Capture iPhone iOS HTTP traffic Using Wireshark

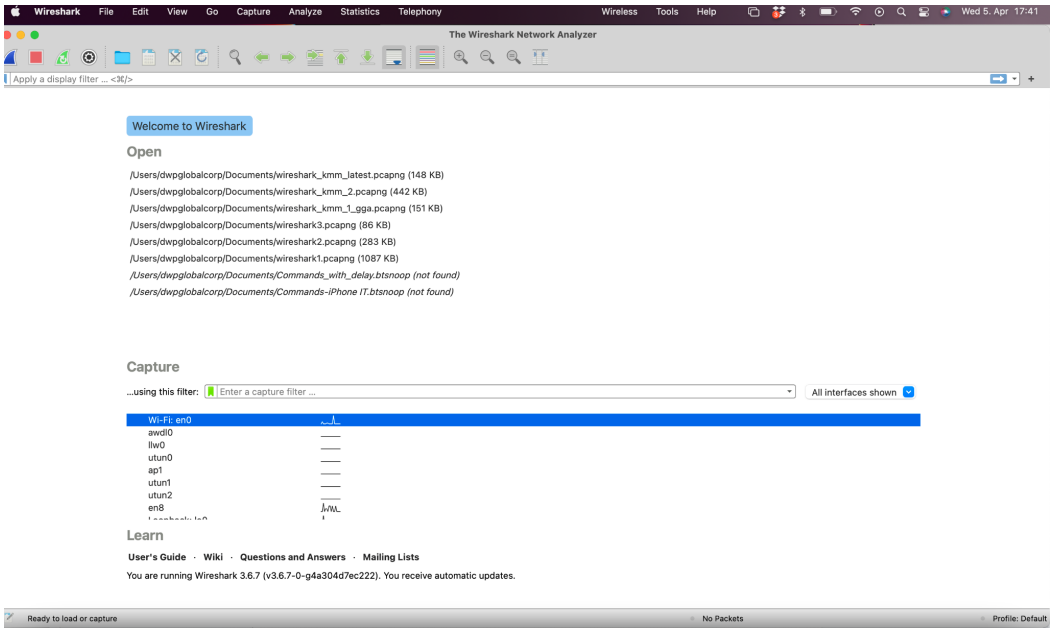
Packet sniffing: How to capture the packets sent and received by iOS Apps on your Mac.

I'm recently doing an IoT project(Ktor-Socket-Client in KMM). Sometimes I have to investigate more complex problems that potentially happen in the network layer, so I use Wireshark to capture the network traffic between my iOS apps and IoT hardware.

Install Wireshark

Wireshark is free and open-source. You can download Wireshark from its official website https://www.wireshark.org/

After completing the installation, you should see a screen like this, showing all the capture interfaces:



You can start capturing the traffic of any of the listed interfaces by double-clicking it now. But if you would like to capture the traffic of your iPhone, you have to do one more step.

Create/Remote Virtual Interface

Since the network communication between your iPhone and IoT hardware is not going through your Mac, to capture the traffic of an iPhone using tools like Wireshark on your Mac, you need to create a remote virtual interface (RVI) dedicated to your iPhone's traffic on your Mac.

We will proceed the following process

1.Connect iPhone and your computer with a cable

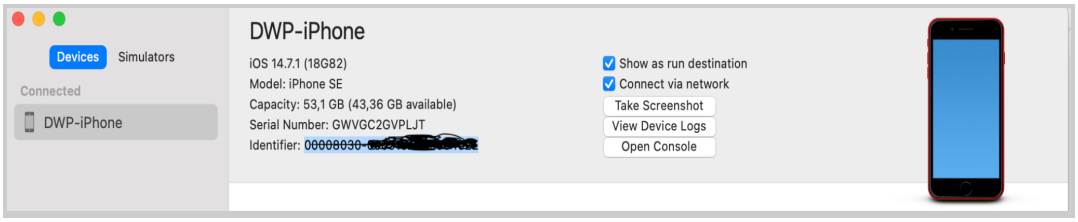
2. Open a terminal window

3. Enter the following command to check the existing interfaces:

```
$ ifconfig -l
lo0 gif0 stf0 en0 en1 en2 bridge0 p2p0 awdl0 llw0 utun0 utun1
```

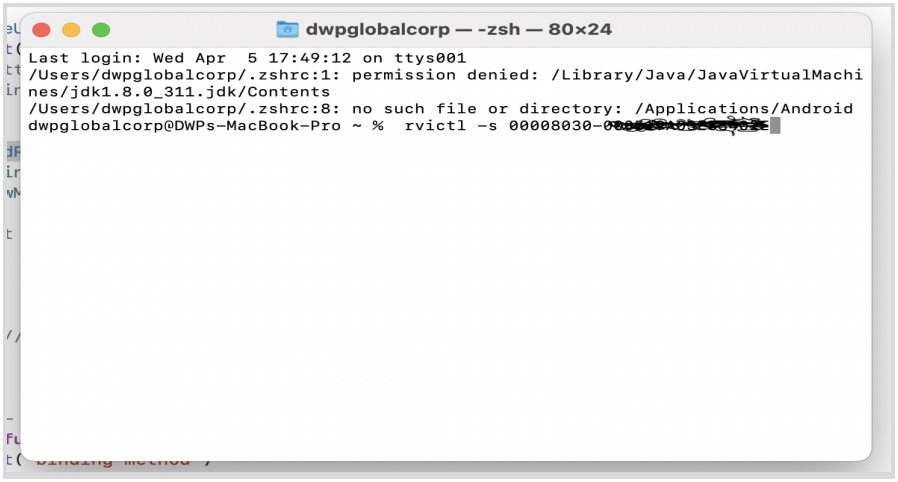
4. Find out your iPhone's UDID through Xcode or Apple Music:

```
Xcode -> Window -> Devices and Simulators
```



5. Use the following command to create a remote virtual interface:

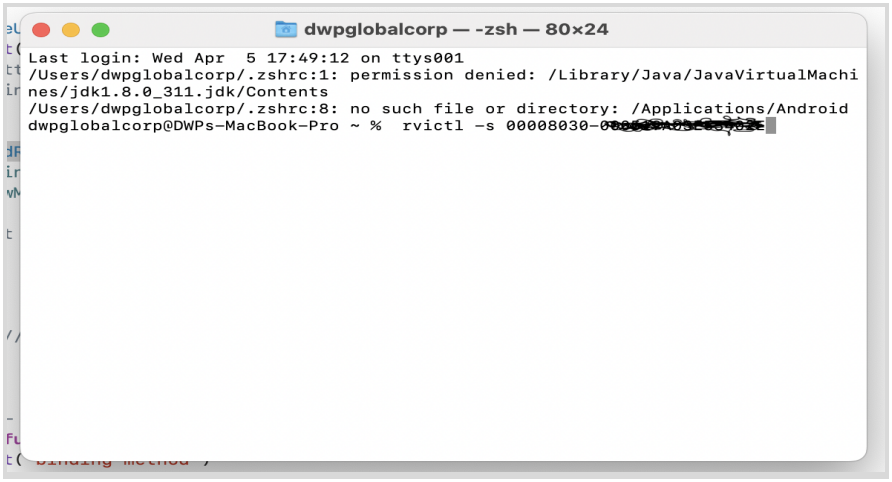
$ rvictl -s [YourUUID]



Starting device [YourUUID] [SUCCEEDED] with interface rvi0

6. Enter the following command to check existing interfaces again:

$ ifconfig -l
lo0 gif0 stf0 en0 en1 en2 bridge0 p2p0 awdl0 llw0 utun0 utun1 rvi0



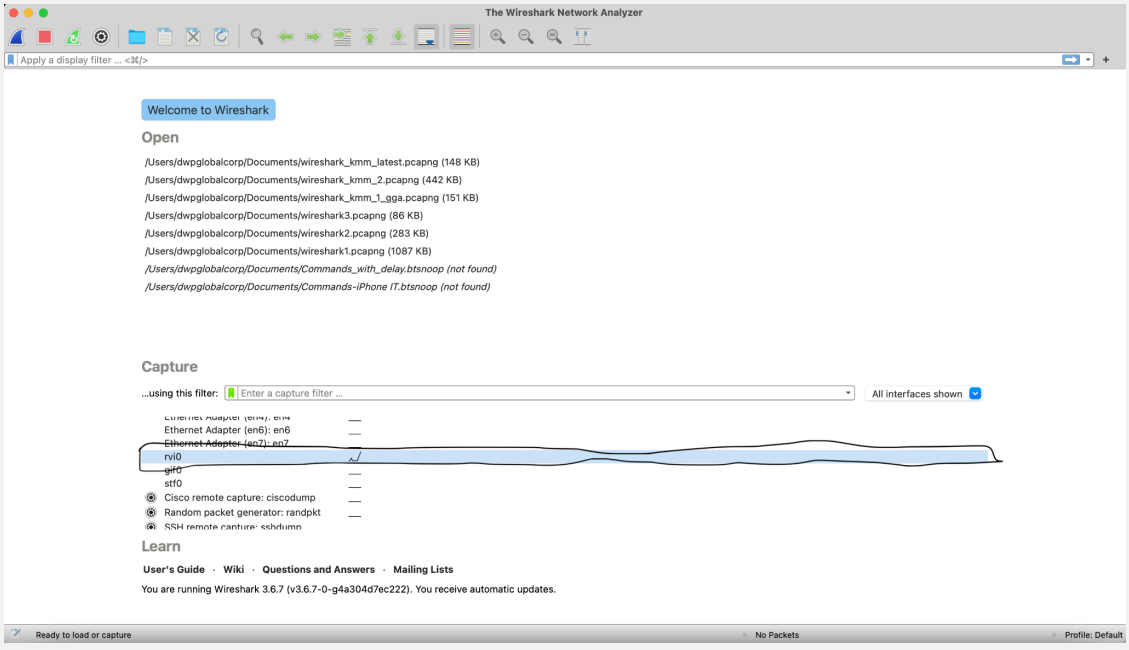
If the interface creation was successful, rvi0 should be appended to the list.

7. To remove this interface rvi0 after you are done with capturing, you can use this below command.

$ rvictl -x *[YourUDID]*

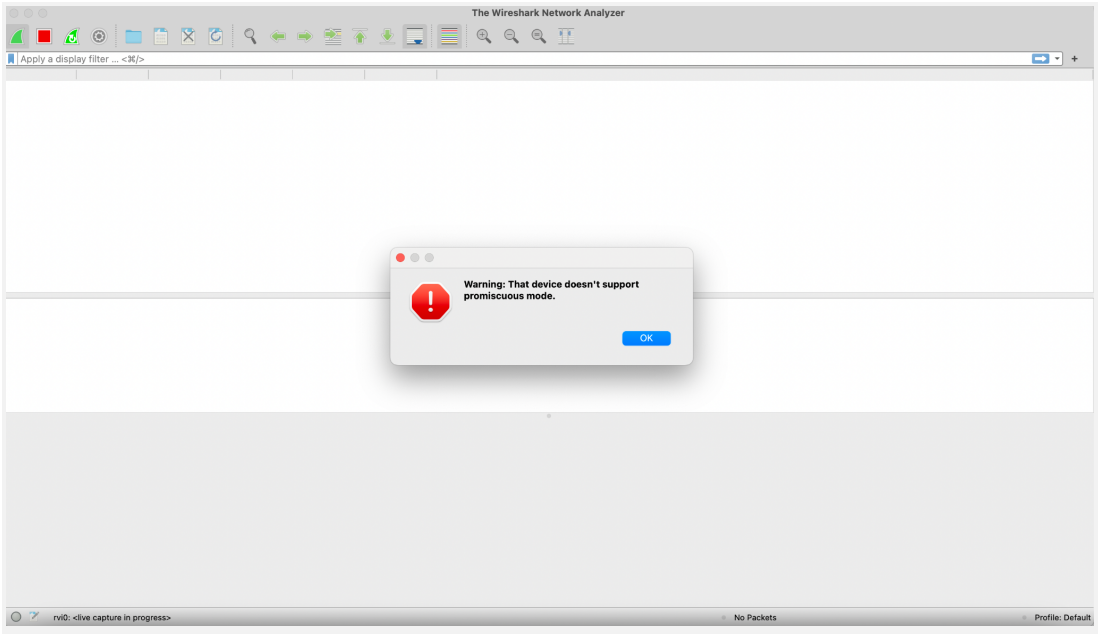
Capture iPhone's Traffic

Open Wireshark, you should see riv0 appeared amongst the capture interfaces.

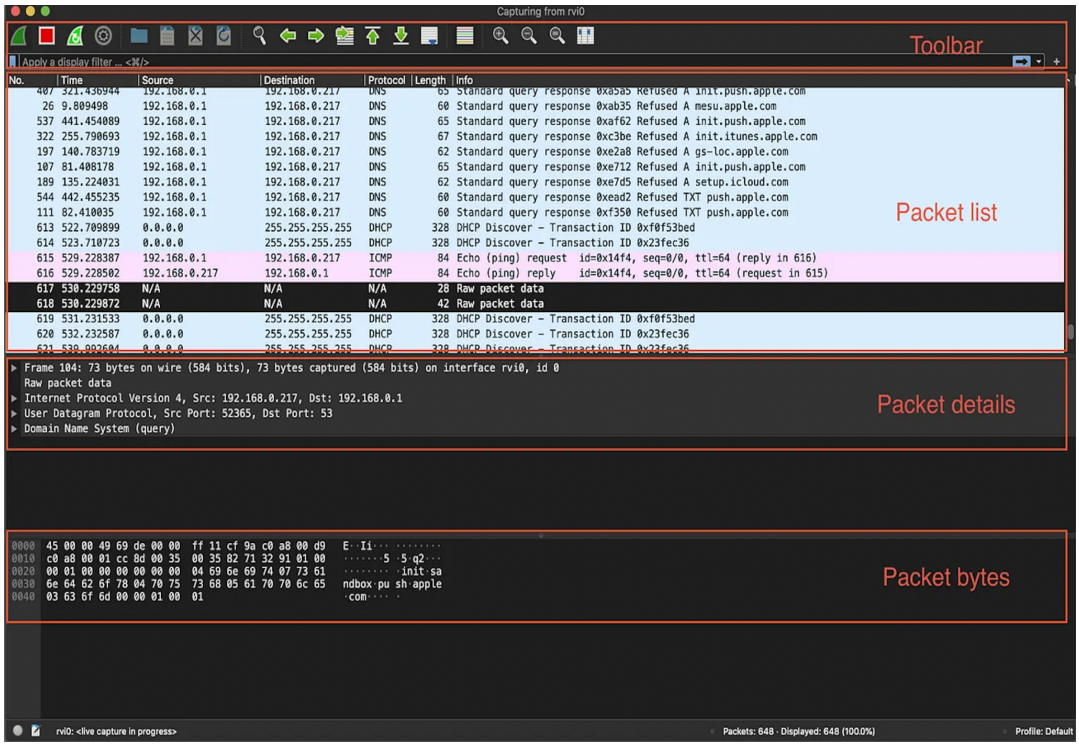


If an alert pops up showing "*You don't have permission to capture on that device*", use the following command to restart Wireshark:

```
$ sudo /Applications/Wireshark.app/Contents/MacOS/Wireshark
```

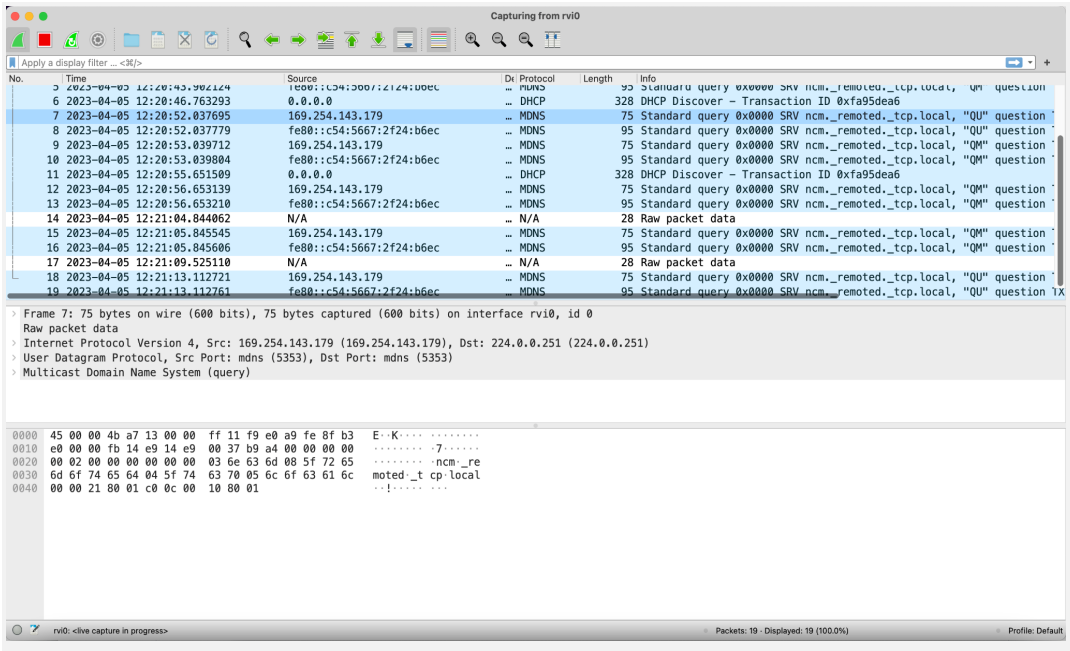


Now open any app that requires HTTP communication, your screen will update every packet sent and received by the iPhone.



There are 4 main areas on the screen

Toolbar: provides basic functions such as start and stop capturing. There is a filter at the bottom of the toolbar. You can filter the captured packets with certain rules, such as IP source and destination.
Packet list pane: shows a summary of each packet sent and received by your iPhone. The columns are customisable. You can add custom columns such as source port and destination port.
Packet details pane: displays the details of the selected packet.
Packet bytes: displays the data of the selected packet in bytes. Highlights the field selected in the packet details pane.



Export the logs