INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

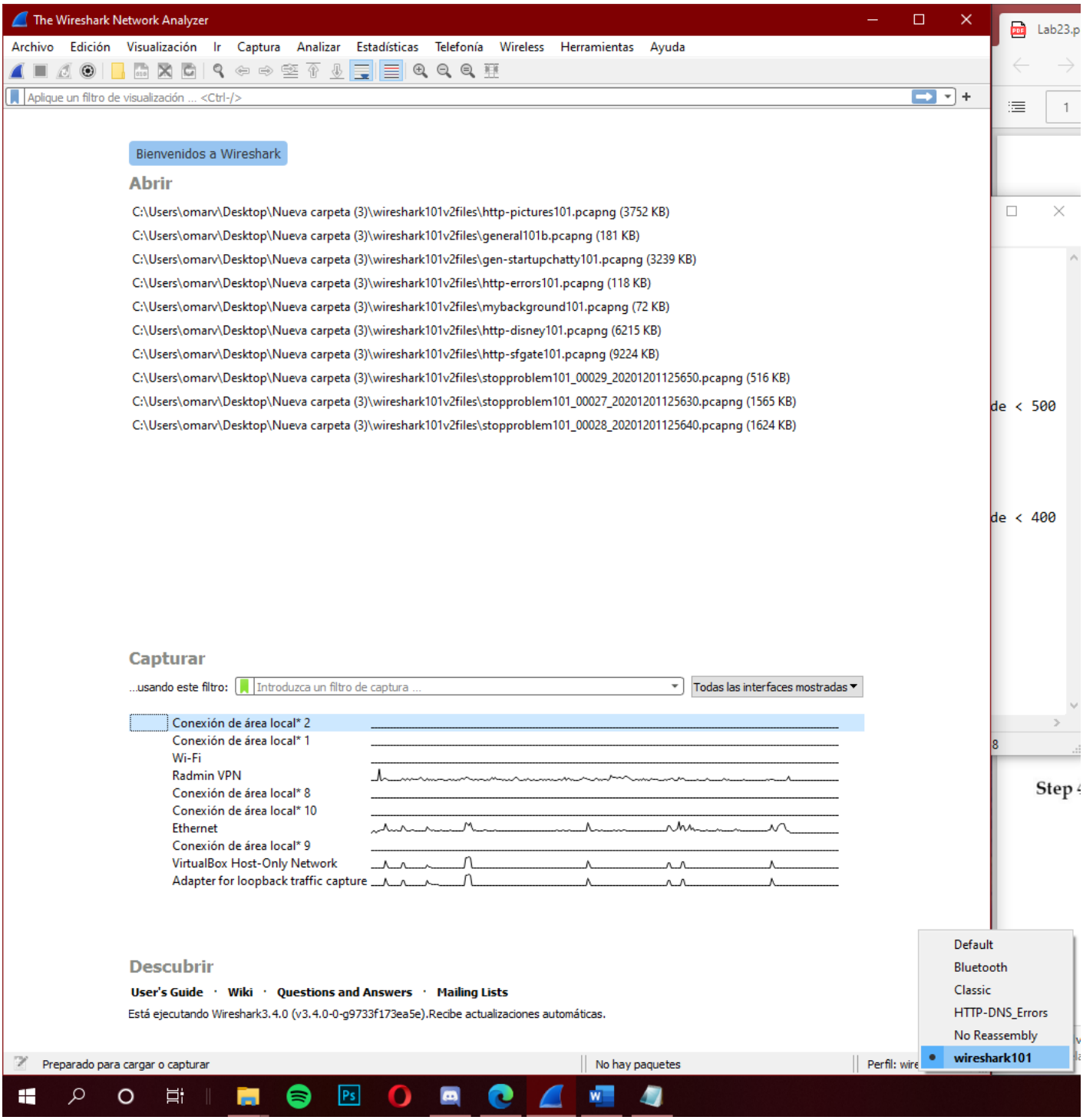
N.º De Actividad: Laboratorio 23

Nombre Del Alumno: Vazquez Canto Andres Omar

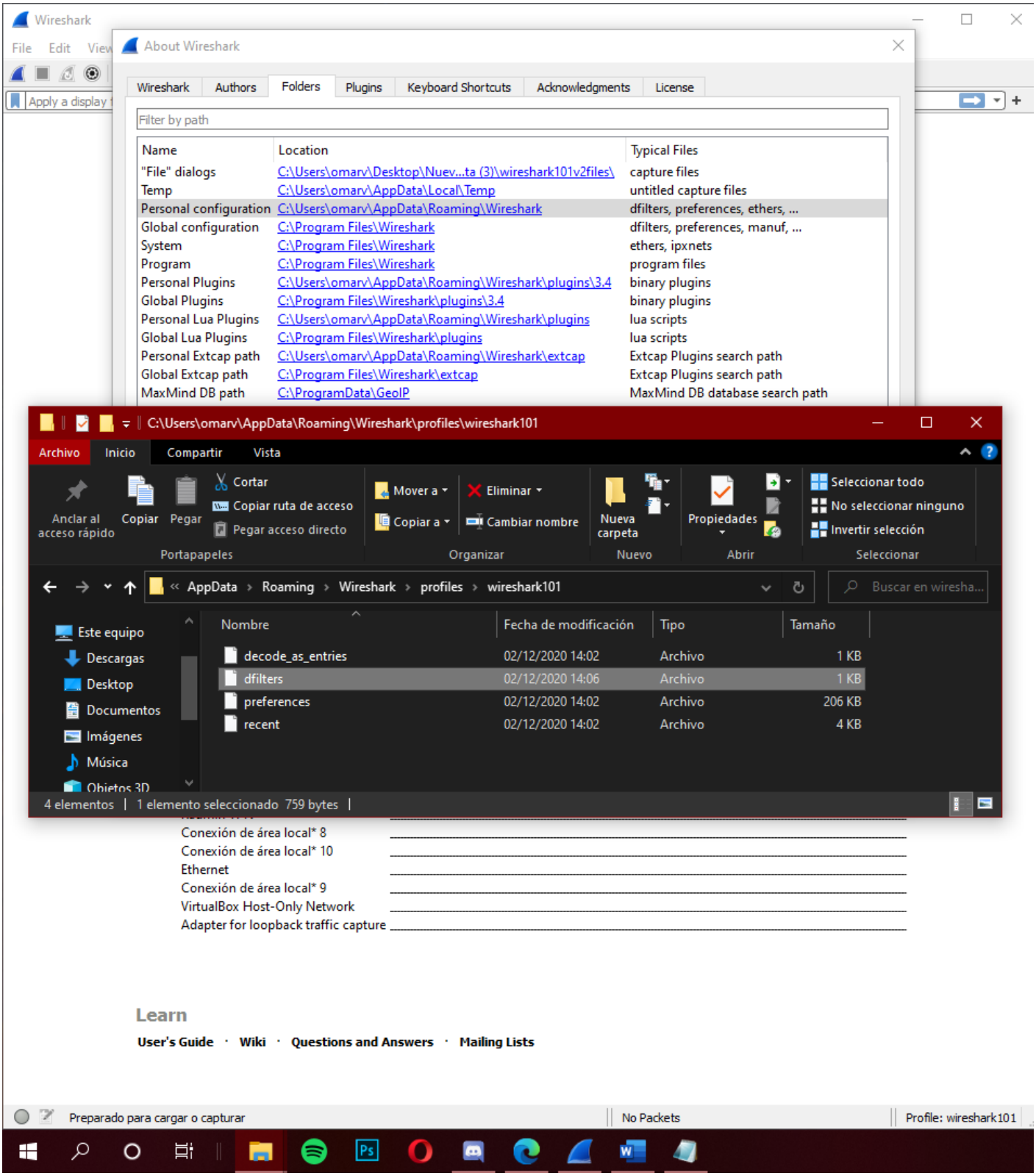
N.º De Control: 17530439

Lab23- Impot Display Filters into a Profile

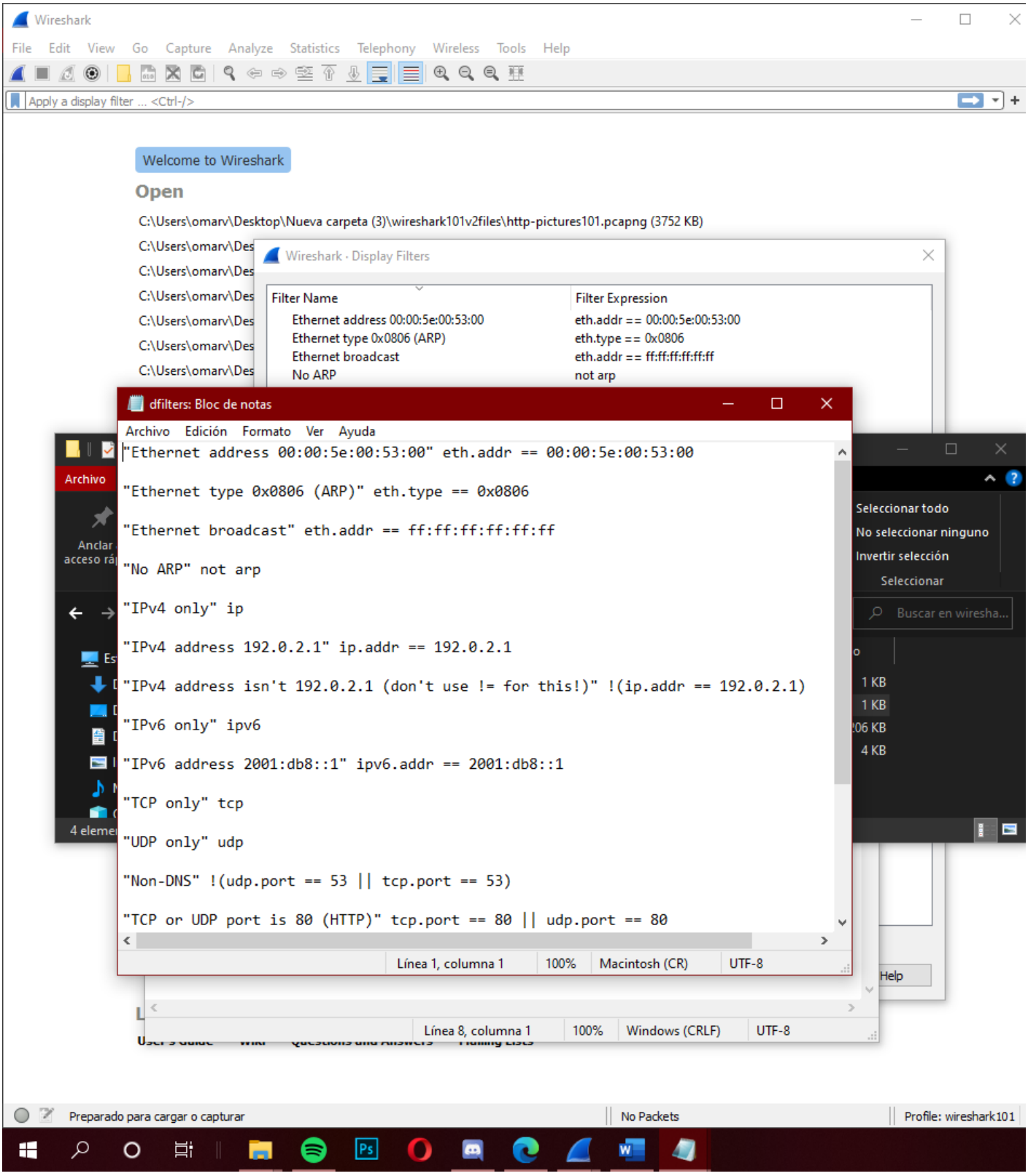
Paso 1:



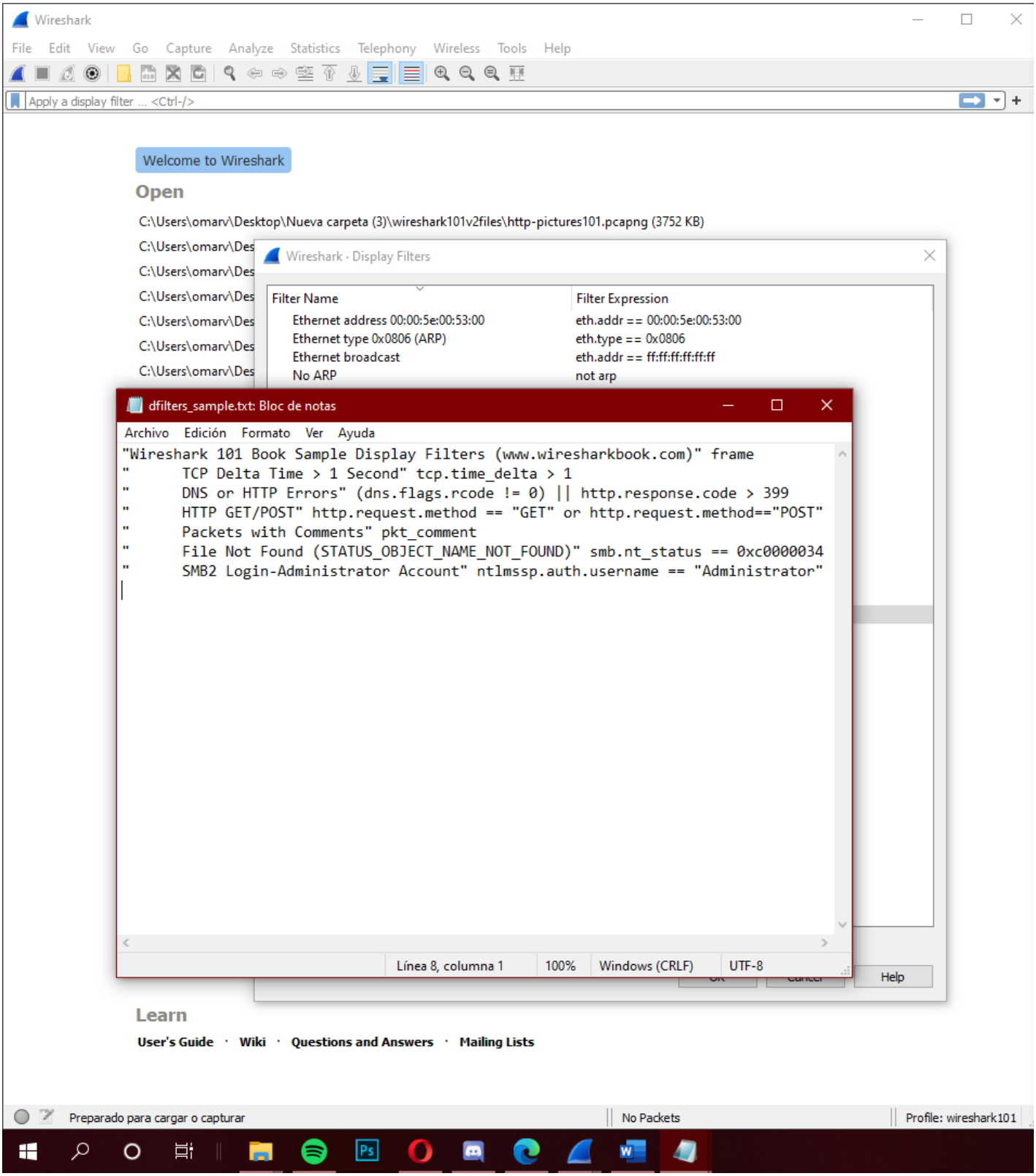
Paso 2:


Wireshark
File Edit View
Apply a display filter
About Wireshark
Wireshark Authors Folders Plugins Keyboard Shortcuts Acknowledgments License
Filter by path
Name Location Typical Files
"File" dialogs C:\Users\omarv\Desktop\Nuev...ta (3)\wireshark101v2files\ capture files
Temp C:\Users\omarv\AppData\Local\Temp untitled capture files
Personal configuration C:\Users\omarv\AppData\Roaming\Wireshark dfilters, preferences, ethers, ...
Global configuration C:\Program Files\Wireshark dfilters, preferences, manuf, ...
System C:\Program Files\Wireshark ethers, ipxnets
Program C:\Program Files\Wireshark program files
Personal Plugins C:\Users\omarv\AppData\Roaming\Wireshark\plugins\3.4 binary plugins
Global Plugins C:\Program Files\Wireshark\plugins\3.4 binary plugins
Personal Lua Plugins C:\Users\omarv\AppData\Roaming\Wireshark\plugins lua scripts
Global Lua Plugins C:\Program Files\Wireshark\plugins lua scripts
Personal Extcap path C:\Users\omarv\AppData\Roaming\Wireshark\extcap Extcap Plugins search path
Global Extcap path C:\Program Files\Wireshark\extcap Extcap Plugins search path
MaxMind DB path C:\ProgramData\GeoIP MaxMind DB database search path
C:\Users\omarv\AppData\Roaming\Wireshark\profiles\wireshark101
Archivo Inicio Compartir Vista
Anclar al acceso rápido
Copiar
Pegar
Cortar
Copiar ruta de acceso
Pegar acceso directo
Portapapeles
Mover a
Copiar a
Eliminar
Cambiar nombre
Organizar
Nueva carpeta
Nuevo
Propiedades
Abrir
Seleccionar todo
No seleccionar ninguno
Invertir selección
Seleccionar
AppData › Roaming › Wireshark › profiles › wireshark101
Buscar en wiresha...
Este equipo
Descargas
Desktop
Documentos
Imágenes
Música
Objetos 3D
Nombre Fecha de modificación Tipo Tamaño
decode_as_entries 02/12/2020 14:02 Archivo 1 KB
dfilters 02/12/2020 14:06 Archivo 1 KB
preferences 02/12/2020 14:02 Archivo 206 KB
recent 02/12/2020 14:02 Archivo 4 KB
4 elementos | 1 elemento seleccionado 759 bytes |
Conexión de área local* 8
Conexión de área local* 10
Ethernet
Conexión de área local* 9
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Preparado para cargar o capturar
No Packets
Profile: wireshark101

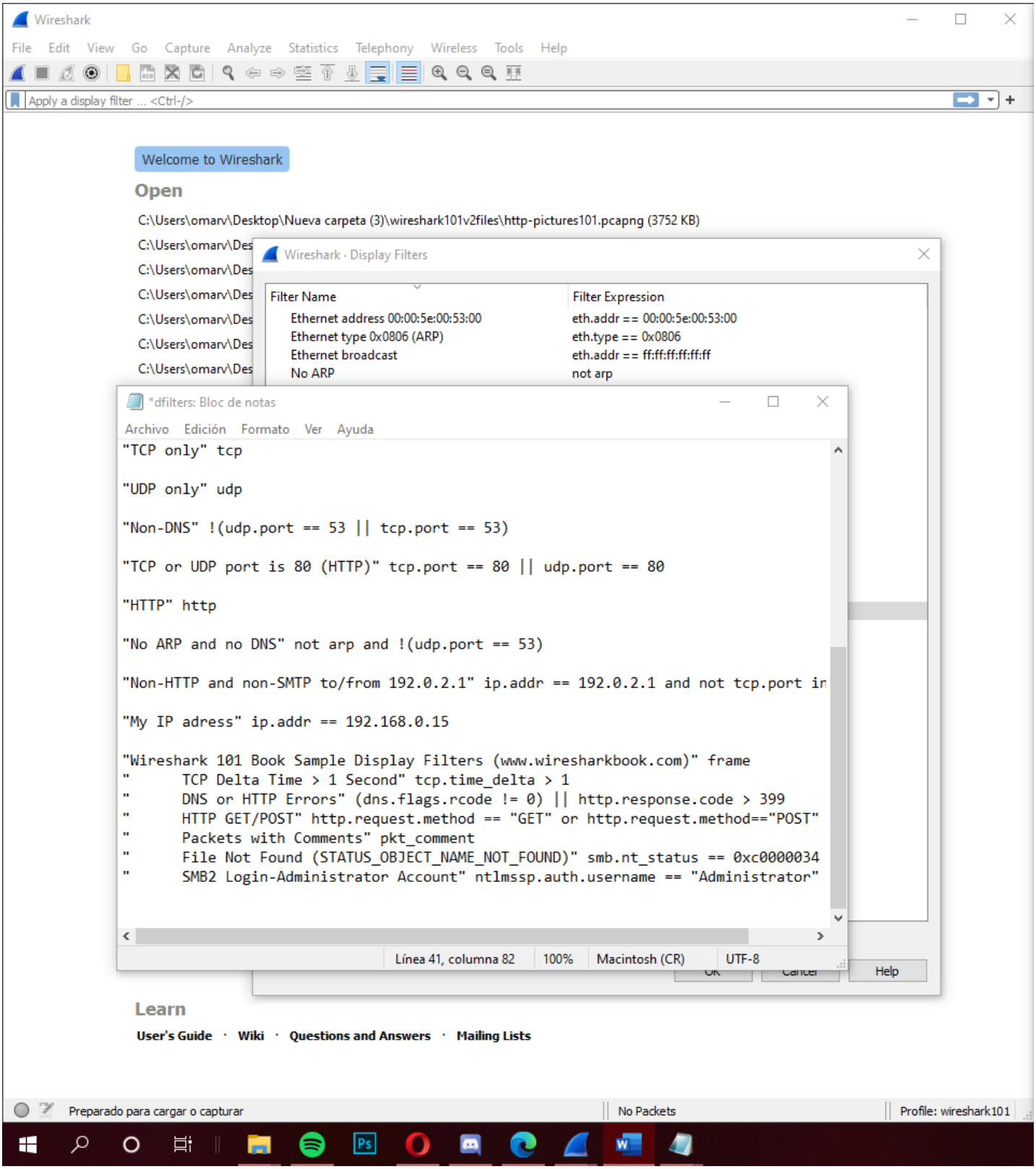
Paso 3:


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pictures101.pcapng (3752 KB)
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
dfilters: Bloc de notas
Archivo Edición Formato Ver Ayuda
"Ethernet address 00:00:5e:00:53:00" eth.addr == 00:00:5e:00:53:00
"Ethernet type 0x0806 (ARP)" eth.type == 0x0806
"Ethernet broadcast" eth.addr == ff:ff:ff:ff:ff:ff
"No ARP" not arp
"IPv4 only" ip
"IPv4 address 192.0.2.1" ip.addr == 192.0.2.1
"IPv4 address isn't 192.0.2.1 (don't use != for this!)" !(ip.addr == 192.0.2.1)
"IPv6 only" ipv6
"IPv6 address 2001:db8::1" ipv6.addr == 2001:db8::1
"TCP only" tcp
"UDP only" udp
"Non-DNS" !(udp.port == 53 || tcp.port == 53)
"TCP or UDP port is 80 (HTTP)" tcp.port == 80 || udp.port == 80
Línea 1, columna 1 100% Macintosh (CR) UTF-8
Línea 8, columna 1 100% Windows (CRLF) UTF-8
Archivo
Seleccionar todo
No seleccionar ninguno
Invertir selección
Seleccionar
Buscar en wiresha...
Help
Preparado para cargar o capturar
No Packets
Profile: wireshark101

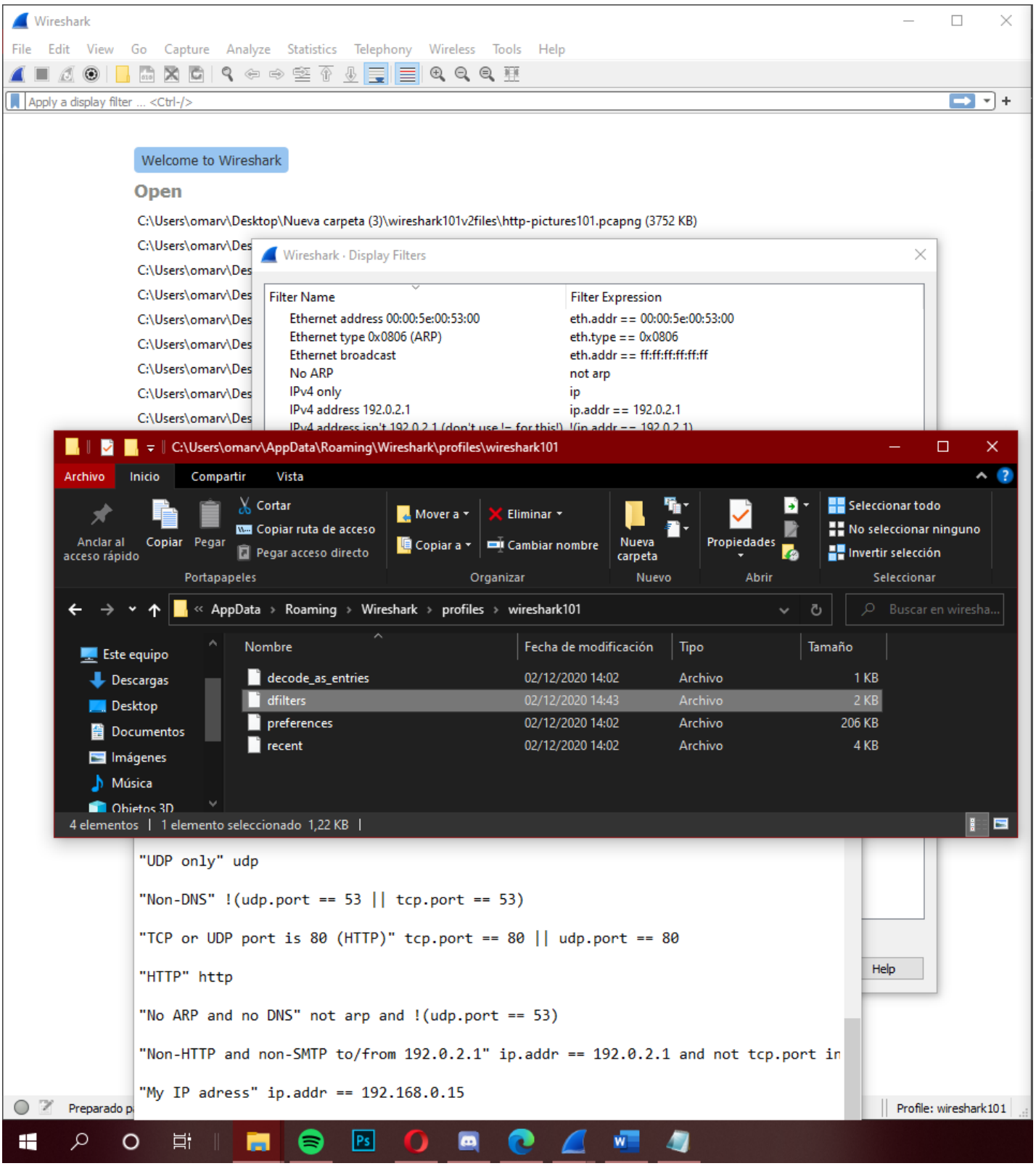
PASO 4:


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pictures101.pcapng (3752 KB)
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
dfilters_sample.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
"Wireshark 101 Book Sample Display Filters (www.wiresharkbook.com)" frame
" TCP Delta Time > 1 Second" tcp.time_delta > 1
" DNS or HTTP Errors" (dns.flags.rcode != 0) || http.response.code > 399
" HTTP GET/POST" http.request.method == "GET" or http.request.method=="POST"
" Packets with Comments" pkt_comment
" File Not Found (STATUS_OBJECT_NAME_NOT_FOUND)" smb.nt_status == 0xc0000034
" SMB2 Login-Administrator Account" ntlmssp.auth.username == "Administrator"
Línea 8, columna 1
100%
Windows (CRLF)
UTF-8
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Preparado para cargar o capturar
No Packets
Profile: wireshark101

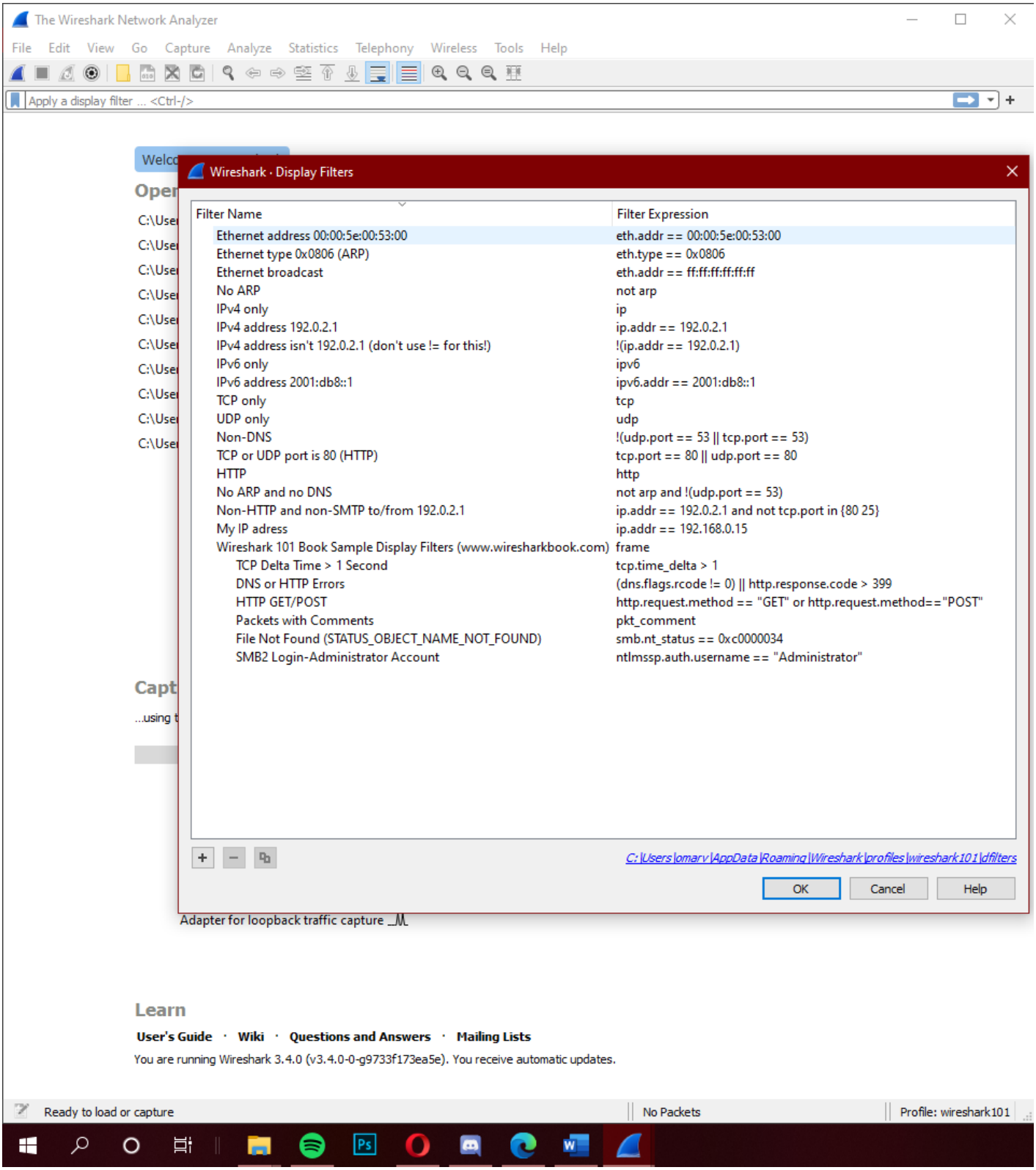
Paso 5:


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pictures101.pcapng (3752 KB)
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
*dfilters: Bloc de notas
Archivo Edición Formato Ver Ayuda
"TCP only" tcp
"UDP only" udp
"Non-DNS" !(udp.port == 53 || tcp.port == 53)
"TCP or UDP port is 80 (HTTP)" tcp.port == 80 || udp.port == 80
"HTTP" http
"No ARP and no DNS" not arp and !(udp.port == 53)
"Non-HTTP and non-SMTP to/from 192.0.2.1" ip.addr == 192.0.2.1 and not tcp.port in
"My IP adress" ip.addr == 192.168.0.15
"Wireshark 101 Book Sample Display Filters (www.wiresharkbook.com)" frame
" TCP Delta Time > 1 Second" tcp.time_delta > 1
" DNS or HTTP Errors" (dns.flags.rcode != 0) || http.response.code > 399
" HTTP GET/POST" http.request.method == "GET" or http.request.method=="POST"
" Packets with Comments" pkt_comment
" File Not Found (STATUS_OBJECT_NAME_NOT_FOUND)" smb.nt_status == 0xc0000034
" SMB2 Login-Administrator Account" ntlmssp.auth.username == "Administrator"
Línea 41, columna 82
100%
Macintosh (CR)
UTF-8
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Preparado para cargar o capturar
No Packets
Profile: wireshark101

Paso 6:


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pictures101.pcapng (3752 KB)
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
ip.addr == 192.0.2.1
C:\Users\omarv\AppData\Roaming\Wireshark\profiles\wireshark101
Archivo Inicio Compartir Vista
Anclar al acceso rápido
Copiar
Pegar
Cortar
Copiar ruta de acceso
Pegar acceso directo
Portapapeles
Mover a
Copiar a
Eliminar
Cambiar nombre
Organizar
Nueva carpeta
Nuevo
Propiedades
Abrir
Seleccionar todo
No seleccionar ninguno
Invertir selección
Seleccionar
AppData › Roaming › Wireshark › profiles › wireshark101
Buscar en wiresha...
Este equipo
Descargas
Desktop
Documentos
Imágenes
Música
Objetos 3D
Nombre
Fecha de modificación
Tipo
Tamaño
decode_as_entries
02/12/2020 14:02
Archivo
1 KB
dfilters
02/12/2020 14:43
Archivo
2 KB
preferences
02/12/2020 14:02
Archivo
206 KB
recent
02/12/2020 14:02
Archivo
4 KB
4 elementos | 1 elemento seleccionado 1,22 KB
"UDP only" udp
"Non-DNS" !(udp.port == 53 || tcp.port == 53)
"TCP or UDP port is 80 (HTTP)" tcp.port == 80 || udp.port == 80
"HTTP" http
"No ARP and no DNS" not arp and !(udp.port == 53)
"Non-HTTP and non-SMTP to/from 192.0.2.1" ip.addr == 192.0.2.1 and not tcp.port in
"My IP adress" ip.addr == 192.168.0.15
Help
Profile: wireshark101

Paso 7 y 8


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00 eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP) eth.type == 0x0806
Ethernet broadcast eth.addr == ff:ff:ff:ff:ff:ff
No ARP not arp
IPv4 only ip
IPv4 address 192.0.2.1 ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!) !(ip.addr == 192.0.2.1)
IPv6 only ipv6
IPv6 address 2001:db8::1 ipv6.addr == 2001:db8::1
TCP only tcp
UDP only udp
Non-DNS !(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP) tcp.port == 80 || udp.port == 80
HTTP http
No ARP and no DNS not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1 ip.addr == 192.0.2.1 and not tcp.port in {80 25}
My IP adress ip.addr == 192.168.0.15
Wireshark 101 Book Sample Display Filters (www.wiresharkbook.com) frame
TCP Delta Time > 1 Second tcp.time_delta > 1
DNS or HTTP Errors (dns.flags.rcode != 0) || http.response.code > 399
HTTP GET/POST http.request.method == "GET" or http.request.method=="POST"
Packets with Comments pkt_comment
File Not Found (STATUS_OBJECT_NAME_NOT_FOUND) smb.nt_status == 0xc0000034
SMB2 Login-Administrator Account ntlmssp.auth.username == "Administrator"
C:\Users\omarv\AppData\Roaming\Wireshark\profiles\wireshark101\dfilters
OK
Cancel
Help
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.4.0 (v3.4.0-0-g9733f173ea5e). You receive automatic updates.
Ready to load or capture
No Packets
Profile: wireshark101