

1-ARP, indicando qué relación IP-MAC se trata de establecer (nota: si no ves tráfico ARP, borra la tabla ARP de tu máquina: <https://linux-audit.com/how-to-clear-the-arp-cache-on-linux/>).

3	5.054936735	PcsCompu_19:03:00	RealtekU_12:35:02	ARP	42 Who has 10.0.2.2? Te
4	5.055017453	RealtekU_12:35:02	PcsCompu_19:03:00	ARP	60 10.0.2.2 is at 52:54
5	23.091300553	PcsCompu_19:03:00	Broadcast	ARP	42 Who has 10.0.2.2? Te
6	23.091400917	RealtekU_12:35:02	PcsCompu_19:03:00	ARP	60 10.0.2.2 is at 52:54
7	23.091404567	10.0.2.15	8.8.8.8	ICMP	98 Echo (ping) request
8	23.106117222	0.0.0.0	10.0.2.15	ICMP	98 Echo (ping) reply

Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: reply (2)	
Sender MAC address: RealtekU_12:35:02 (52:54:00:12:35:02)	
Sender IP address: 10.0.2.2	
Target MAC address: PcsCompu_19:03:00 (08:00:27:19:03:00)	
Target IP address: 10.0.2.15	

0000	08 00 27 19 03 00 52 54 00 12 35 02 08 06 00 01	..'....RT ..5.....
0010	08 00 06 04 00 02 52 54 00 12 35 02 0a 00 02 02RT ..5.....
0020	08 00 27 19 03 00 0a 00 02 0f 00 00 00 00 00 00	..'......
0030	00 00 00 00 00 00 00 00 00 00 00 00

Aquí en la captura vemos la Sender MAC address Sender IP Address, Target MAC address Target IP address, aquí tenemos la relación entre la la MAC y la IP.

2-TCP, indicando los puertos origen y destino e identificando los 3 pasos del 3 way handshake.

Aquí el three way handshake

217.853410731	10.0.2.15	35.224.170.84	TCP	74 57540 → 80 [SYN] Seq=0 Win=642
217.980051649	35.224.170.84	10.0.2.15	TCP	60 80 → 57540 [SYN, ACK] Seq=0 Ac
217.980083725	10.0.2.15	35.224.170.84	TCP	54 57540 → 80 [ACK] Seq=1 Ack=1 W
217.980202961	10.0.2.15	35.224.170.84	HTTP	141 GET / HTTP/1.1
217.980278752	35.224.170.84	10.0.2.15	TCP	60 80 → 57540 [ACK] Seq=1 Ack=88
218.109223380	35.224.170.84	10.0.2.15	HTTP	202 HTTP/1.1 204 No Content
218.109241008	10.0.2.15	35.224.170.84	TCP	54 57540 → 80 [ACK] Seq=88 Ack=14
219.100249225	10.0.2.15	35.224.170.84	TCP	54 57540 → 80 [FIN, ACK] Seq=89.1

Aquí vemos que el puerto usado de origen es el 57540 y el de destino es el 80 (HTTP)

▶ Internet Protocol version 4, Src: 10.0.2.15, Dst: 35.224.170.84
 ▶ Transmission Control Protocol, Src Port: 57540, Dst Port: 80, Seq: 0, Len: 0

3-DNS, mostrando las "preguntas" IPv4 e IPv6 , así como las respuestas.

Aquí tienes las "Preguntas"

No.	Time	Source	Destination	Protocol	Length	Info
33	127.819674508	10.0.2.15	192.168.10.1	DNS	100	Standard query 0x2b99
34	127.919321438	192.168.10.1	10.0.2.15	DNS	161	Standard query response 0x2b99
35	127.919976567	10.0.2.15	192.168.10.1	DNS	100	Standard query 0xbbbf
36	127.986819214	192.168.10.1	10.0.2.15	DNS	161	Standard query response 0xbbbf
41	217.807602769	10.0.2.15	192.168.10.1	DNS	100	Standard query 0xc55f
42	217.852967872	192.168.10.1	10.0.2.15	DNS	148	Standard query response 0xc55f
54	222.749944783	10.0.2.15	192.168.10.1	DNS	92	Standard query 0x1aa8
55	222.751963857	10.0.2.15	192.168.10.1	DNS	92	Standard query 0x9b8f
56	222.814869616	192.168.10.1	10.0.2.15	DNS	156	Standard query response 0x9b8f
57	222.822568166	192.168.10.1	10.0.2.15	DNS	148	Standard query response 0x9b8f

Frame 33: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_19:03:00 (08:00:27:19:03:00), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.10.1
 User Datagram Protocol, Src Port: 49208, Dst Port: 53

Domain Name System (query)
 Transaction ID: 0x2b99
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 1
 Queries
 ▶ connectivity-check.ubuntu.com: type AAAA, class IN
 Additional records
[\[Response In: 34\]](#)

dns

No.	Time	Source	Destination	Protocol	Length	Info
32320	425.591019880	192.168.10.1	10.0.2.15	DNS	162	Standard query response 0x5bf2
32334	425.624373132	192.168.10.1	10.0.2.15	DNS	74	Standard query response 0x5bf2
32349	425.658129624	192.168.10.1	10.0.2.15	DNS	103	Standard query response 0x5bf2
32361	425.690334084	192.168.10.1	10.0.2.15	DNS	115	Standard query response 0x5bf2
32390	425.756281462	192.168.10.1	10.0.2.15	DNS	174	Standard query response 0x5bf2
32419	425.789093706	10.0.2.15	192.168.10.1	DNS	98	Standard query 0xf9c0
32420	425.789184974	10.0.2.15	192.168.10.1	DNS	98	Standard query 0x5bf2
32421	425.789847869	192.168.10.1	10.0.2.15	DNS	109	Standard query response 0x5bf2
32442	425.825621931	192.168.10.1	10.0.2.15	DNS	174	Standard query response 0x5bf2
32500	425.885105022	192.168.10.1	10.0.2.15	DNS	144	Standard query response 0x5bf2

Frame 32531: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface enp0s3, id 0
 Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_19:03:00 (08:00:27:19:03:00)
 Internet Protocol Version 4, Src: 192.168.10.1, Dst: 10.0.2.15
 User Datagram Protocol, Src Port: 53, Dst Port: 60903

Domain Name System (response)
 Transaction ID: 0x5bf2
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 1
 Queries
 ▶ googleads.g.doubleclick.net: type AAAA, class IN
 Answers
 Additional records
[\[Request In: 32420\]](#)

0020 02 0f 00 35 ed e7 00 5c 32 b8 5b f2 81 80 00 01 ...5... 2. [.....]
 Domain Name System (dns), 84 byte(s) Packets: 34878 · Displayed: 544 (1.6%) Profile: Default