

Se hace en VM a menos que vaya a ser versión estable.

**Operación con sniffers:
Wireshark, Microsoft Network
Monitor y NetworkMiner
TCPDUMP
Capturas en Windows
NTOPNG para Linux**



Alfredo Abad
PARP401-Sniffers.pptx
UA: 7-nov-2022

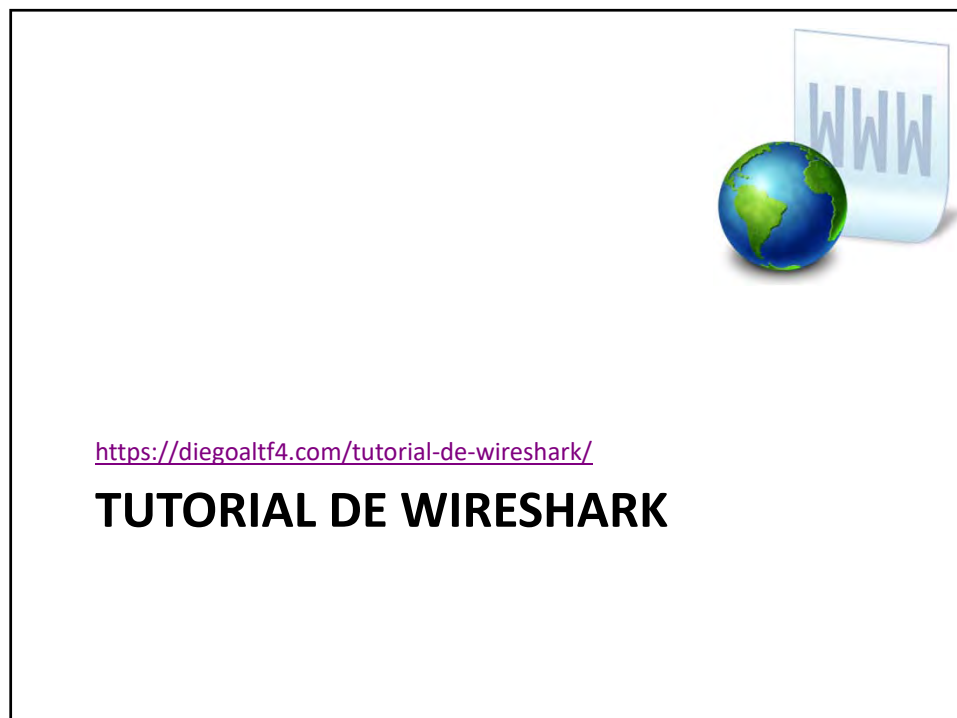
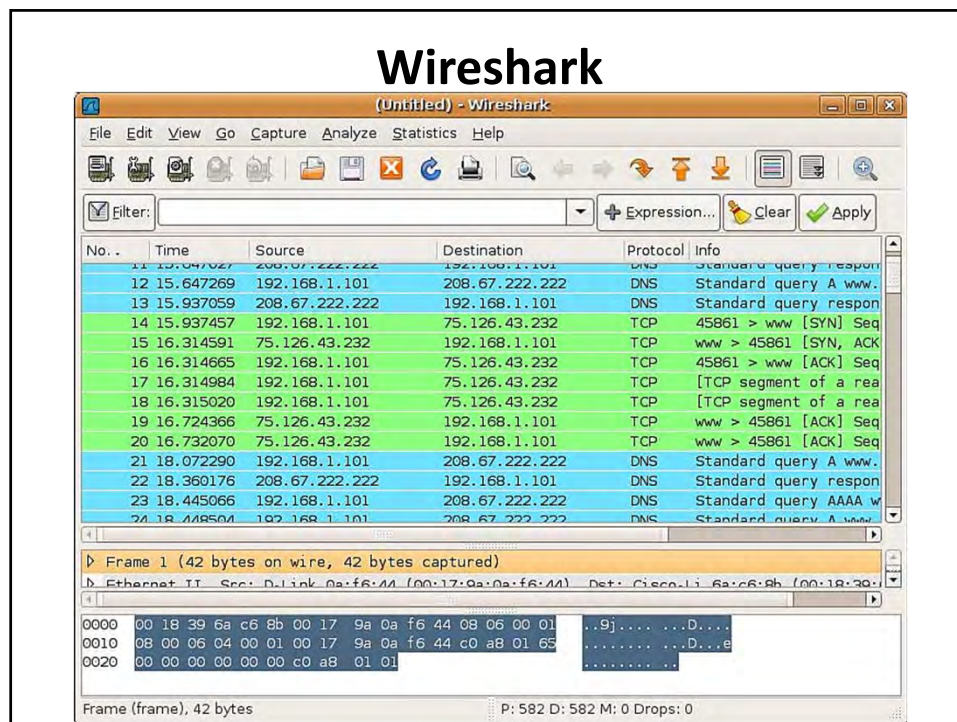
**Primera parte:
Wireshark, Microsoft Network
Monitor y NetworkMiner**

Objetivo de la práctica

- Conocer algunos de los escuchadores de red (sniffers) más comunes en la gestión de redes
- Determinar las condiciones necesarias para la escucha de la red
- Trabajar con ficheros de captura en formatos estándar
- Aprender a buscar información concreta dentro de los ficheros de captura
- Tomar conciencia de la necesidad de una ética profesional

Materiales necesarios para la operación

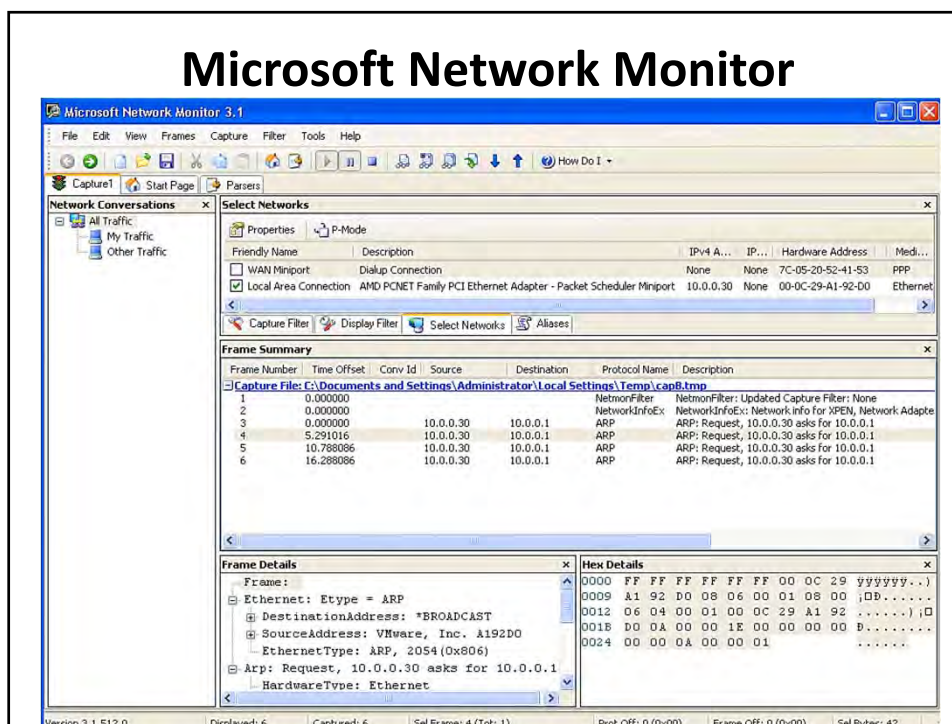
- Una máquina virtual Ubuntu y otra Windows ^{Mejor Desktop}
- Software gratuito: WinPcap <sup>Antivirus desactivado
Dentro de la VM</sup>
 - Puede descargarse de <https://www.winpcap.org/>
- Escuchadores de red: utilizaremos los tres siguientes
 - Wireshark (open source)
 - Puede descargarse de <https://www.wireshark.org/> para Windows o del repositorio estándar de Ubuntu
 - Nota: hay una versión derivada de Wireshark para línea de comandos en Linux: **Tshark**
 - Más info en <https://noticiasseguridad.com/tutoriales/un-analizador-de-paquetes-ligero-y-facil-de-usar-tshark/>
 - Microsoft Network Monitor (propietario, pero gratuito)
 - Puede descargarse de la web de Microsoft 3.4 (<https://www.microsoft.com/downloads/en/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f&displaylang=en>)
 - NetworkMiner (freeware, sólo para Windows)
 - Puede descargarse desde <https://networkminer.sourceforge.net/>
 - Se puede instalar en GNU/Linux a través de Wine (para ello, buscar información en Internet)



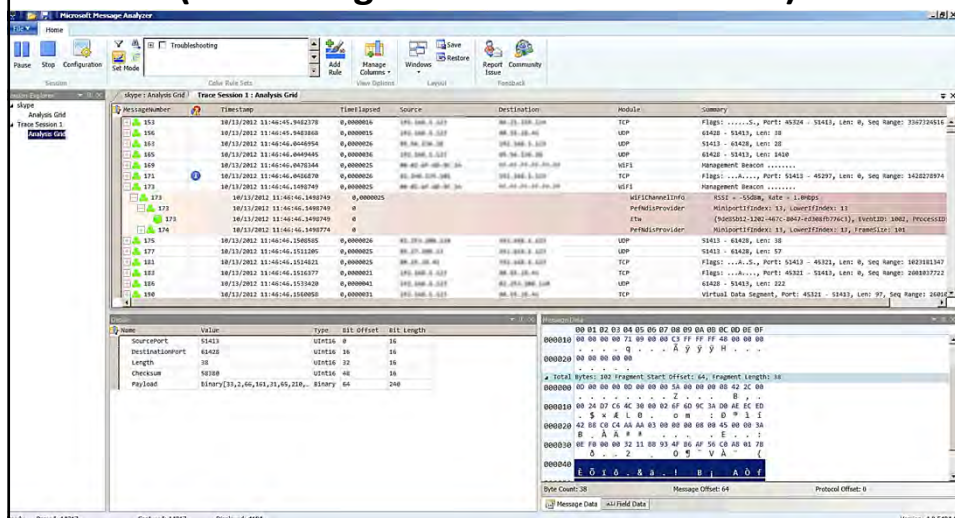


<https://noticiasseguridad.com/importantes/como-interceptar-el-trafico-de-usb/>

CÓMO INTERCEPTAR EL TRÁFICO DE USB UTILIZANDO WIRESHARK



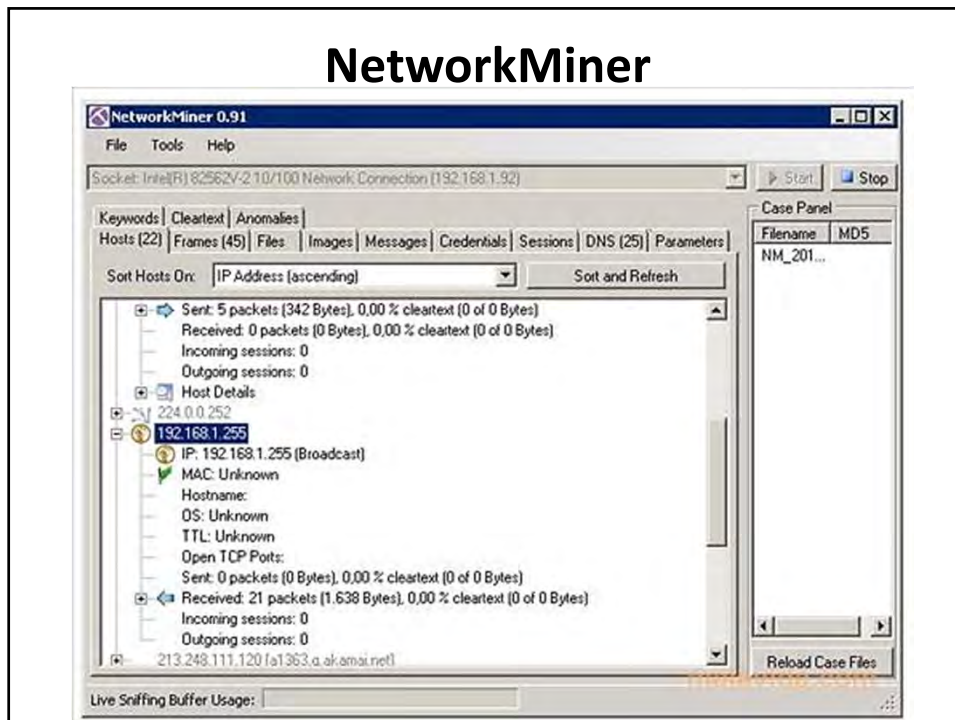
Hay una nueva versión (sucesor de Network Monitor) que se denomina Microsoft Message Analyzer, compatible con W10 (se descarga de Microsoft Connect)



<https://www.microsoft.com/en-us/download/details.aspx?id=4865>

DESCARGA E INFORMACIÓN DE MICROSOFT NETWORK MONITOR

NetworkMiner



<https://www.netresec.com/index.ashx?page=NetworkMiner>

**DESCARGA E INFORMACIÓN DE
NETRESEC NETWORKMINER**



- Total Network Monitor: <https://www.softinventive.com/total-network-monitor/>
- OpenNMS: <https://www.opennms.com/>
- PRTG Network Monitor: <https://www.paessler.com/prtg>
- Free Network Analyzer:
https://www.colasoft.com/download/products/capsa_free.php

OTRAS HERRAMIENTAS Y MONITORES ALTERNATIVOS

Operación

- Sobre una máquina virtual limpia instala el escuchador de red
 - Cuando instales NetworkMiner deberás instalar previamente las librerías WinPcap
 - Los otros dos escuchadores instalan de serie las librerías que necesitan
- Genera tráfico de red mediante ping, telnet, http, etcétera y visualiza el contenido capturado con el escuchador de red
 - Estudia todas las posibilidades del escuchador
- Repite esta operación para los tres escuchadores y familiarízate con ellos
 - En el caso de NetworkMiner y Microsoft Network Monitor sólo podrás trabajar con ellos en Windows
 - En el caso de Wireshark, deberás poder trabajar en Windows y en GNU/Linux
- Como opción avanzada, busca información en Internet sobre cómo instalar NetworkMiner en Ubuntu y procede a ello
 - Antes, tendrás que averiguar para qué sirve y cómo se usa Wine

<https://windowserver.wordpress.com/2014/08/05/windows-server-2012-r2-resolucion-de-nombres-de-mquina-incluye-capturas-de-red-explicadas/>

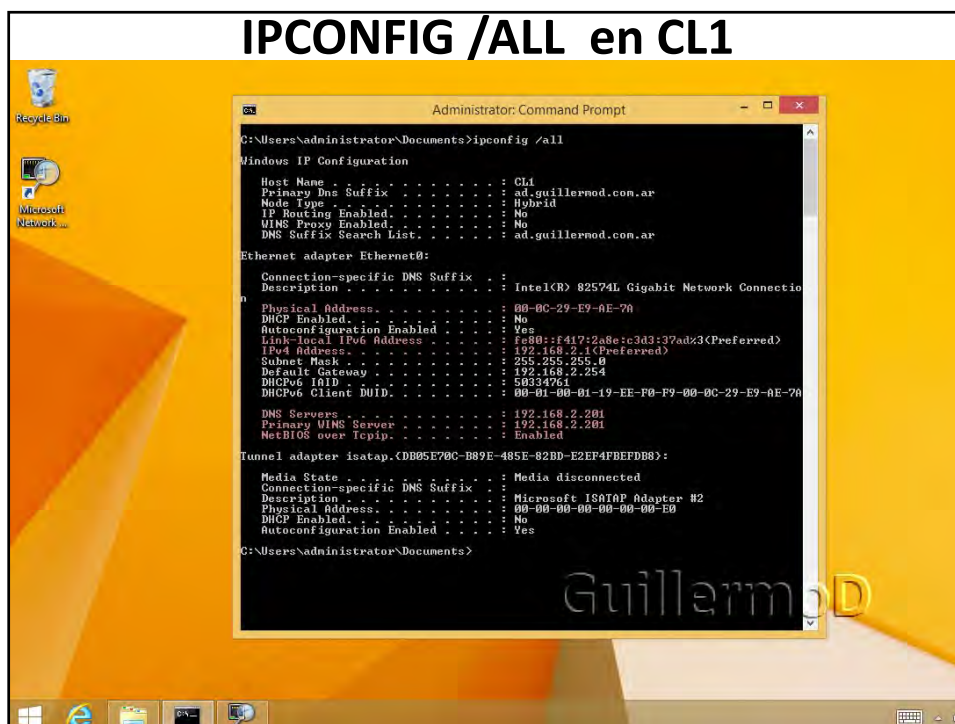
EJEMPLO: RESOLUCIÓN DE NOMBRES DE SISTEMAS EN WINDOWS VISTOS DESDE WIRESHARK

Contexto tecnológico

- Se conoce con “Resolución de Nombres de Máquina” al procedimiento por el cual cuando una máquina quiere contactar a otra, usando el nombre de destino, debe resolver cuál es la dirección IP de la máquina de destino
- La posible complicación, es que en realidad, y por omisión, cada máquina perteneciente a un Dominio Active Directory tiene dos nombres que pueden ser diferentes: el nombre NetBIOS, y el “Hostname” que forma parte del FQDN (“Fully Qualified Domain Name”)
 - Para aclarar y por las dudas, si el “Hostname” es servidor, el FQDN es servidor.dominio.sufijo
- Además hay que tener en cuenta que hay métodos para resolución de nombres NetBIOS, y otros diferentes para resolver “Hostnames/FQDNs”;
 - Y cada uno tiene un orden en particular que ha cambiado en diferentes versiones del sistema operativo
 - Y como si fuera poca la complicación, independientemente del nombre que use la aplicación, el sistema si no puede resolver de una forma, intentará por la otra

Escenario

- La infraestructura que se utilizará para esta demostración es sencilla:
 - DC1.ad.guillermmod.com.ar
Windows Server 2012 R2
Controlador de Dominio
Servicio DNS
Servicio WINS (para resolución NetBIOS)
IPv4: 192.168.2.201/24
IPv6: por omisión (Link-local)
 - CL1.ad.guillermmod.com.ar
Windows 8.1
Cliente del Dominio
Configurado DNS a DC1
Configurado WINS a DC1
IPv4: 192.168.2.1/24
IPv6: por omisión (Link-local)



Pruebas de red

- En CL1 se ha instalado el analizador de protocolo [Microsoft Network Monitor 3.4](#) que es de descarga gratuita para hacer las capturas de red
- Para forzar a que el sistema utilice todos los métodos de resolución posibles, ejecutaré un comando que acepta tanto nombre NetBIOS, como "Hostname" o FQDN, como es "PING" usando un nombre no-especificando de qué tipo es
 - Por tanto ,el comando será "**PING NoExiste**" y veremos qué formas de resolución utiliza sobre la red
- Como la parte que hace en memoria no podremos verla en la red, vamos a aclararla:
 - Cuando tiene que resolver un nombre de tipo "Hostname/FQDN" siempre lo primero que se revisa es si la información no está ya presente en memoria
 - Puede estar en memoria porque fue resuelta anteriormente y aún resta tiempo para tenerla "cacheada", o porque está incluida en el archivo HOSTS ya que la implementación de Microsoft es mantener en este "cache" el contenido del archivo
 - Si de esta forma no consigue resolver el nombre, procederá como se muestra en las siguientes capturas
 - Cuando tiene que resolver un nombre de tipo NetBIOS, también lo primero que hace es ver si la información no está "cacheada" en memoria
 - Puede estar en memoria por haber sido resuelta anteriormente, este tiempo es fijo de 10 minutos

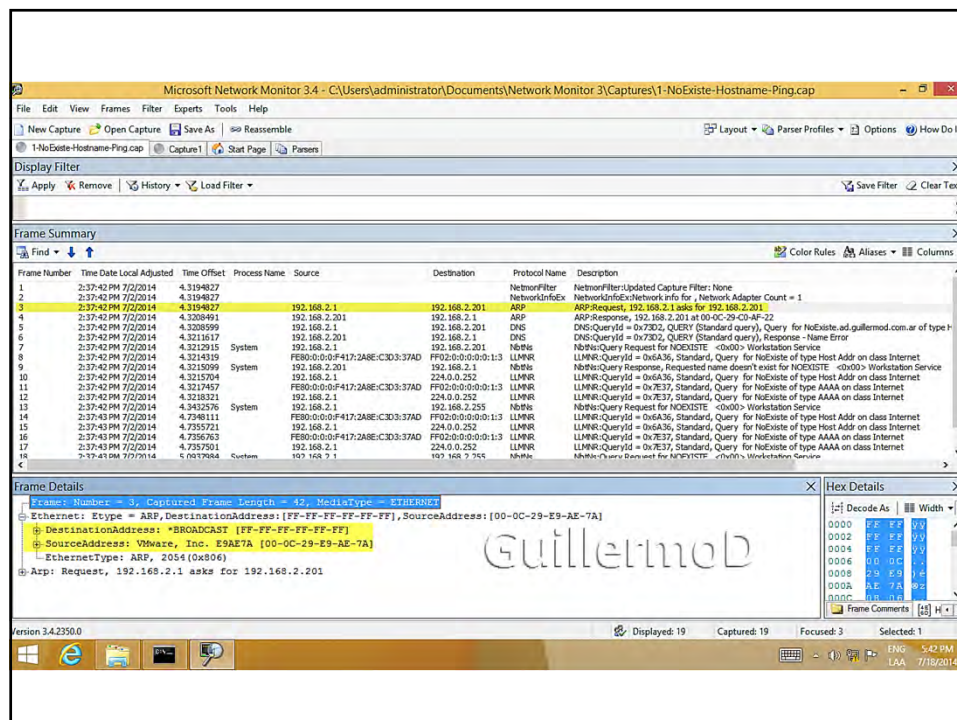
BAT de ejecución de prueba ping

- Para hacer la demostración limpia y prolija el PING lo ejecutaré desde un archivo BAT que se encarga de borrar la información "cacheada" de "MAC Address", cache NetBIOS y cache Hostnames/FQDNs
- El contenido del BAT es:

```
arp -d *  
nbtstat -R  
ipconfig /flushdns  
ping NoExiste
```

Primera prueba

- Como tiene que contactar a DC1 que es servidor tanto de DNS como de WINS, lo primero que debe hacer el cliente es resolver la “MAC Address” de DC1, que hace a través del protocolo ARP
- Podemos observar en el “frame 3” que es un “Broadcast” a nivel Ethernet preguntando por la “MAC Address” de 192.168.2.201, y adjuntando su propia “MAC Address” para que la guarde DC1



Como DC1 ya conoce la “MAC Address” de CL1, le responde por ARP, pero esta vez con tráfico dirigido a nivel Ethernet en el “frame 4”

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble

1-NoExiste-Hostname-Ping.cap Capture 1 Start Page Parsers

Display Filter

Apply Remove History Load Filter

Save Filter Clear Text

Frame Summary

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.1194827				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
2	2:37:42 PM 7/2/2014	4.1194827				ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
3	2:37:42 PM 7/2/2014	4.1194827				ARP	ARP-Response, 192.168.2.201 at 00-0C-29-C0-AF-22
4	2:37:42 PM 7/2/2014	4.1208999		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00-0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.1208999		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermob.com.ar of type Host
6	2:37:42 PM 7/2/2014	4.1211617		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response - Name Error
7	2:37:42 PM 7/2/2014	4.1212915	System	FE80::0:0:F417:2A8E::C3D3:37AD	FE80::0:0:0:0:0:0:1:3	NbName	NbName:Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.1214319	System	192.168.2.1	192.168.2.1	NbName	NbName:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
9	2:37:42 PM 7/2/2014	4.1215704	System	FE80::0:0:F417:2A8E::C3D3:37AD	FE80::0:0:0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA636, Standard, Query for NoExiste of type Host Addr on class Internet
10	2:37:42 PM 7/2/2014	4.1217497	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0xA636, Standard, Query for NoExiste of type AAAA on class Internet
11	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type Host Addr on class Internet
12	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet
13	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type Host Addr on class Internet
14	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet
15	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type Host Addr on class Internet
16	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet
17	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type Host Addr on class Internet
18	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	LLMNR	LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet

Frame Details

Frame Number: 4, Captured Frame Length: 60, Media Type: ETHERNET II

Ethernet II Type = ARP, DestinationAddress: [00-0C-29-E9-AE-7A], SourceAddress: [00-0C-29-C0-AF-22]

DestinationAddress: VMware, Inc. E9AE7A [00-0C-29-E9-AE-7A]

SourceAddress: VMware, Inc. C0AF22 [00-0C-29-C0-AF-22]

EthernetType: ARP, 2054 (0x806)

UnknownData: Binary Large Object (18 Bytes)

ARP: Response, 192.168.2.201 at 00-0C-29-C0-AF-22

Hex Details

Decode As Width

0000 00 00 00 00 00 00 00

0002 29 E9 AE 7A

0004 00 00 00 00 00 00 00

0006 00 00 00 00 00 00 00

0008 29 E9 AE 7A

000A 00 00 00 00 00 00 00

000C 00 00 00 00 00 00 00

000E 00 00 00 00 00 00 00

0010 00 00 00 00 00 00 00

0012 00 00 00 00 00 00 00

0014 00 00 00 00 00 00 00

0016 00 00 00 00 00 00 00

0018 00 00 00 00 00 00 00

001A 00 00 00 00 00 00 00

001C 00 00 00 00 00 00 00

001E 00 00 00 00 00 00 00

0020 00 00 00 00 00 00 00

0022 00 00 00 00 00 00 00

0024 00 00 00 00 00 00 00

0026 00 00 00 00 00 00 00

0028 00 00 00 00 00 00 00

002A 00 00 00 00 00 00 00

002C 00 00 00 00 00 00 00

002E 00 00 00 00 00 00 00

0030 00 00 00 00 00 00 00

0032 00 00 00 00 00 00 00

0034 00 00 00 00 00 00 00

0036 00 00 00 00 00 00 00

0038 00 00 00 00 00 00 00

003A 00 00 00 00 00 00 00

003C 00 00 00 00 00 00 00

003E 00 00 00 00 00 00 00

0040 00 00 00 00 00 00 00

0042 00 00 00 00 00 00 00

0044 00 00 00 00 00 00 00

0046 00 00 00 00 00 00 00

0048 00 00 00 00 00 00 00

004A 00 00 00 00 00 00 00

004C 00 00 00 00 00 00 00

004E 00 00 00 00 00 00 00

0050 00 00 00 00 00 00 00

0052 00 00 00 00 00 00 00

0054 00 00 00 00 00 00 00

0056 00 00 00 00 00 00 00

0058 00 00 00 00 00 00 00

005A 00 00 00 00 00 00 00

005C 00 00 00 00 00 00 00

005E 00 00 00 00 00 00 00

0060 00 00 00 00 00 00 00

0062 00 00 00 00 00 00 00

0064 00 00 00 00 00 00 00

0066 00 00 00 00 00 00 00

0068 00 00 00 00 00 00 00

006A 00 00 00 00 00 00 00

006C 00 00 00 00 00 00 00

006E 00 00 00 00 00 00 00

0070 00 00 00 00 00 00 00

0072 00 00 00 00 00 00 00

0074 00 00 00 00 00 00 00

0076 00 00 00 00 00 00 00

0078 00 00 00 00 00 00 00

007A 00 00 00 00 00 00 00

007C 00 00 00 00 00 00 00

007E 00 00 00 00 00 00 00

0080 00 00 00 00 00 00 00

0082 00 00 00 00 00 00 00

0084 00 00 00 00 00 00 00

0086 00 00 00 00 00 00 00

0088 00 00 00 00 00 00 00

008A 00 00 00 00 00 00 00

008C 00 00 00 00 00 00 00

008E 00 00 00 00 00 00 00

0090 00 00 00 00 00 00 00

0092 00 00 00 00 00 00 00

0094 00 00 00 00 00 00 00

0096 00 00 00 00 00 00 00

0098 00 00 00 00 00 00 00

009A 00 00 00 00 00 00 00

009C 00 00 00 00 00 00 00

009E 00 00 00 00 00 00 00

00A0 00 00 00 00 00 00 00

00A2 00 00 00 00 00 00 00

00A4 00 00 00 00 00 00 00

00A6 00 00 00 00 00 00 00

00A8 00 00 00 00 00 00 00

00AA 00 00 00 00 00 00 00

00AC 00 00 00 00 00 00 00

00AE 00 00 00 00 00 00 00

00B0 00 00 00 00 00 00 00

00B2 00 00 00 00 00 00 00

00B4 00 00 00 00 00 00 00

00B6 00 00 00 00 00 00 00

00B8 00 00 00 00 00 00 00

00BA 00 00 00 00 00 00 00

00BC 00 00 00 00 00 00 00

00BE 00 00 00 00 00 00 00

00C0 00 00 00 00 00 00 00

00C2 00 00 00 00 00 00 00

00C4 00 00 00 00 00 00 00

00C6 00 00 00 00 00 00 00

00C8 00 00 00 00 00 00 00

00CA 00 00 00 00 00 00 00

00CC 00 00 00 00 00 00 00

00CE 00 00 00 00 00 00 00

00D0 00 00 00 00 00 00 00

00D2 00 00 00 00 00 00 00

00D4 00 00 00 00 00 00 00

00D6 00 00 00 00 00 00 00

00D8 00 00 00 00 00 00 00

00DA 00 00 00 00 00 00 00

00DC 00 00 00 00 00 00 00

00DE 00 00 00 00 00 00 00

00E0 00 00 00 00 00 00 00

00E2 00 00 00 00 00 00 00

00E4 00 00 00 00 00 00 00

00E6 00 00 00 00 00 00 00

00E8 00 00 00 00 00 00 00

00EA 00 00 00 00 00 00 00

00EC 00 00 00 00 00 00 00

00EE 00 00 00 00 00 00 00

00F0 00 00 00 00 00 00 00

00F2 00 00 00 00 00 00 00

00F4 00 00 00 00 00 00 00

00F6 00 00 00 00 00 00 00

00F8 00 00 00 00 00 00 00

00FA 00 00 00 00 00 00 00

00FC 00 00 00 00 00 00 00

00FE 00 00 00 00 00 00 00

0100 00 00 00 00 00 00 00

0102 00 00 00 00 00 00 00

0104 00 00 00 00 00 00 00

0106 00 00 00 00 00 00 00

0108 00 00 00 00 00 00 00

010A 00 00 00 00 00 00 00

010C 00 00 00 00 00 00 00

010E 00 00 00 00 00 00 00

0110 00 00 00 00 00 00 00

0112 00 00 00 00 00 00 00

0114 00 00 00 00 00 00 00

0116 00 00 00 00 00 00 00

0118 00 00 00 00 00 00 00

011A 00 00 00 00 00 00 00

011C 00 00 00 00 00 00 00

011E 00 00 00 00 00 00 00

0120 00 00 00 00 00 00 00

0122 00 00 00 00 00 00 00

0124 00 00 00 00 00 00 00

0126 00 00 00 00 00 00 00

0128 00 00 00 00 00 00 00

012A 00 00 00 00 00 00 00

012C 00 00 00 00 00 00 00

012E 00 00 00 00 00 00 00

0130 00 00 00 00 00 00 00

0132 00 00 00 00 00 00 00

0134 00 00 00 00 00 00 00

0136 00 00 00 00 00 00 00

0138 00 00 00 00 00 00 00

013A 00 00 00 00 00 00 00

013C 00 00 00 00 00 00 00

013E 00 00 00 00 00 00 00

0140 00 00 00 00 00 00 00

0142 00 00 00 00 00 00 00

0144 00 00 00 00 00 00 00

0146 00 00 00 00 00 00 00

0148 00 00 00 00 00 00 00

014A 00 00 00 00 00 00 00

014C 00 00 00 00 00 00 00

014E 00 00 00 00 00 00 00

0150 00 00 00 00 00 00 00

0152 00 00 00 00 00 00 00

0154 00 00 00 00 00 00 00

0156 00 00 00 00 00 00 00

0158 00 00 00 00 00 00 00

015A 00 00 00 00 00 00 00

015C 00 00 00 00 00 00 00

015E 00 00 00 00 00 00 00

0160 00 00 00 00 00 00 00

0162 00 00 00 00 00 00 00

0164 00 00 00 00 00 00 00

0166 00 00 00 00 00 00 00

0168 00 00 00 00 00 00 00

016A 00 00 00 00 00 00 00

016C 00 00 00 00 00 00 00

016E 00 00 00 00 00 00 00

0170 00 00 00 00 00 00 00

0172 00 00 00 00 00 00 00

0174 00 00 00 00 00 00 00

0176 00 00 00 00 00 00 00

0178 00 00 00 00 00 00 00

017A 00 00 00 00 00 00 00

017C 00 00 00 00 00 00 00

017E 00 00 00 00 00 00 00

0180 00 00 00 00 00 00 00

0182 00 00 00 00 00 00 00

0184 00 00 00 00 00 00 00

0186 00 00 00 00 00 00 00

0188 00 00 00 00 00 00 00

018A 00 00 00 00 00 00 00

018C 00 00 00 00 00 00 00

018E 00 00 00 00 00 00 00

0190 00 00 00 00 00 00 00

0192 00 00 00 00 00 00 00

0194 00 00 00 00 00 00 00

0196 00 00 00 00 00 00 00

0198 00 00 00 00 00 00 00

019A 00 00 00 00 00 00 00

019C 00 00 00 00 00 00 00

019E 00 00 00 00 00 00 00

01A0 00 00 00 00 00 00 00

01A2 00 00 00 00 00 00 00

01A4 00 00 00 00 00 00 00

01A6 00 00 00 00 00 00 00

01A8 00 00 00 00 00 00 00

01AA 00 00 00 00 00 00 00

01AC 00 00 00 00 00 00 00

01AE 00 00 00 00 00 00 00

01B0 00 00 00 00 00 00 00

01B2 00 00 00 00 00 00 00

01B4 00 00 00 00 00 00 00

01B6 00 00 00 00 00 00 00

01B8 00 00 00 00 00 00 00

01BA 00 00 00 00 00 00 00

01BC 00 00 00 00 00 00 00

01BE 00 00 00 00 00 00 00

01C0 00 00 00 00 00 00 00

01C2 00 00 00 00 00 00 00

01C4 00 00 00 00 00 00 00

01C6 00 00 00 00 00 00 00

01C8 00 00 00 00 00 00 00

01CA 00 00 00 00 00 00 00

01CC 00 00 00 00 00 00 00

01CE 00 00 00 00 00 00 00

01D0 00 00 00 00 00 00 00

01D2 00 00 00 00 00 00 00

01D4 00 00 00 00 00 00 00

01D6 00 00 00 00 00 00 00

01D8 00 00 00 00 00 00 00

01DA 00 00 00 00 00 00 00

01DC 00 00 00 00 00 00 00

01DE 00 00 00 00 00 00 00

01E0 00 00 00 00 00 00 00

01E2 00 00 00 00 00 00 00

01E4 00 00 00 00 00 00 00

01E6 00 00 00 00 00 00 00

01E8 00 00 00 00 00 00 00

01EA 00 00 00 00 00 00 00

01EC 00 00 00 00 00 00 00

01EE 00 00 00 00 00 00 00

01F0 00 00 00 00 00 00 00

01F2 00 00 00 00 00 00 00

01F4 00 00 00 00 00 00 00

01F6 00 00 00 00 00 00 00

01F8 00 00 00 00 00 00 00

01FA 00 00 00 00 00 00 00

01FC 00 00 00 00 00 00 00

01FE 00 00 00 00 00 00 00

0200 00 00 00 00 00 00 00

0202 00 00 00 00 00 00 00

0204 00 00 00 00 00 00 00

0206 00 00 00 00 00 00 00

0208 00 00 00 00 00 00 00

020A 00 00 00 00 00 00 00

020C 00 00 00 00 00 00 00

020E 00 00 00 00 00 00 00

0210 00 00 00 00 00 00 00

0212 00 00 00 00 00 00 00

0214 00 00 00 00 00 00 00

0216 00 00 00 00 00 00 00

0218 00 00 00 00 00 00 00

021A 00 00 00 00 00 00 00

021C 00 00 00 00 00 00 00

021E 00 00 00 00 00 00 00

0220 00 00 00 00 00 00 00

0222 00 00 00 00 00 00 00

0224 00 00 00 00 00 00 00

0226 00 00 00 00 00 00 00

0228 00 00 00 00 00 00 00

022A 00 00 00 00 00 00 00

022C 00 00 00 00 00 00 00

022E 00 00 00 00 00 00 00

0230 00 00 00 00 00 00 00

0232 00 00 00 00 00 00 00

0234 00 00 00 00 00 00 00

0236 00 00 00 00 00 00 00

0238 00 00 00 00 00 00 00

023A 00 00 00 00 00 00 00

023C 00 00 00 00 00 00 00

023E 00 00 00 00 00 00 00

0240 00 00 00 00 00 00 00

0242 00 00 00 00 00 00 00

0244 00 00 00 00 00 00 00

0246 00 00 00 00 00 00 00

0248 00 00 00 00 00 00 00

024A 00 00 00 00 00 00 00

024C 00 00 00 00 00 00 00

024E 00 00 00 00 00 00 00

0250 00 00 00 00 00 00 00

0252 00 00 00

Y en el “frame 6” el servidor DNS le responde que ese nombre no existe (“Name error”)

The screenshot shows the Microsoft Network Monitor 3.4 interface. The main pane displays a list of captured frames. Frame 6 is selected, showing a DNS response from 192.168.2.1 to 192.168.2.1. The details pane shows the Ethernet II, Internet Protocol (IPv4), and DNS sections. The DNS section indicates a 'Name Error' response for the query 'guillemod.com.ar'.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.3194827				NetworkFilter	NetworkFilter:Updated Capture Filter: None
2	2:37:42 PM 7/2/2014	4.3194827				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
3	2:37:42 PM 7/2/2014	4.3194827				ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
4	2:37:42 PM 7/2/2014	4.3208491		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00-0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.3208599		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExist.ad.guillemod.com.ar of type T
6	2:37:42 PM 7/2/2014	4.3211617		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response - Name Error
7	2:37:42 PM 7/2/2014	4.3212915	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.3214319	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
9	2:37:42 PM 7/2/2014	4.3215704	System	192.168.2.1	192.168.2.1	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
10	2:37:42 PM 7/2/2014	4.3217457	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
11	2:37:42 PM 7/2/2014	4.3218371	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
12	2:37:42 PM 7/2/2014	4.3219576	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
13	2:37:42 PM 7/2/2014	4.3220781	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
14	2:37:42 PM 7/2/2014	4.3221986	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
15	2:37:42 PM 7/2/2014	4.3223191	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
16	2:37:42 PM 7/2/2014	4.3224396	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
17	2:37:42 PM 7/2/2014	4.3225601	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
18	2:37:42 PM 7/2/2014	4.3226806	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service

El paso siguiente es tratar de resolver por WINS, como si se tratara de un nombre NetBIOS, para lo cual en el “frame 7” le envía a WINS un “Query request”

The screenshot shows the Microsoft Network Monitor 3.4 interface. The main pane displays a list of captured frames. Frame 7 is selected, showing a WINS query request from 192.168.2.1 to 192.168.2.201. The details pane shows the Ethernet II, Internet Protocol (IPv4), and WINS sections. The WINS section indicates a 'Query Request for NOEXISTE'.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.3194827				NetworkFilter	NetworkFilter:Updated Capture Filter: None
2	2:37:42 PM 7/2/2014	4.3194827				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
3	2:37:42 PM 7/2/2014	4.3194827				ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
4	2:37:42 PM 7/2/2014	4.3208491		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00-0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.3208599		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExist.ad.guillemod.com.ar of type T
6	2:37:42 PM 7/2/2014	4.3211617		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response - Name Error
7	2:37:42 PM 7/2/2014	4.3212915	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.3214319	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
9	2:37:42 PM 7/2/2014	4.3215704	System	192.168.2.1	192.168.2.1	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
10	2:37:42 PM 7/2/2014	4.3217457	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
11	2:37:42 PM 7/2/2014	4.3218371	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
12	2:37:42 PM 7/2/2014	4.3219576	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
13	2:37:42 PM 7/2/2014	4.3220781	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
14	2:37:42 PM 7/2/2014	4.3221986	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
15	2:37:42 PM 7/2/2014	4.3223191	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
16	2:37:42 PM 7/2/2014	4.3224396	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
17	2:37:42 PM 7/2/2014	4.3225601	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Request for NOEXISTE <0x00> Workstation Service
18	2:37:42 PM 7/2/2014	4.3226806	System	192.168.2.1	192.168.2.201	NBNS	NBNS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service

WINS le responderá que no tiene registrado a nadie con ese nombre. Pero antes que WINS responda, va a intentar resolver por LLMNR. De todas formas podemos verificar en el “frame 9” la no resolución

The screenshot shows the Microsoft Network Monitor 3.4 interface. The 'Frame Summary' pane displays a list of captured frames. Frame 9 is highlighted, showing a NetBIOS Query Response from 192.168.2.1 to 192.168.2.1, indicating that the requested name does not exist for NOEXISTE. The 'Frame Details' pane for frame 9 shows the Ethernet II, Internet Protocol (IPv4), and User Datagram Protocol (UDP) details. The UDP details show the destination port is 137 (NetBIOS Name Service). The 'Hex Details' pane shows the raw data of the packet.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.1194827				NetworkFilter	NetworkFilter:Updated Capture Filter: None
2	2:37:42 PM 7/2/2014	4.1194827				NetworkInfo	NetworkInfo:Network info for , Network Adapter Count = 1
3	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.201	ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
4	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00-0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExist.ad.gultermob.com.ar of type H
6	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response - Name Error
7	2:37:42 PM 7/2/2014	4.1194827	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.1214319	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
9	2:37:42 PM 7/2/2014	4.1215099	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
10	2:37:42 PM 7/2/2014	4.1215704	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
11	2:37:42 PM 7/2/2014	4.1217457	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
12	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
13	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
14	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
15	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
16	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
17	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
18	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
19	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service

No habiendo resolución por DNS ni WINS, CL1 trata de resolver a través del protocolo LLMNR (“Link-Local Multicast Name Resolution” – RFC 4795). Para ello utiliza tanto IPv6 como IPv4, y las direcciones de “Multicast” utilizadas por este protocolo (IPv6: FF02::1:3 – IPv4: 224.0.0.252)

Hace cuatro intentos por IPv6 como muestran los “frames 8, 11, 14 y 16”

The screenshot shows the Microsoft Network Monitor 3.4 interface. The 'Frame Summary' pane displays a list of captured frames. Frame 8 is highlighted, showing a Link-Local Multicast Name Resolution (LLMNR) query from 192.168.2.1 to 224.0.0.252. The 'Frame Details' pane for frame 8 shows the Ethernet II, Internet Protocol (IPv4), and User Datagram Protocol (UDP) details. The UDP details show the destination port is 5355 (Link-Local Multicast Name Resolution). The 'Hex Details' pane shows the raw data of the packet.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.1194827				NetworkFilter	NetworkFilter:Updated Capture Filter: None
2	2:37:42 PM 7/2/2014	4.1194827				NetworkInfo	NetworkInfo:Network info for , Network Adapter Count = 1
3	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.201	ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
4	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00-0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExist.ad.gultermob.com.ar of type H
6	2:37:42 PM 7/2/2014	4.1194827		192.168.2.1	192.168.2.1	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response - Name Error
7	2:37:42 PM 7/2/2014	4.1194827	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.1214319	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
9	2:37:42 PM 7/2/2014	4.1215099	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
10	2:37:42 PM 7/2/2014	4.1215704	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
11	2:37:42 PM 7/2/2014	4.1217457	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
12	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
13	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
14	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
15	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
16	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
17	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
18	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
19	2:37:42 PM 7/2/2014	4.1218321	System	192.168.2.1	192.168.2.1	NetBIOS	NetBIOS-Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service

Y simultáneamente hace el mismo intento por IPv4 como se observa en los "frames 10, 12, 15 y 17"

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble

1-NoExiste-Hostname-Ping.cap Capture 1 Start Page Parse

Display Filter

Apply Remove History Load Filter

Save Filter Clear Text

Find

Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.3194827				NetworkFilter	NetworkFilter:Updated Capture Filter: None
2	2:37:42 PM 7/2/2014	4.3194827				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
3	2:37:42 PM 7/2/2014	4.3194827				ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
4	2:37:42 PM 7/2/2014	4.3208491		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00:0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.3208599		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermod.com.ar of type Host
6	2:37:42 PM 7/2/2014	4.3211617		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response = Name Error
7	2:37:42 PM 7/2/2014	4.3212915	System	192.168.2.1	192.168.2.201	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.3214319		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
9	2:37:42 PM 7/2/2014	4.3215099	System	192.168.2.201	192.168.2.1	NbtNs	NbtNs:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
10	2:37:42 PM 7/2/2014	4.3215704		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
11	2:37:42 PM 7/2/2014	4.3217457		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
12	2:37:42 PM 7/2/2014	4.3218321		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
13	2:37:42 PM 7/2/2014	4.3432576	System	192.168.2.1	192.168.2.255	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service
14	2:37:43 PM 7/2/2014	4.3438111		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
15	2:37:43 PM 7/2/2014	4.3555721		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
16	2:37:43 PM 7/2/2014	4.3556763		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
17	2:37:43 PM 7/2/2014	4.3557501		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
18	2:37:43 PM 7/2/2014	5.0937984	System	192.168.2.1	192.168.2.255	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service
19	2:37:44 PM 7/2/2014	5.0945615	System	192.168.2.1	192.168.2.255	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service

Frame Details

Frame Number: 10, Captured Frame Length: 46, MediaType: ETHERNET II

Ethernet II: Etype = Internet IP (IPv4), DestinationAddress: [01-00-5E-00-00-FC], SourceAddress: [00-0C-29-E9-AE-7A]

IPv4: Src = 192.168.2.1, Dest = 224.0.0.252, Next Protocol = UDP, Packet ID = 1914, Total IP Length = 54

UDP: SrcPort = 58071, DestPort = Linklocal Multicast Name Resolution(5355), Length = 28

LLMNR: QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet

Hex Details

Decode As Width

0000 01 00 5E 00 00 00 FC

0002 00 0C 29 E9 AE 7A

0004 00 00 00 00 00 00 00

0006 00 00 00 00 00 00 00

0008 29 E9 AE 7A

Frame Comments

Version 3.4.2350.0

Displayed: 19 Captured: 19 Focused: 10 Selected: 1

ENG 6:04 PM 7/2/2014

Finalmente, al no poder resolver el nombre ni por DNS, ni WINS, ni LLMNR tanto por IPv4 como por IPV6, prueba la última opción que es "Broadcast" por IPv4, aunque como se puede observar antes de finalizar con LLMNR Acá hay una diferencia con anteriores versiones del sistema operativo pues antes utilizaba "Subnet Broadcast = 255.255.255.255", y actualmente utiliza "Net Broadcast 192.168.2.255"

Esto se puede ver en los "frames 13, 18 y 19"

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble

1-NoExiste-Hostname-Ping.cap Capture 1 Start Page Parse

Display Filter

Apply Remove History Load Filter

Save Filter Clear Text

Find

Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	2:37:42 PM 7/2/2014	4.3194827				NetworkFilter	NetworkFilter:Updated Capture Filter: None
2	2:37:42 PM 7/2/2014	4.3194827				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
3	2:37:42 PM 7/2/2014	4.3194827				ARP	ARP-Request, 192.168.2.1 asks for 192.168.2.201
4	2:37:42 PM 7/2/2014	4.3208491		192.168.2.1	192.168.2.201	ARP	ARP-Response, 192.168.2.201 at 00:0C-29-C0-AF-22
5	2:37:42 PM 7/2/2014	4.3208599		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermod.com.ar of type Host
6	2:37:42 PM 7/2/2014	4.3211617		192.168.2.1	192.168.2.201	DNS	DNS-QueryId = 0x73D2, QUERY (Standard query), Response = Name Error
7	2:37:42 PM 7/2/2014	4.3212915	System	192.168.2.1	192.168.2.201	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service
8	2:37:42 PM 7/2/2014	4.3214319		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
9	2:37:42 PM 7/2/2014	4.3215099	System	192.168.2.201	192.168.2.1	NbtNs	NbtNs:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service
10	2:37:42 PM 7/2/2014	4.3215704		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
11	2:37:42 PM 7/2/2014	4.3217457		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
12	2:37:42 PM 7/2/2014	4.3218321		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
13	2:37:42 PM 7/2/2014	4.3432576	System	192.168.2.1	192.168.2.255	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service
14	2:37:43 PM 7/2/2014	4.3438111		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
15	2:37:43 PM 7/2/2014	4.3555721		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
16	2:37:43 PM 7/2/2014	4.3556763		FE80::0:0:F417:2A8E::C:D3:37AD	FF02::0:0:0:0:1:3	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
17	2:37:43 PM 7/2/2014	4.3557501		192.168.2.1	224.0.0.252	LLMNR	LLMNR:QueryId = 0xA36, Standard, Query for NoExiste of type Host Addr on class Internet
18	2:37:43 PM 7/2/2014	5.0937984	System	192.168.2.1	192.168.2.255	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service
19	2:37:44 PM 7/2/2014	5.0945615	System	192.168.2.1	192.168.2.255	NbtNs	NbtNs:Query Request for NOEXISTE <0x00> Workstation Service

Frame Details

Frame Number: 13, Captured Frame Length: 67, MediaType: ETHERNET II

Ethernet II: Etype = Internet IP (IPv4), DestinationAddress: [01-00-5E-00-00-FC], SourceAddress: [00-0C-29-E9-AE-7A]

IPv4: Src = 192.168.2.1, Dest = 192.168.2.255, Next Protocol = UDP, Packet ID = 4934, Total IP Length = 78

UDP: SrcPort = NETBIOS Name Service(137), DestPort = NETBIOS Name Service(137), Length = 18

NbtNs: Query Request for NOEXISTE <0x00> Workstation Service

Hex Details

Decode As Width

0000 01 00 5E 00 00 00 FC

0002 00 0C 29 E9 AE 7A

0004 00 00 00 00 00 00 00

0006 00 00 00 00 00 00 00

0008 29 E9 AE 7A

Frame Comments

Version 3.4.2350.0

Displayed: 19 Captured: 19 Focused: 13 Selected: 1

ENG 6:08 PM 7/2/2014

Conclusión del ejemplo

- Resumiendo, al indicarle un nombre no calificado, siendo parte de un Dominio y teniendo configurado tanto DNS como WINS, el sistema utiliza varios métodos, tanto de resolución NetBIOS como de Hostname/FQDN
- La resolución de nombres de red es algo que hay que prestarle mucha atención
 - Es habitual que cuando se experimenta un largo tiempo hasta poder conectarse a una máquina, pero luego todo funciona normalmente, se deba a un problema de resolución de nombres
 - Por ejemplo si no lo puede resolver por DNS y termine resolviendo por “Net Broadcasts”
- Información adicional:
 - [Link-local Multicast Name Resolution \(LLMNR\)](#)
 - [Multicast Address](#)

Segunda parte: Utilización de tcpdump, Windump y Fing

Descripción de las utilidades

- Se trata de tres utilidades que se utilizan como escuchadores de red
 - **TCPDUMP**: entorno GNU/Linux
 - **Windump**: semejante a TCPDUMP para entorno Windows
 - **FING**: Ofrece información muy ordenada y se suele utilizar con redes WiFi

Ejemplos de utilización (I)

- Capturar desde un interfaz de red
tcpdump -i eth0
- Capturar desde una fuente por un adaptador de red concreto
tcpdump -i eth0 src host 192.168.1.12
- Capturar por un adaptador de red los paquetes con un destino concreto
tcpdump -i eth0 dst host 192.168.1.12

Ejemplos de utilización (II)

- Capturar paquetes con origen y destino en una IP
tcpdump -i eth0 host 192.168.1.12
- Capturar paquetes con destino en una MAC
tcpdump ether dst XX:XX:XX:XX:XX:XX
- Capturar paquetes que vengan desde una red
tcpdump dst net 192.168.1.0

Ejemplos de utilización (III)

- Capturar paquetes con un destino en un puerto concreto
tcpdump dst host 192.168.2.1 and dst port 3128
- Captura de todo el tráfico web
tcpdump tcp and port 80
- Captura de todo lo que no vaya dirigido a una IP
tcpdump not dst host 192.168.1.2

Ejemplos de utilización (IV)

- Capturar peticiones DNS
`tcpdump udp and dst port 53`
- Capturar peticiones LDAP
`tcpdump tcp port ldap`

Vista inicial de la red

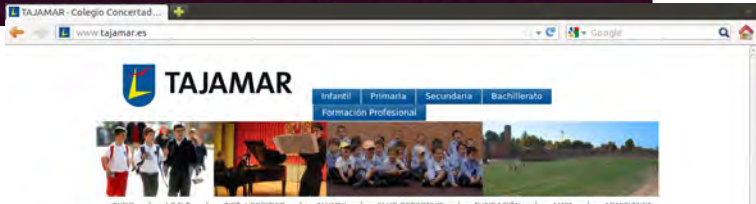
```
aabad@pruebas: ~  
aabad@pruebas:~$ ifconfig  
eth0      Link encap:Ethernet  direcciónHW 00:0c:29:c2:d2:cc  
          Direc. inet:192.168.111.136  Difus.:192.168.111.255  Másc:255.255.255.0  
          Dirección inet6: fe80::20c:29ff:fec2:d2cc/64  Alcance:Enlace  
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1  
          Paquetes RX:12123 errores:0 perdidos:0 overruns:0 frame:0  
          Paquetes TX:5544 errores:0 perdidos:0 overruns:0 carrier:0  
          colisiones:0 long.colaTX:1000  
          Bytes RX:14237476 (14.2 MB)  TX bytes:352260 (352.2 KB)  
          Interrupción:19 Dirección base: 0x2024  
  
lo        Link encap:Bucle local  
          Direc. inet:127.0.0.1  Másc:255.0.0.0  
          Dirección inet6: ::1/128  Alcance:Anfitrión  
          ACTIVO BUCLE FUNCIONANDO  MTU:16436  Métrica:1  
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0  
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0  
          colisiones:0 long.colaTX:0  
          Bytes RX:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
aabad@pruebas:~$
```

Captura desde eth0

```

aabad@pruebas: ~
aabad@pruebas:~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

```



```

aabad@pruebas: ~
ags [FP.], seq 8579, ack 465, win 64239, length 0
17:04:41.303883 IP pruebas.local.48875 > 168.219.106.212.static.jazztel.es.www: FL
ags [..], ack 8580, win 35040, length 0
17:04:41.306950 IP mad01s08-in-f2.1e100.net.https > pruebas.local.42015: Flags [FP
..], seq 1, ack 28, win 64239, length 0
17:04:41.306966 IP pruebas.local.42015 > mad01s08-in-f2.1e100.net.https: Flags [..
, ack 2, win 26280, length 0
17:04:41.327627 IP we-in-f138.1e100.net.www > pruebas.local.34890: Flags [FP.], se
q 89835, ack 622, win 64239, length 0
17:04:41.327647 IP pruebas.local.34890 > we-in-f138.1e100.net.www: Flags [..], ack
89836, win 62780, length 0
17:04:41.341762 IP privet.canonical.com.www > pruebas.local.52606: Flags [FP.], se
q 1, ack 1, win 64239, length 0

```

Captura desde una fuente

```

aabad@pruebas: ~
aabad@pruebas:~$ sudo tcpdump -i eth0 src host 192.168.111.136
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
17:08:03.970940 IP pruebas.local.55551 > 192.168.111.2.domain: 33317+ A? www.google
e.es. (31)
17:08:03.972273 IP pruebas.local.52102 > 192.168.111.2.domain: 29893+ PTR? 2.111.1
68.192.in-addr.arpa. (44)
17:08:04.049736 IP pruebas.local > mad01s08-in-f24.1e100.net: ICMP echo request, i
d 8412, seq 1, length 64
^C17:08:04.153888 IP pruebas.local.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 2.111.168.
192.in-addr.arpa. (44)

4 packets captured
17 packets received by filter
0 packets dropped by kernel
aabad@pruebas:~$

```

```

aabad@pruebas: ~
aabad@pruebas:~$ ping www.google.es
PING www-cctld.l.google.com (173.194.34.216) 56(84) bytes of data.
64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=1 ttl=128 tin
e=118 ms
64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=2 ttl=128 tin
e=45.2 ms
64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=3 ttl=128 tin
e=74.5 ms
^C
--- www-cctld.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 45.215/79.566/118.885/30.280 ms
aabad@pruebas:~$

```

Captura desde una MAC

```
aabad@pruebas:~$ sudo tcpdump ether dst 00:0c:29:c2:d2:cc
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
17:13:03.351949 IP 192.168.111.2.domain > pruebas.local.44537: 49765 2/0/0 CNAME w
ww-cttld.l.google.com., A 173.194.34.216 (83)
17:13:03.437061 IP 192.168.111.2.domain > pruebas.local.38275: 55973 NXDomain 0/0/
0 (46)
17:13:03.437062 IP mad01s08-in-f24.1e100.net > pruebas.local: ICMP echo reply, id
29102, seq 1, length 64
17:13:03.479951 IP 192.168.111.2.domain > pruebas.local.40641: 18721 1/0/0 PTR mad
01s08-in-f24.1e100.net. (84)
17:13:03.598298 IP 192.168.111.2.domain > pruebas.local.45522: 32254 NXDomain 0/0/
0 (44)
17:13:04.401055 IP mad01s08-in-f24.1e100.net > pruebas.local: ICMP echo reply, id
29102, seq 2, length 64
17:13:04.455365 IP 192.168.111.2.domain > pruebas.local.52528: 5171 1/0/0 PTR mad0
1s08-in-f24.1e100.net. (84)
17:13:05.473917 IP mad01s08-in-f24.1e100.net > pruebas.local: ICMP echo reply, id
29102, seq 3, length 64
17:13:05.557002 IP 192.168.aabad@pruebas:~$ ping www.google.es
PING www-cttld.l.google.com (173.194.34.216) 56(84) bytes of data.
17:13:08.644497 IP 192.168.64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=1 ttl=128 tim
e=83.9 ms
17:13:08.644497 IP 192.168.64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=2 ttl=128 tim
e=46.1 ms
17:13:08.644497 IP 192.168.64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=3 ttl=128 tim
e=117 ms
AC
--- packet-cttld.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 46.195/82.455/117.189/29.003 ms
aabad@pruebas:~$
```

Captura del tráfico web

```
aabad@pruebas:~$ sudo tcpdump tcp and port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
17:17:03.504332 IP pruebas.local.48196 > ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www: Flags [S], seq 1472108627, win 14600, options [mss 1460,sackOK,TS val 325823 ecr 0,nop,wscale 4], length 0
17:17:03.580760 IP ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www > pruebas.local.48196: Flags [S.], seq 688221526, ack 1472108628, win 64240, options [mss 1460], length 0
17:17:03.580796 IP pruebas.local.48196 > ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www: Flags [.], ack 1, win 14600, length 0
17:17:06.060708 IP pruebas.local.48196 > ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www: Flags [P.], seq 1:6, ack 1, win 14600, length 5
17:17:06.061259 IP ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www > pruebas.local.48196: Flags [.], ack 6, win 64240, length 0
17:17:06.318377 IP pruebas.local.48196 > ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www: Flags [P.], seq 6:11, ack 1, win 14600, length 5
17:17:06.318705 IP ec2-79-125-24-179.eu-west-1.compute.amazonaws.com.www > pruebas.local.48196: Flags [.], ack 11, win 64240, length 0
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
aabad@pruebas:~$
```

Operación

- Sobre un sistema Linux, practica escuchas con TCPDUMP
- Intenta hacer algo semejante con Windump y con Fing
- Construye con cada utilidad un sencillo manual de usuario sobre cómo usar cada una de las utilidades
- Nomenclatura identificativa de práctica:
 - **PARP401B-Sniffers-tcpdump**

Tercera parte: Operación con sniffers (Capturar tráfico con Windows)

Objetivo de la práctica

- Conocer algunas herramientas de Windows que permiten la escucha de la red
- Aprender a salvar capturas en formatos legibles por las aplicaciones de análisis

Capturar tráfico desde la línea de comandos

- En ocasiones el administrador de sistemas requiere realizar capturas de tráfico para poder analizar y solucionar problemas
- A partir de Windows 7 y Windows Server 2008 R2 disponemos de la posibilidad de capturar tráfico sin instalar software de terceros en el equipo utilizando el comando:
 - **netsh trace**

Operación con netsh trace



```
Administrador: C:\Windows\system32\cmd.exe

C:\>md SYSADMIT 1

C:\>netsh trace start persistent=yes capture=yes tracefile=C:\SYSADMIT\Trazas-Red.etl

Configuración de seguimiento: 2
-----
Estado: En ejecución
Archivo de seguimiento: C:\SYSADMIT\Trazas-Red.etl
Anexar: Desactivar
Circular: Activar
Tamaño máx.: 250 MB
Informe: Desactivar

C:\>netsh trace stop 3
Seguimientos correlativos... listo
Generando recolección de datos... listo
El archivo de seguimiento y otros datos de solución de problemas se compila como "C:\SYSADMIT\Trazas-Red.cab".
Ubicación del archivo = C:\SYSADMIT\Trazas-Red.etl
La sesión de seguimiento se detuvo correctamente.

C:\>dir C:\SYSADMIT /B 4
Trazas-Red.cab
Trazas-Red.etl
```

Pasos para realizar una captura

- 1) Creamos un directorio, en el ejemplo C:\SYSADMIT
- 2) Ejecutamos el capturador de tráfico:
 - **netsh trace start persistent=yes capture=yes tracefile=C:\SYSADMIT\Trazas-Red.etl**
- 3) Detenemos el capturador de tráfico:
 - **netsh trace stop**
 - Nota: Si quisiéramos ver el estado de la captura antes de detenerla, bastaría con ejecutar: netsh trace show status
- 4) Resultados generados en C:\SYSADMIT:
 - Fichero ETL: Trazas capturadas (Event Trace Log)
 - Fichero CAB: En su interior veremos ficheros de report

Contenido del fichero .cab

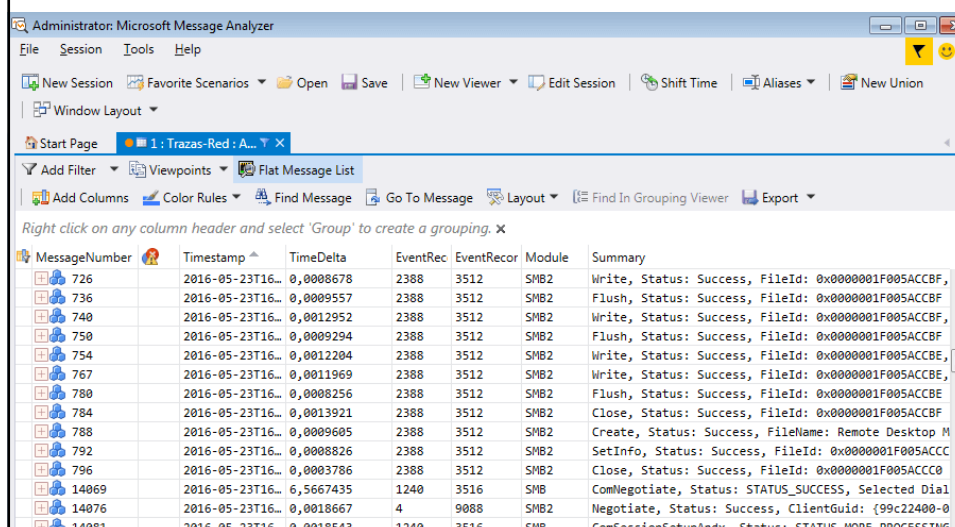
- Si descomprimos el fichero CAB, veremos toda una serie de ficheros correspondientes a los reports generados
- Entre los formatos de los ficheros de los reports veremos: TXT, XML, EVTX (Visor de eventos), entre otros
- También encontraremos el fichero: report.html con enlaces a los reports generados, muy útil para disponer de un índice de los mismos
 - Ver fichero report.html en diapo siguiente

- **Configuración general**
- OS Information
- Credential Providers
- **Configuración de red**
- Environment Information
- Adapter Information
- DNS Information
- Neighbor Information
- **Configuración inalámbrica**
- WLAN Auto-Config Eventlog
- **Windows Connect Now**
- WCN Information
- **Firewall de Windows**
- Windows Firewall Configuration
- Windows Firewall Effective Rules
- Connection Security Eventlog
- Connection Security Eventlog (Verbose)
- Firewall Eventlog
- Firewall Eventlog (Verbose)
- **Configuración Winsock**
- Winsock LSP Catalog
- **Uso compartido de archivos**
- File Sharing Configuration
- **Volcados de memoria de claves del Registro**
- Credential Providers
- Credential Provider Filters
- API Permissions
- WlanSvc HKLM Dump
- WinLogon Notification Subscribers
- Network Profiles
- **Archivos de seguimiento**
- Primary Event Trace Log (ETL)

Contenido del fichero ETL

- El fichero ETL generado puede ser analizado con "Microsoft Message Analyzer", herramienta gratuita que podemos descargar de la web de Microsoft
- Con "Microsoft Message Analyzer" podremos analizar el tráfico capturado, filtrarlo, etc...
- Con "Microsoft Message Analyzer" también podemos exportar el fichero ETL a formato CAP. Con formato CAP podremos leer el fichero desde Wireshark
- Vista ejecución de "Microsoft Message Analyzer" (ver diapo siguiente)

Vista del fichero .ETL con la utilidad Microsoft Message Analyzer



Administrator: Microsoft Message Analyzer

File Session Tools Help

New Session Favorite Scenarios Open Save New Viewer Edit Session Shift Time Aliases New Union

Window Layout

Start Page 1: Trazas-Red : A...

Add Filter Viewpoints Flat Message List

Add Columns Color Rules Find Message Go To Message Layout Find In Grouping Viewer Export

Right click on any column header and select 'Group' to create a grouping.

MessageNumber	Timestamp	TimeDelta	EventRec	EventReco	Module	Summary
726	2016-05-23T16...	0,0008678	2388	3512	SMB2	Write, Status: Success, FileId: 0x0000001F005ACCBF,
736	2016-05-23T16...	0,0009557	2388	3512	SMB2	Flush, Status: Success, FileId: 0x0000001F005ACCBF,
740	2016-05-23T16...	0,0012952	2388	3512	SMB2	Write, Status: Success, FileId: 0x0000001F005ACCBF,
750	2016-05-23T16...	0,0009294	2388	3512	SMB2	Flush, Status: Success, FileId: 0x0000001F005ACCBF,
754	2016-05-23T16...	0,0012204	2388	3512	SMB2	Write, Status: Success, FileId: 0x0000001F005ACCBF,
767	2016-05-23T16...	0,0011969	2388	3512	SMB2	Write, Status: Success, FileId: 0x0000001F005ACCBF,
780	2016-05-23T16...	0,0008256	2388	3512	SMB2	Flush, Status: Success, FileId: 0x0000001F005ACCBF,
784	2016-05-23T16...	0,0013921	2388	3512	SMB2	Close, Status: Success, FileId: 0x0000001F005ACCBF,
788	2016-05-23T16...	0,0009605	2388	3512	SMB2	Create, Status: Success, FileName: Remote Desktop M
792	2016-05-23T16...	0,0008826	2388	3512	SMB2	SetInfo, Status: Success, FileId: 0x0000001F005ACCBF,
796	2016-05-23T16...	0,0003786	2388	3512	SMB2	Close, Status: Success, FileId: 0x0000001F005ACCBF,
14069	2016-05-23T16...	6,5667435	1240	3516	SMB	ComNegotiate, Status: STATUS_SUCCESS, Selected Dial
14076	2016-05-23T16...	0,0018667	4	9088	SMB2	Negotiate, Status: Success, ClientGuid: {99c22400-0
14081	2016-05-23T16...	0,0018667	1240	3516	SMB	ComSessionSetup, Status: STATUS_SUCCESS, Mapped

Algunos parámetros de netsh trace

- **persistent:**
 - Los valores posibles son yes o no, el valor por defecto es no
 - Si configuramos el valor persistent a yes, conseguiremos que la captura siga aunque reiniciemos el equipo
 - Solo se detendrá la captura cuando ejecutemos: netsh trace stop
- **maxSize:**
 - Valor en MB correspondiente al fichero generado, el valor por defecto es de 250
 - Si configuramos 0, corresponde a ilimitado
- **fileMode:**
 - Circular, significa que la captura, al llegar al valor especificado como maxSize por defecto 250MB, empezará a sobrescribirse la información

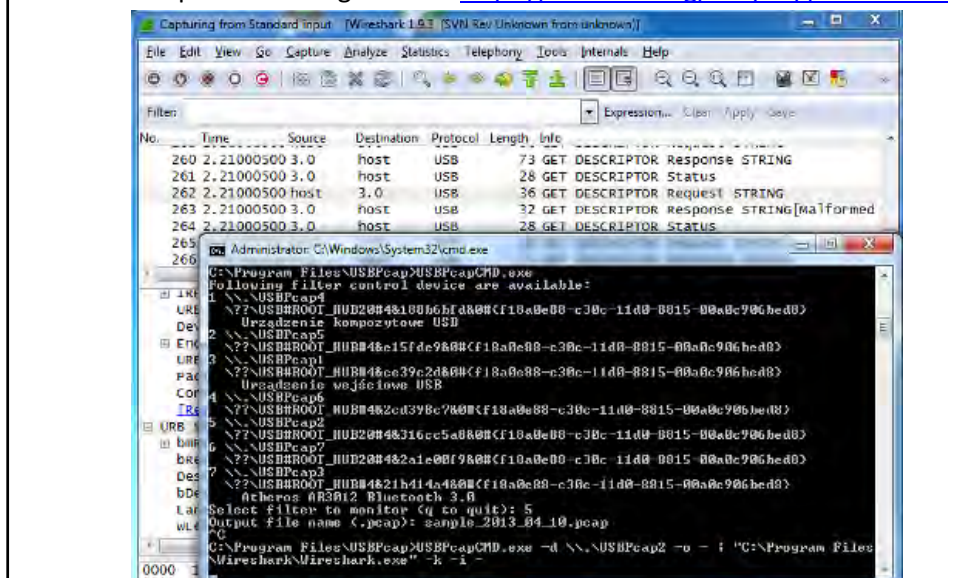
Recomendación:

filtrar el tráfico al realizar la captura

- Si filtramos el tráfico en la propia captura conseguiremos un tamaño de fichero muy mas manejable para su posterior análisis.
- Si ejecutamos el comando siguiente, veremos todas las parámetros disponibles de filtrado:
 - netsh trace show CaptureFilterHelp
- Algunos ejemplos sobre la posibilidad de filtrado:
 - Indicar el interfaz de red a utilizar en la captura
 - Filtrado por dirección MAC: Origen, destino o ambas
 - Filtrado por IP origen / destino
 - Filtrado por IPv4 o IPv6
 - Filtrado TCP / UDP
- También es posible concatenar filtros

Sugerencia de estudio

- USBPcap: aplicación Windows libre para realizar capturas
 - Se puede descargar desde <https://desowin.org/usbpcap/index.html>



Cuarta parte: Operación con sniffers (Uso de ntopng sobre Ubuntu Server para monitorizar tráfico de redes)

¿Qué es ntopng?

- Ntopng is a free and open source software for monitoring network traffic that provides a web interface for real-time network monitoring. It is the next generation version of the original ntop that shows the network usage, similar to what the popular top Unix command does
- It supports different operating system like, Unix, Linux, Mac OS, BSD and Windows
- We will use Ubuntu Server

Install Ntopng

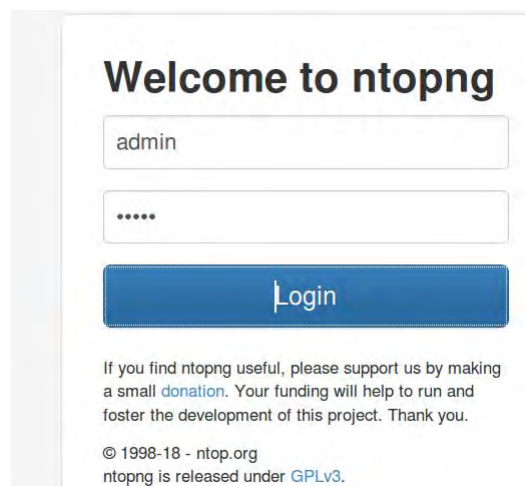
- By default, Ntopng is not available in Ubuntu 18.04 default repository
- So you will need to install the repository for Ntopng. You can download and install Ntopng repository with the following command:
 - **wget <http://apt.ntop.org/18.04/all/apt-ntop.deb>**
 - **sudo dpkg -i apt-ntop.deb**
- Once the repository is installed, update the repository and install Ntopng with the following command:
 - **sudo apt-get update -y**
 - **sudo apt-get install pfring-dkms nprobe ntopng n2disk cento -y**

Configure Ntopng

- After installing Ntopng, you will need to modify Ntopng default configuration file located at `/etc/ntopng/ntopng.conf`:
 - `sudo nano /etc/ntopng/ntopng.conf`
- Make the following changes:
 - `-G=/var/run/ntopng.pid`
 - `##Specifies the network interface or collector endpoint to be used by ntopng for network monitoring.`
 - `-i=enp0s3`
 - `##Sets the HTTP port of the embedded web server.`
 - `-w=3000`
- Save and close the file, then create a `ntopng.start` file:
 - `sudo nano /etc/ntopng/ntopng.start`
- Add the following lines as per your network:
 - `--local-networks "192.168.0.0/24" ## give your local IP Ranges here.`
 - `--interface 1`
- Save and close the file, then restart Ntopng and enable it to start on boot time:
 - `sudo systemctl start ntopng`
 - `sudo systemctl enable ntopng`

Access Ntopng

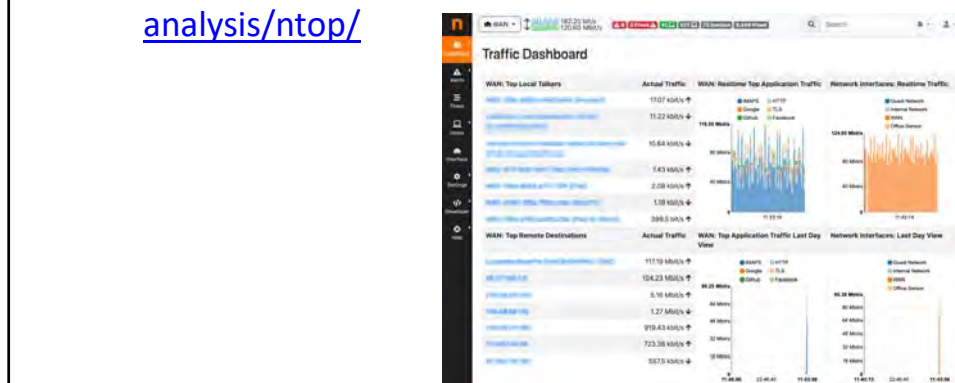
- Ntopng is now installed and listening on port 3000. Now, open your web browser and type the URL `http://your-server-ip:3000`. You will be redirected to the following page:



The screenshot shows the Ntopng web interface. At the top, it says "Welcome to ntopng". Below this, there are two input fields: the first contains the text "admin" and the second contains six dots, indicating a password field. Below the input fields is a blue button with the text "Login". At the bottom of the page, there is a small text block that reads: "If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you." Below this, it says "© 1998-18 - ntop.org" and "ntopng is released under [GPLv3](#)."

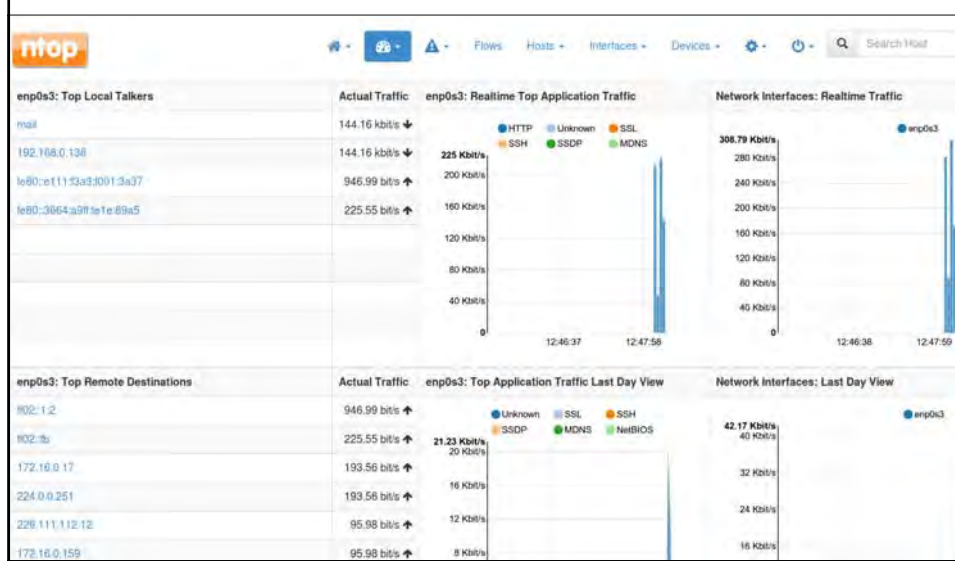
Existe versión ntopng para Windows

- Puede obtenerse información y descargarse desde :
 - <https://www.ntop.org/products/traffic-analysis/ntop/>



Más información:

<https://www.ntop.org/products/traffic-analysis/ntop/>



Para entregar

- Una vez finalizada la práctica deberás entregar:
 - El informe de práctica con los detalles de ejecución según la plantilla de prácticas
 - Las pantallas más significativas que demuestren la ejecución (no necesariamente del ejemplo, pero si hay que utilizar el resto de herramientas con un escenario imaginado por ti)

Simplificando y resumiendo la entrega de esta práctica

- 1. Estudiar el contenido de las diapositivas propuestas, explorando también los enlaces adjuntos.
- 2. Montar un Linux en que instalemos wireshark (sugiero un Ubuntu Desktop para poder iniciar un Firefox y navegar con él para capturar tráfico de navegación). Hacer algunas pruebas de captura y documentarlas.
- 3. Lo mismo sobre un Windows pero con Microsoft Message Analyzer y con NetworkMiner en vez de con Wireshark.
- 4. Sobre un Linux (cualquiera), explorar las posibilidades de tcpdump, hacer unas pruebas semejantes a las que se describen en las diapositivas y documentarlas. Opcional. lo mismo con Windows y Windump.
- 5. Sobre un Windows (cualquiera), hacer capturas con "netsh trace" como aparece en las diapos.
- 6. Opcional, para quien quiera nota: ensayar la instalación y configuración básica de ntopng.
- Notas:
 - 1. En los sistemas Windows, conviene tener los antivirus desactivados porque Windows detectará algunos sniffers como malware, ya que se pueden utilizar para producir ataques.
 - 2. Recordar (muy importante): utilizar sistemas con nombres que os identifiquen, así como las cuentas de usuario y nombres de ficheros o carpetas que se utilicen