

Aplicación de captura de tramas PPP

Santiago Rios Valero - 20181020017

Jhojan Esneyder Rizo Arias - 20192020027

Dylan Alejandro Solarte - 20201020088

Luis David Bautista Pérez - 20202020144

Johnatan Guillermo Ruiz – 20181020034

El propósito de este escrito es el de documentar la aplicación de captura de tramas del protocolo PPP y sus protocolos derivados.

Manual de instalación

La aplicación consiste en un ejecutable portable, el cual puede ser ejecutado en cualquier equipo con sistema operativo Windows.

Los únicos requisitos necesarios para el funcionamiento de la aplicación son: Primero, tener instalado Npcap y Winpcap. No hay necesidad de instalar la librería Scapy ya que esta se encuentra dentro del ejecutable. Segundo, hay que tener instalado Python para que la aplicación pueda ser ejecutada en su consola.

Si se cumplen estos requisitos simplemente se abre el ejecutable para iniciar la aplicación:

Nombre	Fecha de modificación	Tipo	Tamaño
Capturador.exe	15/10/2022 7:06 p. m.	Aplicación	44.037 KB
Capturador.py	15/10/2022 6:41 p. m.	Python File	11 KB



```
C:\Users\luis david bautista\Downloads\SOFTWARE CAPTURA PPP\Capturador.exe
Matplotlib is building the font cache; this may take a moment.

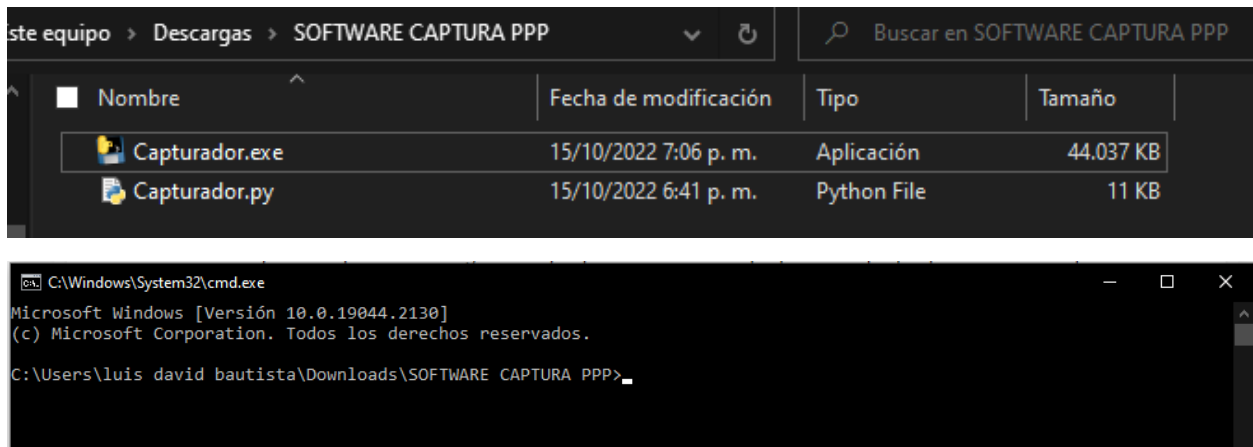
Capturador de tramas PPP (Point to Point Protocol)
Elija una de las siguientes opciones:
1- Capturar un número fijo de paquetes
2- Capturar por un tiempo determinado (Los resultados se guardarán en un archivo pcap)
3- Salir de la aplicación
_
```

Método alternativo de instalación

Junto con el ejecutable hay un archivo .py donde está alojado el código fuente de la aplicación. Dicho archivo se puede ejecutar como un Script de Python como alternativa al ejecutable. A continuación, se describen los pasos para ejecutar el Script.

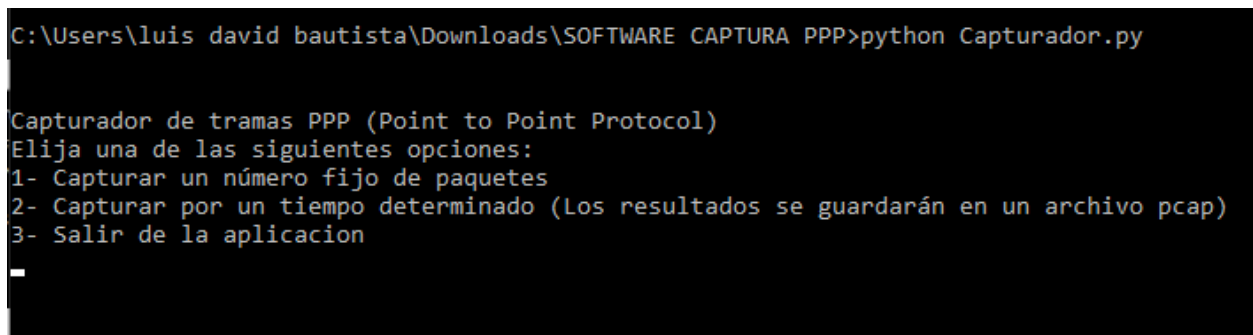
Paso 1

Ubicar la consola del sistema en la ubicación del archivo .py



Paso 2

Ejecutar el comando “python” seguido del nombre del archivo con su extensión



Nota: Hay que tener en cuenta que para usar este método si hay que tener instalada la librería Scapy.

Manual de Funcionamiento

Cuando se inicia la aplicación hay que dejarla cargar unos 3-4 minutos, mientras carga las librerías necesarias para su funcionamiento. Si han pasado más de 5 minutos y la aplicación no muestra el menú inicial, hay que digitar Enter para que lo muestre, aunque casi siempre inicia de forma automática sin problemas.

La aplicación tiene dos funcionalidades principales: Primero, le permite al usuario capturar el número de paquetes que él especifique, y segundo, el usuario puede definir una cantidad de segundos en los que la aplicación estará capturando paquetes para después almacenarlos en un archivo con extensión pcap.

1. Capturar un número fijo de paquetes

En el menú inicial seleccionar la opción 1

```
Capturador de tramas PPP (Point to Point Protocol)
Elija una de las siguientes opciones:
1- Capturar un número fijo de paquetes
2- Capturar por un tiempo determinado (Los resultados se guardarán en un archivo pcap)
3- Salir de la aplicacion
```

Luego digitar el número de paquetes a capturar

```
Ingresa el número de capturas que desee realizar: _
```

```
Ingresa el número de capturas que desee realizar: 5
Capturando paquetes...
Paquete #1 Ether / IP / UDP 192.168.1.13:54317 > 239.255.255.250:ssdp / Raw
Paquete #2 Ether / IP / UDP 142.250.78.170:https > 192.168.1.13:63307 / Raw
Paquete #3 Ether / IP / UDP 192.168.1.13:63307 > 142.250.78.170:https / Raw
Paquete #4 Ether / IP / UDP 192.168.1.13:54317 > 239.255.255.250:ssdp / Raw
Paquete #5 Ether / IP / UDP 192.168.1.13:54317 > 239.255.255.250:ssdp / Raw
```

```
Se han capturado 5 paquetes
```

```
Que desea realizar?
```

```
1- Revisar la trama de un paquete especifico
2- Guardar las capturas en un archivo pcap
3- Salir del menu
```

Después de la captura, se puede consultar la trama de cada uno de los paquetes capturados o guardar las capturas en un archivo pcap.

a. Consultar la trama de un solo paquete

Del menú actual seleccionar la opción 1

```
Se han capturado 5 paquetes

Que desea realizar?
1- Revisar la trama de un paquete específico
2- Guardar las capturas en un archivo pcap
3- Salir del menu
1

Ingrese el número del paquete al que desea ver los campos de su trama. Rango de entradas disponibles (1, 5 )
```

Digitar el número correspondiente al paquete deseado (siempre y cuando esté dentro del rango de los paquetes capturados. En el caso del ejemplo solo serían válidas las siguientes entradas: (1,2,3,4,5).

```
Ingrese el número del paquete al que desea ver los campos de su trama. Rango de entradas disponibles (1, 5 )
1
Paquete # 4 :
Trama protocolo PPP
###[ DIR_PPP ]###
direction = sent
###[ PPP Link Layer ]###
proto = 94
###[ Raw ]###
load = '\x7f\xff\xfa\xcb\\xd1>zb\x8e\x80\x8e\\xa5\x80\x80\x81\x11\x80\x80\\xc0\\xa8\x81\\r\\xef\\xff\\xff\\xfa\\xd4-\\x87\\x80\\xb2\\xb2sM-SEARCH * HTTP/1.1\\r\\nHOST: 239.255.255.250:1900\\r\\nMAN: "ssdp:discover"\\r\\nMX: 1\\r\\nST: urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ HDLC ]###
address = 0x1
control = 0x8
###[ PPP Link Layer ]###
proto = 24191
###[ Raw ]###
load = '\\\xff\\xfa\\xc0\\xd1>zb\x8e\x80\x8e\\xa5\x80\x80\x81\x11\x80\x80\\xc0\\xa8\x81\\r\\xef\\xff\\xff\\xfa\\xd4-\\x87\\x80\\xb2\\xb2sM-SEARCH * HTTP/1.1\\r\\nHOST: 239.255.255.250:1900\\r\\nMAN: "ssdp:discover"\\r\\nMX: 1\\r\\nST: urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ PPP Link Layer ]###
proto = Padding Protocol
###[ Raw ]###
load = '\x80'\x7f\xff\xfa\\xc0\\xd1>zb\x8e\x80\x8e\\xa5\x80\x80\x81\x11\x80\x80\\xc0\\xa8\x81\\r\\xef\\xff\\xff\\xfa\\xd4-\\x87\\x80\\xb2\\xb2sM-SEARCH * HTTP/1.1\\r\\nHOST: 239.255.255.250:1900\\r\\nMAN: "ssdp:discover"\\r\\nMX: 1\\r\\nST: urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ PPP over Ethernet ]###
version = 0
type = 1
code = Session
sessionid = 0x5e7f
len = 65530
###[ PPP Link Layer ]###
proto = 48276
###[ Raw ]###
load = '\\\xd1>zb\x8e\x80\x8e\\xa5\x80\x80\x81\x11\x80\x80\\xc0\\xa8\x81\\r\\xef\\xff\\xff\\xfa\\xd4-\\x87\\x80\\xb2\\xb2sM-SEARCH * HTTP/1.1\\r\\nHOST: 239.255.255.250:1900\\r\\nMAN: "ssdp:discover"\\r\\nMX: 1\\r\\nST: urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ PPPoE Tag ]###
tag_type = 256
tag_len = 24191
tag_value = '\\\xff\\xfa\\xc0\\xd1>zb\x8e\x80\x8e\\xa5\x80\x80\x81\x11\x80\x80\\xc0\\xa8\x81\\r\\xef\\xff\\xff\\xfa\\xd4-\\x87\\x80\\xb2\\xb2sM-SEARCH * HTTP/1.1\\r\\nHOST: 239.255.255.250:1900\\r\\nMAN: "ssdp:discover"\\r\\nMX: 1\\r\\nST: urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ PPPoE Tag List ]###
\tag_list \
|###[ PPPoE Tag ]###
|tag_type = 256
|tag_len = 24191
|tag_value = '\\\xff\\xfa\\xc0\\xd1>zb\x8e\x80\x8e\\xa5\x80\x80\x81\x11\x80\x80\\xc0\\xa8\x81\\r\\xef\\xff\\xff\\xfa\\xd4-\\x87\\x80\\xb2\\xb2sM-SEARCH * HTTP/1.1\\r\\nHOST: 239.255.255.250:1900\\r\\nMAN: "ssdp:discover"\\r\\nMX: 1\\r\\nST: urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ PPP over Ethernet Discovery ]###
version = 0
type = 1
code = PPP Session Stage
sessionid = 0x5e7f
len = 65530
###[ PPPoE Tag List ]###
\tag_list \
|###[ PPPoE Tag ]###
|tag_type = 48276
```

Cuando se digite el número del paquete, se cargarán todas las tramas relacionadas con el protocolo PPP que tenga dicho paquete. Actualmente hay más de 20 tramas distintas que captura la aplicación. (Para ver todas las tramas cargadas hay que scrollar hacia arriba ya que son muchas).

Luego de cargar todas las tramas con sus respectivos campos para un solo paquete, la aplicación da la opción de digitar el número de otro paquete o volver al menú anterior.

```
None
###[ PPP Link Control Protocol ]###
code      = Configure-Request
id        = 0x0
len       = 24191
rejected_protocol= 65530
\rejected_information\
|###[ Packet ]###
|###[ Raw ]###
|load     = '\\xc0|\\xd1>zb\\x08\\x00E\\x00\\x00\\xa5\\x00\\x00\\x01\\x11\\x00\\x00\\xc0\\xa8\\x01\\r\\xef\\xff\\x
n:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'

None
###[ PPP LCP Option ]###
type      = Maximum-Receive-Unit
len       = 0
quality_protocol= 24191
data      = '\\xff\\xfa\\xc0|\\xd1>zb\\x08\\x00E\\x00\\x00\\xa5\\x00\\x00\\x01\\x11\\x00\\x00\\xc0\\xa8\\x01\\r\\xef\\xff\\x
urn:dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows'
###[ Padding ]###
load      = '\\r\\n\\r\\n'

None
###[ PPP Password Authentication Protocol ]###
code      = Authenticate-Request
id        = 0x0
len       = 24191
username_len= 255
username  = '\\xfa\\xc0|\\xd1>zb\\x08\\x00E\\x00\\x00\\xa5\\x00\\x00\\x01\\x11\\x00\\x00\\xc0\\xa8\\x01\\r\\xef\\xff\\x
dial-multiscreen-org:service:dial:1\\r\\nUSER-AGENT: Chromium/105.0.5195.127 Windows\\r\\n\\r\\n'
passwd_len= None
password  = None




None
Desea seguir observando tramas de paquetes? Digite s para continuar o digite cualquier otra tecla para salir
_
```

b. Guardar las capturas en un archivo pcap

Después de capturar paquetes se pueden guardar dichas capturas en un archivo con extensión pcap, el cual se almacena en la misma ubicación que el ejecutable-Script.

```
Se han capturado 5 paquetes

Que desea realizar?
1- Revisar la trama de un paquete especifico
2- Guardar las capturas en un archivo pcap
3- Salir del menu
2
Guardando paquetes capturados en archivo pcap....
Archivo PCAP generado en la ubicación del ejecutable
```

	Capturador.exe	15/10/2022 7:06 p. m.	Aplicación	44.037 KB
	Capturador.py	15/10/2022 6:41 p. m.	Python File	11 KB
	ResultadosCapturaPPP.pcap	15/10/2022 9:32 p. m.	Wireshark capture...	1 KB

2. Capturar por un tiempo determinado

Esta es la segunda funcionalidad de la aplicación, la cual le permite al usuario capturar paquetes en un tiempo medido en segundos. Cuando finaliza la captura, automáticamente se guarda en un archivo pcap.

```
Capturador de tramas PPP (Point to Point Protocol)
Elija una de las siguientes opciones:
1- Capturar un número fijo de paquetes
2- Capturar por un tiempo determinado (Los resultados se guardarán en un archivo pcap)
3- Salir de la aplicación
2
Elija el tiempo de captura de paquetes (en segundos)
10
Capturando paquetes...
Paquete #1 Ether / IP / TCP 157.240.6.53:https > 192.168.1.13:52574 PA / Raw
Paquete #2 Ether / IP / TCP 157.240.6.53:https > 192.168.1.13:52574 FA / Padding
Paquete #3 Ether / IP / TCP 192.168.1.13:52574 > 157.240.6.53:https A
Paquete #4 Ether / IP / TCP 192.168.1.13:52574 > 157.240.6.53:https FA
Paquete #5 Ether / IP / TCP 157.240.6.53:https > 192.168.1.13:52574 A / Padding
Paquete #6 Ether / IP / UDP 142.250.78.170:https > 192.168.1.13:63307 / Raw
Paquete #7 Ether / IP / UDP 192.168.1.13:63307 > 142.250.78.170:https / Raw
Paquete #8 Ether / IP / UDP 192.168.1.8:45122 > 239.255.255.250:ssdp / Raw
Paquete #9 Ether / IP / UDP 192.168.1.8:45122 > 239.255.255.250:ssdp / Raw
Paquete #10 Ether / IP / UDP 192.168.1.8:45122 > 239.255.255.250:ssdp / Raw
Paquete #11 Ether / IP / TCP 157.240.6.53:https > 192.168.1.13:52575 SA
Paquete #12 Ether / IP / TCP 192.168.1.13:52358 > 173.194.212.188:5228 A / Raw
Paquete #13 Ether / IP / TCP 173.194.212.188:5228 > 192.168.1.13:52358 A
Paquete #14 Ether / IP / UDP 192.168.1.13:49252 > 142.250.78.14:https / Raw
Paquete #15 Ether / IP / UDP 142.250.78.14:https > 192.168.1.13:49252 / Raw
WARNING: PcapWriter: unknown LL type for PPPoETag. Using type 1 (Ethernet)
WARNING: Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: PcapWriter: unknown LL type for PPPoED_Tags. Using type 1 (Ethernet)
WARNING: Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: more PcapWriter: unknown LL type for PPPoED. Using type 1 (Ethernet)
WARNING: more Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: PcapWriter: unknown LL type for PPPoETag. Using type 1 (Ethernet)
WARNING: Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: PcapWriter: unknown LL type for PPPoED_Tags. Using type 1 (Ethernet)
WARNING: Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: more PcapWriter: unknown LL type for PPPoED. Using type 1 (Ethernet)
WARNING: more Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: PcapWriter: unknown LL type for PPP_LCP_Magic_Number_Option. Using type 1 (Ethernet)
WARNING: Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: PcapWriter: unknown LL type for PPP_LCP_Option. Using type 1 (Ethernet)
WARNING: Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
WARNING: more PcapWriter: unknown LL type for PPP_LCP_Protocol_Reject. Using type 1 (Ethernet)
WARNING: more Inconsistent linktypes detected! The resulting PCAP file might contain invalid packets.
Archivo PCAP generado en la ubicación del ejecutable
```

Esta función está diseñada para la captura de grandes volúmenes de paquetes.

Los archivos pcap pueden abrirse en el software de captura Wireshark:

ResultadosCapturaPPP.pcap

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
79	2.280927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
80	2.315929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
81	2.355926	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
82	2.366929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
83	2.393929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
84	2.407930	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
85	2.417926	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
86	2.427928	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
87	2.467930	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
88	2.504926	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
89	2.543929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
90	2.588927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
91	2.597929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
92	2.629927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
93	2.639927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
94	2.649929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
95	2.659927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
96	2.668929	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
97	2.711927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)
98	2.720927	DTE	DCE	0x00e1	1291	PPP Unknown (0x00e1)

Frame 86: 1291 bytes on wire (10328 bits), 1291 bytes captured (10328 bits) on 0
Encapsulation type: PPP with Directional Info (19)

[Time shift for this packet: 0.00000000 seconds]
Epoch Time: 1665880704.258680000 seconds
[Time delta from previous captured frame: 0.010002000 seconds]
[Time delta from previous displayed frame: 0.010002000 seconds]
[Time since reference or first frame: 2.427928000 seconds]
Frame Number: 86

Capture Length: 1291 bytes (10328 bits)
[Frame is marked: False]
[Frame is ignored: False]
Point-to-Point Direction: Sent (0)

Point-to-Point Protocol
[Direction: DTE->DCE (0)]
Protocol: Unknown (0x00e1)

Data: bf15b394c07cd13e7a620800450004fe2bad400080110000c0a8010dacd9ac0eef6701bb...
[Length: 1290]

0000 e1 bf 15 b3 94 c0 7c d1 3e 7a 62 08 00 45 00 04|..>zb..E..
0010 fe 2b ad 40 00 80 11 00 00 c0 a8 01 0d ac d9 ac ..+@.....
0020 0e ef 67 01 bb 04 ea 1f 99 43 71 e3 ff 50 06 f1 ..g.....Cq..P..
0030 b3 db 3f c9 3a 52 a4 c4 fb 79 06 62 7b 34 f0 3e ..?:R...y·b{4>..
0040 35 89 92 26 5a f0 ea 7e 15 e5 78 dc fc 77 df f7 5·&Z·~·x·w..
0050 f1 4e 6d 04 92 77 52 50 ef 56 6c 79 1f 45 ef 55 ·Nm··wRP·Vly·E·U..
0060 7b 2e 2f e8 cd 70 61 13 24 7a 3a 4d 9b 82 9c f3 {./..pa·\$:M..
0070 05 93 0a 13 5e c8 da 50 2d a0 ee db 6a 14 63 63^..P.....j·cc..
0080 7a 0a 16 dc 33 7c be 8c d5 bb e0 f4 74 e1 e5 70 z...3|...t...p..
0090 35 41 00 18 73 8b 5c 2d f4 b1 54 a2 60 83 60 4b 5A··s·\·~··T··`·K

Frame length stored into the capture file (frame.cap_len)