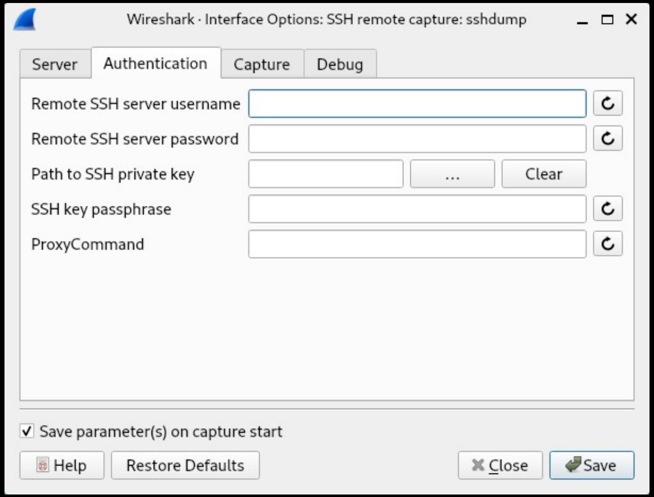


Remote SSH server address 10.1.1.2

Remote SSH server port 22

☑ Save parameter(s) on capture start

Enter IP address



Remote SSH server username

Remote SSH server password

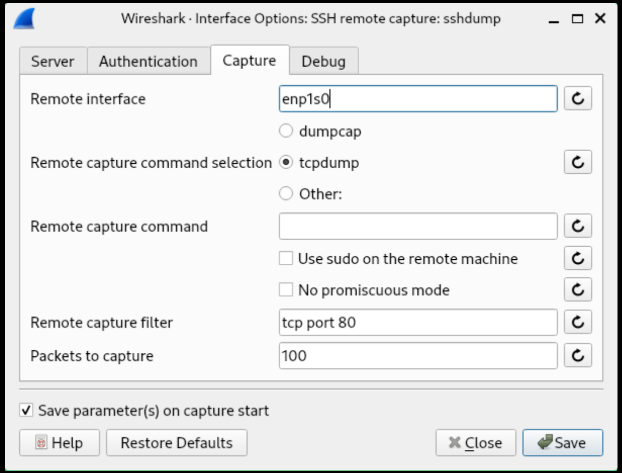
Path to SSH private key

SSH key passphrase

ProxyCommand

☑ Save parameter(s) on capture start

Enter Credentials



Remote interface enp1s0

Remote capture command selection ○ dumpcap ● tcpdump ○ Other:

Remote capture command

□ Use sudo on the remote machine

□ No promiscuous mode

Remote capture filter tcp port 80

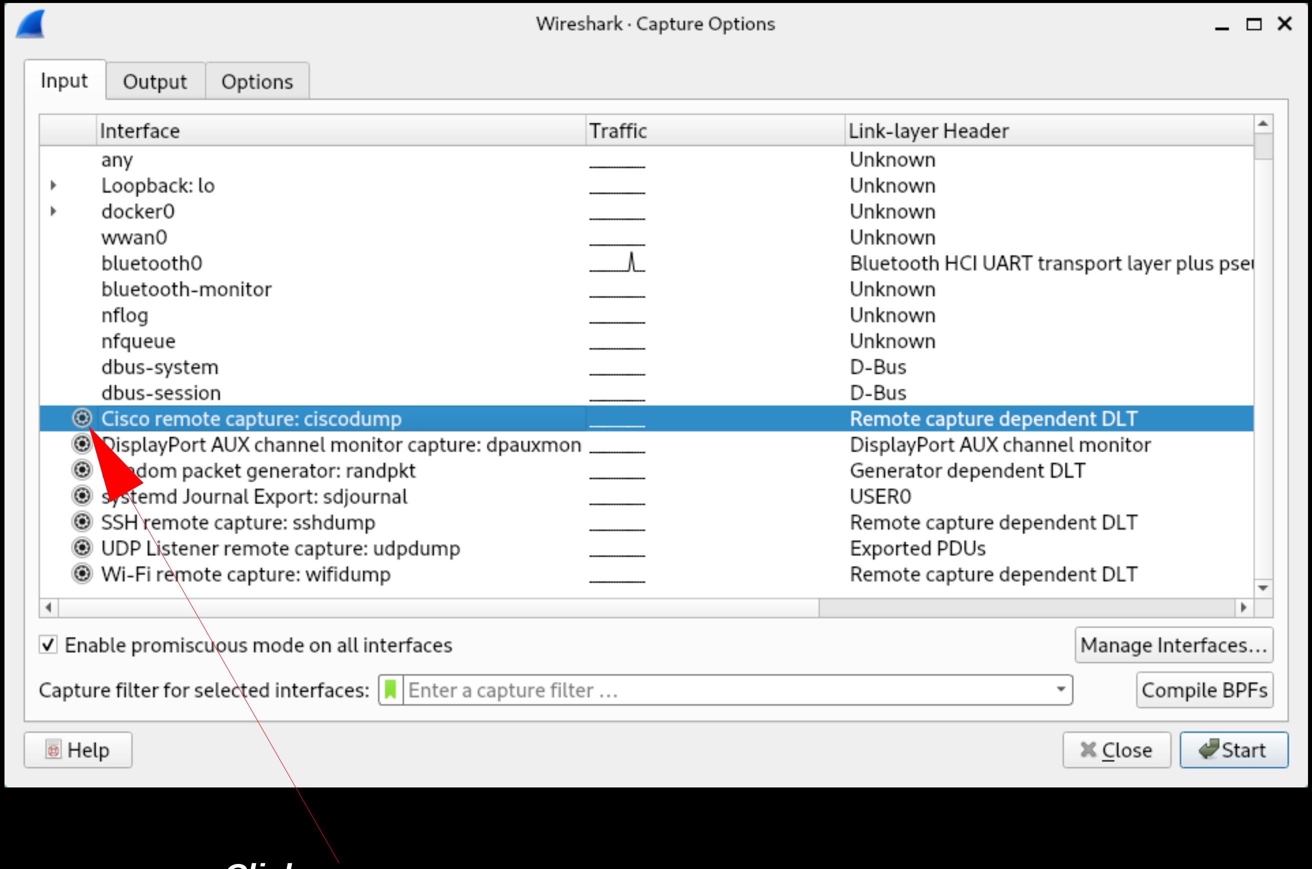
Packets to capture 100

☑ Save parameter(s) on capture start

Enter interface remote ssh server, capture filter

Ciscodump

User needs privelege rights

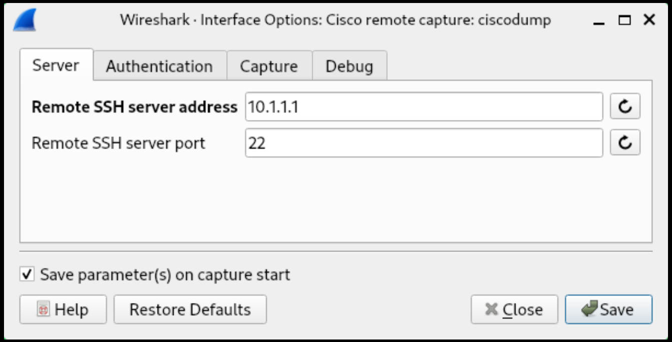


Interface	Traffic	Link-layer Header
any		Unknown
Loopback: lo		Unknown
docker0		Unknown
wwan0		Unknown
bluetooth0		Bluetooth HCI UART transport layer plus pseu
bluetooth-monitor		Unknown
nflog		Unknown
nfqueue		Unknown
dbus-system		D-Bus
dbus-session		D-Bus
Cisco remote capture: ciscodump		Remote capture dependent DLT
DisplayPort AUX channel monitor capture: dpauxmon		DisplayPort AUX channel monitor
Random packet generator: randpkt		Generator dependent DLT
systemd Journal Export: sdjournal		USER0
SSH remote capture: sshdump		Remote capture dependent DLT
UDP Listener remote capture: udpdump		Exported PDUs
Wi-Fi remote capture: wifidump		Remote capture dependent DLT

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

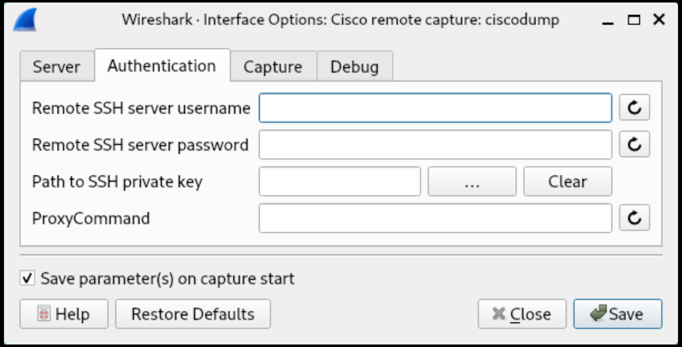
Click on


Wireshark · Interface Options: Cisco remote capture: ciscodump
Server
Authentication
Capture
Debug
Help
Restore Defaults
Close
Save

Remote SSH server address 10.1.1.1

Remote SSH server port 22

☑ Save parameter(s) on capture start



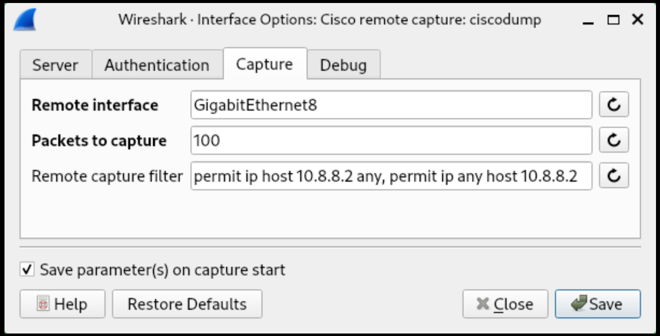
Remote SSH server username

Remote SSH server password

Path to SSH private key

ProxyCommand

☑ Save parameter(s) on capture start


Wireshark · Interface Options: Cisco remote capture: ciscodump
Server
Authentication
Capture
Debug
Help
Restore Defaults
Close
Save

Remote interface GigabitEthernet8

Packets to capture 100

Remote capture filter permit ip host 10.8.8.2 any, permit ip any host 10.8.8.2

☑ Save parameter(s) on capture start

More info:

https://www.wireshark.org/docs/man-pages/sshdump.html

https://www.wireshark.org/docs/man-pages/ciscodump.html