



TECNOLÓGICO NACIONAL DE MÉXICO INSTITUTO TECNOLÓGICO DE NUEVO LEÓN

SUBDIRECCIÓN ACADÉMICA DEPARTAMENTO DE EDUCACIÓN A
DISTANCIA

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Ciberseguridad

Practica WireShark

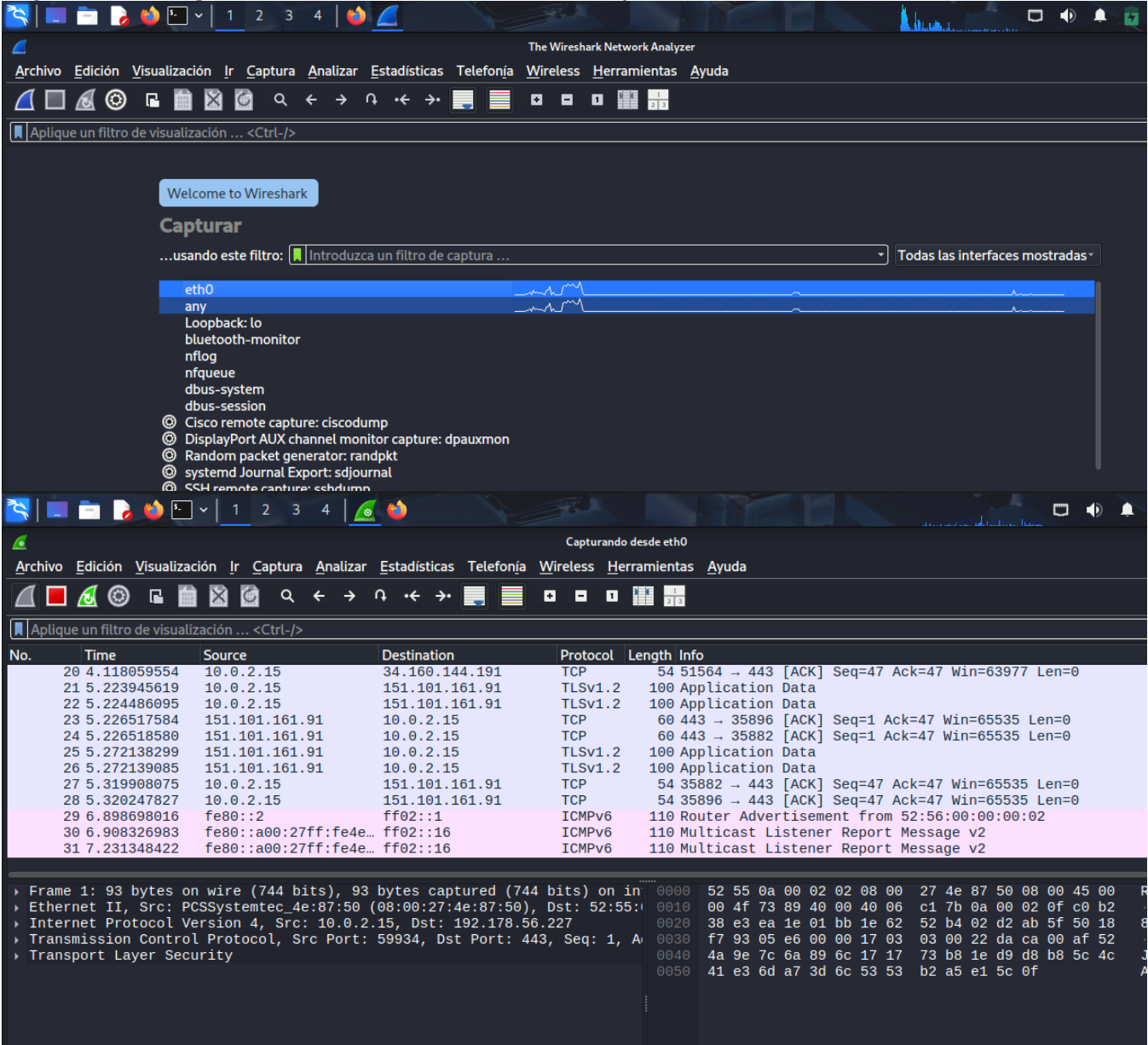
Catedrático.

Antonio Romero

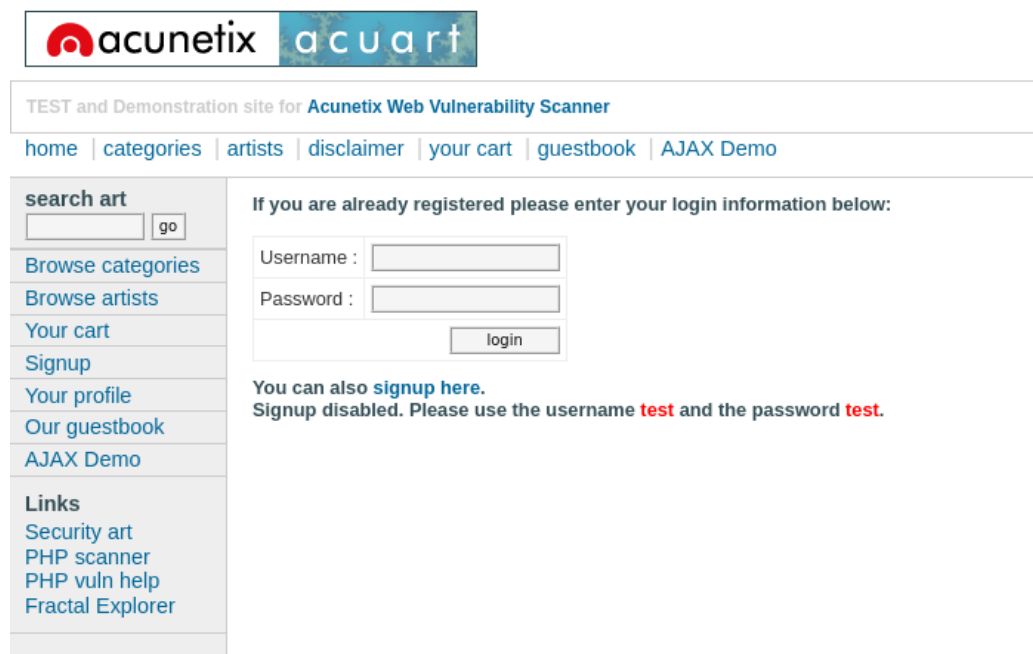
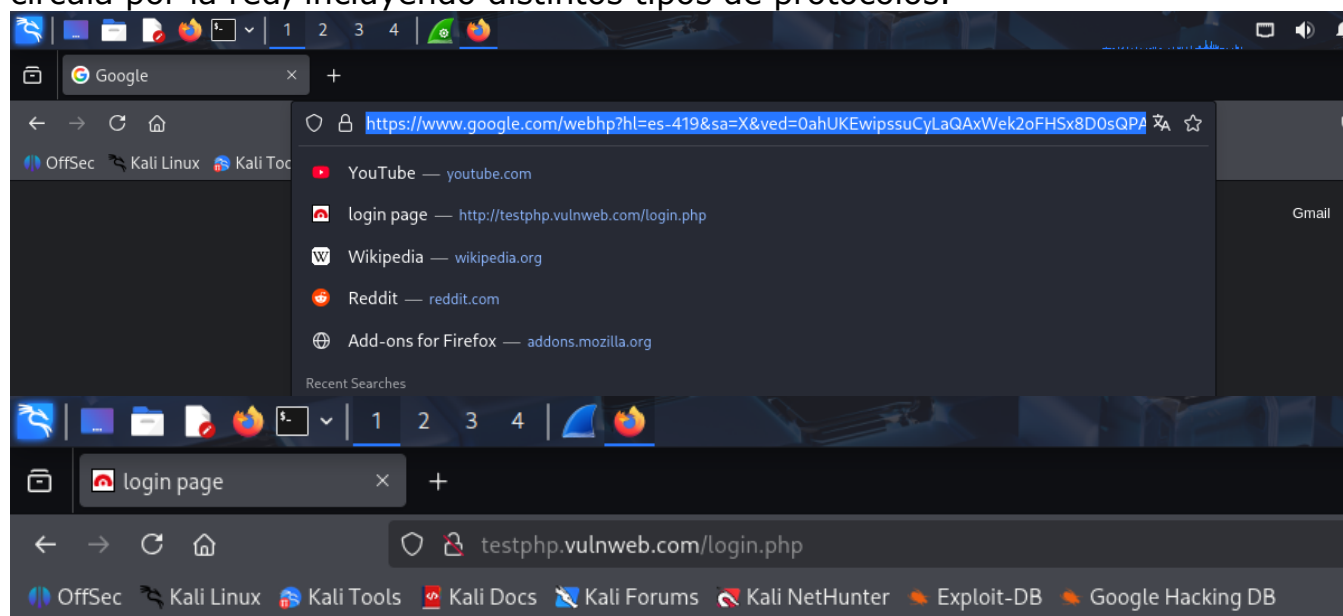
Presenta:

Angel Yahir Martinez Flores #21480677

Para comenzar la práctica, se inició el programa Wireshark en el equipo y se seleccionó la interfaz de red ethernet para acceder a internet. Una vez seleccionada, se inició la captura de paquetes presionando el botón “Start” con el objetivo de registrar el tráfico de red en tiempo real.

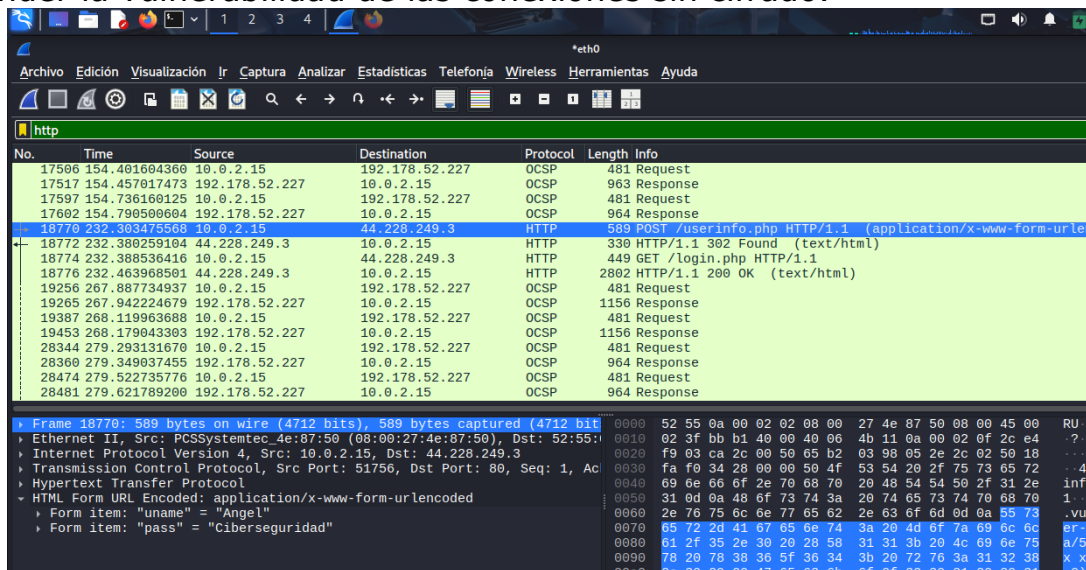


Durante la captura, se generó tráfico de red mediante diversas actividades, como la navegación por diferentes sitios web, la realización de búsquedas en internet. Estas acciones permitieron obtener una muestra representativa del tráfico que circula por la red, incluyendo distintos tipos de protocolos.

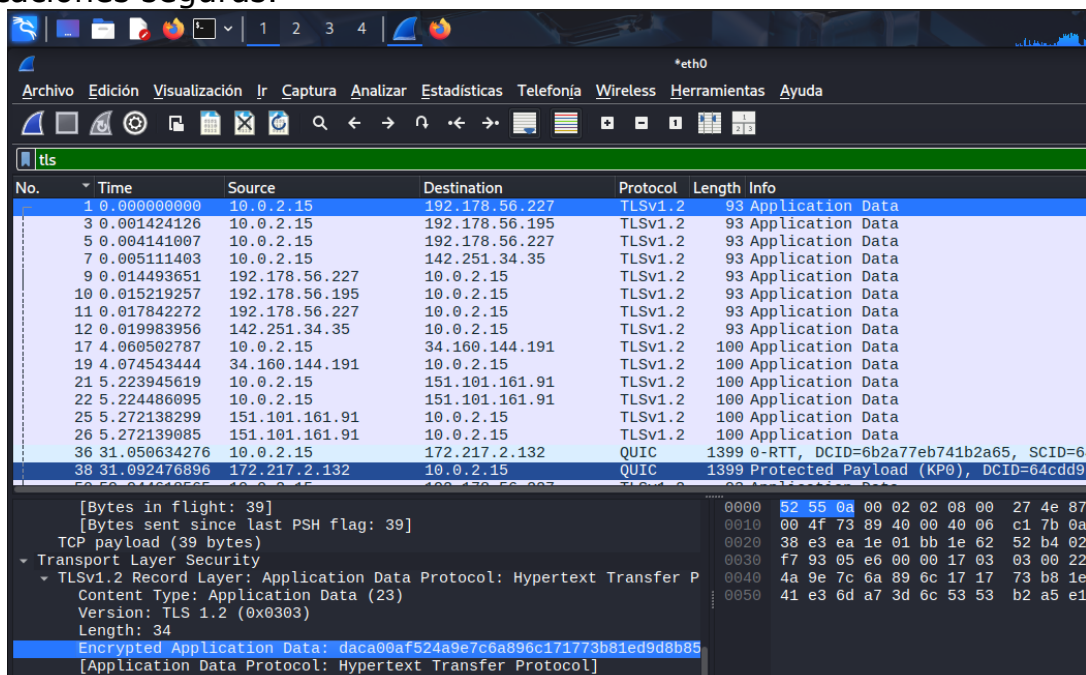


Tras aproximadamente 5 minutos de actividad, se detuvo la captura haciendo clic en el botón "Stop". A continuación, se procedió al análisis del tráfico capturado, aplicando diversos filtros en la barra de búsqueda de Wireshark para identificar protocolos específicos:

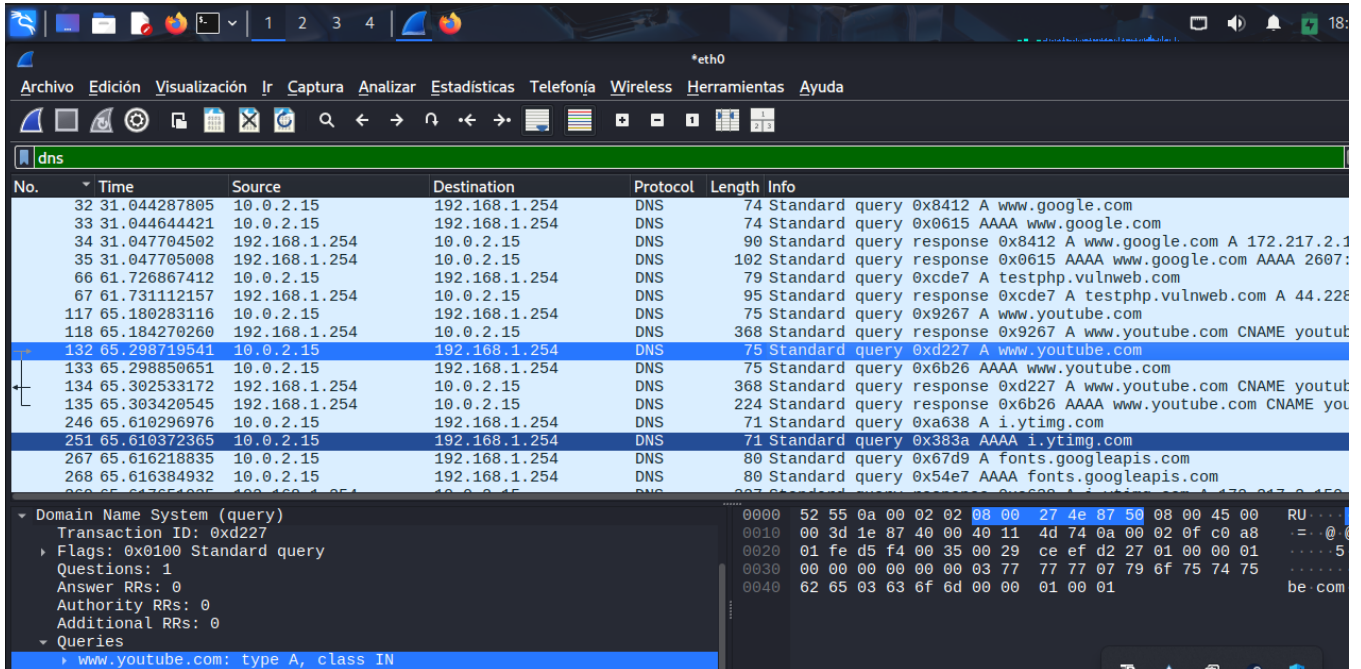
http: para observar el tráfico no cifrado y revisar solicitudes GET y POST. En esta parte se identificaron algunos datos visibles en texto claro, lo que permitió comprender la vulnerabilidad de las conexiones sin cifrado.



tls/https: para comparar el tráfico cifrado. Se observó que el contenido de los paquetes no era legible, evidenciando la protección que ofrece el cifrado en las comunicaciones seguras.



dns: para analizar las solicitudes de resolución de nombres de dominio, relacionando direcciones IP con los dominios consultados.

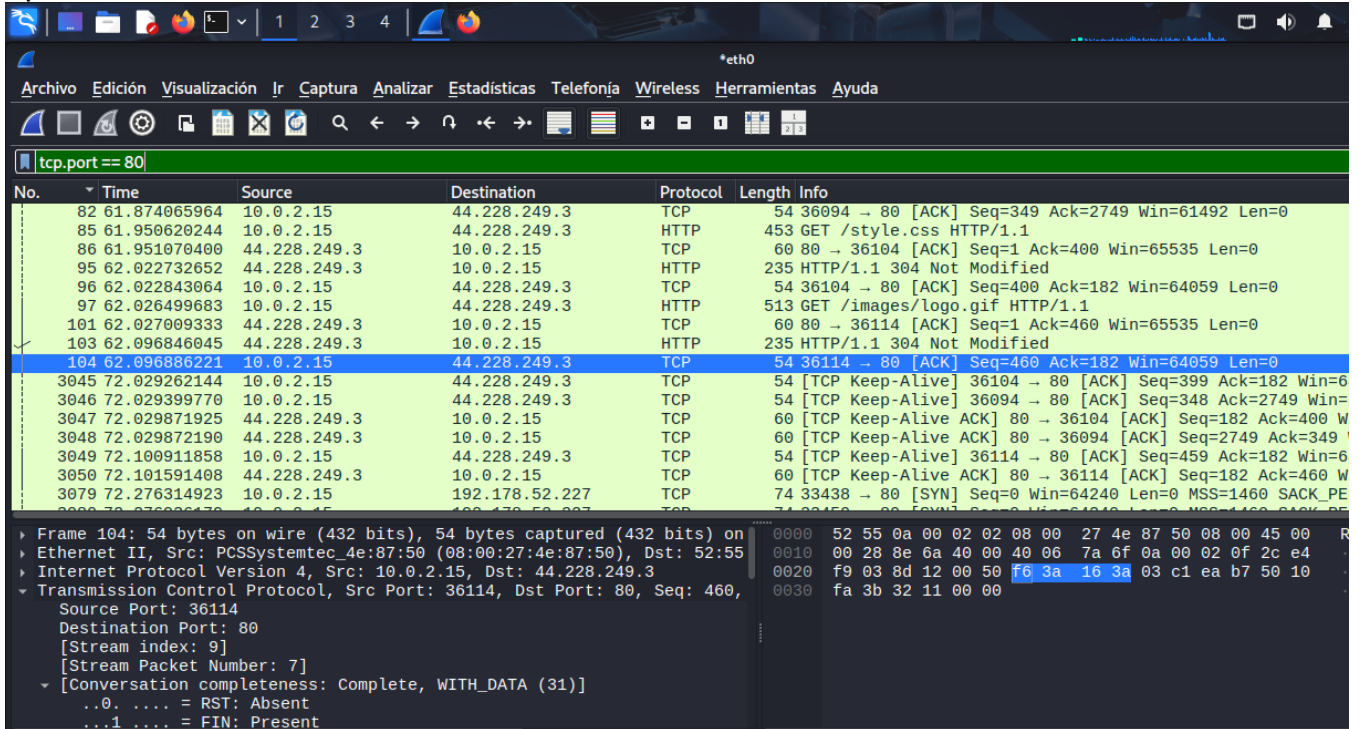


The screenshot shows a Wireshark capture of DNS traffic on the eth0 interface. The packet list on the left shows a series of queries and responses to 192.168.1.254. The selected packet (No. 132) is a query for www.youtube.com. The packet details pane on the left shows the transaction ID 0xd227 and the query type A. The packet bytes pane on the right shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
32	31.044287805	10.0.2.15	192.168.1.254	DNS	74	Standard query 0x8412 A www.google.com
33	31.044644421	10.0.2.15	192.168.1.254	DNS	74	Standard query 0x0615 AAAA www.google.com
34	31.047704502	192.168.1.254	10.0.2.15	DNS	90	Standard query response 0x8412 A www.google.com A 172.217.2.1
35	31.047705008	192.168.1.254	10.0.2.15	DNS	102	Standard query response 0x0615 AAAA www.google.com AAAA 2607:
66	61.726867412	10.0.2.15	192.168.1.254	DNS	79	Standard query 0xcde7 A testphp.vulnweb.com
67	61.731112157	192.168.1.254	10.0.2.15	DNS	95	Standard query response 0xcde7 A testphp.vulnweb.com A 44.228.
117	65.180283116	10.0.2.15	192.168.1.254	DNS	75	Standard query 0x9267 A www.youtube.com
118	65.184270260	192.168.1.254	10.0.2.15	DNS	368	Standard query response 0x9267 A www.youtube.com CNAME youtut
132	65.298719541	10.0.2.15	192.168.1.254	DNS	75	Standard query 0xd227 A www.youtube.com
133	65.298850651	10.0.2.15	192.168.1.254	DNS	75	Standard query 0x6b26 AAAA www.youtube.com
134	65.302533172	192.168.1.254	10.0.2.15	DNS	368	Standard query response 0xd227 A www.youtube.com CNAME youtut
135	65.303420545	192.168.1.254	10.0.2.15	DNS	224	Standard query response 0x6b26 AAAA www.youtube.com CNAME you
246	65.610296976	10.0.2.15	192.168.1.254	DNS	71	Standard query 0xa638 A i.ytimg.com
251	65.610372365	10.0.2.15	192.168.1.254	DNS	71	Standard query 0x383a AAAA i.ytimg.com
267	65.616218835	10.0.2.15	192.168.1.254	DNS	80	Standard query 0x67d9 A fonts.googleapis.com
268	65.616384932	10.0.2.15	192.168.1.254	DNS	80	Standard query 0x54e7 AAAA fonts.googleapis.com

Domain Name System (query)
Transaction ID: 0xd227
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.youtube.com: type A, class IN

tcp/udp: para examinar el transporte de datos entre los distintos protocolos de aplicación.



The screenshot shows a Wireshark capture of TCP traffic on the eth0 interface. The packet list on the left shows a series of HTTP requests and responses to 44.228.249.3. The selected packet (No. 104) is a TCP ACK. The packet details pane on the left shows the source port 36114 and destination port 80. The packet bytes pane on the right shows the raw data of the ACK.

No.	Time	Source	Destination	Protocol	Length	Info
82	61.874065964	10.0.2.15	44.228.249.3	TCP	54	36094 → 80 [ACK] Seq=349 Ack=2749 Win=61492 Len=0
85	61.950620244	10.0.2.15	44.228.249.3	HTTP	453	GET /style.css HTTP/1.1
86	61.951070400	44.228.249.3	10.0.2.15	TCP	60	80 → 36104 [ACK] Seq=1 Ack=400 Win=65535 Len=0
95	62.022732652	44.228.249.3	10.0.2.15	HTTP	235	HTTP/1.1 304 Not Modified
96	62.022843064	10.0.2.15	44.228.249.3	TCP	54	36104 → 80 [ACK] Seq=400 Ack=182 Win=64059 Len=0
97	62.026499683	10.0.2.15	44.228.249.3	HTTP	513	GET /images/logo.gif HTTP/1.1
101	62.027009333	44.228.249.3	10.0.2.15	TCP	60	80 → 36114 [ACK] Seq=1 Ack=460 Win=65535 Len=0
103	62.096846045	44.228.249.3	10.0.2.15	HTTP	235	HTTP/1.1 304 Not Modified
104	62.096886221	10.0.2.15	44.228.249.3	TCP	54	36114 → 80 [ACK] Seq=460 Ack=182 Win=64059 Len=0
3045	72.029262144	10.0.2.15	44.228.249.3	TCP	54	[TCP Keep-Alive] 36104 → 80 [ACK] Seq=399 Ack=182 Win=6
3046	72.029399770	10.0.2.15	44.228.249.3	TCP	54	[TCP Keep-Alive] 36094 → 80 [ACK] Seq=348 Ack=2749 Win=
3047	72.029871925	44.228.249.3	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 36104 [ACK] Seq=182 Ack=400 W
3048	72.029872190	44.228.249.3	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 36094 [ACK] Seq=2749 Ack=349
3049	72.100911858	10.0.2.15	44.228.249.3	TCP	54	[TCP Keep-Alive] 36114 → 80 [ACK] Seq=459 Ack=182 Win=6
3050	72.101591408	44.228.249.3	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 36114 [ACK] Seq=182 Ack=460 W
3079	72.276314923	10.0.2.15	192.178.52.227	TCP	74	33438 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE

Frame 104: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on
Ethernet II, Src: PCSSystemtec_4e:87:50 (08:00:27:4e:87:50), Dst: 52:55
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 36114, Dst Port: 80, Seq: 460,
Source Port: 36114
Destination Port: 80
[Stream index: 9]
[Stream Packet Number: 7]
[Conversation completeness: Complete, WITH_DATA (31)]
...0. = RST: Absent
...1 = FIN: Present

*eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
123	65.202552772	142.251.218.142	10.0.2.15	TCP	60	443 → 39574 [ACK] Seq=1 Ack=1234 Win=65535 Len=0
124	65.202569457	10.0.2.15	142.251.218.142	TLSv1.3	152	Change Cipher Spec, Application Data
125	65.203091017	142.251.218.142	10.0.2.15	TCP	60	443 → 39574 [ACK] Seq=1 Ack=1332 Win=65535 Len=0
126	65.243653270	142.251.218.142	10.0.2.15	TLSv1.3	915	Server Hello, Change Cipher Spec, Application Data, App
127	65.243749328	10.0.2.15	142.251.218.142	TCP	54	39574 → 443 [ACK] Seq=1332 Ack=862 Win=63379 Len=0
128	65.244560265	10.0.2.15	142.251.218.142	TLSv1.3	138	Application Data, Application Data
129	65.245031156	142.251.218.142	10.0.2.15	TCP	60	443 → 39574 [ACK] Seq=862 Ack=1416 Win=65535 Len=0
130	65.245432771	10.0.2.15	142.251.218.142	TLSv1.3	85	Application Data
131	65.245918878	142.251.218.142	10.0.2.15	TCP	60	443 → 39574 [ACK] Seq=862 Ack=1447 Win=65535 Len=0
136	65.312468613	10.0.2.15	142.251.218.142	TLSv1.3	1833	Application Data
137	65.312932994	142.251.218.142	10.0.2.15	TCP	60	443 → 39574 [ACK] Seq=862 Ack=2907 Win=65535 Len=0
138	65.312933366	142.251.218.142	10.0.2.15	TCP	60	443 → 39574 [ACK] Seq=862 Ack=3226 Win=65535 Len=0
147	65.434780783	142.251.218.142	10.0.2.15	TLSv1.3	4374	Application Data, Application Data, Application Data
148	65.434859608	10.0.2.15	142.251.218.142	TCP	54	39574 → 443 [ACK] Seq=3226 Ack=5182 Win=65535 Len=0
149	65.435290256	142.251.218.142	10.0.2.15	TLSv1.3	3008	Application Data, Application Data, Application Data
150	65.435302611	10.0.2.15	142.251.218.142	TCP	54	39574 → 443 [ACK] Seq=3226 Ack=8136 Win=65535 Len=0

Frame 131: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
 Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSystem
 Internet Protocol Version 4, Src: 142.251.218.142, Dst: 10.0.2.15
 Transmission Control Protocol, Src Port: 443, Dst Port: 39574, Seq: 862,
 Source Port: 443
 Destination Port: 39574
 [Stream index: 10]
 [Stream Packet Number: 13]
 [Conversation completeness: Complete, WITH_DATA (31)]
 ..0. = RST: Absent

¿Qué datos fueron visibles en el tráfico no cifrado?

Por lo visto en el escaneo de los paquetes los datos que fueron visibles son los de las paginas no seguras como fue el caso de la pagina que simula un login, que como se logra ver en la imagen, muestra las credenciales usadas.

*eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
17506	154.401604360	10.0.2.15	192.178.52.227	OCSP	481	Request
17517	154.457017473	192.178.52.227	10.0.2.15	OCSP	963	Response
17597	154.736160125	10.0.2.15	192.178.52.227	OCSP	481	Request
17602	154.790500604	192.178.52.227	10.0.2.15	OCSP	964	Response
18770	232.303475568	10.0.2.15	44.228.249.3	HTTP	589	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
18772	232.380259104	44.228.249.3	10.0.2.15	HTTP	330	HTTP/1.1 302 Found (text/html)
18774	232.388536416	10.0.2.15	44.228.249.3	HTTP	449	GET /login.php HTTP/1.1
18776	232.463968501	44.228.249.3	10.0.2.15	HTTP	2802	HTTP/1.1 200 OK (text/html)
19256	267.887734937	10.0.2.15	192.178.52.227	OCSP	481	Request
19265	267.942224679	192.178.52.227	10.0.2.15	OCSP	1156	Response
19387	268.119963688	10.0.2.15	192.178.52.227	OCSP	481	Request
19453	268.179043303	192.178.52.227	10.0.2.15	OCSP	1156	Response
28344	279.293131670	10.0.2.15	192.178.52.227	OCSP	481	Request
28360	279.349037455	192.178.52.227	10.0.2.15	OCSP	964	Response
28474	279.522735776	10.0.2.15	192.178.52.227	OCSP	481	Request
28481	279.621789200	192.178.52.227	10.0.2.15	OCSP	964	Response

Frame 18770: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bit
 Ethernet II, Src: PCSystemtec_4e:87:50 (08:00:27:4e:87:50), Dst: 52:55:0a:00:02:02
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3
 Transmission Control Protocol, Src Port: 51756, Dst Port: 80, Seq: 1, Ac
 Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "uname" = "Angel"
 Form item: "pass" = "Ciberseguridad"

¿Qué información se protegió con cifrado?

En cambio, en las paginas protegidas, en este caso YouTube, la información permanece cifrada, tanto en credenciales como también protegiendo información referente a sus servicios.

No.	Time	Source	Destination	Protocol	Length	Info
17506	154.401604360	10.0.2.15	192.178.52.227	OCSP	481	Request
17517	154.457017473	192.178.52.227	10.0.2.15	OCSP	963	Response
17597	154.736160125	10.0.2.15	192.178.52.227	OCSP	481	Request
17602	154.790500604	192.178.52.227	10.0.2.15	OCSP	964	Response
18770	232.303475568	10.0.2.15	44.228.249.3	HTTP	589	POST /userinfo.php HTTP/1.1 (application/x-www-form-u
18772	232.380259104	44.228.249.3	10.0.2.15	HTTP	330	HTTP/1.1 302 Found (text/html)
18774	232.388536416	10.0.2.15	44.228.249.3	HTTP	449	GET /login.php HTTP/1.1
18776	232.463968501	44.228.249.3	10.0.2.15	HTTP	2802	HTTP/1.1 200 OK (text/html)
19256	267.887734937	10.0.2.15	192.178.52.227	OCSP	481	Request
19265	267.942224679	192.178.52.227	10.0.2.15	OCSP	1156	Response
19387	268.119963688	10.0.2.15	192.178.52.227	OCSP	481	Request
19453	268.179043303	192.178.52.227	10.0.2.15	OCSP	1156	Response
28344	279.293131670	10.0.2.15	192.178.52.227	OCSP	481	Request
28360	279.349037455	192.178.52.227	10.0.2.15	OCSP	964	Response
28474	279.522735776	10.0.2.15	192.178.52.227	OCSP	481	Request
28481	279.621789200	192.178.52.227	10.0.2.15	OCSP	964	Response

Hypertext Transfer Protocol

Online Certificate Status Protocol

tbsRequest

requestList: 1 item

Request

reqCert

hashAlgorithm (SHA-1)

issuerNameHash: ee309c404feb6b6256b48e26bfe4451298bae4dd

issuerKeyHash: 75bec477ae89f644377dcfb1681f1d1aebdc3459

serialNumber: 0x4695234271687d1a097fcaf0875beed7

0000 52 55 0a 00 02 02 08 00 27 4e 87 50 08 00 45 00
0010 01 d3 65 34 40 00 40 06 d2 4c 0a 00 02 0f c0 b2
0020 34 e3 82 9e 00 50 e6 e2 6d d2 03 d8 7e b4 50 18
0030 fa f0 03 6a 00 00 50 4f 53 54 20 2f 77 65 32 20
0040 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20
0050 6f 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 55 73 65 72
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
0070 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20
0080 78 38 36 5f 36 34 3b 20 72 76 3a 31 32 38 2e 30
0090 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31
00a0 20 46 69 72 65 66 6f 78 2f 31 32 38 2e 30 6d 0a

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.178.56.227	TLSv1.2	93	Application Data
3	0.001424126	10.0.2.15	192.178.56.195	TLSv1.2	93	Application Data
5	0.004141007	10.0.2.15	192.178.56.227	TLSv1.2	93	Application Data
7	0.005111403	10.0.2.15	142.251.34.35	TLSv1.2	93	Application Data
9	0.014493651	192.178.56.227	10.0.2.15	TLSv1.2	93	Application Data
10	0.015219257	192.178.56.195	10.0.2.15	TLSv1.2	93	Application Data
11	0.017842272	192.178.56.227	10.0.2.15	TLSv1.2	93	Application Data
12	0.019883956	142.251.34.35	10.0.2.15	TLSv1.2	93	Application Data
17	4.060502787	10.0.2.15	34.160.144.191	TLSv1.2	100	Application Data
19	4.074543444	34.160.144.191	10.0.2.15	TLSv1.2	100	Application Data
21	5.223945619	10.0.2.15	151.101.161.91	TLSv1.2	100	Application Data
22	5.224486095	10.0.2.15	151.101.161.91	TLSv1.2	100	Application Data
25	5.272138299	151.101.161.91	10.0.2.15	TLSv1.2	100	Application Data
26	5.272139085	151.101.161.91	10.0.2.15	TLSv1.2	100	Application Data
36	31.050634276	10.0.2.15	172.217.2.132	QUIC	1399	0-RTT, DCID=6b2a77eb741b2a65, SCID=64
38	31.092476896	172.217.2.132	10.0.2.15	QUIC	1399	Protected Payload (KP0), DCID=64cdd9

[Bytes in flight: 39]

[Bytes sent since last PSH flag: 39]

TCP payload (39 bytes)

Transport Layer Security

TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer P

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 34

Encrypted Application Data: daca00af524a9e7c6a896c171773b81ed9d8b85

[Application Data Protocol: Hypertext Transfer Protocol]

0000 52 55 0a 00 02 02 08 00 27 4e 87
0010 00 4f 73 89 40 00 40 06 c1 7b 0a
0020 38 e3 ea 1e 01 bb 1e 62 52 b4 02
0030 f7 93 05 e6 00 00 17 03 03 00 22
0040 4a 9e 7c 6a 89 6c 17 17 73 b8 1e
0050 41 e3 6d a7 3d 6c 53 53 b2 a5 e1