RawCap (analizador de red)

Página web de RawCap https://www.netresec.com/index.ashx?page=RawCap

RawCap is a free command line network sniffer for Windows that uses raw sockets.

Quick RawCap facts:

- Can sniff any interface that has got an IPv4 address, including 127.0.0.1 (localhost/loopback)
- RawCap.exe is just 48 kB
- No external libraries or DLL's needed other than .NET Framework
- No installation required, just download RawCap.exe and sniff
- Can sniff most interface types, including WiFi, WWAN (Mobile Broadband) and PPP interfaces
- Simple to use

Usage

You will need administrator privileges to run RawCap.F:\Tools>RawCap.exe –help
NETRESEC RawCap version 0.2.0.0

Usage: RawCap.exe [OPTIONS] can be an interface number or IP address
  can be filename, stdout (-) or named pipe (starting with \\.\pipe\)

OPTIONS:
 -f Flush data to file after each packet (no buffer)
 -c Stop sniffing after receiving packets
 -s Stop sniffing after seconds
 -m Disable automatic creation of RawCap firewall entry

```
 -q          Quiet, don’t print packet count to standard out

INTERFACES:
 0.     IP         : 169.254.63.243
        NIC Name   : Local Area Connection
        NIC Type   : Ethernet

 1.     IP         : 192.168.1.129
        NIC Name   : WiFi
        NIC Type   : Wireless80211

 2.     IP         : 127.0.0.1
        NIC Name   : Loopback Pseudo-Interface 1
        NIC Type   : Loopback

 3.     IP         : 10.165.240.132
        NIC Name   : Mobile 12
        NIC Type   : Wwanpp

Example 1: RawCap.exe 0 dumpfile.pcap
Example 2: RawCap.exe -s 60 127.0.0.1 localhost.pcap
Example 3: RawCap.exe 127.0.0.1 \\.\pipe\RawCap
Example 4: RawCap.exe -q 127.0.0.1 – | Wireshark.exe -i – -k
```

An alternative to supplying the interface number is to supply the IP address of the preferred interface instead, i.e. like this:RawCap.exe 127.0.0.1 localhost_capture.pcap

Interactive Console Dialog

You can also start RawCap without any arguments, this will leave you with an interactive dialog:F:\Tools>RawCap.exe

```
Network interfaces:
0.     192.168.0.17    Local Area Connection
1.     192.168.0.47    Wireless Network Connection
2.     90.130.211.54   3G UMTS Internet
3.     192.168.111.1   VMware Network Adapter VMnet1
4.     192.168.222.1   VMware Network Adapter VMnet2
5.     127.0.0.1       Loopback Pseudo-Interface
```

```
Select network interface to sniff [default '0']: 1
Output path or filename [default 'dumpfile.pcap']:
Sniffing IP : 192.168.0.47
Output File : dumpfile.pcap
 – Press [Ctrl]+C to stop –
Packets     : 1337
```

Streaming PCAP to Wireshark

The easiest way to analyze packets captured by RawCap in Wireshark is to save them to a capture file and open it in Wireshark. But you can also use alternative output methods to analyze the captured packets using Wireshark in real-time.

The simplest way to analyze packets in real-time is to write the PCAP data to standard output (stdout) using the «-» switch, and then reading that data in Wireshark with the «-i -» switch.RawCap.exe -q 127.0.0.1 – | Wireshark.exe -i – -k

Another alternative is to write the PCAP data to a named pipe, and then let Wireshark «sniff» packets from that named pipe.

1. Start RawCap and let it write PCAP data to a named pipe called «RawCap».
   RawCap.exe 127.0.0.1 \\.\pipe\RawCap
2. Start Wireshark (version 2.3.0 or later)
3. Press: Capture > Options
4. Click «Manage Interfaces…»
5. Select the «Pipes» tab
6. Press the «+» button to add a named pipe
7. Name the pipe «\\.\pipe\RawCap» and press ENTER to save it
8. Press «OK» in the Manage Interface window
9. Press «Start» to see the packets sniffed by RawCap in real-time