

DAW 2 - 18/09/2019

WIRESHARK

JORGE MARTÍN GARCÍA



Introducción

Pasos:

- Instalar wireshark. (incluir la captura de que está instalado, así como todas en las que has modificado algún parámetro. Si has pulsado solo siguiente, no incluirla).
 - Iniciar la captura de tramas con el wireshark
 - Acceder a una página web.
-

- Parar la captura de tramas.

- Localizar las dos tramas correspondientes a la solicitud del servidor (GET), y la respuesta del servidor.

Documentación:

- Capturas de pantalla, y descripción del proceso realizado.

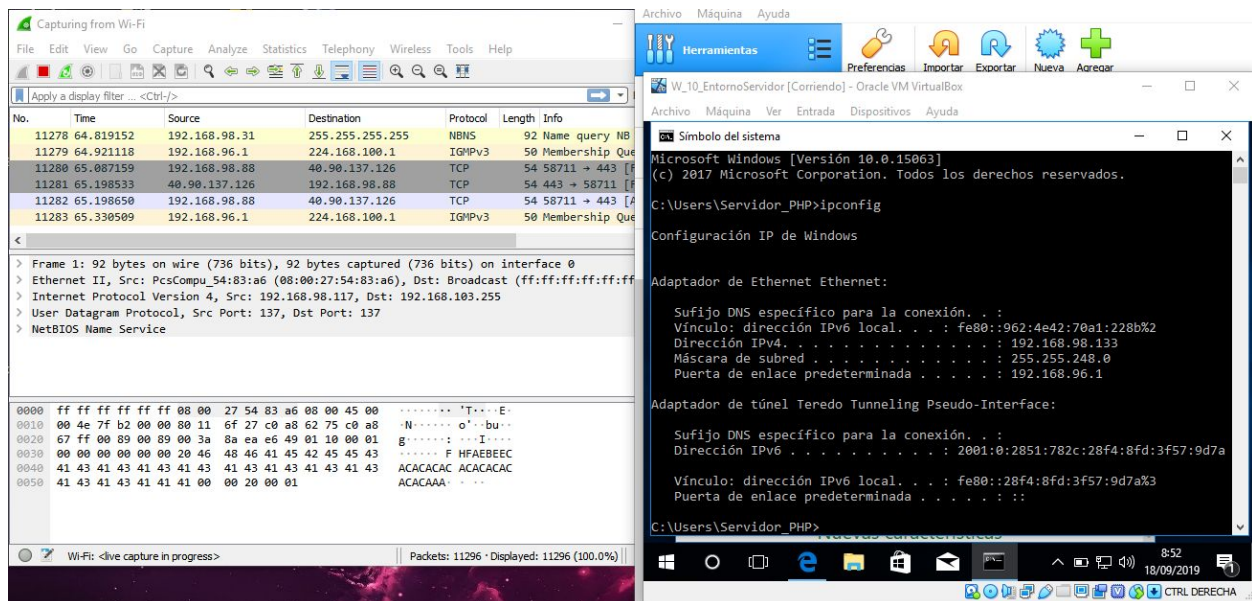
- Captura de pantalla de las tramas relacionadas.

- guardar el archivo de las tramas de wireshark, para revisarlo después.

Capturas:

Primero entramos en Wireshark, en la red WI-FI que es la que estoy usando en mi caso.

Miramos la IP de la VM, que está en modo bridge.



Filtramos en wireshark con ip.addr y http.request.method para buscar solamente los GET de la IP de mi VM.

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows several HTTP GET requests from 192.168.98.133 to 93.184.220.29. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
8650	-343.344579	192.168.98.133	93.184.220.29	HTTP	294	GET //MFewTzBNMEswSTA3gUgUgKCGUA88TBL0V27RVZ7LBduom%2FnyB45SPUEwQUSZ1ZNIJH%ys%28ghUNoZ70rUETFACEAtqs7A%28sanZ...
8924	-340.015093	192.168.98.133	93.184.220.29	HTTP	290	GET //MFewTzBNMEswSTA3gUgUgKCGUA88TBL0V27RVZ7LBduom%2FnyB45SPUEwQUSZ1ZNIJH%ys%28ghUNoZ70rUETFACEAtqs7A%28sanZ...
9089	-332.884700	192.168.98.133	13.107.4.52	HTTP	142	GET /connecttest.txt HTTP/1.1
9867	-320.679359	192.168.98.133	205.185.216.10	HTTP	303	GET /d/msdownload/update/others/2019/09/29921747_16ac0a065a4ddel1bd8263d4a5a88c3468ee7f6f4.cab HTTP/1.1
9880	-320.670062	192.168.98.133	205.185.216.10	HTTP	303	GET /d/msdownload/update/others/2019/09/29921746_534f7678e7390145f56470b67e4bc36ae18e256a.cab HTTP/1.1
9890	-320.659620	192.168.98.133	205.185.216.10	HTTP	303	GET /d/msdownload/update/others/2019/09/29921289_31d04062f939d92a21c329d7b3ccca08007c1225.cab HTTP/1.1
9956	-320.360603	192.168.98.133	205.185.216.10	HTTP	303	GET /d/msdownload/update/others/2019/09/29921288_acf4a09bd8d671e048920b64e0f9a0bbd2c2164e2.cab HTTP/1.1
9970	-320.349657	192.168.98.133	205.185.216.10	HTTP	303	GET /c/msdownload/update/others/2019/09/29924229_f3689816cbae42f03f47f47d86019141d0d6815c.cab HTTP/1.1
10047	-320.229258	192.168.98.133	205.185.216.10	HTTP	303	GET /d/msdownload/update/others/2019/09/29923475_433ff098b80aa849e82885068d23cac13e131732.cab HTTP/1.1
10168	-319.612871	192.168.98.133	205.185.216.10	HTTP	303	GET /c/msdownload/update/others/2019/09/29922922_c76c15bee0ee2514081152b436f66df1a37a0468.cab HTTP/1.1

Frame 8650: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
 Ethernet II, Src: HonHaiPr_93:73:0f (70:77:81:93:73:0f), Dst: Tp-LinkT_ed:ee:4c (ec:08:6b:ed:ee:4c)
 Internet Protocol Version 4, Src: 192.168.98.133, Dst: 93.184.220.29
 Transmission Control Protocol, Src Port: 49804, Dst Port: 80, Seq: 1, Ack: 1, Len: 240
 Hypertext Transfer Protocol

Adaptador de Ethernet Ethernet:
 Sufijo DNS específico para la conexión. . . :
 Vínculo: dirección IPv6 local. . . : fe80::962:4e42:70a1:228b%2
 Dirección IPv4. : 192.168.98.133
 Máscara de subred. : 255.255.248.0
 Puerta de enlace predeterminada. : 192.168.96.1

Adaptador de túnel Teredo Tunneling Pseudo-Interface:
 Sufijo DNS específico para la conexión. . . :
 Dirección IPv6. : 2001::2851:782c:28f4:8fd:3f57:9d70
 Vínculo: dirección IPv6 local. . . : fe80::28f4:8fd:3f57:9d7a%3
 Puerta de enlace predeterminada. : ::

Paramos la captura de tramas, y listo.