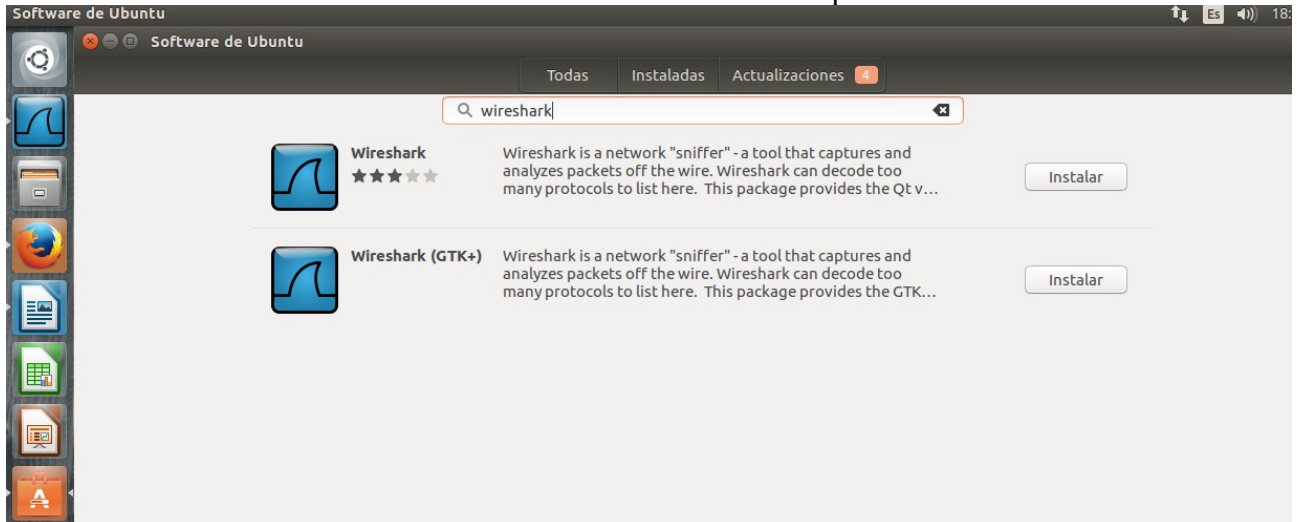


## INSTALACIÓN DE WIRESHARK EN UBUNTU:

1/ Desde software de Ubuntu lo buscamos e instalamos las dos aplicaciones:

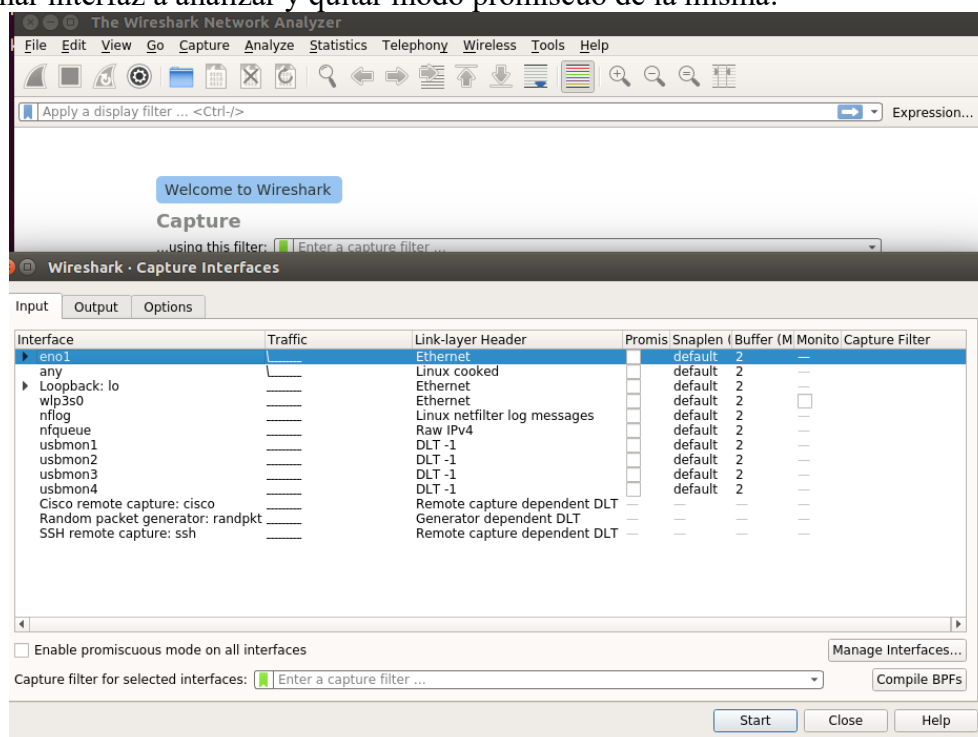


2/ Para ejecutarlo tenemos que tener permisos de administración por lo que lo hacemos con gksudo, si no está instalada esa utilidad primero habrá que instalarla:

```
$sudo apt-get install gksu
```

```
$gksudo wireshark
```

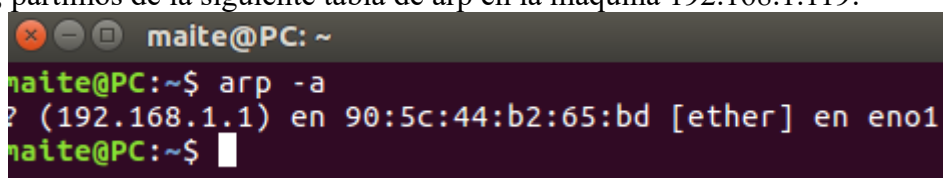
3/ Seleccionar interfaz a analizar y quitar modo promiscuo de la misma:



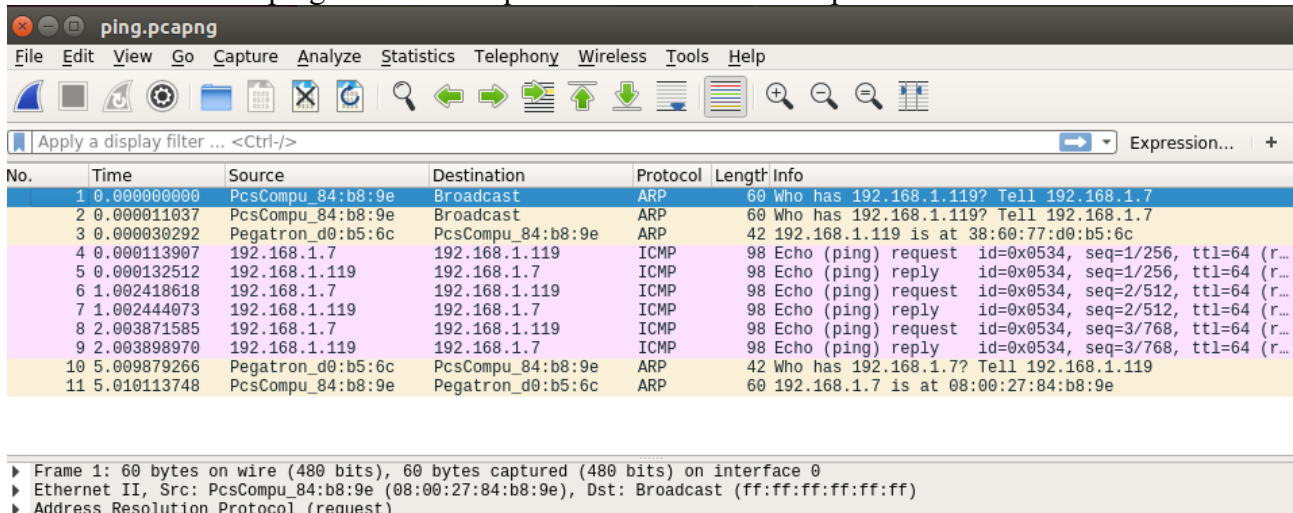
4/ Una vez seleccionada la interfaz comenzad el análisis pulsando START

Previamente dejar preparado en otra máquina la petición que queramos que realice, por ejemplo un ping a la máquina en donde estamos ejecutando el wireshark:

Por ejemplo, partimos de la siguiente tabla de arp en la máquina 192.168.1.119:



Y vamos a hacer un ping a nuestra máquina desde una MV con ip 192.168.1.7:



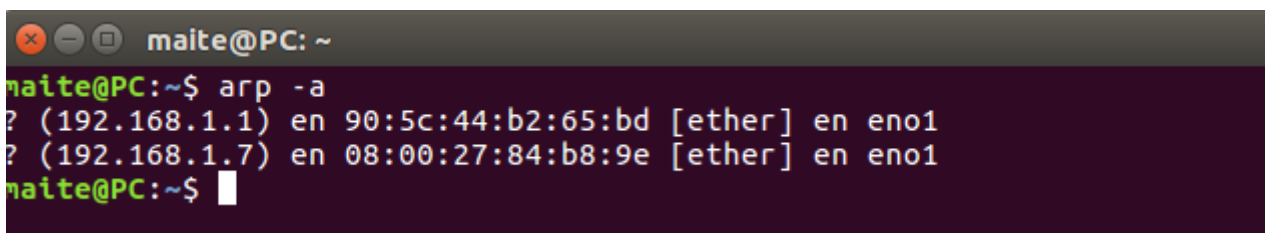
The image shows a Wireshark capture titled 'ping.pcapng'. The packet list shows 11 packets. The first three are ARP requests and replies for 192.168.1.119. The next three are ICMP echo requests and replies. The last five are ARP requests and replies for 192.168.1.7. The packet details pane shows the first packet is an ARP request from PcsCompu\_84:b8:9e to Broadcast.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_84:b8:9e	Broadcast	ARP	60	Who has 192.168.1.119? Tell 192.168.1.7
2	0.000011037	PcsCompu_84:b8:9e	Broadcast	ARP	60	Who has 192.168.1.119? Tell 192.168.1.7
3	0.000030292	Pegatron_d0:b5:6c	PcsCompu_84:b8:9e	ARP	42	192.168.1.119 is at 38:60:77:d0:b5:6c
4	0.000113907	192.168.1.7	192.168.1.119	ICMP	98	Echo (ping) request id=0x0534, seq=1/256, ttl=64 (r...
5	0.000132512	192.168.1.119	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0534, seq=1/256, ttl=64 (r...
6	1.002418618	192.168.1.7	192.168.1.119	ICMP	98	Echo (ping) request id=0x0534, seq=2/512, ttl=64 (r...
7	1.002444073	192.168.1.119	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0534, seq=2/512, ttl=64 (r...
8	2.003871585	192.168.1.7	192.168.1.119	ICMP	98	Echo (ping) request id=0x0534, seq=3/768, ttl=64 (r...
9	2.003898970	192.168.1.119	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0534, seq=3/768, ttl=64 (r...
10	5.009879266	Pegatron_d0:b5:6c	PcsCompu_84:b8:9e	ARP	42	Who has 192.168.1.7? Tell 192.168.1.119
11	5.010113748	PcsCompu_84:b8:9e	Pegatron_d0:b5:6c	ARP	60	192.168.1.7 is at 08:00:27:84:b8:9e

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: PcsCompu\_84:b8:9e (08:00:27:84:b8:9e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Address Resolution Protocol (request)

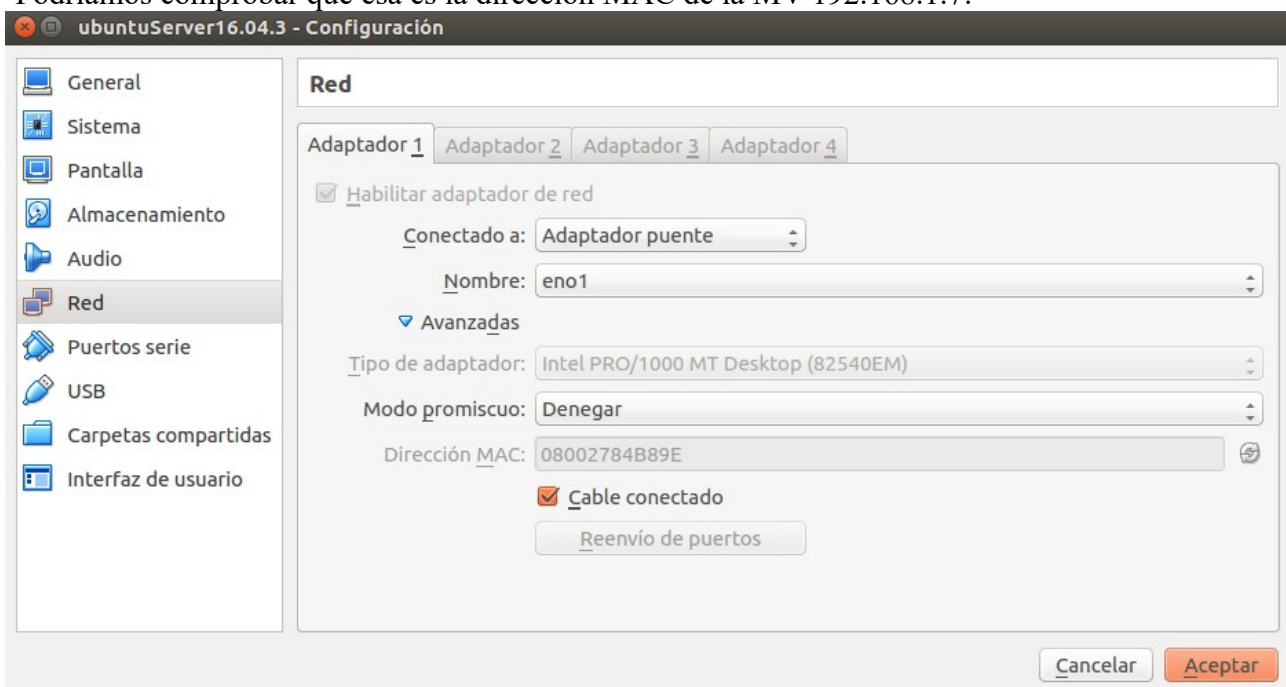
Hay que observar como antes de producirse la petición de eco (protocolo ICMP) el equipo 192.168.1.7 que es el que hace el ping está enviando un broadcast a la red para ver si alguien conoce la MAC del equipo 192.168.1.119 (petición ARP) y en la siguiente trama se observa como el equipo 119 le contesta cuál es su MAC, una vez determinada la MAC del equipo destino ya se puede lanzar la petición de eco mediante el protocolo ICMP, en este caso se han enviado 3 paquetes.

Si ahora volvemos a lanzar el comando arp -a, veremos que la tabla de ARP se ha ido rellenando con más asociaciones IP-MAC:



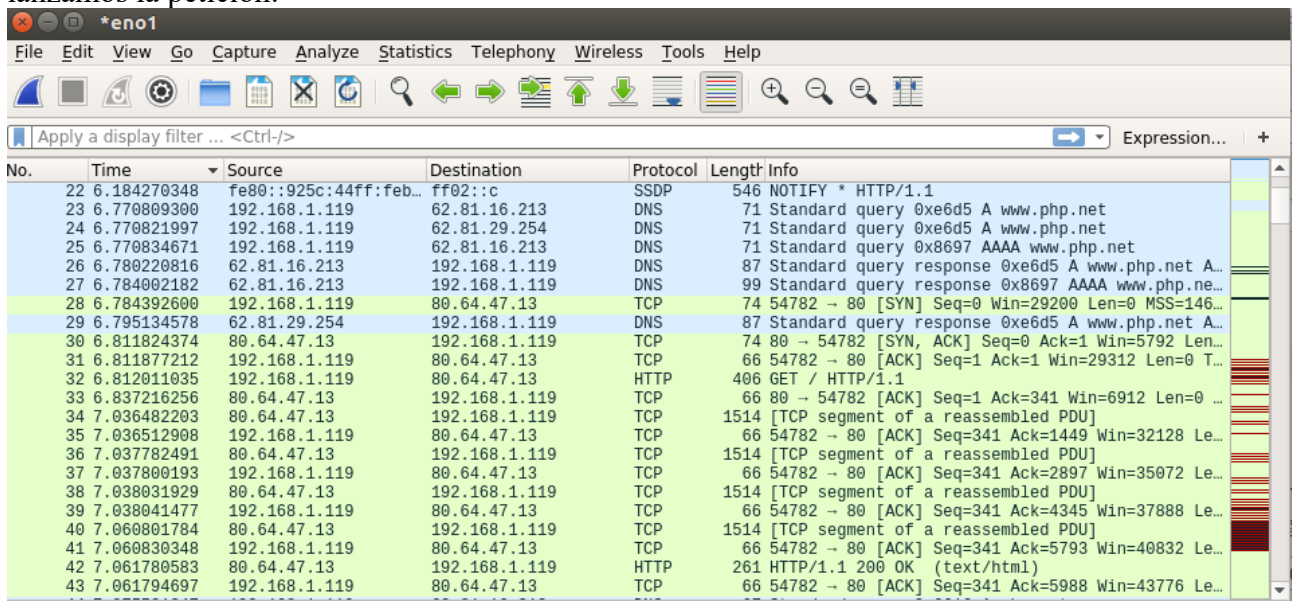
```
maite@PC: ~  
maite@PC:~$ arp -a  
? (192.168.1.1) en 90:5c:44:b2:65:bd [ether] en eno1  
? (192.168.1.7) en 08:00:27:84:b8:9e [ether] en eno1  
maite@PC:~$
```

Podríamos comprobar que esa es la dirección MAC de la MV 192.168.1.7:



Probemos realizar ahora una petición http desde el navegador:

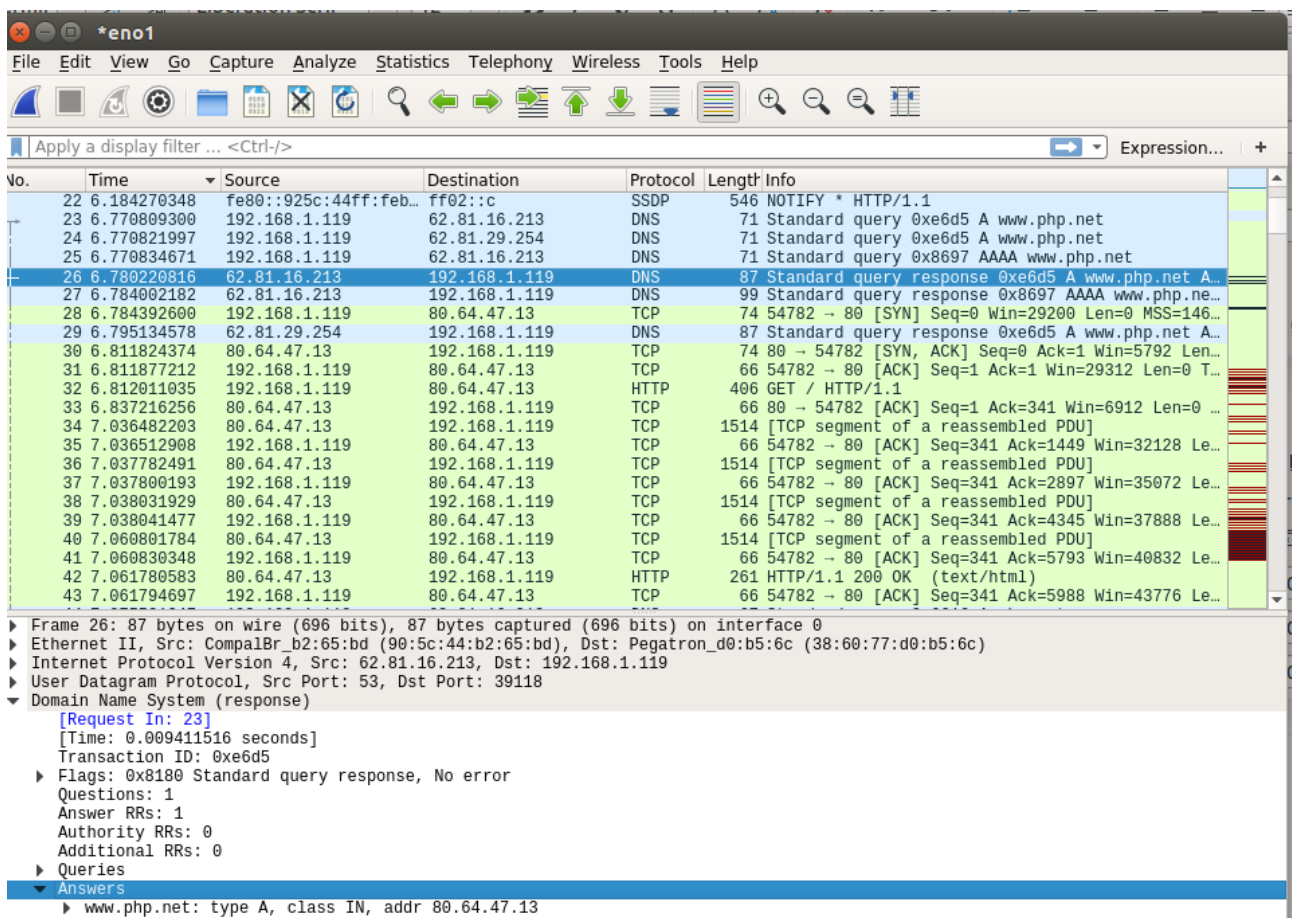
Dejamos preparada la petición en el navegador, volvemos a pulsar en START y rápidamente lanzamos la petición:



The screenshot shows a Wireshark packet capture with the following table of packets:

No.	Time	Source	Destination	Protocol	Length	Info
22	6.184270348	fe80::925c:44ff:feb...	ff02::c	SSDP	546	NOTIFY * HTTP/1.1
23	6.770809300	192.168.1.119	62.81.16.213	DNS	71	Standard query 0xe6d5 A www.php.net
24	6.770821997	192.168.1.119	62.81.29.254	DNS	71	Standard query 0xe6d5 A www.php.net
25	6.770834671	192.168.1.119	62.81.16.213	DNS	71	Standard query 0x8697 AAAA www.php.net
26	6.780220816	62.81.16.213	192.168.1.119	DNS	87	Standard query response 0xe6d5 A www.php.net A...
27	6.784002182	62.81.16.213	192.168.1.119	DNS	99	Standard query response 0x8697 AAAA www.php.ne...
28	6.784392600	192.168.1.119	80.64.47.13	TCP	74	54782 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=146...
29	6.795134578	62.81.29.254	192.168.1.119	DNS	87	Standard query response 0xe6d5 A www.php.net A...
30	6.811824374	80.64.47.13	192.168.1.119	TCP	74	80 → 54782 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=...
31	6.811877212	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 T...
32	6.812011035	192.168.1.119	80.64.47.13	HTTP	406	GET / HTTP/1.1
33	6.837216256	80.64.47.13	192.168.1.119	TCP	66	80 → 54782 [ACK] Seq=1 Ack=341 Win=6912 Len=0 ...
34	7.036482203	80.64.47.13	192.168.1.119	TCP	1514	[TCP segment of a reassembled PDU]
35	7.036512908	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK] Seq=341 Ack=1449 Win=32128 Le...
36	7.037782491	80.64.47.13	192.168.1.119	TCP	1514	[TCP segment of a reassembled PDU]
37	7.037800193	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK] Seq=341 Ack=2897 Win=35072 Le...
38	7.038031929	80.64.47.13	192.168.1.119	TCP	1514	[TCP segment of a reassembled PDU]
39	7.038041477	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK] Seq=341 Ack=4345 Win=37888 Le...
40	7.060801784	80.64.47.13	192.168.1.119	TCP	1514	[TCP segment of a reassembled PDU]
41	7.060830348	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK] Seq=341 Ack=5793 Win=40832 Le...
42	7.061780583	80.64.47.13	192.168.1.119	HTTP	261	HTTP/1.1 200 OK (text/html)
43	7.061794697	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK] Seq=341 Ack=5988 Win=43776 Le...

Observamos como antes de producirse la conexión a nivel de la capa de transporte (TCP) se ha producido una petición DNS ya que conocemos el nombre de dominio [www.php.net](http://www.php.net) pero no su dirección IP, en este caso el servidor DNS que se está utilizando no es el 8.8.8.8 si no el proporcionado por la empresa de telefonía (62.81.16.213 y 62.81.29.254) y el servicio DNS contesta proporcionando la dirección IP de php.net (80.64.47.13)



The screenshot shows the same Wireshark packet capture, but with the packet details pane expanded for packet 26. The details are as follows:

- Frame 26: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
- Ethernet II, Src: CompalBr\_b2:65:bd (90:5c:44:b2:65:bd), Dst: Pegatron\_d0:b5:6c (38:60:77:d0:b5:6c)
- Internet Protocol Version 4, Src: 62.81.16.213, Dst: 192.168.1.119
- User Datagram Protocol, Src Port: 53, Dst Port: 39118
- Domain Name System (response)
  - [Request In: 23]
  - [Time: 0.009411516 seconds]
  - Transaction ID: 0xe6d5
  - Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 1
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
  - Answers
    - www.php.net: type A, class IN, addr 80.64.47.13

23	6.770809300	192.168.1.119	62.81.16.213	DNS	71	Standard query 0xe6d5 A <a href="http://www.php.net">www.php.net</a>
26	6.780220816	62.81.16.213	192.168.1.119	DNS	87	Standard query response 0xe6d5 A <a href="http://www.php.net">www.php.net</a> A 80.64.47.13

A partir de ese momento ya se puede establecer la conexión TCP mediante el saludo de tres vías:  
El equipo 192.168.1.119 le envía un datagrama SYN al servidor de php (80.64.47.13), éste le envía a nuestro equipo SYN y ACK y finalmente nuestro equipo le envía ACK quedando establecida la conexión.

28	6.784392600	192.168.1.119	80.64.47.13	TCP	74	54782 → 80 [SYN]
30	6.811824374	80.64.47.13	192.168.1.119	TCP	74	80 → 54782 [SYN, ACK]
31	6.811877212	192.168.1.119	80.64.47.13	TCP	66	54782 → 80 [ACK]

Finalmente se envía el mensaje http de petición:

32	6.812011035	192.168.1.119	80.64.47.13	HTTP	406	GET / HTTP/1.1
----	-------------	---------------	-------------	------	-----	----------------

GET / HTTP/1.1

Host: www.php.net

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:56.0) Gecko/20100101 Firefox/56.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: es-ES;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Connection: keep-alive

Y se recibe la respuesta:

42	7.061780583	80.64.47.13	192.168.1.119	HTTP	261	HTTP/1.1 200 OK (text/html)
----	-------------	-------------	---------------	------	-----	-----------------------------

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Tue, 17 Oct 2017 18:00:13 GMT\r\n
    Server: Apache\r\n
    X-Powered-By: PHP/5.3.3-7+squeeze27\r\n
    Last-Modified: Tue, 17 Oct 2017 16:50:11 GMT\r\n
    Content-language: en\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    Set-Cookie: COUNTRY=NA%2C62.83.121.209; expires=Tue, 24-Oct-2017 18:00:13 GMT; path=/; domain=.php.net\r\n
    Set-Cookie: LAST_NEWS=1508263213; expires=Wed, 17-Oct-2018 18:00:13 GMT; path=/; domain=.php.net\r\n
    Link: <http://php.net/index>; rel=shorturl\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
  Content-Length: 5370\r\n
  Keep-Alive: timeout=2, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=utf-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.249769548 seconds]
[Request in frame: 32]
Content-encoded entity body (gzip): 5370 bytes -> 29054 bytes
File Data: 29054 bytes

```

```
GET / HTTP/1.1
Host: www.php.net
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES;es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Tue, 17 Oct 2017 18:00:13 GMT
Server: Apache
X-Powered-By: PHP/5.3.3-7+squeeze27
Last-Modified: Tue, 17 Oct 2017 16:50:11 GMT
Content-language: en
X-Frame-Options: SAMEORIGIN
Set-Cookie: COUNTRY=NA%2C62.83.121.209; expires=Tue, 24-Oct-2017 18:00:13 GMT;
path=/; domain=.php.net
Set-Cookie: LAST_NEWS=1508263213; expires=Wed, 17-Oct-2018 18:00:13 GMT; path=/;
domain=.php.net
Link: <http://php.net/index>; rel=shorturl
Content-Encoding: gzip
Vary: Accept-Encoding
Content-Length: 5370
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

```
.....W.o.6.....v...]k..5i.`X...0.}.I.Y.,...|...
(.v.....b...#)R"=;.....g.t..02."J*.G.s..4]....e..2=..f...DDR...#P.....!
Y...VRc..Q..x.....J....E.i.@..ZpW..V.A.....T..Q   .ar..Ik.   'a~...
....8.8ra.6....di.A.L
uE..<.%d.#..F.4P.1.e.(piAW~5..w{W..aeD.Z.#Z.R0..V..A.U...Q{.....6../Q..
+.A3..!.....qN0:/L.:7}...Q..>w...=.....<A..`M...*.....5vW..
[ycTi.....d.s..s...1.....
.H...Lv....[.~.|.)...lFY.2...../0^N..U.....M?.C...I.T...m1..
>.)|...`u...e.....9.N...G.?./u%T./f.....^.....z.....^.....t.....,....`i..
3r...)..Qgr...5.Q.&.N.[G..@qQ|..=.L[_...k...h...c..N...W.P-'..4..U.
.....=.....?.....m.Uri..=q...59.....[.$...c..vU....9(.#.."......W\..
....x.V7.b....a.C.V
.h.`...U.o2Q-.....K.p....b....2"aV....+.....GmxYJ;K.#.GE..@5..r)!..k
$.zQ.....>/x...B.]G....;vL...g#..+V...rL.i...R).Te6$.T...qm.}.....a.
%.....#...`.....@.7u....W.Mu+.....')..{.
0.t...Rp.G.....#...A.G#..._....k.|[...-?..
0  2(  F  \  S  a  \  -  X  U  T  U  >  0  3  3  i  a  U
```

3 client pkt(s), 7 server pkt(s), 3 turn(s).

Entire conversation (6327 bytes)

Show and save data as

ASCII

Stream

2

Find:

Find Next

Filter Out This Stream

Print

Save as...

Back

Close

Help