Capturing and Decrypting SSL Packets

Table of Contents

- Introduction
- DD-WRT (IPtables)
- Mac OS
    - Wireshark
    - Tcpdump

Introduction

There are different ways to *capture and read traffic* from your Roku Streaming device.

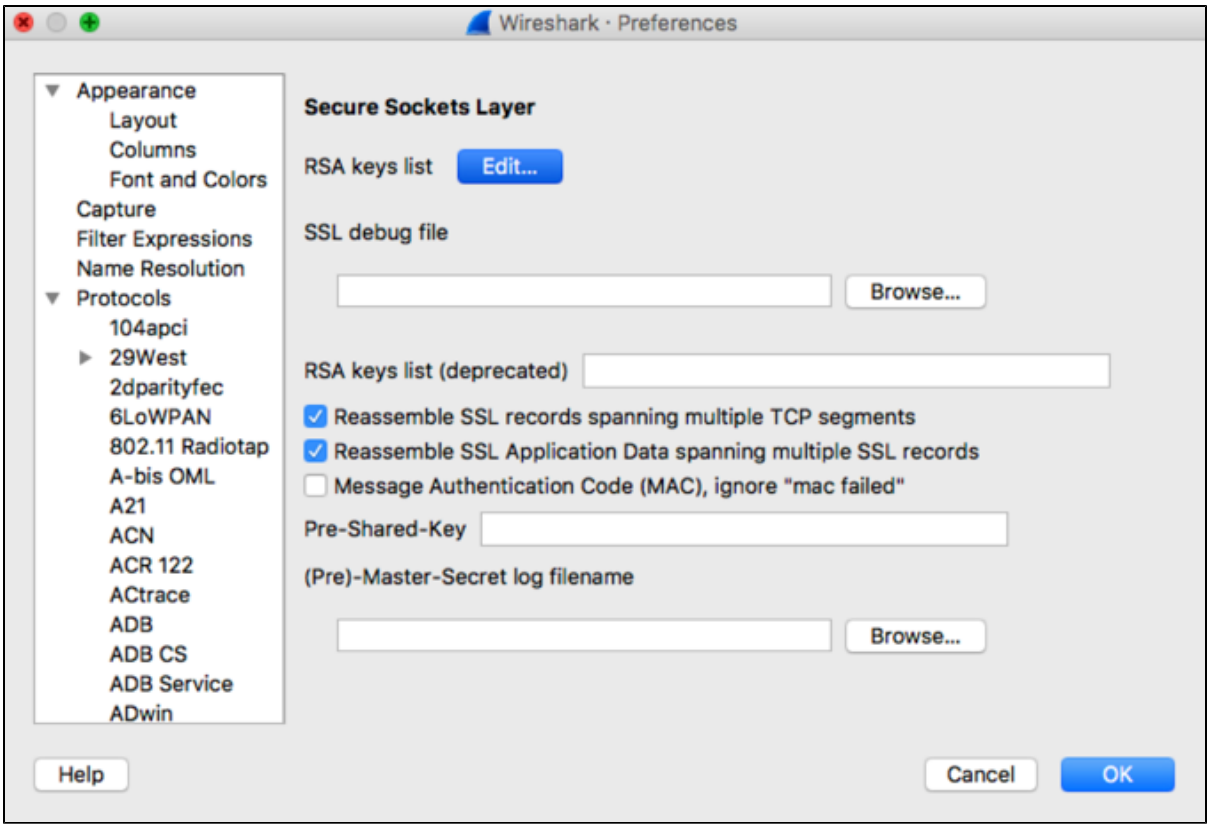
The following are some useful links:

- DD-WRT (If router firmware is too standard)
- Wireshark (Free for decrypting tcpdump)
- Charles Proxy (Easy setup, Easy GUI, Not free, Optional)

> Before performing any of the methods that use Wireshark, make sure you have the correct keys for SSL decryption. Click for more information on Wireshark SSL.
>
> Click for more information on how to create a self-signed SSL certificate.

Important: Before performing the following steps, make sure you have established your own SSL encryption (the method in this sample is a self-signed CA).

1. Create and sign **CA certificate**.
2. Create and sign **web server certificate** with CA certificate.
3. Include your **CA certificate** inside your Roku Streaming player.
4. Navigate to **Wireshark** -> **Preferences** -> **Protocols** -> **SSL**
5. Click **Edit** and add your private key to the RSA keys list.



DD-WRT (IPtables)

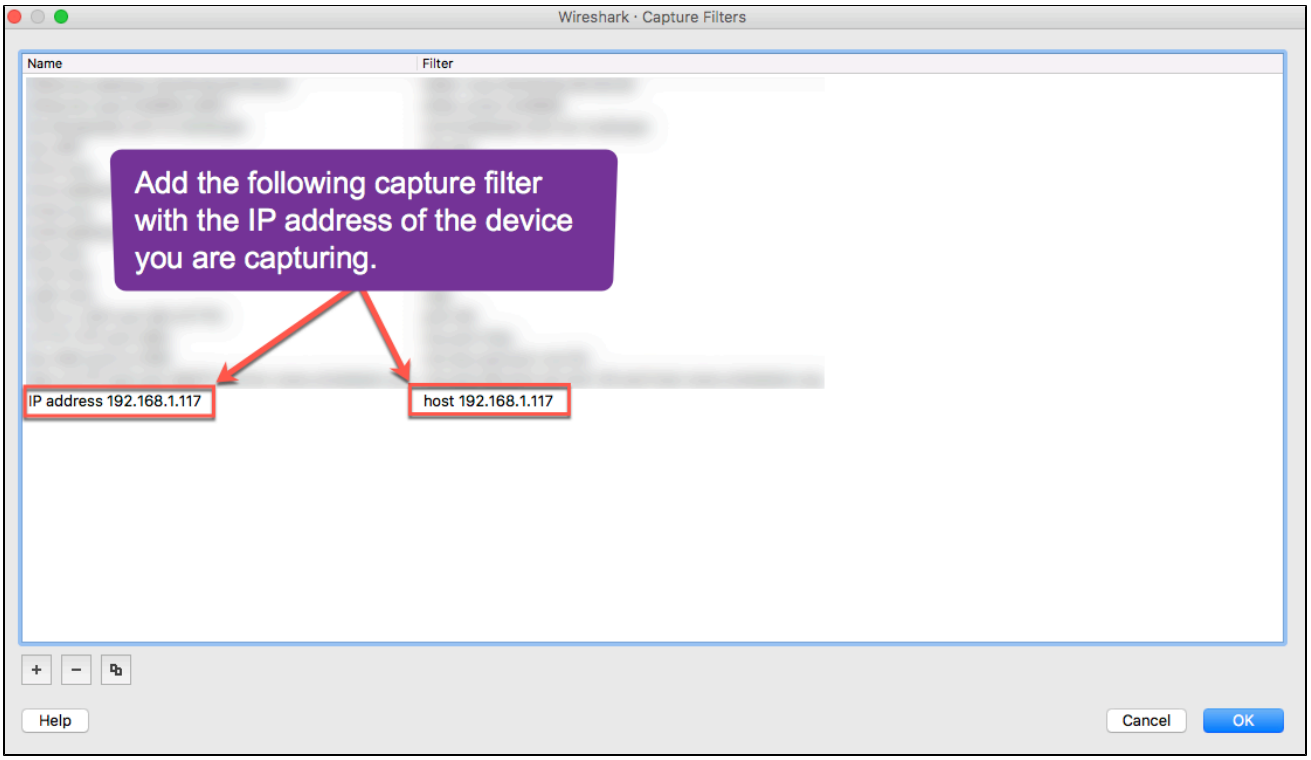
Important: Before performing the following steps, make sure that **SSH management** is enabled on **DD-WRT**.

1. SSH into DD-WRT as root root.
2. Add DD-WRT to monitor traffic by entering the following console commands:

```
root@DD-WRT:~# iptables -t mangle -A POSTROUTING -d <Device-To-Monitor-IP> -j
ROUTE --tee --gw <Listening-Device-IP>
root@DD-WRT:~# iptables -t mangle -A PREROUTING -s <Device-To-Monitor-IP> -j ROUTE
--tee --gw <Listening-Device-IP>
```

3. Launch **Wireshark**, select **Capture** from the top menu, and add the following capture filter with the **IP address** of the device that you want to capture.
   Select **OK** when done.

Field 1: IP address <IP Address>	Field 2: host <IP Address>



4. Go to the Wireshark preferences and open the **columns** tab.
5. Add a new filter with title: "**channel**" and select "**Frequency/Channel**" in the drop-down menu for the field type.
6. Start your application and start Wireshark Port Monitoring capture and sort through packets.

Mac OS

Wireshark

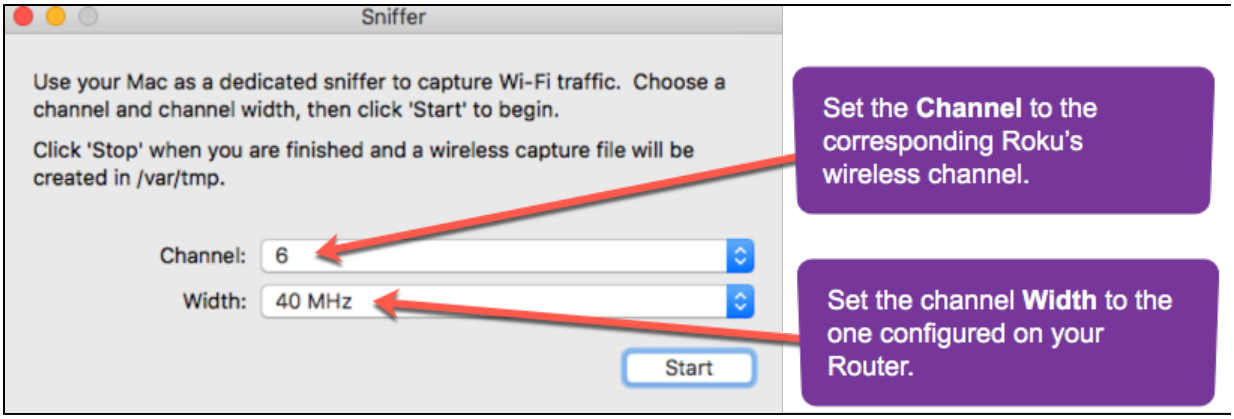
Another easy way to capture SSL packets using Mac OS is through the wireless diagnostics tool that comes with your Macbook®.

All you need is:

- the wireless channel of your Wifi connection, and
- the channel width (20MHz, 40MHz, 80MHz).

These settings can be set in the Web GUI of your router. If this is not possible through the Web GUI of your router, find the default channel setting of your Wifi or install a different firmware on your router that can change this.

1. Setup your Wifi connection and open the Wireless Diagnostics tool (Pre-installed on later versions of Mac OS).
2. In the top bar, find the field labeled **window** and choose the **Sniffer tool**.
3. In the window for the sniffer tool:
    - set the **Channel** to the corresponding Roku's wireless channel (Same channel as one displayed on router Web GUI) and,
    - set the channel **Width** to the one configured on your Router. Select from the Drop-Down menus.



4. Start the **Sniffer tool** and launch your Roku application. Once you have stopped the recording, the file containing your recorded internet traffic will be exported to the file path displayed in the *Sniffer* window (In this case /var/tmp).
5. Launch **Wireshark** and open the cap file exported from your **Sniffer tool**.

Tcpdump

1. The previous method can also be viewed using **tcpdump**.
2. After going through steps 1 through 4 in the section above, you can open the cap file.

```
$ tcpdump -r /path/to/packetfile.cap
```