Wireshark para novatos - Español



Wireshark para novatos Por Anmol K Sachan

anmol221999@gmail.com Linkedin: https://linkedin.com/in/anmolksachan/ lg: <u>https://instagram.com/the_guy_that_hacks</u>

Traducción por: Carla Cortés y Luis Rodríguez

ÍNDICE

- 1. Cómo empezar
- Empezar el análisis: Realizar una captura en vivo del tráfico de red/tráfico web
 2.1 2.1 Filtrar los paquetes con la barra de filtros durante la captura y explicar todos los posibles filtros utilizados por usted.
- 3. Ver los resúmenes de los paquetes con la ventana de la lista de paquetes
- 4. Estudiar los detalles del paquete con la ventana de detalles del paquete

5. Ver los datos de los paquetes con la ventana de bytes de paquetes individuales

6. Simplemente navegar por Internet

7. Visualización de los datos de la cabecera del paquete

7.1 Captura de paquetes con Wireshark

- 7.2. Explorar la capa de interfaz de red / capa de enlace de datos
- 7.2.2. Ver datos de tramas Ethernet capturados con Wireshark

8. Exploración de la capa de Internet

8.1.1 Cabecera IPv4: Imagen de abajo

8.1.2. Ver los datos de la cabecera IP de un paquete TCP capturado con Wireshark

8.1.3 Ver los datos de la cabecera IP de un paquete UDP

8.1.4. Ver los datos de la cabecera IP de un paquete ARP

9. Exploración de la capa de transporte

9.1.1. Cabecera TCP: Imagen de abajo

9.1.2 Ver los datos de la cabecera TCP de un paquete TCP capturado con Wireshark

9.1.3 Cabecera UDP: En la imagen de abajo

9.1.4 Ver los datos de la cabecera UDP de un paquete UDP capturado con Wireshark

9.1.5 Comparar y contrastar IP, TCP y UDP

10. 10. Explorar la capa de aplicación

- 10.1.1 Analizar un paquete HTTP
- 10.1.2 Analizar un paquete DNS

11. Preguntas comunes

1. Comenzando con Wireshark



Wireshark está preinstalado en kali linux.

Wireshark es un analizador de paquetes gratuito y de código abierto. Se utiliza para la resolución de problemas de red, el análisis, el desarrollo de software y protocolos de comunicación, y la educación. Originalmente llamado Ethereal, el proyecto fue rebautizado como Wireshark en mayo de 2006 debido a problemas de marca.

La GUI de wireshark tiene

- 1. Barra de título
- 2. Menú principal
- 3. Barra de herramientas principal
- 4. Barra de herramientas del filtro
- 5. Lista de paquetes
- 6. Barra de desplazamiento inteligente
- 7. Detalles del paquete
- 8. Packet Bytes
- 9. Barra de estado

		Google - Mozilla Fir	efox		ľ		- 0
Google	× +						
← → × ŵ	🛈 🔒 https://www.go	ogle.com		••• 🖾	습	■ ①	
		1	Capturing	from eth0			_ = ×
		File Edit View Go	apture <u>A</u> nalyze <u>S</u>	tatistics Telephony <u>V</u>	<u>Vireless</u> <u>Tools</u>	<u>H</u> elp	
		📶 🗖 🔬 🎯 土	n 12 6 a	← → ∩ ·< →	- 📑 🔲		٥
		Apply a display filter <c< td=""><td></td><td></td><td>=</td><td>Expressio</td><td>on +</td></c<>			=	Expressio	on +
		No. Time	Source	Destination	Prot	tocol Len	gth Infc
		511 27.382042668	192.168.81.136	192.168.81.2	DNS		85 Sta
		512 27.797039760	192.168.81.136	192.168.81.2	DNS		78 Sta
		513 27.823717768	192.168.81.2	192.168.81.1	36 DNS		94 Sta
		514 27,823898440	192,108,81,130	192.108.81.2	26 DNC		78 SLa
		516 28 279449868	192.108.81.2	192.108.81.1	30 UNS	-	85 Sta
		01010110445000	102.100.01.100	152.100.01.1	UND		os ore
	(Q			and the second s			
		Frame 1: 60 bytes o	n wire (480 bits), 60 bytes capture	d (480 bits)	on inte	erface (
		▶ Ethernet II, Src: V	mware_2d:7b:05 (0	00:0c:29:2d:7b:05),	Dst: Broadc	ast (ff:	: ff:ff :
		Address Resolution	Protocol (reques	τ)			
					<u> </u>		
India		LOODO IT IT IT IT IT	ff 00 0c 20 2d	70 05 08 06 00 01			
		0010 08 00 06 04 00	01 00 0c 29 2d	7b 05 c0 a8 51 8c	· · · · · · · · · · · · · · · · · · ·		
Read www.google.com	the state of the s	F 0020 00 00 00 00 00	00 c0 a8 51 02	00 00 00 00 00 00	Q		

Haciendo clic en la interfaz eth0 se inicia la captura de paquetes, mientras que el **sniffing** podemos **analizar** y puede aplicar **filtros** para ver la necesidad exacta.

Definir las cuatro capas del modelo de referencia TCP/IP.

La capa TCP maneja el mensaje que se va a transmitir. Este mensaje se suele dividir en pequeñas unidades. Estas pequeñas unidades se conocen como paquetes. Además, estos paquetes se transmiten por la red.

Estos paquetes son recibidos por la capa TCP correspondiente en el receptor y reensamblados en el mensaje original.

El modelo TCP/IP tiene 4 capas, que son:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
 Capa de red



Capa de aplicación:

La primera capa es la de aplicación. Esta capa proporciona a las aplicaciones un intercambio de datos estandarizado. A continuación se indican los protocolos de estas capas:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo de transferencia de archivos (FTP)
- Protocolo de oficina de correos 3 (POP3)
- Protocolo simple de transferencia de correo (SMTP)
- Protocolo simple de gestión de redes (SNMP)

Este trabajo en capas con todos estos protocolos.

Capa de transporte:

La capa de transporte es la segunda capa del modelo TCP/IP. El trabajo básico de la capa de transporte es mantener las comunicaciones de extremo a extremo. A continuación se indican los protocolos de estas capas:

TCP
Protocolo de Datagramas de Usuario (UDP)
Estos dos protocolos se utilizan para la capa de transporte en TCP/IP.

Capa de red:

La tercera capa de TCP IP es una capa de red. También se conoce como capa de Internet. La capa de red se ocupa de los paquetes. Los siguientes son los protocolos que se utilizan en esta capa.

- IP
- Protocolo de mensajes de control de Internet (ICMP) Capa física

La última capa es la capa física. Esta capa trabaja con los siguientes protocolos.

- Ethernet para LAN (redes de área local)
- Protocolo de resolución de direcciones (ARP)

Examinar los datos de la cabecera del paquete con Wireshark

File	<u>E</u> dit	View	<u>G</u> •	<u>C</u> api	ture	<u>A</u> nalyze	e <u>S</u> t	atistic	5 T	elepi	hony	<u>W</u> ir	eless	Tool	ls <u>H</u> e	lp	
		0	1			6	۹	÷	→	U,	•	≁	-		۵		1
📘 ip													8		Exp	ression	i +
No.	Ti 171 20 172 20	ne .036 037	0558: 0171	S 17 1 91 1	ource 92.10 92.10	68.81. 58.81	2 136		De: 192	stina 2.16 2.16	tion 8.81 8.81	.136		Pro DN	otocol S	Leng 12	
▶ Tra ➡ Hyp	nsmis: ertext	ion Tra	Cont Insfe	rol P r Pro	roto	col, S l	rc P	ort:	456	58,	Dst	Port	: 80,	Seq	: 1,	ACk:	1, L(
F G H U A	ET /s lost: lser-A lccept	detec gent: ; *//	s.tx tpor Moz \\r\n	t HT tal.f illa/	P/1. firef /5.0	1\r\n ox.com (X11;	I\r\r Linu	ו 8א אנ	6_64	; r\	/:68.	0) (Gecko/	/2010	0101	Fire	fox/6
A C	Accept: */*\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n Cache-Control: no-cache\r\n Pragma: no-cache\r\n																
artister antiste				and the second					000004		un de la composition de la com		Service Service				

Imagen. Encabezados de los paquetes de datos mostrados arriba

Definir los campos de cabecera de las tramas Ethernet, del Protocolo de Internet (IP), del Protocolo de Control de Transporte (TCP) y del Protocolo de Datagramas de Usuario (UDP) / diferentes tipos de cabeceras de paquetes, incluyendo los campos de cabecera y sus valores.



Ethernet

IP header format

 ≼ 32 bits 													
version	İHL	type of service		total length									
215	identi	fication	O D M F F	fragment offset									
time t	o live	protocol		checksum									
		source	addres	s									
		destinatio	n addr	ess									
		[opti	ons]										

Protocolo IP

TCP header format

(32 bits	5
	source port	destination port
	sequence n	umber
	acknowledgeme	ent number
Hlen		window
	checksum	urgent pointer
	[option	s]

Cabecera TCP

UDP header format

◄ 32	bits
source port	destination port
length	checksum

Cabecera UDP

Compare y contraste **TCP** y **UDP**.

Differences are-

Properties	TCP	UDP
Header	Dynamic header (20 – 60 B)	Static header of 8 Bytes
Max segment	any size or 2^30 B	short message 65536 Bytes
Flow Control	Yes, Window and seq. no.	NO
Checksum	Compulsory	Optional
Connection nature	TCP+ IP = connection oriented	UDP+IP= connection less
Error control	Own mechanism	Depends on ICMP (No self feature)
Support multicast	NO	YES
Support broadcast	NO	Yes
Examples service	HTTP, SMTP, FTP, TELNET	TFTP,DNS,SNMP

2. Empezar el análisis: Realice una captura en vivo del tráfico de red/tráfico web

2.1 Filtrar los paquetes con la barra de filtros durante la captura y explicar todos los posibles filtros utilizados por usted.

*eth0 _ □													
File E	dit <u>V</u> ie	w <u>G</u> o	Capture	Analy	ze <u>S</u> t	atistic	s Tel	ephony	Wirele	ss <u>T</u> o	ols <u>H</u>	elp	
		<u>ا</u> (E 💼	8	٩	÷	→	n •←	→•			•	1
📕 ip.ado	dr == 192	.0.2.1									Exp	ressio	n +
No.	Time		Sou	ce			Dest	ination		F	Protocol	Leng	ıt
1	76 20.0	815477	68 192	168.81	.136		99.8	6.47.	48	I	CP	1	5 U
1	77 20 A	836797	1/1 192	168 81	136	-	23 F	1 140	19	H	ITTP	3	N
▶ Fram	e 177:	342 by	tes on	wire (2	736 b	its),	342	bytes	captur	ed (27	736 bi	ts) o	n inte
▶ Ethe	rnet II	, Src:	Vmware	_a8:90:	73 (0	0:0c:	29:a8	3:90:7	3), Dst	: Vmwa	are_e6	:f0:d	e (00
▶ Inte	rnet Pr	otocol	. Versio	n 4, Sr	c: 19	2.168	8.81.1	L36, D	st: 23.	64.140	9.19		
▶ Tran	smissio	n Cont	rol Pro	tocol,	Src P	ort:	45658	3, Dst	Port:	80, Se	eq: 1,	Ack:	1, L(
- Нуре	rtext T	ransfe	r Proto	col									•
GE	I /succ	ess.t)	CT HITP/	1.1\r\r)								
HO	st: det	ectpor	tal.Tir	G (V11		1 1V V96	5 64.	ru-69		ko /20	100101	Fire	fox /8
Ac	cent: *	/*\r\r	1111a/ J . 1	0 (/11)	LINU	1 100	,_04,	10.00) dec	KU7 20.	100101	гле	1007 0
۵c	cent-la	naliane	• en-lls	en:0=(1 5\r\	n							
	£- £0 1	c ha	00.00.4	AE E		5 70	75.0	0.00	х.е.	0.5	+ /		
0030	73 73 2	Pe 74	30 00 47 78 74 20	45 5	1 54 5	21 73 50 2f	31 2	3 03 0 e 31 (oo ad ss	txt H	TTP/1	cce	
0050	0a 48 6	of 73	74 3a 20	64 6	5 74 6	55 63	74 7	0 6f	72 Ho	ost: d	etect	por	1
0060	74 61 6	ic 2e	66 69 72	65 6	6 6f 7	78 2e	63 6	f 6d (9d ta	L.fire	fox.c	om	J
0070	Oa 55	3 65	72 2d 41	67 6	5 6e 7	74 3a	20 4	d 61	7a Us	ser-Ag	ent:	Moz	
0090	69 6e 7	75 78	20 78 38	36 5	F 36 3	34 3b	20 7	2 76	Ba in	IX X86	64;	rv:	
00a0	36 38 2	2e 30	29 20 47	65 6	3 6b 6	of 2f	32 3	0 31 3	30 <mark>68</mark>	0) Ge	cko/2	010	

Capturar sólo el tráfico hacia o desde la dirección IP 172.18.5.4: host 172.18.5.4

Capturar el tráfico hacia o desde un rango de direcciones IP: 192.168.0.0/24 o 192.168.0.0 máscara 255.255.255.0

Capturar el tráfico de un rango de direcciones IP: 192.168.0.0/24 o 192.168.0.0 máscara de red 255.255.255.0

Capturar el tráfico hacia un rango de direcciones IP: 192.168.0.0/24 o 192.168.0.0 máscara de red 255.255.255.0

Capturar sólo el tráfico DNS (puerto 53): puerto 53

Capture el tráfico no HTTP y no SMTP en su servidor (ambos son equivalentes):

host www.example.com y no (puerto 80 o puerto 25) host www.example.com y no puerto 80 y no puerto 25

Captura excepto todo el tráfico ARP y DNS: puerto no 53 y no arp

Para capturar el tráfico de la vlan

No.		Time	Source	Destination	Protocol	Lengt
	3	0.000020180	192.168.81.140	192.168.81.2	NBNS	11
	4	1.511808997	192.168.81.140	192.168.81.2	NBNS	11
	5	3.024931189	192.168.81.140	192.168.81.2	NBNS	11
	6	3.400696460	192.168.81.136	192.168.81.2	DNS	8
	7	3.400823404	192.168.81.136	192.168.81.2	DNS	8
	8	3.509137922	192.168.81.2	192.168.81.136	DNS	24
	9	4.862447872	192.168.81.136	192.168.81.2	DNS	7
	10	4.862660426	192.168.81.136	192.168.81.2	DNS	7
	11	4.863220065	192.168.81.136	192.168.81.2	DNS	7
	10	4 962206621	102 169 91 126	102 169 91 2	DMC	7

3. Ver los resúmenes de los paquetes con la ventana de la lista de paquetes

Número de paquete (No.): Los números de cada paquete comienzan con 1 para el primer paquete.

₩ain Toolbar	Show Packet in New <u>W</u> indow
🔽 📝 <u>F</u> ilter Toolbar	Reload as File Format/Capture
<u>File</u> Edit <u>View</u> I Wireless Toolbar	🖻 <u>R</u> eload
📶 🔲 🔬 🎯 🗟 Status Bar	O Date and Time of Day (1970, 01, 01, 01, 02, 02, 122455)
Apply a display fil	O Date and Time of Day (1970-01-01 01:02:03:123436)
No Timo Packet List	Treat, Day of Tear, and Time of Day (1970/001 01:02:03:12)430) Treat, of Day (01:02:03:12)430)
3 0.0000 I Packet Details	
4 1.5118	
5 3.0249 5.2.4005 Time Display Format	Seconds Since Beginning of Capture
7 3.4008 Name Resolution	Seconds Since Previous Captured Packet
8 3.5091 Zoom	O Seconds Since Previous Displayed Packet
9 4,8624 to 4 essas Expand Subtrees	O UTC Date and Time of Day (1970-01-01 01:02:03.123456)
11 4.8632 Collapse Subtrees	UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
12 4 9622	O UTC Time of Day (01:02:03.123456)
Expand All	 Automatic (from capture file)
Collapse <u>All</u>	⊖ Seconds
Colorize Packet List	O Tenths of a second
0030 Ta TO D6 <u>C</u> oloring Rules	O Hundredths of a second
0650 0a 48 6f Colorize Conversation	O Milliseconds
0070 0a 55 73 Reset Layout	O Microseconds
0080 69 6c 6c 🖬 Resize Columns	O Nanoseconds
OBAO 36 38 2e Internals	Display Seconds With Hours and Minutes

Timestamp (Time): Por defecto es el número de segundos desde el inicio de la captura

*eth0 -														. 0	×								
File	Edit	V	iew	G	•	Capt	ure	An	alyze	<u>s</u>	tatis	tics	Т	elep	hony	w	ireless	Too	ls	Hel	p		
4		J	0		t		×		2	٩	÷		÷	U,	•÷	÷				۵		۵	
📜 ip.	addr =	= 19	92.0.	2,1																Expre	ssion	-	+
No.		Tim	ė			s	ourc	e					Des	stina	tion			Pr	oto	col	Lengt		
	168	19.	834	924	129	1	92.1	.68	81.	136			99.	86.	47.4	18		TC	P		5		
	169	19.	836	888	543	1	92.1	68.	81.	2			192	2.16	18.81	1.13	6	DN	IS		17		-11
F	170	19.	838	399	996	1	92.1	168.	81.	136			23.	64.	140	.19		TO	P		7	-	- "
	171	20.	036	055	817	1	92.1	168.	81.	2			192	2.16	8.81	1.13	6	DN	IS		12		
	172	20.	037	017	191	1	92.1	68.	81.	136			192	2.16	8.81	1.2		DI	IS		7	_	
	173	20.	081	399	237	2	3.64	1.14	0.1	9			192	2.16	8.81	1.13	6	TC	P		6		
	174	20.	081	456	707	1	92.1	.68	81.:	136			23.	64.	140.	.19		TC	P		5		
	175	20.	081	532	998	9	9.86	5.47	.48				192	2.16	18.8	1.13	6	TL	SV	1.2	57		
	176	20.	081	547	768	1	92.1	168.	81.	136			99.	86.	47.4	18		TO	P		5		
	177	20	002	070	711	- 14	62 1	60	01	126			33	64	140	10		ил	тю	1	24	-	
► Tr ► HV	ansmi nerte	ssi vt	.on Tra	Con	tro er	1 P Pro	roto		., s	rc I	Port	t: 4	156	58,	Dst	Por	t: 80), Sec	9:	1, A	k:	1,	Lŧ_
0036	fa	ŤØ	b 6	be	00	00	47	45	54	20	2f	73	75	63	63 6	5		GE	17	suce	ce		
6646	73	73	2e	74	78	74	20	48	54	54	50	21	31	2e	31 0	d	ss.t	xt H	TTP	11.:	1		
DOG	Ua 74	48	6T	73	14	38	20	64 65	65	14	55	53	63	/0	bT /	2	+HOS	t: d	for	ectpo	or "		
0000	- 74 - 198	55	73	55	72	2d	41	67	65	66	74	3a	20	4d	60 0 6f 7	a	uar.	r_Aa	ent	C. COI	" 07		
0080	69	60	60	61	2f	35	28	30	20	28	58	31	31	3b	20 4	c	illa	/5.0	0	(11:			
0090	69	6e	75	78	20	78	38	36	5f	36	34	3b	20	72	76 3	a	inux	x86	_64	1; m	v :		
00a6	36	38	2e	30	29	20	47	65	63	6b	6f	2F	32	30	31 3	iΘ	68.0) Ge	cko	/20	10		

Direcciones IP (Origen: Source, Destino: Destination): La dirección de origen y destino del paquete.

*eth0		_ 0 X		*eth0		_ = ×
File Edit View Go Capture Analyze Statistic	s Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> el	lp	File Edit View Go G	apture <u>A</u> nalyze <u>S</u> tatistic	s Telephony <u>Wireless</u>	Tools Help
<u> </u>	→ ∩ · ← → 🛄 🔲 🖬			🗎 🔀 🙆 Q 🗧	→ n ++ 🛄	
tcp	🖾 🗂 - Expr	ression	📕 udp		8	Expression
No. Time Source	Destination Protocol	Lengt	No. 🔻 Time	Source	Destination	Protocol Lengt
165 19.834476737 99.86.47.48 166 19.834708076 192.168.81.136	192.168.81.136 TLSv1.2 99.86.47.48 TCP	5	87 18.412714321 92 18.613489059	192.168.81.136	192.168.81.2 192.168.81.136	DNS 9
167 19.834905635 99.86.47.48 168 19 834924129 192 168 81 136	192.168.81.136 TLSv1.2	22	93 18.613526742	192.168.81.136	192,168,81,2	ICMP 14
T 178 19.838399996 192.168.81.136	23.64.140.19 TCP	7	119 19.099468645	192.168.81.136	192.168.81.2	DNS 15
173 20.081399237 23.64.140.19 174 20.081456707 192.168.81.136	192.168.81.136 TCP 23.64.140.19 TCP	6	157 19.440049514 158 19.460107752	192.168.81.136 192.168.81.136	192.168.81.2 192.168.81.2	DNS 7 DNS 7
175 20.081532998 99.86.47.48 176 20 081547768 192 158 81 136	192.168.81.136 TLSv1.2	57	169 19.836888543	192.168.81.2	192.168.81.136	DNS 17
177 90 089070744 409 168 84 496	01 01 01 01 01 01 01 01 01 01 01 01 01 0	22	172 20 032017101	102 169 91 196	102 169 81 2	
 Transmission Control Protocol, Src Port: Hymertext Transfer Protocol 	45658, Dst Port: 80, Seq: 1, .	Ack: 1, L(_	Frame 172: 73 bytes	on wire (584 bits), i ware a8:90:73 (00:0c	3 bytes captured (58 29:a8:90:73) Detrie	84 bits) on interfac /mware e6:f0:de CAO
10133 Fa f0 b6 be 60 60 47 45 54 20 2f 73 10160 73 2e 74 70 74 2e 46 54 45 59 2f 10160 73 73 2e 74 70 74 2e 46 54 54 59 2f 10160 73 73 74 3a 26 64 65 74 65 66 78 2e 10160 75 73 65 72 2d 41 67 78 56 67 78 2e 10180 66 65 72 2d 41 67 65 66 74 2e 10180 66 65 12 73 2e 30 2e 20 2e 28 53 31 10180 68 6e 75 78 2e 378 2B 36 55 65 66 61 f 10180 68 56 2e 37 78 2B 78 38 36 5f 36 34 36 66 f 10180 68 3e 2a 92 2e 27 40 76 36 36 66 66 f	75 63 63 65 6E T /suc 31 2e 31 0d ss.txt H TTP/1. 74 76 67 Host: d etectric 63 66 6d 6d fire 63 66 6d 6d fire for.co 20 4d 6f 7d User-Ag ent: M 3d 3d 20 4c illa/5.6 (Xii) 2d for.co 3d 3d 6d for.co 3d 3d 6d for.co 3d 3d 6d for.co 3d for.co for.co	sce 1; por m Noz L V: 100 F 5	10000 00 35 56 66 76 0010 00 3b ee dd 40 0010 60 00 e0 00 60 60 0040 67 6f 67 60 67 66 67 60 67	le 00 0c 29 a8 96 73 96 40 11 27 f9 c0 a8 55 00 27 24 14 11 64 96 04 6f 63 73 76 03 96 1C 00 01	68 96 45 96 PV 51 88 c0 88 ; 6 61 96 90 91 Q 76 65 69 94 goog) s E @ ' Q 5 ' S • o csp pki

Protocolos (Protocol) : El protocolo de paquetes (TCP, UDP, NBNS, etc.).

										*•	th0											- 0	×
File	Edit	V	iew	Go		Capt	ure	Ana	lyze	: 5	Stati	stics	5 T	Felep	hon	y y	Virele	55	Tools	He	lp		
1		A	0			-			1	~				~								-	
	— ,	10	0		L		X	C	2	Q	1		7	14	•*	~ 7	•			•	-	u	
📕 tcp	o.flags	.syn																	- 12	Ехр	ressio	n	ж.
No.	*	Tim	e			s	ource						De	stina	ation	i			Prot	locol	Len	gt	
	160	19.	628	4229	937	1	92.1	68.8	31.1	136	8		21	6.58	3.19	96.10	96		TCP	5		5	- 1
	161	19.	628	541	353	2	16.5	8.1	96.1	106			19	2.10	58.8	31.13	36		TCP		12	9	
	162	19.	628	5620	908	1	92.1	.68.8	31.1	136			21	6.58	8.19	96.10	96		TCP			5	
	163	19.	628	628	668	2	16.5	8.19	06.1	106			19	2.10	68.8	81.13	36		TLS	v1.3	6	54	
	164	19.	628	644	409	1	92.1	.68.8	31.1	136			21	6.58	8.19	96.10	96		TCP			5	
	165	19.	834	476	737	9	9.86	.47	.48				19	2.16	58.8	81.13	36		TLS	v1.2	2	22	
	166	19.	834	7080	976	1	92.1	68.8	31.1	136			99	.86	.47	.48			TCP			5	
	167	19.	834	905	635	9	9.86	.47	.48				19	2.16	58.8	81.13	36		TLS	v1.2	2	2	
	168	19.	834	924:	129	1	92.1	68.8	31.1	136			99	.86	.47	.48			TCP			5	
	170	10	838	3000	906	1	02 1	68 9	21 -	136			23	64	110	a 10			TCD			7	-
▶ Er	ame 1	170:	74	by	tes	on	wi	-e (592	bi	ts)	, 7	4 b	yte	s c	aptu	red	(592	bit	s) o	n in	terf	a(_
F.F.F	herne	∍t T	т	Src	·v	mwa	re /	คาล	n•7:	3 (ดด	001	29.	A8 -	90.	731	Dst	• Vm	ware	e6:	Ford	le (0	A
DAD	00	50	56	eñ	ŤΘ	de	00	00	29	aß	90	73	68	00	45	66	- PV				E.		
0010	00	3c	a0	35	40	00	40	06	e5	02	c0	a8	51	88	17	40	. < .	50.0	a .	0	. a		
0020	8c	13	b2	5a	00	50	03	b7	44	f5	00	00	00	00	aØ	02		Z-P	- D				
0030	fa	f0	b5	b2	00	00	02	04	05	b 4	04	02	80	0a	44	cØ					- D -		
0040	48	d9	00	00	00	00	01	03	03	07							н						
l																							

Información adicional del protocolo (info): Ejemplo: para un paquete TCP, este campo indica si es un paquete SYN, ACK o FIN.

4. Estudiar los detalles del paquete con la ventana de detalles del paquete

Google+ N	Aozilla Firefox	_ = ×
*eth0	_ = ×	
<u>File Edit View Go Capture Analyze Statistics Te</u>	elephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
@ @ ± 🗎 🛛 @ ⊂ < → .	n + + 🜉 📃 🛛 🖬 🖬	
tcp.flags.syn	Expression +	Gmail Images 🗰 Sign in
No. Time Source Dest 160 19.628422937 192.168.81.136 216		th0 _ ت x
161 19.628541353 216.58.196.106 192 162 19.628562008 192.168.81.136 216 Frame 161: 1294 bytes on wire (10352 bits), 1 Ethernet II, Src: Vmware_e5:f0:de (00:50:56:e) Internet Protocol Version 4, Src: 216.58.196. Transmission Control Protocol, Src Port: 443,	 Frame 161: 1294 bytes on wire (10) Ethernet II, Src: Vmware_e6:f0:d0 Internet Protocol Version 4, Src Transmission Control Protocol, S 	0352 bits), 1294 bytes captur∉ e (00:50:56:e6:f0:de), Dst: Vr : 216.58.196.106, Dst: 192.16{ rc Port: 443, Dst Port: 44268,
6000 00 0c 29 a8 90 73 00 50 56 c6 f0 de 08 c 6010 05 00 00 e9 00 00 80 66 39 d8 3a c4 c 6020 51 88 01 bb ac c3 73 5f a1 84 6b 88 c 6030 fa f0 bb 3b 00 00 77 63 f5 ea ac 30 06 c6 37 d5 a6 ac 30 06 c6 c7 c6 c6 c7 c7 c6 c7 c7 c6 c7 c7 c6 c7 c	0000 0000 0000 00000 77 63 75 00300 fa fg eb 30 00000 77 63 75 00400 63 76 c3 c4 76 00300 fa fg eb 30 000 000 77 63 75 00400 63 76 c3 c4 76 0000 fa 76 30 76 77 70000 76 30 30 76 30 61 12 00000 ft ft a 60	e6 f0 de 08 00 45 00) 30 d8 3a c4 6a c0 a8 a1 84 6b e8 43 50 18 Q a1 84 6b e8 43 50 18 Q a5 37 d5 a6 95 7b 62 c-YC a3 7f c3 cf 50 f1 eb b0 eb af ce c8 a2 dd

5. Ver los datos de los paquetes con la ventana de bytes de paquetes individuales

00	00	Ac	20	28	90	73	00	50	56	86	fA	de	68	00	15	00	A SPV F
	05	00	00	00	00	00	80	86	86	30	dB	3.9	00	69	c.0	28) 3 T V L
	51	00	01	hh	00	00	26	72	5f	91	94	6h	00	12	50	10	0 6c k CP
20	£0	60 fo	ab	26	au	00	30	63	-fr	al	64	00	00	40	40	10	
30	1 d	10	en	SU	00	00	11	23	10	ea	od	20	00	ou	49	02	
40	03	/e	29	43	10	es	ca	50	аг	as	31	05	ab	95	10	02	c~YCV]{D
50	ee	30	та	ar	OT	cc	C4	D4	4e	a3	(T	C3	ст	50	11	eb	·<····
60	fe	22	0e	fe	37	e3	e8	0e	41	b0	eb	af	ce	C8	a2	dd	·"··7··· A·····
70	51	05	08	a2	8b	27	ae	19	4a	c3	d1	e4	05	02	46	fc	Q J
80	78	b0	33	ba	e2	70	ac	ce	77	e6	12	1e	6e	06	2f	6e	x·3··p·· w···n·/n
90	df	4a	60	03	93	fo	hd	61	h2	86	57	88	15	dΘ	e7	hØ	·]`aW

6. Simplemente navegar por Internet

	32 	88					*eth0								_ 0 X
File	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>(</u>	apture <u>A</u>	alyze	<u>Statistic</u>	Telepho	n <u>y W</u> ireless	Tools	Help	P					
	□ 🛯 🎯	t		C	ι (⇒ ∩ ·	+ > 🌉		۵	•	0				
📕 🏼 🗛 p	ply a display fil	ter <c< td=""><th></th><th></th><td></td><td></td><td></td><td></td><td></td><th></th><th></th><th></th><td>=</td><th>Expressio</th><td>n +</td></c<>											=	Expressio	n +
No.	Time		Source			Destinatio	n	Proto	ocol	Length	Info				
7*	1 0.0000	00000	192.168	8.81.136	5	192.168.	81.2	DNS		75	Standa	rd quei	ry 0x19cf	A www.gsta	t
	20.0001	79873 95124	192.160	8.81.130 8.81.130	5	192.168.	81.2 160 164	DNS TI SU	12	205	Annlica	ra que	ny exp5d9	AAAA WWW.g	s
	4 0.0123	77016	172.217	7.160.10	54	192.168.	81.136	TCP	1.2	60	443 - 3	36006	[ACK] Sea	=1 Ack=152	W
4	5 0.0697	36603	192.168	8.81.2		192.168.	81.136	DNS		91	Standa	d que	ry respons	se 0x19cf A	
L	6 0.1431	31898	192.168	8.81.2		192.168.	81.136	DNS		103	Standa	rd quei	ry respons	se Øxb5d9 A	^
-	7.0 1441	11172	192 168	8 81 136	1	172 217	166 67	TCP	_	74	40834 -	- 443	SYN1 Sen	=0_Win=6424	0
 Fr Et In Us Do 	ame 1: 75 b hernet II, ternet Prot er Datagram main Name S	ytes o Src: V ocol V Proto ystem	n wire (mware_a8 ersion 4 col, Src (query)	600 bit: :90:73 , Src: Port: -	s), 75 (00:0c: 192.168 46429,	bytes caµ 29:a8:90 .81.136, Dst Port	otured (600 73), Dst: Dst: 192.1 53) bits) Vmware_ 168.81.2	on i _e6:f	Interf ©:d e	ace 0 (00:50:	56:e6:	f0:de)		
0000 0010 0020 0030 0040	00 50 56 00 3d a9 51 02 b5 00 00 00 69 63 03	e6 f0 ce 40 5d 00 00 00 63 6f	de 00 00 00 40 11 35 00 29 00 03 77 6d 00 00	29 a8 6d 06 24 16 77 77 0 01 00	90 73 c0 a8 19 cf 07 67 01	08 00 45 51 88 c0 01 00 00 73 74 61	00 PV a8 = 01 Q] 74 ic c	000 m 5)\$ www.	•s I Q gsta	E at					
• 2	wireshark_	eth0_20	20033015	1131_IfSQ	aC.pcapr	g	Packet	s: 631 · Di	isplay	ed: 631	(100.0%)	• Dropp	ed: 0 (0.0%) Profile: De	efault

Datos después de navegar por Internet

7. Visualización de los datos de la cabecera del paquete

								*eth0					4,9	u x
File	Edit View	Go	Capture	Analyze	<u>S</u> tatis	ics Te	lephony	Wireless	Tools	Help				
1) <u>+</u>		1	a +	÷	∩ •←	÷.						
р Ар	oly a display fi	iter <	ctrl-/>									•	Expression	*
No.	Time		Sourc	e		Dest	ination		Proto	col Ler	ngth Ir	nfo		
T	10.0000 20.0001	000000	192. 192.	168.81.1 168.81.1	.36 .36	192 192	.168.81	1.2 1.2	DNS DNS		75 S 75 S	tandard query 0x19cf A tandard query 0xb5d9 A	www.gstat AAA www.gs	I
	3 0.0119	95124	192.	168.81.1	.36	172	.217.10	50.164	TLSV	1.2	205 A	pplication Data		
1	4 0.0123	377016	172.	217.160.	164	192	.168.81	1.136	TCP		60 4	43 - 36006 [ACK] Seq=1	Ack=152 W	
	5 0.0697	36603	192.	168.81.2		192	.168.81	L.136	DNS		91 5	tandard query response	0x19ct A	-
L_	6 0.1431	31898	192.	168.81.2	26	192	.168.81	1.136	DNS	-	103 5	tandard query response	OXD5d9 AA	
_	deadland Mithel		- Anderson	100 01	-20				and the local	DIRECT PARTY	TA D			
+ Fr	ame 5: 91 b	oytes	on wire	(728 b:	its), 9	1 byte	s capti	ured (728	bits)	on int	erfac			
► Eti	nernet II,	Src:	Vmware_	e6:f0:de	e (00:5	0:56:e	6:f0:de	e), Dst: '	Vmware_	a8:90:	73 (0	00:0c:29:a8:90:73)		
▶ In	ternet Prot	tocol	Version	4, Src	: 192.1	68.81.	2, Dst	: 192.168	.81.136					
► Us	er Datagram	n Prot	ocol, S	rc Port	: 53, D	st Por	t: 464:	29						
Doi	nain Name S	System	(respo	nse)										
0000	00 0c 29	a8 90	73 00	50 56	e6 f0 (e 08 6	0 45 0	i@ · ·) · ·	s P V·	E				
0010	00 4d 05	ba 00	00 80	11 11	0b c0 a	6 51 6	2 c0 a	8 M	107	Q				
0020	00 01 00	00 00	00 03	77 77	77 07 6	7 73 7	4 61 7	u Quo.	1.9 (astat				
0040	69 63 03	63 61	6d 00	00 01	00 01 0	0 0c 0	0 01 0	0 ic co	m	goene				
0056	01 00 00	00 05	00 04	ac d9	a6 43				• • • • •	C				
• 2	wireshark_	eth0_2	0200330	151131_If	5QaC.pc	ipng		Packets	:: 631 · Di	splayed:	631 (1	00.0%) · Dropped: 0 (0.0%)	Profile: Defaul	lt

7.1 Captura de paquetes con Wireshark

7.2. Explorar la capa de interfaz de red / capa de enlace de datos



The job of the data link layer is to make the communication on the physical link reliable and efficient

7.2.2. Ver datos de tramas Ethernet capturados con Wireshark

	*eth0	
<u>File Edit View</u>	<u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
) 🛓 🛅 🔀 🧭 직 순 → ቡ +ć → 📰 📰 🗖 🗖 🖬 🖬 🖬	
📜 tcp	🛛 🗖 🚽 Expression	mac
No. Time	Source Destination Protocol Length Info	
	Wireshark-Packet 4 - eth0	- • ×
7 () Frame 4) Etherne	Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethernet II, Src: Vmware_e0:f0:de (00:50:56:e0:f0:de), Dst: Vmware_a8:90:73 (00:0C:29:a8:90:73) Enternet Protocol Version 4, Src: 172.217.160.164, Dst: 192.168.81.136 Fransmission Control Protocol, Src Port: 443, Dst Port: 36006, Seq: 1, Ack: 152, Len: 0	
Interne Transmi Transmi O	00 0c 29 a8 90 73 90 56 66 10 de 98 90 45 90 s P E 10 00 28 95 b9 90 90 90 66 65 68 ac d9 ae ac ae h	

8.1 Exploración de la capa de Internet

8.1.1. Cabecera IPv4: En la imagen de abajo

Version = 4	HL	Т	ype Of service		Total Length				
	Iden	tifica	ition	Flag	Fragment offset				
Time to	Live		Protocol	Header Checksum					
Home Ad	ldress : 1	home	agent address 13	0.45.10.20	/16				
Destinatio	on Addı	ess :	14.56.8.9/8	838					
Proto	col	S	Reserved	Header Checksum					
Destinatio	on Addı	ess n	nobile host home a	address130	.45.6.7/16				
Source A	ddress (remo	te host) 200.4.7.1	4/24					
			Pa	yload					

8.1.2. Ver los datos de la cabecera IP de un paquete TCP capturado con Wireshark



8.1.3 Ver los datos de la cabecera IP de un paquete UDP



8.1.4. Ver los datos de la cabecera IP de un paquete ARP



9 Exploración de la capa de transporte

9.1.1. Cabecera TCP: Imagen de abajo

Transmission Control Protocol (TCP) Header 20-60 bytes



9.1.2 Ver los datos de la cabecera TCP de un paquete TCP capturado con Wireshark

stury Beauty WAF\Ubuntu Modisecutiy.vrv _a8:90:73 (00:0c:29:a8:90:73)
➤ Source: Vmware_e6:T0:de (00:50:56:e6:F0:de) Type: IPv4 (0x0800) Padding: 0000000000000
<pre> Internet Protocol Version 4, Src: 172.217.160.164, Dst: 192.168.81.136 0100 = Version: 4 0101 = Header Length: 20 bytes (5) bifferentiated Services Field: 8x88 (DSCP: CS8_ECN: Not-ECT) </pre>
Total Length: 40 Identification: 0x05b9 (1465) ▶ Flags: 0x0000 Time to live: 128
Protocol: TCP (6) Header checksum: 0xd568 [validation disabled] [Header checksum status: Unverified] Source: 172.217.160.164 Destination: 192.168.81.136
Transmission Control Protocol, Src Port: 443, Dst Port: 36006, Seq: 1, Ack: 152, Len: 0
0000 00 0c 29 a8 96 73 06 50 56 66 f0 de 08 00 45 00 .).s.P VE. 0010 00 28 05 b9 06 00 88 06 d5 68 ac d9 a0 a4 c0 a8

9.1.3 Cabecera UDP: En la imagen de abajo

UDP header format <u>32 bits</u> source port length Checksum

9.1.4 Ver los datos de la cabecera UDP de un paquete UDP capturado con Wireshark



9.1.5 Comparar y contrastar IP, TCP y UDP



10. Explorar la capa de aplicación

10.1.1 Analizar un paquete HTTP



10.1.2 Analizar un paquete DNS

							*eth0						_ = ×	
File	Edit V	ew <u>G</u> o	Capture	Analyz	e <u>S</u> tatis	tics Teleph	on <u>y W</u> ireles	s <u>T</u> ools	Help					
		() <u>1</u>	. 💼 🕅		Q (+	→ ∩	• ← →•			o 🔛				
🕅 dn	5											Expression	+ mac	
No.	Tim	e×	Sourc	e		Destinati	on	Protoc	ol Len	gth Info				
-li-	575 8.5	1129643	192.:	168.81.	.2	192,168	.81.136	DNS	1	155 Standar	rd query re	sponse 0x057e	AA	
	583 8.8	16898723	192.1	168 81	136	192 168	81.2	DNS	-	73 Standar	rd query Ox	6d75 A ocso pl	i la	
	584 8.						Wireshark-	Packet 575 • et l	10					- ×
	585 8.	• Eran	e 575 · 1	55 hvte	es on wi	TE (1248)	nits) 155	hytes can	tured	(1240 bit	s) on inter	face A		
	586 8.	- Ethe	rnet II	Src: \	/mware e	-6:f0:de ()	0:50:56:e6	f0:de)	Dst: \	/mware a8:	90:73 (00:0	c:29:a8:90:73	5	
	587 8.	► De	stinatio	n: Viiw	are a8:	90:73 (00:	Bc:29:a8:90	:73)						
-	388.8.	► So	urce: Vm	ware_e	6:f0:de	(00:50:56	:e6:f0:de)							
► Fr	ame 575	Ту	pe: IPv4	(0x08	00)									
👻 Et	hernet	▶ Inte	rnet Pro	tocol \	Version	4, Src: 1	2.168.81.2	, Dst: 19	2.168.	.81.136				
•	Destin	+ User	Datagra	m Proto	ocol, Sr	c Port: 5	3, Dst Port	: 40513						
Þ	Source	So	urce Por	t: 53										
	Туре:	De	stinatio	n Port	: 40513									
× T-	+	Le	ngt <mark>h: 1</mark> 2	1										
0000	000	Ch	ecksum:	0xd01e	[unveri	ified]								
0020	51 8	[Checksum Status: Unverified]												
0030	0 00	o [Stream index: 8]												
0840	01 6	0000	00 0c 29) a8 90	73 00 1	50 56 e6	f0 de 08 00	45 00)	s P V	E			
0050	65 7													
00.01	05 0	0.11-												- feet
•	i wires	r He	φ.											se

11. Preguntas comunes

Que. 1. ¿Captura Wireshark todo el tráfico de Internet? Si es así, explica por qué. Si no es así, ¿qué tráfico captura?

Respuesta: Lo más probable es que sólo vea el tráfico en el que participa su máquina, o que se difunde a todas las máquinas.

Esto se debe a que, durante años, la mayoría de las redes LAN se han construido sobre la base de la tecnología Ethernet conmutada, a diferencia de las redes basadas en concentradores o en buses. En esas tecnologías más antiguas, todos los equipos de la LAN veían todo el tráfico, simplemente porque todos estaban conectados eléctricamente entre sí. Con Ethernet conmutada, el conmutador decide qué paquetes enviar a cada puerto. Esto hace que la red sea más rápida y ligeramente más segura.

(La Ethernet conmutada no es una muy buena medida de seguridad, porque es fácil de derrotar con el envenenamiento ARP).

Ahora bien, es posible que todavía estés en una Ethernet basada en un hub, o algo similar. Eso sólo puede ocurrir con redes de 100 Mbit/s y más lentas. Parte de la especificación de Gigabit Ethernet es un requisito para los conmutadores. No encontrarás un concentrador GigE.

También hay que tener en cuenta que las redes inalámbricas se comportan efectivamente como las LAN de antaño: todos los equipos conectados a una determinada red Wi-Fi pueden ver todo el tráfico, debido puramente a la naturaleza de la comunicación por radio. Si estás en una LAN cableada con switches gestionados y tienes acceso administrativo a esos switches, probablemente encontrarás una característica que puedes activar en ellos llamada port mirroring. Esa característica existe específicamente para restaurar el antiguo comportamiento de la LAN preconmutada: designa un puerto como especial, dirigiendo copias de todo el tráfico hacia él, incluso los paquetes que no están dirigidos a las direcciones MAC conectadas a ese puerto.

Que. 2. Escriba los filtros de Wireshark para: Ver el tráfico UDP cuando se realiza la exploración.

Respuesta: simplemente escriba UDP y presione enter, y podrá ver todos los paquetes udp que fueron capturados.

Que. 3. Vea el tráfico ICMP de cualquier dirección.

Respuesta: Para analizar el tráfico ICMP Echo Request:

1. Observe el tráfico capturado en el panel superior de la lista de paquetes de Wireshark. Busque el tráfico con ICMP como protocolo. Para ver sólo el tráfico ICMP, escriba **icmp** (en minúsculas) en el cuadro Filtro y pulse **Intro.**

2. Seleccione el primer paquete ICMP, etiquetado como Echo (ping) request.

3. Observe los detalles del paquete en el panel central de detalles del paquete de Wireshark. Observe que se trata de una trama Ethernet II / Protocolo de Internet versión 4 / Protocolo de mensajes de control de Internet.

4. Expanda el Protocolo de Mensajes de Control de Internet para ver los detalles de ICMP.

5. Observe el tipo. Observe que el tipo es 8 (solicitud de eco (ping)).

6. Seleccione Datos en el panel central de detalles de paquetes de Wireshark para resaltar la parte de datos de la trama.

7. Observe el contenido del paquete en el panel inferior de bytes de paquetes de Wireshark. Observe que Windows envía una secuencia alfabética durante las solicitudes de ping.

Que. 4. ¿Por qué los paquetes ARP no tienen cabeceras IP?

Respuesta: Aunque hay direcciones IP o de protocolo utilizadas en este mensaje, en realidad no tiene una cabecera IP. Las direcciones IP que se ven son simplemente parte de la cabecera ARP. Esto significa que los mensajes ARP no son enrutables y que los routers no pasarán el tráfico ARP a otra red.

En consecuencia, no se puede determinar la dirección MAC de un nodo que no esté en la LAN del nodo de origen.

También significa que el Ethertype en una trama Ethernet que lleva un mensaje ARP es diferente que en el tráfico de datos estándar. Esta diferencia se muestra a continuación

```
    Source: D-Link_c1:d2:01 (00:50:ba:c1:d2:01)
```

```
Туре: ІР (0х0800)
```

```
■ Internet Protocol, Src: 192.168.10.11 (192.168.10.11), Dst: 129.21.21.1 (129.21.21.1)
■ Internet Control Message Protocol
```

Que. 5. Compare y contraste las cabeceras UDP y TCP.

Respuesta:

Item	TCP	UDP
Stands For	Transmission Control Protocol	User Datagram Protocol
Protocol	Connection Oriented	Connectionless
Security	Makes Checks For Errors And	Makes Error Checking But
	Reporting	No Reporting
Data Sending	Slower	Faster
Header Size	20 Bytes	8 Bytes
Segments	Acknowledgement	No Acknowledgement
Typical Applications	- Email	- VoIP

Que. 6. ¿Los paquetes ICMP especifican un puerto? Busca en Internet y explica por qué sí o por qué no.

Respuesta: **ICMP** es un protocolo diseñado específicamente para fines de diagnóstico y **el ping** no es más que una solicitud de eco ICMP y una respuesta de eco, por lo que no existe el concepto de números de puerto en **ICMP**. Los números de **puerto** son direcciones de la capa de transporte utilizadas por algunos protocolos de transporte.