

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 17

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab17- Filter on Traffic to or from Online Backup Subnets

Paso 1:

The image shows a Windows desktop with a Wireshark packet capture window in the background and a 'Wireshark - Open Capture File' dialog box in the foreground.

Wireshark - Open Capture File Dialog:

- Buscar en:** wireshark 101v2files
- Nombre:** List of files including 'http-winpcap101.cap', 'http-wiresharkdownload101.pcapng', 'mybackground101.pcapng' (selected), and several 'mydns101_00001_20201201190000.pcapng' files.
- Fecha de modificación:** Dates ranging from 25/10/2012 to 01/12/2020.
- Tipo:** All files are 'Wireshark capture...'.
- Tamaño:** File sizes ranging from 1 KB to 20.714 KB.
- Nombre de archivo:** mybackground101.pcapng
- Tipo de archivo:** All Files
- Read filter:** Automatically detect file type
- Format:** Wireshark/... - pcapng
- Size:** 72 KB, 514 data records
- Start / elapsed:** 2012-10-22 18:28:45 / 00:02:49

Background Wireshark Packet Capture:

The background shows a packet capture of an HTTP request. The packet list shows a packet of type 'HTTP Request Method' with a size of 3 bytes. The packet details show the following information:

- Agent:** Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Language:** en-US,en;q=0.5
- Accept-Encoding:** gzip, deflate
- Connection:** keep-alive

The packet bytes pane shows the raw data of the request, including the HTTP method and headers.

Paso 2:

The image shows a Wireshark network traffic capture window. The title bar reads "mybackground101.pcapng". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The packet list pane on the left shows a list of captured packets, with packet 31 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS response. The packet bytes pane at the bottom shows the raw data of the packet in hexadecimal and ASCII.

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 88, Info: Standard query 0x5183 A javadl-esd-secure.oracle.com

Source: 75.75.75.75, Destination: 24.6.173.220, Protocol: DNS, Length: 191, Info: Standard query response 0x5183 A javadl-esd-secure.oracle.com CNAME

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 88, Info: Standard query 0x5ae1 AAAA javadl-esd-secure.oracle.com

Source: 75.75.75.75, Destination: 24.6.173.220, Protocol: DNS, Length: 233, Info: Standard query response 0x5ae1 AAAA javadl-esd-secure.oracle.com C...

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 74, Info: Standard query 0x4372 A api.memeo.info

Source: 75.75.75.75, Destination: 24.6.173.220, Protocol: DNS, Length: 90, Info: Standard query response 0x4372 A api.memeo.info A 216.115.74.235

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 74, Info: Standard query 0x027b AAAA api.memeo.info

Source: 75.75.75.75, Destination: 24.6.173.220, Protocol: DNS, Length: 146, Info: Standard query response 0x027b AAAA api.memeo.info SOA a4.nstld.com

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 73, Info: Standard query 0x81b6 A api.memeo.com

Source: 75.75.75.75, Destination: 24.6.173.220, Protocol: DNS, Length: 89, Info: Standard query response 0x81b6 A api.memeo.com A 216.115.74.202

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 73, Info: Standard query 0xe061 AAAA api.memeo.com

Source: 75.75.75.75, Destination: 24.6.173.220, Protocol: DNS, Length: 142, Info: Standard query response 0xe061 AAAA api.memeo.com SOA a4.nstld.com

Source: 24.6.173.220, Destination: 75.75.75.75, Protocol: DNS, Length: 70, Info: Standard query 0xaad8 A memeo.info

> Frame 31: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B5}

> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)

> Internet Protocol Version 4, Src: 75.75.75.75, Dst: 24.6.173.220

> User Datagram Protocol, Src Port: 53, Dst Port: 58835

> Domain Name System (response)

0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 40 ..d.... \1....E@

0010 00 db 00 00 40 00 3b 11 e2 59 4b 4b 4b 4b 18 06@.;. YKKKK

0020 ad dc 00 35 e5 d3 00 c7 9c af 5a e1 81 80 00 01 ...5.... Z....

0030 00 02 00 01 00 00 11 6a 61 76 61 64 6c 2d 65 73j avadl-es

0040 64 2d 73 65 63 75 72 65 06 6f 72 61 63 6c 65 03 d-secure .oracle.

0050 63 6f 6d 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 com.....

0060 01 06 00 2a 11 6a 61 76 61 64 6c 2d 65 73 64 2d ...*.jav adl-esd-

0070 73 65 63 75 72 65 06 6f 72 61 63 6c 65 03 63 6f secure.o racle.co

0080 6d 07 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 3a m edgeke y net.:

0090 00 05 00 01 00 00 13 7f 00 15 05 65 35 34 38 36e5486

00a0 01 67 0a 61 6b 61 6d 61 69 65 64 67 65 c0 5f c0 .g.akama iedge_.

00b0 76 00 06 00 01 00 00 00 6e 00 2e 03 6e 30 67 c0 v.....n..n0g

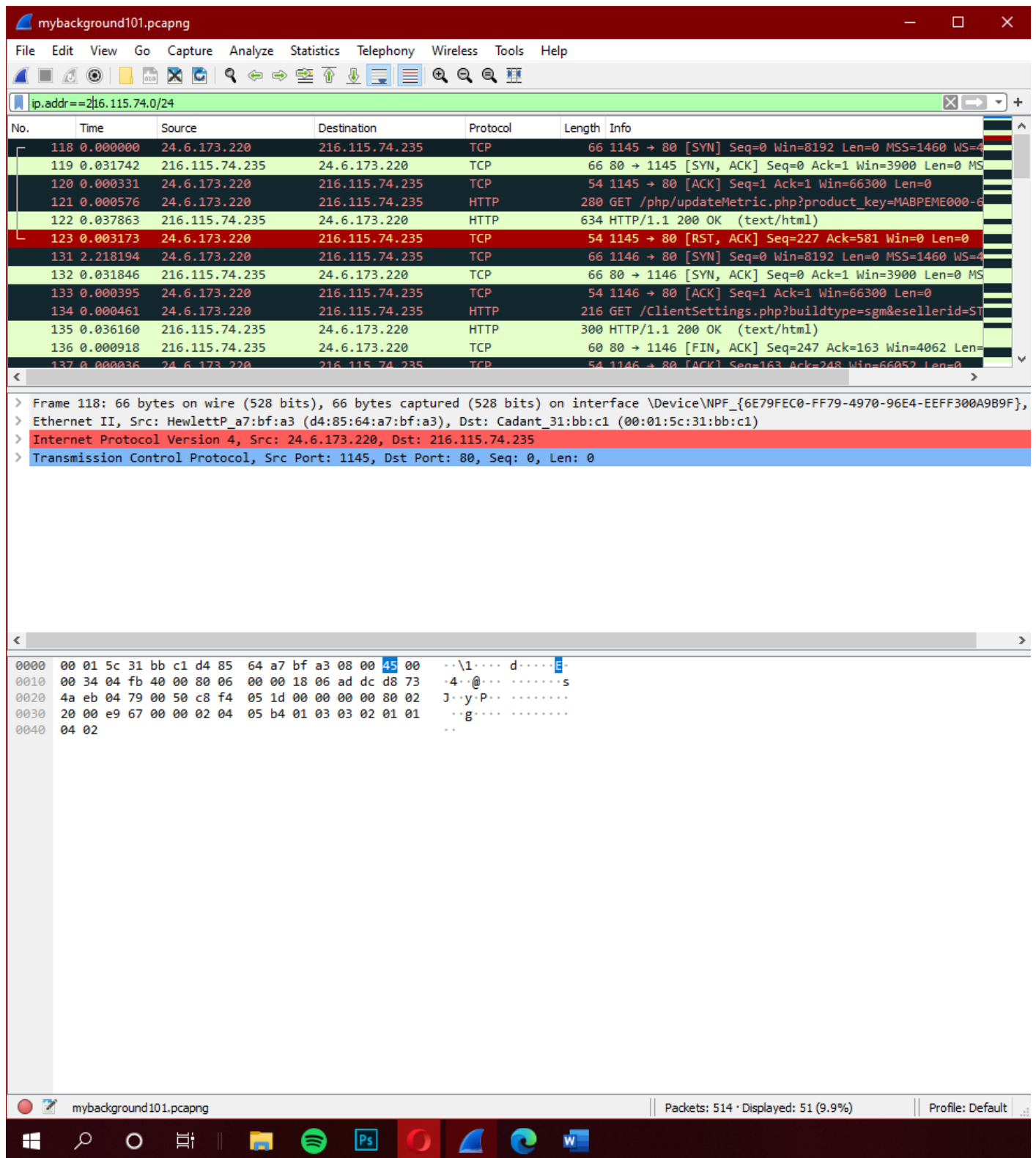
00c0 78 0a 68 6f 73 74 6d 61 73 74 65 72 06 61 6b 61 x hostma ster aka

00d0 6d 61 69 c0 25 50 85 d3 28 00 00 03 e8 00 00 03 mai.%P.. (.....

00e0 e8 00 00 03 e8 00 00 07 08

Domain Name System: Protocol | Packets: 514 · Displayed: 16 (3.1%) | Profile: Default

Paso 3:



The image shows a Wireshark packet capture analysis of a file named `mybackground101.pcapng`. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a filter bar set to `ip.addr==216.115.74.0/24`.

The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
118	0.000000	24.6.173.220	216.115.74.235	TCP	66	1145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
119	0.031742	216.115.74.235	24.6.173.220	TCP	66	80 → 1145 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MS
120	0.000331	24.6.173.220	216.115.74.235	TCP	54	1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
121	0.000576	24.6.173.220	216.115.74.235	HTTP	280	GET /php/updateMetric.php?product_key=MABPEME000-6
122	0.037863	216.115.74.235	24.6.173.220	HTTP	634	HTTP/1.1 200 OK (text/html)
123	0.003173	24.6.173.220	216.115.74.235	TCP	54	1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0
131	2.218194	24.6.173.220	216.115.74.235	TCP	66	1146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
132	0.031846	216.115.74.235	24.6.173.220	TCP	66	80 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MS
133	0.000395	24.6.173.220	216.115.74.235	TCP	54	1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
134	0.000461	24.6.173.220	216.115.74.235	HTTP	216	GET /ClientSettings.php?buildtype=sgm&esellerid=ST
135	0.036160	216.115.74.235	24.6.173.220	HTTP	300	HTTP/1.1 200 OK (text/html)
136	0.000918	216.115.74.235	24.6.173.220	TCP	60	80 → 1146 [FIN, ACK] Seq=247 Ack=163 Win=4062 Len=
137	0.000036	24.6.173.220	216.115.74.235	TCP	54	1146 → 80 [ACK] Seq=163 Ack=248 Win=66052 Len=0

The packet details pane for packet 118 shows the following structure:

- > Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F},
- > Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- > Internet Protocol Version 4, Src: 24.6.173.220, Dst: 216.115.74.235
- > Transmission Control Protocol, Src Port: 1145, Dst Port: 80, Seq: 0, Len: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00  ..\1... d....E-
0010 00 34 04 fb 40 00 80 06 00 00 18 06 ad dc d8 73  4..@... ..s
0020 4a eb 04 79 00 50 c8 f4 05 1d 00 00 00 00 80 02  J..y.P... ..
0030 20 00 e9 67 00 00 02 04 05 b4 01 03 03 02 01 01  ..g... ..
0040 04 02
```

The status bar at the bottom indicates: `mybackground101.pcapng`, `Packets: 514 · Displayed: 51 (9.9%)`, and `Profile: Default`.