



# **Centro Universitario de Ciencias Exactas e Ingenierías**

*Departamento de ciencias computacionales*

**Administración de redes**

**Reporte semanal**

**Semana 2**

WireShark y protocolos de conexión

Prof: Ing. Luis Ignacio Sánchez Salazar  
Alumno: Diego Martín Domínguez Hernández  
Carrera: Ingeniería Informática  
Materia: i5907 (Administración de Redes)  
NRC: 42241  
Sección: D04  
Calendario: 2023A

En esta segunda semana se vieron la historia en los protocolos de comunicación entre dispositivos:

- Tipos de topología (estrella, bus, PPP)
- Cómo se le reconoce a cada una de las regiones de conexiones (LAN, MAN Y WAN)
- Los tipos de cable utilizados para conectarlos (¡muy grandes y gruesos!)
- Cómo se implica el hacking ético desde la incorporación del internet en la sociedad
- La historia del protocolo OSI (y cómo no ha sido exitoso a que llegó demasiado tarde para ser incorporado)
- El popular protocolo TCP/IP
- El protocolo UDP

Toda esta información para entrar al mundo del sniffeo de paquetes utilizando WireShark, una herramienta de código abierto que descifra los paquetes enviados por los equipos en una red.

Se nos indicó utilizar el programa para capturar unos cuantos paquetes en nuestra red.

En mi caso, fue un conjunto de símbolos que no entiendo; desde el amontonamiento de direcciones IP, hasta mensajes de descripción mal descifrados, pero me decían para qué estaban siendo mandados.

El primer documento al cual le saque captura tiene más de mil hojas, así que, como evidencia y demostración para el documento, tomé captura de un solo paquete y describirlo.










No.	Time	Source	Destination	Protocol	Length	Info	
	1 0.000000000	2607:f8b0:4012:814::200a	2806:103e:29:a65:acda:ffde:6035:f163	UDP	660		
443 → 37400 Len=596							
Frame 1: 660 bytes on wire (5280 bits), 660 bytes captured (5280 bits) on interface any, id 0							
Linux cooked capture v1							
Internet Protocol Version 6, Src: 2607:f8b0:4012:814::200a, Dst: 2806:103e:29:a65:acda:ffde:6035:f163							
User Datagram Protocol, Src Port: 443, Dst Port: 37400							
Data (596 bytes)							
0000	50 f0 78 50 a3 d3 2b 14 9e 04 28 bc b9 b8 04 4b	P.xP...+...(.K					
0010	1e 6f d7 46 5e 5d cd c3 a9 4c 1f 06 e6 47 75 ad	.o.F^]...L...Gu.					
0020	45 49 d1 b5 f1 10 69 a9 50 d9 13 7e 64 2e f4 a9	EI....i.P..~d...					
0030	91 9e 2b 12 fa 47 70 4b d7 e6 f8 3c f7 d1 25 94	..+..GpK...<.%.					
0040	96 24 3c 00 89 6a 81 e2 a8 f8 7c cd 3d 06 b3 a4	.\$<..j.... .=-...					
0050	2f 78 79 78 e7 6b 8a 6e 86 e7 40 5e d1 56 51 c0	/xyx.k.n..@^VQ.					
0060	a9 ea 72 5f 4c 74 12 cc 85 61 16 c6 66 1a f6 30	..r_Lt...a..f..0					
0070	e6 d4 1d 5e 17 b1 53 92 2d 80 5e 83 4d 10 03 f0	...^..S.-.^..M...					
0080	79 d0 8f 9b e3 28 c6 53 92 9f 2f a6 54 3d e9 63	y....(.S../.T=.c					
0090	eb c6 7e f6 7c a9 87 62 87 a8 fa cd 24 6c 19 ff	..~. ..b....\$l..					
00a0	bc 56 7a 3c d6 64 7d 39 a4 26 8c bc 2a 99 c3 93	.Vz<.d}9.&..*...					
00b0	7e 88 d3 4f b0 25 03 bc 85 73 ac ef ec dc 86 71	~..0.%...s.....q					
00c0	a5 cc 97 df 12 6f a5 79 5a 02 d0 80 f0 c2 da 09	.....o.yZ.....					
00d0	5d 7e a2 37 a6 d6 1f 24 bc 95 28 16 2a c9 a2 ff	]~.7...\$.(*...					
00e0	ec 42 e1 22 89 ee 09 f3 a2 6b 22 b9 7c b7 79 d1	.B.".....k".. .y.					
00f0	ec f1 c2 36 ea 33 37 c8 68 62 2e 02 48 00 a8 0a	...6.37.hb..H...					
0100	27 21 be e7 64 98 40 f1 2a 65 69 85 14 8d 0d 00	'!..d.@.*ei.....					
0110	70 16 9e a7 34 cd 50 76 9c 02 25 7c 51 b9 3a 3e	p...4.Pv..% Q.:>					
0120	8d 65 e2 08 26 9d 0d a4 58 3e d0 a8 44 04 30 20	.e..&...X>..D.0					
0130	2e 65 df 53 bd d5 00 0e a5 a7 d2 10 89 59 72 bb	.e.S.....Yr.					
0140	69 ec c1 88 3e 18 14 9f eb a7 ff 70 67 ca 59 66	i...>.....pg.Yf					
0150	fd 17 73 a8 1a 82 b2 42 37 ab 3f 98 e5 5a 4b 09	..s....B7.?..ZK.					
0160	48 ce e2 74 b9 45 b7 b2 06 f0 a5 46 88 5b 05 c1	H..t.E.....F.[..					
0170	a4 86 80 d7 47 50 5c a1 52 5d d6 4c 2f c1 6a 61	....GP\R].L/.ja					
0180	a6 7e 18 60 0f 4a 45 6b 93 56 d7 d5 05 a3 ac a9	.~.`.JEk.V.....					
0190	ca a6 32 0b b1 1f da a9 a2 86 5d 87 5b 65 46 fe	..2.....].[eF.					
01a0	dc de 65 96 bc 75 35 f4 5a 06 05 19 31 ae 87 9f	..e..u5.Z...1...					
01b0	7a 8f be 85 28 94 12 fc 03 9b b5 da 69 e0 e1 e8	z...(.i....					
01c0	b0 30 ab a0 05 ad cb 4c 78 9c 62 a3 5c 2d a5 b6	.0....Lx.b.\-...					
01d0	83 84 74 9e 68 81 25 8a 95 2c 1e 67 cf d9 b2 99	..t.h.%.,.g....					
01e0	95 3d fa 6e 7c dc 8f 0e 2a 35 5c ef 67 a0 e0 44	.=.n ...*5\g..D					
01f0	f5 22 3e ed a1 14 fb f3 2f bd 94 13 b8 7d fe 9c	.">...../....}..					
0200	3c fd b8 d7 80 59 f8 82 a5 9c 4b 66 29 09 81 79	<....Y....Kf)..y					
0210	b1 d5 71 fb f5 1d 9a 55 cf ce 2e d2 32 1a 3d d9	..q....U....2.=.					
0220	19 a8 7e b0 69 b0 fa 9e a6 53 1f 0e 1d 28 85 b9	..~.i....S...(..					
0230	b5 6d 01 61 88 e4 cd fa cb 03 79 47 ed 61 aa 32	.m.a.....yG.a.2					
0240	10 88 d7 bd be b7 3a bc 85 16 b7 8f 18 8b 8e b4	.....:.....					
0250	c3 0d 75 56	..uV					

La captura es muy extensa, pero desglosándolo todo se entiende un poco qué está pasando:

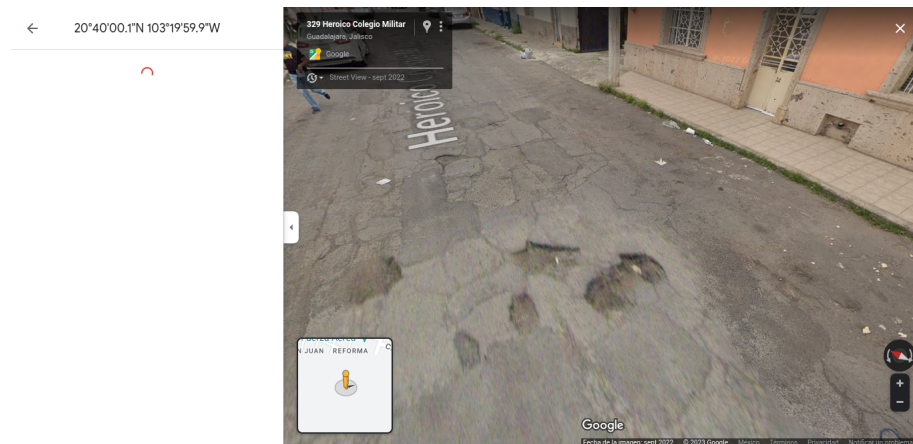
- La primer dirección IP es una IP versión 6, la cual está representada por 8 grupos de, generalmente cuatro caracteres hexadecimales, en este caso es la dirección IP corresponde a la de mi celular.
- La dirección de destino es también una dirección IPv6

La dirección destinatario apunta a

**Geolocation data from IP2Location (Product: DB6, 2023-1-1)**

 <b>IP ADDRESS:</b> 2806:103e:29:a65:acda:ffde:6035:f163	 <b>ISP:</b> Uninet S.A. de C.V.
 <b>COUNTRY:</b> Mexico 	 <b>ORGANIZATION:</b> Not available
 <b>REGION:</b> Jalisco	 <b>LATITUDE:</b> 20.6667
 <b>CITY:</b> Guadalajara	 <b>LONGITUDE:</b> -103.3333

Que parece ser la dirección del servidor de Telmex en San Pedro Tlaquepaque



Aunque en Google Maps muestre lo contrario.

Aún así, interesante.

El protocolo que utiliza la conexión es UDP, protocolo que especifica el puerto al cual quiere mandar la información.

Todo este tipo de información me es fascinante, aunque es mucha terminología de golpe, siento que con un poco de paciencia y dedicación, puedo en-

tender por lo menos la mitad de lo que dice un mensaje en WireShark, que parece ser una herramienta muy útil para el hackeo ético.