

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](mailto: ritorvgsms@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.

The image shows the Wireshark 1.8.2 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture, and analysis. The Filter field is set to "ptracks" and is highlighted with a green box. Below it, the Channel is set to "802.11 Channel" and the Channel Offset is "None". A green box with the text "1. Apply 'ptracks' filter" points to the Filter field.

The packet list shows several UDP packets. A blue box with the text "3. Follow and save UDP's payload" points to the "Destination" column of a packet. The packet details pane shows the "PtrackS Protocol Data" section, which includes the source (192.168.3.26:58243), destination (235.12.2.4:1970), and conversation (192.168.3.26:58243->235.12.2.4:1970). A green box with the text "2. 'PtrackS Protocol Data tree'" points to this section.

The packet bytes pane shows the raw data in hexadecimal and ASCII. A red box with the text "Follow UDP Stream" points to the "Follow UDP Stream" button in the packet details pane. The stream content pane shows the stream data in hexadecimal and ASCII. A red box with the text "Follow UDP Stream" points to the "Follow UDP Stream" button in the stream content pane.

The bottom status bar shows "Pseudo-device that captures on all ...", "Packets: 53623 Displayed: 27184 Marked: 0", and "Profile: Default".

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

Wireshark 1.6.7

Filter: ptracks

1. Fake protocol

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
60	3.415210	192.168.0.101	231.12.2.4	UDP	144	Source port: 42983 Destination port: netop-rc
61	3.497617	192.168.0.101	227.12.2.4	UDP	52	Source port: 42983 Destination port: netop-rc
62	3.498022	192.168.0.101	227.12.2.4	UDP	68	Source port: 42983 Destination port: netop-rc
63	3.520170	192.168.0.101	231.12.2.4	UDP	143	Source port: 42983 Destination port: netop-rc
64	3.520195	192.168.0.101	231.12.2.4	UDP	144	Source port: 42983 Destination port: netop-rc

▼ PtrackS Protocol

Source: 192.168.0.101:42983

Destination: 231.12.2.4:1970

Conversation: 192.168.0.101:42983 -> 231.12.2.4:1970

Data set

ID: 111 (Simulated registered ID)

Aircraft register: FAB1234 (Aircraft Registration)

Aircraft type: C130 (Aircraft Type)

Time: 620.6848 (t1 Time in miliseconds)

Status: VN (Status, VN: Flying Normally)

Longitude: -88.5593 (Longitude)

Latitude: 0.109141 (Latitude)

Prow: -4288066 (Prow (Degrees))

Altitude: 180.0 (Altitude (Meters))

Speed: 92.599 (Speed (Meters/Second))

3. Data format of its payload

0040 23 36 32 30 2e 36 38 34 38 37 37 38 37 32 23 56 #620.684 877872#V

0050 4e 23 2d 38 38 2e 35 35 39 33 30 38 36 39 37 37 N#-88.55 93086977

0060 23 30 2e 31 30 39 31 34 31 35 35 38 36 39 33 23 #0.10914 1558693#

0070 2d 34 32 38 38 30 36 36 2e 36 32 32 39 31 23 31 -4288066 .62291#1

0080 38 30 2e 30 23 39 32 2e 35 39 39 39 39 39 32 80.0#92.59999992

Text (ptracks.speed), 6 bytes

Packets: 65 Displayed: 65 Marked: 0 Dropped: 0

Profile: Default

[illegible]

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: vitorvgms@icea.gov.br