

1. Abre con Wireshark el archivo lab_-01.pcap:

a. ESTADÍSTICAS: Analiza la captura y responde:

- N° de equipos que a nivel de enlace intervienen en la captura: **en la captura hay 5 direcciones MAC. Una de ellas es la de broadcast (ff:ff:ff:ff:ff:ff) por lo que serían 4 equipos. NOTA: siendo estrictos y fijándonos en la dirección 01:00:5e:00:00:fb vemos que tiene el bit I/G a 1 y se trata de una dirección multicasta; por lo que la respuesta correcta sería 3 equipos.**
- Qué equipo a nivel de enlace es el más activo (indica n° total de paquetes, paquetes enviados y recibidos, total de Bytes, total de Bytes enviados y total de Bytes recibidos):

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:30:d4:ed:43:ad	8.358	5.640 k	4.817	5.256 k	3.541	383 k
08:00:27:c1:18:96	4.293	2.595 k	1.939	260 k	2.354	2.335 k
00:11:d8:12:56:c4	4.112	3.047 k	1.637	124 k	2.475	2.922 k
ff:ff:ff:ff:ff:ff	14	588	0	0	14	588
01:00:5e:00:00:fb	9	774	0	0	9	774

- Repite el apartado anterior para el nivel de red, TCP y UDP.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.0.101	4.283	2.595 k	1.933	260 k	2.350	2.334 k	—	—	—	—
192.168.0.1	4.080	3.040 k	1.619	123 k	2.467	2.922 k	—	—	—	—
173.194.34.8	2.560	2.537 k	1.729	2.478 k	831	58 k	United States	—	15169	GOOGLE
92.43.17.150	693	394 k	378	348 k	315	46 k	United Kingdom	Slough	198047	Host Europe GmbH
74.125.230.204	666	546 k	457	524 k	209	22 k	United States	—	15169	GOOGLE
192.168.0.100	487	37 k	201	16 k	286	20 k	—	—	—	—
74.125.230.202	391	302 k	230	288 k	161	13 k	United States	—	15169	GOOGLE
194.224.66.34	356	262 k	178	230 k	178	31 k	Spain	Santa Perpetua de Mogoda	3352	Telefonica De Espana
74.125.230.230	328	313 k	221	305 k	107	8.012	United States	—	15169	GOOGLE
74.125.230.217	319	235 k	170	215 k	149	19 k	United States	—	15169	GOOGLE
80.58.32.97	224	24 k	108	15 k	116	9.581	Spain	—	3352	Telefonica De Espana
74.125.230.201	221	155 k	120	142 k	101	12 k	United States	—	15169	GOOGLE

Nivel de red

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
173.194.34.8	80	2.560	2.537 k	1.729	2.478 k	831	58 k
192.168.0.1	36448	733	729 k	201	17 k	492	711 k
192.168.0.1	36435	733	742 k	218	16 k	515	726 k
92.43.17.150	80	693	394 k	378	348 k	315	46 k
74.125.230.204	443	666	546 k	457	524 k	209	22 k
192.168.0.1	36463	631	655 k	193	13 k	438	642 k
192.168.0.101	34208	582	494 k	175	19 k	407	474 k
194.224.66.34	80	356	262 k	178	230 k	178	31 k
74.125.230.230	80	328	313 k	221	305 k	107	8.012
74.125.230.217	80	319	235 k	170	215 k	149	19 k

Nivel de transporte TCP

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
80.58.32.97	53	218	23 k	108	15 k	110	8.733
192.168.0.1	5353	9	774	9	774	0	0
224.0.0.251	5353	9	774	0	0	9	774
192.168.0.1	51780	5	1.710	5	1.710	0	0
192.168.0.1	41101	5	395	3	237	2	158
192.168.0.1	4434	5	345	3	207	2	138
192.168.0.1	34637	5	395	3	237	2	158
192.168.0.1	4890	5	345	3	207	2	138
192.168.0.100	33566	5	1.710	0	0	5	1.710

Nivel de transporte UDP

- Indica los elementos participantes de nivel de enlace, ip, tcp y udp, de la conversación más activa en cada nivel del TCP/IP.

Wireshark · Conversations · lab-01.pcap

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
00:30:da:ed:43:ad	08:00:27:c1:18:96	4,281	2,595 k	2,349	2,334 k	1,932	
00:11:d8:12:56:c4	08:00:27:c1:18:96	14	588	14	588	0	
00:11:d8:12:56:c4	08:00:27:c1:18:96	12	952	5	434	7	
00:11:d8:12:56:c4	01:00:5e:00:00:fb	9	774	9	774	0	

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾

Ayuda Copy Follow Stream... Graph... Cerrar

Nivel de enlace: 00:30:da:ed:43:ad ↔ 08:00:27:c1:18:96

Wireshark · Conversations · lab-01.pcap

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
173.194.34.8	192.168.0.1	2,560	2,537 k	1,729	2,478 k	831	
92.43.17.150	192.168.0.101	693	394 k	378	348 k	315	
74.125.230.204	192.168.0.101	666	546 k	457	524 k	209	
192.168.0.1	192.168.0.100	487	37 k	286	20 k	201	
74.125.230.202	192.168.0.101	391	302 k	230	288 k	161	
192.168.0.101	194.224.66.34	356	262 k	178	31 k	178	
74.125.230.230	192.168.0.1	328	313 k	221	305 k	107	
74.125.230.217	192.168.0.101	319	235 k	170	215 k	149	
74.125.230.201	192.168.0.101	221	155 k	130	142 k	91	
74.125.230.108	192.168.0.101	162	101 k	91	94 k	71	

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾

Ayuda Copy Follow Stream... Graph... Cerrar

Nivel de red: 173.194.34.8 ↔ 192.168.0.1

Wireshark · Conversations · lab-01.pcap

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B
192.168.0.1	36448	173.194.34.8	80	753	729 k	261	17 k
192.168.0.1	36435	173.194.34.8	80	733	742 k	218	16 k
192.168.0.1	36463	173.194.34.8	80	631	655 k	193	13 k
192.168.0.101	34208	74.125.230.204	443	582	494 k	175	19 k
192.168.0.1	36430	173.194.34.8	80	286	271 k	101	7.138
192.168.0.101	46474	74.125.230.201	443	221	155 k	91	13 k
192.168.0.101	36402	74.125.230.202	443	213	159 k	84	7.157
192.168.0.101	58267	74.125.230.217	80	186	162 k	76	10 k
192.168.0.101	37058	74.125.230.198	443	162	101 k	71	7.737
192.168.0.1	40408	74.125.230.230	80	157	157 k	50	3.551

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾

Ayuda Copy Follow Stream... Graph... Cerrar

Nivel de transporte TCP: 192.168.0.1:36448 ↔ 173.194.34.8:80

Wireshark · Conversations · lab-01.pcap

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B
192.168.0.1	5353	224.0.0.251	5353	9	774	9	774
192.168.0.1	51780	192.168.0.100	5353	5	1,710	5	1,710
192.168.0.1	34637	80.58.32.97	53	4	316	2	158
192.168.0.1	4890	80.58.32.97	53	4	276	2	138
192.168.0.1	41101	80.58.0.33	53	3	237	2	158
192.168.0.1	4434	80.58.0.33	53	3	207	2	138
192.168.0.1	32458	80.58.32.97	53	2	160	1	72
192.168.0.1	32458	80.58.0.33	53	2	160	1	72
192.168.0.1	41414	80.58.0.33	53	2	216	1	78
192.168.0.1	36124	80.58.0.33	53	2	160	1	72

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾

Ayuda Copy Follow Stream... Graph... Cerrar

Nivel de transporte UDP: 192.168.0.1:5353 ↔ 224.0.0.251:5353

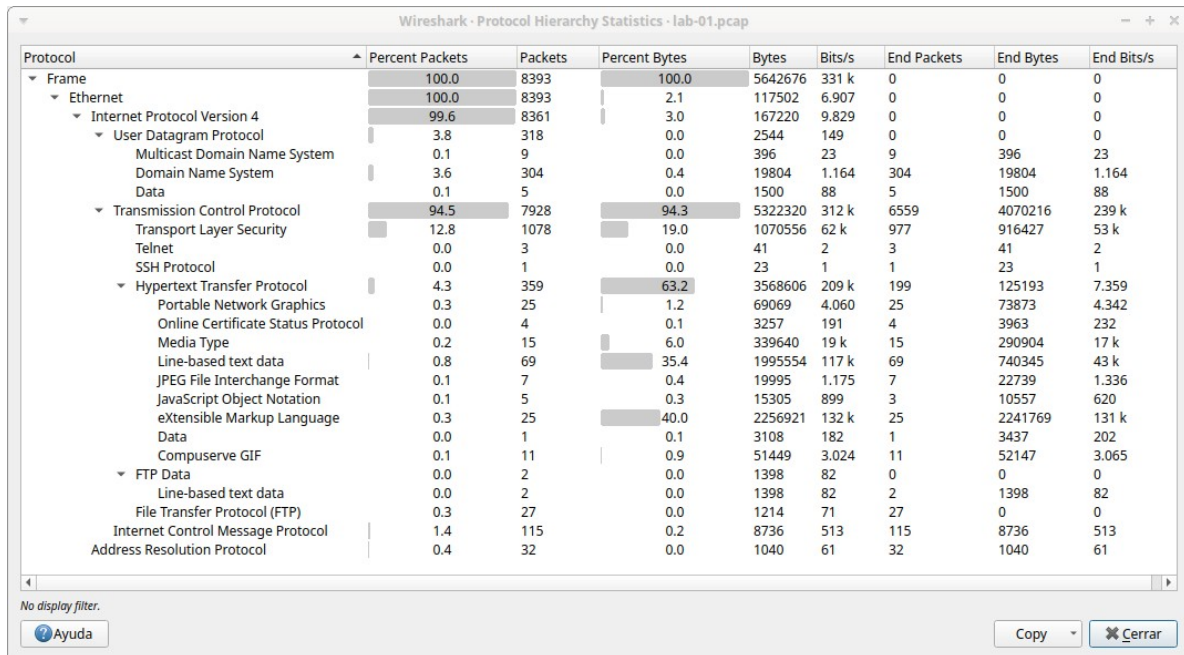
NOTAS:

- A nivel de transporte se trabaja con sockets¹ por lo que hay que indicar IP:puerto
- En el caso de UDP, la conversación más activa son envíos multicast lanzados por el equipo 192.168.0.1. Entre equipos reales sería la que aparece en segundo lugar, que

¹ Socket: <protocolo de transporte, dirección IP, puerto>. Por ejemplo: <tcp, 18.75.4.1, 443>

como se ve son dirección de tipo unicast (de equipos).

- Teniendo en cuenta la jerarquía de protocolos haz un dibujo del modelo TCP/IP usando los protocolos presentes en la captura.



Nivel aplicación	Telnet, SSH, HTTP, FTP, TLS	DNS, MDNS
Nivel de transporte	TCP	UDP
Nivel de internet	IP, ICMP, ARP	
Network interface and hardware	Ethernet	

b. Haz los siguientes DISPLAY FILTERS:

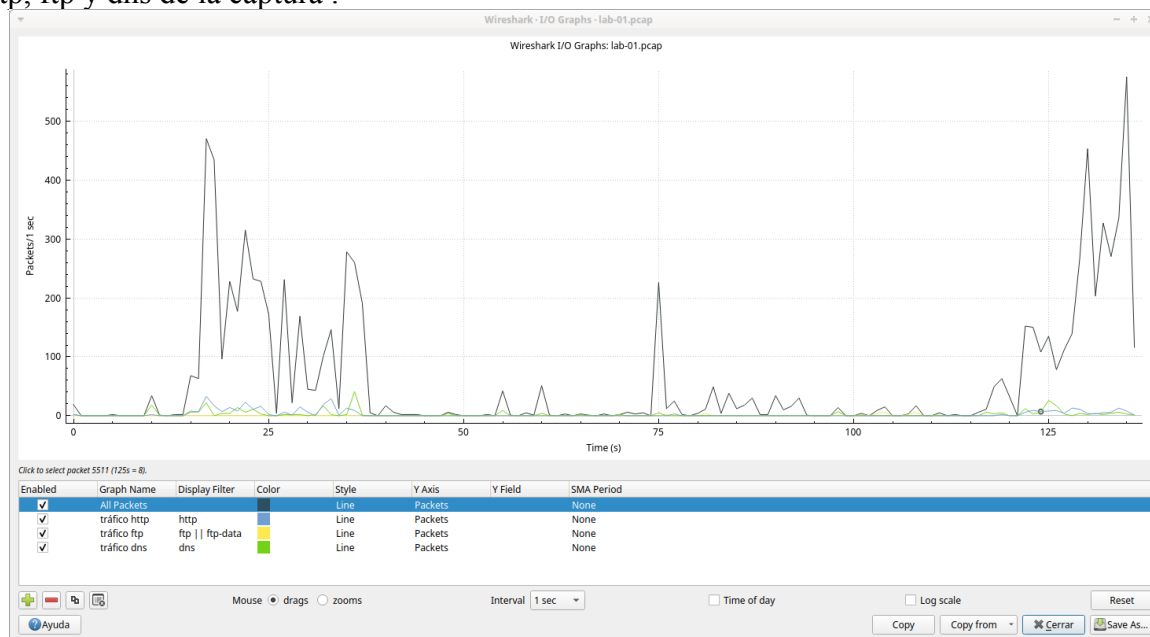
Nombre	Acción
Broadcast	eth.addr == ff:ff:ff:ff:ff:ff
Eth. origen PC1	eth.src == 00:11:d8:12:56:c4
Eth. destino PC2	eth.dst == 00:30:da:ed:43:ad
Eth. PC3	eth.addr == 01:00:5e:00:00:fb
Eth. PC2 ↔ PC3	eth.addr == 00:11:d8:12:56:c4 && eth.addr == 01:00:5e:00:00:fb
ARP	arp
ARP Request	arp.opcode == 0x0001
Eth. NO PC1	! eth.addr == 00:11:d8:12:56:c4
IP origen 50.57.203.250	ip.src == 50.57.203.250
IP destino 192.16.192.166	ip.dst == 192.16.192.166
IP_101 ↔ IP_80.58.32.97	ip.addr == 192.168.0.101 && ip.addr == 80.58.32.97
IP_80.58.32.97	ip.addr == 80.58.32.97
NO IP_80.58.32.97	! ip.addr == 80.58.32.97
ICMP	icmp
ICMP Echo Request	icmp.type == 8

ICMP Tiempo Excedido	icmp.type == 11
TTL 1	ip.ttl == 1
TTL 6	ip.ttl <= 6
ICMP IP_74 ↔ IP_1	(ip.addr == 192.168.0.100 && ip.addr == 192.168.0.20) && (icmp.type == 0 icmp.type == 8)
DNS	udp.srcport == 53
www.atareao.es	ip.dst == 92.43.17.150 && tcp.dstport == 80
Atareao.es	ip matches "atareao.es"
Atareao.es_js	http.request.full_uri matches "js\$" Siendo más estrictos: http.request.full_uri matches "\\js\$"
FTP-Control	Sol. #1: ip.addr == 192.168.0.1 && ip.addr == 130.206.1.5 && ftp Sol. #2: ip.addr == 192.168.0.1 && ip.addr == 130.206.1.5 && tcp.port==21 La diferencia está en que la Sol.#1 únicamente muestra los mensajes FTP de control que transportan datos ftp y la segunda muestra todos los mensajes incluyendo los tcp de establecimiento de conexión, fin, ...
FTP-Data	ip.addr == 192.168.0.1 && ip.addr == 130.206.1.5 && ftp-data

c. Crea, siguiendo el orden indicado, las siguientes reglas de coloreado:

Nombre	Acción
ARP	arp
Errores ICMP	icmp.type == 3 icmp.type == 11 icmp.type == 5 icmp.type == 4
ICMP	icmp
TTL	ip.ttl <= 10

d. GRÁFICOS: Haz un gráfico donde se vea a la vez la evolución temporal del tráfico de los protocolos http, ftp y dns de la captura .



e. GeoIP: Instala y activa las librerías necesarias para tener Geolocalización en Wireshark e indica el filter string para ver únicamente los paquetes enviados desde España
ip.geoip.src_country == "Spain"