PtracksSPostDissector V.0.1

This is a simple “How to install and configure the post dissector plugin”.

Created by: **Vitor Sgobbi** at ICEA - Brazilian Air Traffic Control Institute.
E-mail: vitorvgsms@icea.gov.br

Issue: How to extract all bytes of a payload as raw text from a UDP packets? And format then as data fields?

Steps to be followed:

1. First install **wireshark** and **tshark** with all dependencies with apt-get, including **libpcap** and **dumpcap (or pcaputils under Ubuntu)**.

2. Give **user permission** to run wireshark and tshark. Command:
"`setcap 'CAP_NET_RAW+eip CAP_NET_ADMIN+eip' /usr/sbin/dumpcap`"
(NOTE: Replace /usr/sbin with /usr/bin in case you receive an error that indicates that dumpcap isn't in /usr/sbin)

Give the command: "`chown root /usr/sbin/dumpcap`"
(NOTE: Replace /usr/sbin with /usr/bin in this command and the next command in case you receive an error that indicates that dumpcap isn't in /usr/sbin)

Note: If you are under Debian (like me) follow these steps:

```
$ sudo apt-get install wireshark

$ sudo dpkg-reconfigure wireshark-common

$ sudo usermod -a -G wireshark $USER

$ sudo reboot
```

If the solution above still fails on your system, an alternative is to set the setuid bit for dumpcap (which lets dumpcap run effectively as the owner of the file, which is root in this case):

```
$ sudo chmod 4711 `which dumpcap`
```

3. Start Wireshark as non-root and ensure you see the list of interfaces and can do live capture.

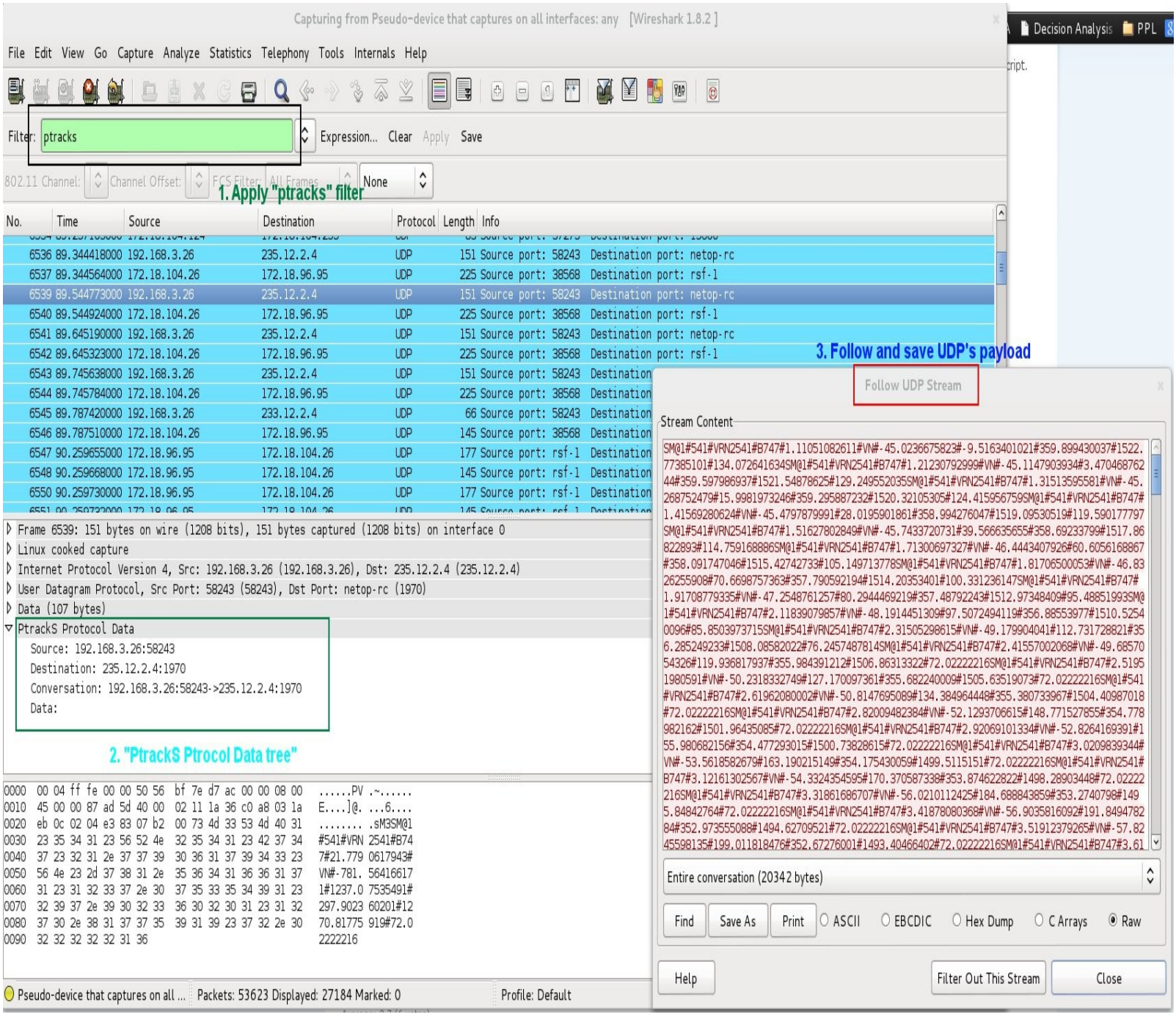
4. Extract the LUA script on the same folder as wireshark was installed, it runs on all platforms.

5. Run Wireshark via command line as: "`wireshark -X lua_script:PtrackSPostDissector.lua`".

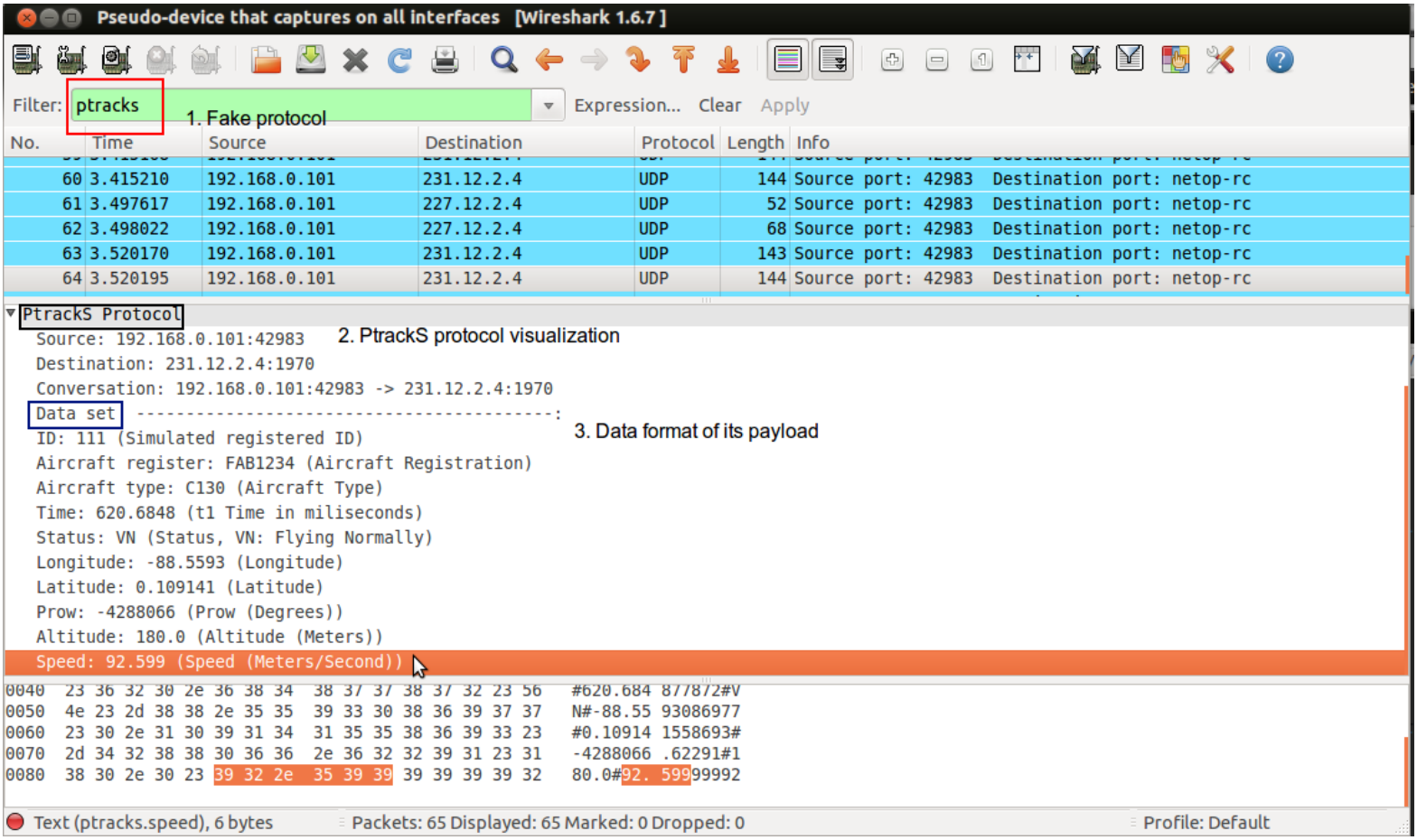
6. Apply "ptracks" as a filter, as ilustred on the screen shot.

7. The plugin will show all the protocol payload and only the “udp.port==1970” packets.

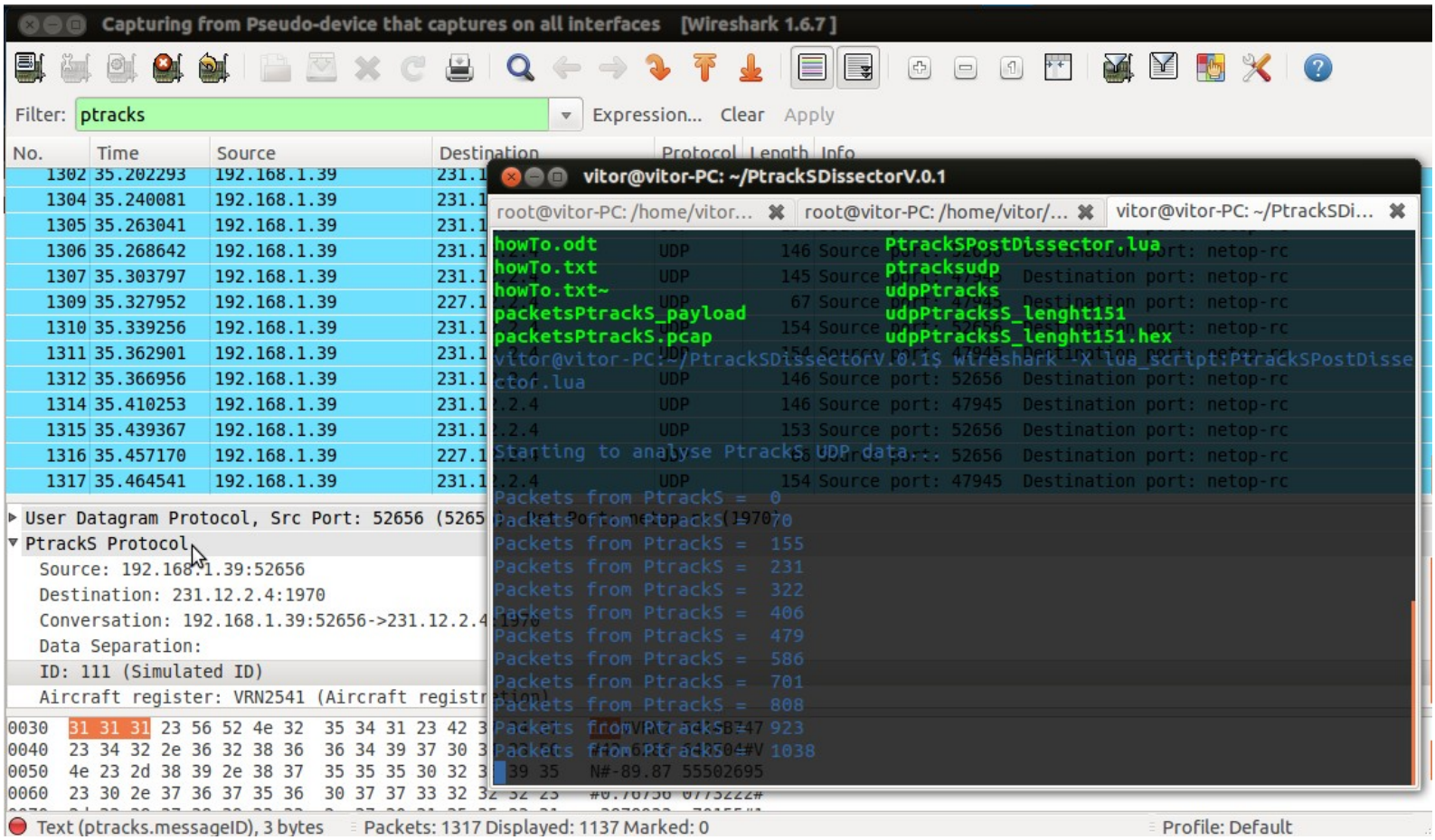
8. The image below illustrates how the Wireshark GUI can extract its payload in hexadecimal format.



9. The image below illustrates how the Wireshark GUI can be set to visualize the Ptracks protocol formatted payload.



10. There is also a function called “packets counter” to set via command line how many packet were read by Ptracks simulator. As illustrated on the image below.



Append

Issues:

Wireshark only works with user permission to run dumpcap, do not start wireshark as root command, if you get the packet counter equal zero after you start wireshark -X lua_script:PtrackSPostDissector.lua maybe you are not running Ptracks simulator neither connected on a network.

The Ptracks simulator only uses the UDP.PORT==1970, do not set other stuffs to run on this port.

Notes:

This plugin is based on how to use tshark and wireshark to extract hex values of the payload of each UDP packet created by Ptracks simulator.

This project were created under open source license, GNU GPLv3, it means you are granted to change it!

Using the follow command at terminal: **"**tshark -r ptracksudp.cap -X lua_script:extract.lua -X lua_script1:dns -T fields -e extractor.value.hex**".** This will create a text file containing all the extracted fields of its payload.
*** // Where ptracksudp.cap is a pcap file saved from PtrackSPostDissector.lua *//extract script still to be added**
Any issues regarding Wireshark PtrackS plugin e-mail to: vitorvgsms@icea.gov.br