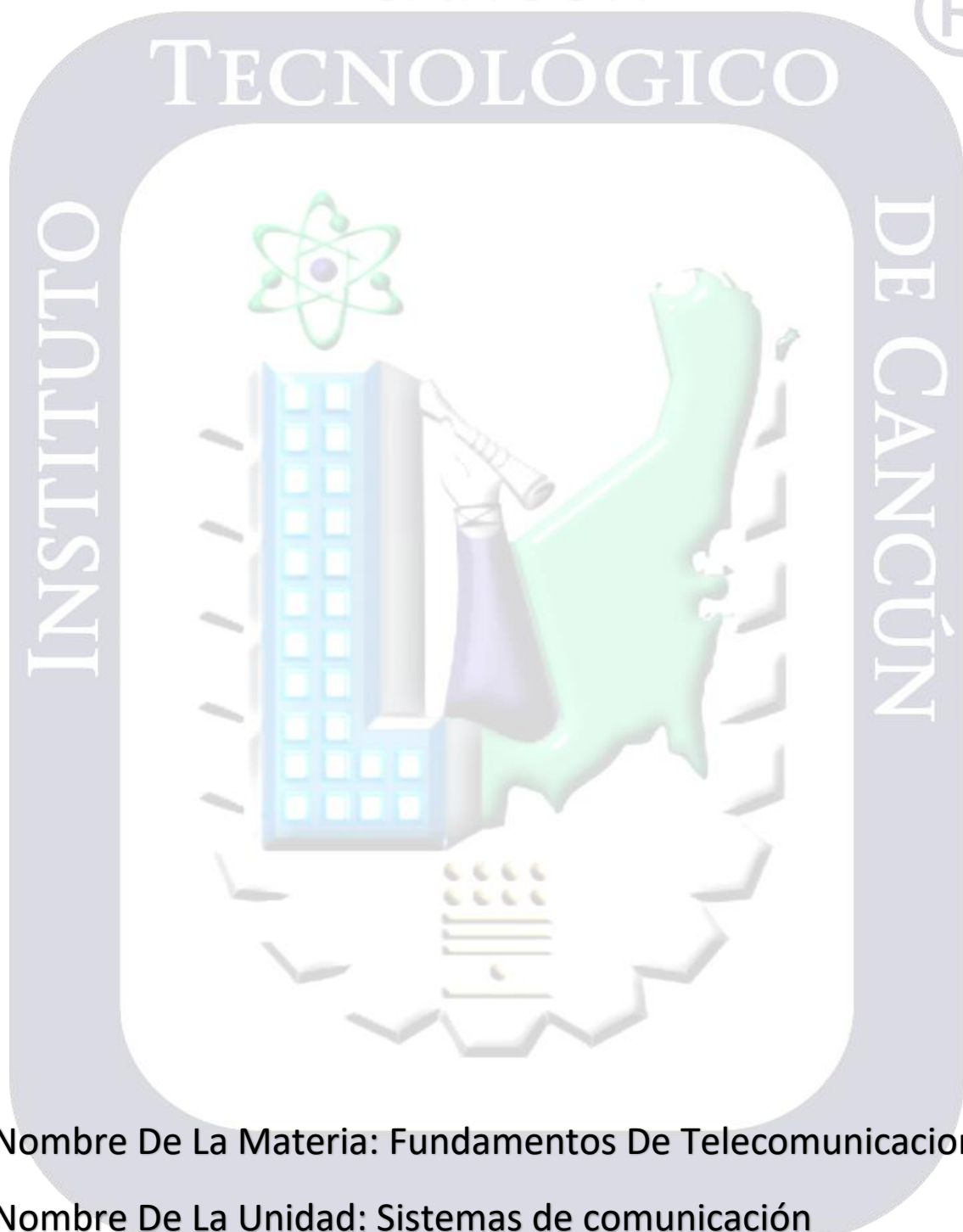


INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 15

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab15- Use a Default Filter as a Seed for a New Filter

Paso 1:

The screenshot shows two windows from a Windows operating system. The top window is Wireshark, displaying a packet capture filter 'http.request.method=="POST"' and a list of three OCSP requests to 'ocsp.verisign.com'. The bottom window is 'Selección de Símbolo del sistema' (System Information), showing details about the laptop's network configuration, including the Ethernet adapter 'Realtek PCIe GbE Family Controller' with IP address '192.168.0.15' and the NetBIOS over TCP/IP status as 'enabled'.

Wireshark window details:

- Filter: http.request.method=="POST"
- Table with 4 columns: Protocol, Length, Info, Host
- Three entries: OCSP, 522, Request, ocsp.verisign.com

System Information window details:

- Nombre de host: LAPTOP-PUTH40FI
- Sufijo DNS principal: (empty)
- Tipo de nodo: híbrido
- Enrutamiento IP habilitado: no
- Proxy WINS habilitado: no
- Adaptador de Ethernet Ethernet:
 - Sufijo DNS específico para la conexión: (empty)
 - Descripción: Realtek PCIe GbE Family Controller
 - Dirección física: C4-65-16-BF-8D-83
 - DHCP habilitado: sí
 - Configuración automática habilitada: sí
 - Vínculo: dirección IPv6 local: fe80::f87c:7da1:ba5a:888f%13(Preferido)
 - Dirección IPv4: 192.168.0.15(Preferido)
 - Máscara de subred: 255.255.255.0
 - Concesión obtenida: martes, 1 de diciembre de 2020 15:41:48
 - La concesión expira: martes, 1 de diciembre de 2020 21:26:38
 - Puerta de enlace predeterminada: 192.168.0.1
 - Servidor DHCP: 192.168.0.1
 - IAID DHCPv6: 113534230
 - DUID de cliente DHCPv6: 00-01-00-01-26-C2-36-F4-A4-FC-77-6A-E9-85
 - Servidores DNS: fe80::1%13, 10.223.234.2, 187.253.45.10
- NetBIOS sobre TCP/IP: habilitado
- Adaptador de Ethernet Radmin VPN: (empty)

Network traffic details (bottom of System Information window):

Time	Source	Destination	Protocol	Length	Info
0050	61 6e 64 6c 65 72 73 2f	73 66 67 53 75 70 70 6f	andlers/	sfgSuppo	
0060	72 74 4d 61 69 6c 48 61	6e 64 6c 65 72 2e 70 68	rtMailHa	ndler.ph	
0070	70 20 48 54 54 50 2f 31	2e 31 0d 0a 48 6f 73 74	p HTTP/1	.1·Host	
0080	3a 20 65 78 74 72 61 73	2e 73 66 67 61 74 65 2e	:	extras .sfgate.	
0090	63 6f 6d 0d 0a 55 73 65	72 2d 41 67 65 6e 74 3a	com·Use	r-Agent:	
00a0	20 4d 6f 7a 69 6c 6c 61	2f 35 2e 30 20 28 57 69	Mozilla	/5.0 (Wi	
00b0	6e 64 6f 77 73 20 4e 54	20 36 2e 31 3b 20 57 4f	ndows NT	6.1; W0	
00c0	57 36 34 3b 20 72 76 3a	31 36 2e 30 29 20 47 65	W64; rv:	16.0) Ge	
00d0	63 6b 6f 2f 32 30 31 30	30 31 30 31 20 46 69 72	cko/2010	0101 Fir	
00e0	65 66 6f 78 2f 31 36 2e	30 0d 0a 41 63 63 65 70	efox/16.	0·Accep	
00f0	74 3a 20 74 65 78 74 2f	68 74 6d 6c 2c 61 70 70	t: text/	html,app	
0100	6c 69 63 61 74 69 6f 6e	2f 78 68 74 6d 6c 2b 78	lication	/xhtml+x	
0110	6d 6c 2c 61 70 70 6c 69	63 61 74 69 6f 6e 2f 78	ml,appli	cation/x	
0120	6d 6c 3b 71 3d 30 2e 39	2c 2a 2f 2a 3b 71 3d 30	ml;q=0.9	,*/*;q=0	
0130	2e 38 0d 0a 41 63 63 65	70 74 2d 4c 61 6e 67 75	.8·Acce	pt-Langu	
0140	61 67 65 3a 20 65 6e 2d	55 53 2c 65 6e 3b 71 3d	age: en-	US,en;q=	
0150	30 2e 35 0d 0a 41 63 63	65 70 74 2d 45 6e 63 6f	0.5·Acc	ept-Enco	
0160	64 69 6e 67 3a 20 67 7a	69 70 2c 20 64 65 66 6c	ding: gz	ip, defl	
0170	61 74 65 0d 0a 43 6f 6e	6e 65 63 74 69 6f 6e 3a	ate·Con	nection:	
0180	20 6b 65 65 70 2d 61 6c	69 76 65 0d 0a 52 65 66	keep-al	ive·Ref	
0190	65 72 65 72 3a 20 68 74	74 70 3a 2f 2f 77 77 77	erer: ht	tp://www	
01a0	2e 73 66 67 61 74 65 2e	63 6f 6d 2f 66 65 65 64	.sfgate.	com/feed	

Paso 2:

The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture of an HTTP request from 'http-sfgate101.pcapng'. The packet list on the left shows several packets, with packet 27 selected, which is an HTTP GET request to 'http-sfgate101.pcapng'. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

The 'Wireshark · Display Filters' dialog box is open, showing a list of filter names and their corresponding filter expressions. The filter expressions are as follows:

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}

The dialog box has 'OK', 'Cancel', and 'Help' buttons at the bottom right.

Paso 3:

The screenshot shows the Wireshark network protocol analyzer interface. A 'Display Filters' dialog box is open, allowing the user to refine the packet list. The dialog has two columns: 'Filter Name' and 'Filter Expression'. The 'Filter Name' column lists various network protocols and their attributes, while the 'Filter Expression' column shows the corresponding filter syntax. The 'IPv4 address 192.0.2.1' filter is currently selected and highlighted in blue. Below the list, there are buttons for '+', '-', and a button with a square icon. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

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}
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1

The background shows the main Wireshark window with a packet capture of an HTTP request. The packet list on the left shows a sequence of packets, with the selected packet being an HTTP request. The packet details pane on the right shows the structure of the selected packet, including the Ethernet II, Internet Protocol, and Hypertext Transfer Protocol layers. The packet bytes pane at the bottom shows the raw data of the selected packet.

Paso 4:

The screenshot shows the Wireshark network protocol analyzer interface. The main window displays a packet capture of `http-sfgate101.pcapng`. The packet list on the left shows several HTTP requests to `ojsp.verisign.com`. The packet details pane on the right shows the structure of a POST request. The packet bytes pane at the bottom shows the raw data. A "Wireshark - Display Filters" dialog box is open, showing a list of filter expressions, with `ip.addr == 10.1.10.1` selected.

Protocol	Length	Info	Host
OCSP	522	Request	ojsp.verisign.com
OCSP	522	Request	ojsp.verisign.com
OCSP	522	Request	ojsp.verisign.com
OCSP	522	Request	ojsp.verisign.com
OCSP	522	Request	ojsp.verisign.com
HTTP	805		
HTTP	944		
HTTP	1007		
HTTP	1338		
HTTP	1595		
HTTP	1233		
HTTP	841		

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}
IPv4 address	ip.addr == 10.1.10.1

Paso 5: Darle ok: