

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 28

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab28- Use the Intelligent Scrollbar to quickly Find Problems

Paso 1:

The screenshot shows the Wireshark 'Open Capture File' dialog box and the main packet list. The dialog box is open, showing a list of files in the 'wireshark101v2files' directory. The file 'net-lost-route.pcapng' is selected. A tooltip for this file shows its type as 'Wireshark capture file', size as '86,8 KB', and modification date as '08/05/2012 15:17'. The dialog box also shows the file name, type, read filter, format, size, and start/elapsed time.

Wireshark - Open Capture File

Buscar en: wireshark101v2files

| Nombre | Fecha de modificación | Tipo | Tamaño |
|--|-------------------------|-----------------------------|--------------|
| mydns101_00018_20201201190240.pcapng | 01/12/2020 19:02 | Wireshark capture... | 1 KB |
| mydns101_00019_20201201190250.pcapng | 01/12/2020 19:03 | Wireshark capture... | 2 KB |
| mydns101_00020_20201201190300.pcapng | 01/12/2020 19:03 | Wireshark capture... | 1 KB |
| net-lost-route.pcapng | 08/05/2012 15:17 | Wireshark capture... | 87 KB |
| sec-concern101.pcapng | 14/11/2012 10:17 | Wireshark capture... | 157 KB |
| sec-nessus101.pcapng | 04/07/2016 12:11 | Wireshark capture... | 249 KB |
| sec-suspicious101.pcapng | 04/07/2016 12:11 | Wireshark capture... | 121 KB |
| smb-join101.pcapng | 24/10/2012 13:55 | Wireshark capture... | 127 KB |
| split250_00000_20160704110754.pcapng | 04/07/2016 12:11 | Wireshark capture... | 262 KB |
| split250_00001_20160704110759.pcapng | 04/07/2016 12:11 | Wireshark capture... | 265 KB |
| split250_00002_20160704110759.pcapng | 04/07/2016 12:11 | Wireshark capture... | 252 KB |
| split250_00003_20160704110759.pcapng | 04/07/2016 12:11 | Wireshark capture... | 253 KB |
| split250_00004_20160704110759.pcapng | 04/07/2016 12:11 | Wireshark capture... | 244 KB |
| split250_00005_20160704110804.pcapng | 04/07/2016 12:11 | Wireshark capture... | 1 KB |
| stopproblem101_00027_20201201125630.pca... | 01/12/2020 12:56 | Wireshark capture... | 1.566 KB |
| stopproblem101_00028_20201201125640.pca... | 01/12/2020 12:56 | Wireshark capture... | 1.625 KB |
| stopproblem101_00029_20201201125650.pca... | 01/12/2020 12:56 | Wireshark capture... | 517 KB |
| tcp-decodeas.pcapng | 23/10/2012 14:01 | Wireshark capture... | 4.169 KB |
| tr-twohosts.pcapng | 02/12/2013 14:07 | Wireshark capture... | 54.526 KB |
| tr-winsize.pcapng | 02/12/2013 14:07 | Wireshark capture... | 7.252 KB |
| wlan-ipadstartstop101.pcapng | 14/11/2012 11:01 | Wireshark capture... | 66 KB |

Nombre de archivo: net-lost-route.pcapng
Tipo de archivo: All Files
Read filter:
Format: Wireshark/... - pcapng
Size: 86KiB, 159 data records
Start / elapsed: 2003-02-12 01:00:22 / 00:02:05

net-lost-route.pcapng

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------|-------------|-------------|----------|--------|------|
| 0000 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0010 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0020 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0030 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0040 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0050 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0060 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0070 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0080 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0090 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 00a0 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 00b0 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 00c0 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 00d0 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 00e0 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 00f0 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0100 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0110 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0120 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |
| 0130 | 00.00.00.00 | 00:00:00:00 | 00:00:00:00 | ... | ... | ... |

Packets: 159 · Displayed: 159 (100.0%) | Profile: wireshark101

Paso 2:

The image shows the Wireshark network protocol analyzer interface. The 'View' menu is open, displaying various options for customizing the interface. The main window shows a packet capture of an HTTP 401 Unauthorized response from 34.12.108 to 80. The packet details pane shows the raw data of the response, including the status bar, packet list, packet details, and packet bytes.

View Menu Options:

- ✓ Main Toolbar
- ✓ Filter Toolbar
- ✓ Status Bar
- Full Screen (F11)
- ✓ Packet List
- ✓ Packet Details
- ✓ Packet Bytes
- Packet Diagram
- Time Display Format
- Name Resolution
- Zoom
- Expand Subtrees (Shift+Right)
- Collapse Subtrees (Shift+Left)
- Expand All (Ctrl+Right)
- Collapse All (Ctrl+Left)
- Colorize Packet List
- Coloring Rules...
- Colorize Conversation
- Reset Layout (Ctrl+Shift+W)
- Resize Columns (Ctrl+Shift+R)
- Internals
- Show Packet in New Window
- Reload as File Format/Capture (Ctrl+Shift+F)
- Reload (Ctrl+R)

Packet List:

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|-----------|-------------|----------|---|
| 1 | 0.000000 | 34.12.108 | 80 | HTTP | HTTP/1.0 401 Authorization Required (text/html) |
| 2 | 0.000000 | 34.12.108 | 80 | TCP | 80 → 1124 [FIN, ACK] Seq=1306 Ack=1 Win=49152 Len=0 |
| 3 | 0.000000 | 58.73.170 | 80 | TCP | 1124 → 80 [ACK] Seq=1 Ack=1307 Win=63207 Len=0 |
| 4 | 0.000000 | 58.73.170 | 80 | TCP | 1124 → 80 [FIN, ACK] Seq=1 Ack=1307 Win=63207 Len=0 |
| 5 | 0.000000 | 58.73.170 | 80 | TCP | 1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 |
| 6 | 0.000000 | 34.12.108 | 80 | TCP | 80 → 1124 [ACK] Seq=1307 Ack=2 Win=49152 Len=0 |
| 7 | 0.000000 | 58.73.170 | 80 | TCP | [TCP Retransmission] 1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 |
| 8 | 0.000000 | 58.73.170 | 80 | TCP | [TCP Retransmission] 1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 |
| 9 | 0.000000 | 34.12.108 | 80 | TCP | 80 → 1125 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 |
| 10 | 0.000000 | 58.73.170 | 80 | TCP | 1125 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0 |
| 11 | 0.000000 | 58.73.170 | 80 | HTTP | GET /stats HTTP/1.1 |
| 12 | 0.000000 | 34.12.108 | 80 | TCP | 80 → 1125 [ACK] Seq=1 Ack=382 Win=49152 Len=0 |
| 13 | 0.000000 | 34.12.108 | 80 | HTTP | HTTP/1.0 301 Moved Permanently (text/html) |
| 14 | 0.000000 | 34.12.108 | 80 | TCP | 80 → 1125 [FIN, ACK] Seq=508 Ack=382 Win=49152 Len=0 |
| 15 | 0.000000 | 58.73.170 | 80 | TCP | 1125 → 80 [ACK] Seq=382 Ack=509 Win=64005 Len=0 |
| 16 | 0.000000 | 58.73.170 | 80 | TCP | 1125 → 80 [FIN, ACK] Seq=382 Ack=509 Win=64005 Len=0 |
| 17 | 0.000000 | 58.73.170 | 80 | TCP | 1126 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 |
| 18 | 0.000000 | 34.12.108 | 80 | TCP | 80 → 1126 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 |

Packet Details:

captured (10872 bits) on interface unknown, id 0

a estándar del Este (México)

0000 seconds]

00000 seconds]

seconds]

Packet Bytes:

```
0000 00 d0 59 aa af 80 00 01 96 3c 3f a8 08 00 45 00 ..Y....<?...E.
0010 05 41 b7 47 40 00 2e 06 8c 35 a1 3a 49 aa 0c ea .A.G@.. .5:I...
0020 0c 6c 00 50 04 64 69 3f 63 d1 7c 05 aa c6 50 18 .l.P.di? c|...P.
0030 c0 00 43 a9 00 00 48 54 54 50 2f 31 2e 30 20 34 ..C...HT TP/1.0 4
0040 30 31 20 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 01 Autho rization
0050 20 52 65 71 75 69 72 65 64 0d 0a 44 61 74 65 3a Require d..Date:
0060 20 57 65 64 2c 20 31 32 20 46 65 62 20 32 30 30 Wed, 12 Feb 200
0070 33 20 30 36 3a 30 33 3a 35 30 20 47 4d 54 0d 0a 3 06:03: 50 GMT..
0080 53 65 72 76 65 72 3a 20 52 61 70 69 64 73 69 74 Server: Rapidsit
0090 65 2f 41 70 61 2f 31 2e 33 2e 32 36 20 28 55 6e e/Apa/1. 3.26 (Un
00a0 69 78 29 20 46 72 6f 6e 74 50 61 67 65 2f 35 2e ix) Fron tPage/5.
00b0 30 2e 32 2e 32 35 31 30 20 6d 6f 64 5f 73 73 6c 0.2.2510 mod_ssl
00c0 2f 32 2e 38 2e 31 30 20 4f 70 65 6e 53 53 4c 2f /2.8.10 OpenSSL/
00d0 30 2e 39 2e 36 65 0d 0a 57 57 57 2d 41 75 74 68 0.9.6e.. WWW-Auth
00e0 65 6e 74 69 63 61 74 65 3a 20 42 61 73 69 63 20 enticate : Basic
00f0 72 65 61 6c 6d 3d 22 43 6f 6e 74 72 6f 6c 20 50 realm="C ontrol P
0100 61 6e 65 6c 22 0d 0a 43 6f 6e 6e 65 63 74 69 6f anel"...C onnectio
0110 6e 3a 20 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e n: close ..Conten
0120 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d t-Type: text/htm
0130 6c 0d 0a 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 l....<HT ML><HEAD
```

Paso 3:

The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture from the file 'net-lost-route.pcapng'. The packet list on the left shows 18 packets, with packet 1 selected. 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 packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

A 'Wireshark · Coloring Rules wireshark101' dialog box is open in the foreground. It contains a table of coloring rules with columns for 'Name' and 'Filter'. The rules are as follows:

| Name | Filter |
|---|---|
| <input checked="" type="checkbox"/> T-Retransmissions | tcp.analysis.retransmission |
| <input checked="" type="checkbox"/> S-FTP Arguments | ftp.request.arg |
| <input checked="" type="checkbox"/> New coloring rule | ftp.request.arg == "merlin" |
| <input checked="" type="checkbox"/> Bad TCP | tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive |
| <input checked="" type="checkbox"/> HSRP State Change | hsrp.state != 8 && hsrp.state != 16 |
| <input checked="" type="checkbox"/> Spanning Tree Topology Change | stp.type == 0x80 |
| <input checked="" type="checkbox"/> OSPF State Change | ospf.msg != 1 |
| <input checked="" type="checkbox"/> ICMP errors | icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.t |
| <input checked="" type="checkbox"/> ARP | arp |
| <input checked="" type="checkbox"/> ICMP | icmp icmpv6 |
| <input checked="" type="checkbox"/> TCP RST | tcp.flags.reset eq 1 |
| <input checked="" type="checkbox"/> SCTP ABORT | sctp.chunk_type eq ABORT |
| <input checked="" type="checkbox"/> TTL low or unexpected | (! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) (ip.dst == 224.0.0.0/4 |
| <input checked="" type="checkbox"/> Checksum Errors | eth.fcs.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == |
| <input checked="" type="checkbox"/> SMB | smb nbss nbns netbios |
| <input checked="" type="checkbox"/> HTTP | http tcp.port == 80 http2 |
| <input checked="" type="checkbox"/> DCERPC | dcerpc |
| <input checked="" type="checkbox"/> Routing | hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp |
| <input checked="" type="checkbox"/> TCP SYN/FIN | tcp.flags & 0x02 tcp.flags.fin == 1 |
| <input checked="" type="checkbox"/> TCP | tcp |
| <input checked="" type="checkbox"/> UDP | udp |
| <input checked="" type="checkbox"/> Broadcast | eth[0] & 1 |
| <input checked="" type="checkbox"/> System Event | systemd_journal sysdig |

At the bottom of the dialog box, there are buttons for '+', '-', 'Copy from', 'Foreground', 'Background', 'Apply as filter', 'OK', 'Copy from', 'Cancel', 'Import...', 'Export...', and 'Help'. A status bar at the bottom of the dialog box indicates the path to the color filters: 'C:\Users\lomarv\AppData\Local\Wireshark\profiles\wireshark101\colorfilters'.

The status bar at the bottom of the Wireshark window shows the following information: 'tcp.analysis.re' is neither a field nor a protocol name. | Packets: 159 · Displayed: 159 (100.0%) | Profile: wireshark101

Paso 4:

net-lost-route.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | TCP Delta | Source | Destination | Protocol | Info |
|-----|-----------|-------------|---------------|---------------|----------|---|
| 1 | 0.000000 | 0.000000... | 161.58.73.170 | 12.234.12.108 | HTTP | HTTP/1.0 401 Authorization Required (text/html) |
| 2 | 0.000083 | 0.000083... | 161.58.73.170 | 12.234.12.108 | TCP | 80 → 1124 [FIN, ACK] Seq=1306 Ack=1 Win=49152 |
| 3 | 0.000038 | 0.000038... | 12.234.12.108 | 161.58.73.170 | TCP | 1124 → 80 [ACK] Seq=1 Ack=1307 Win=63207 Len=0 |
| 4 | 10.536317 | 10.53631... | 12.234.12.108 | 161.58.73.170 | TCP | 1124 → 80 [FIN, ACK] Seq=1 Ack=1307 Win=63207 |
| 5 | 0.000629 | 0.000000... | 12.234.12.108 | 161.58.73.170 | TCP | 1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 |
| 6 | 0.096437 | 0.097066... | 161.58.73.170 | 12.234.12.108 | TCP | 80 → 1124 [ACK] Seq=1307 Ack=2 Win=49152 Len=0 |
| 7 | 2.869444 | 2.965881... | 12.234.12.108 | 161.58.73.170 | TCP | [TCP Retransmission] 1125 → 80 [SYN] Seq=0 Win= |
| 8 | 6.008476 | 6.008476... | 12.234.12.108 | 161.58.73.170 | TCP | [TCP Retransmission] 1125 → 80 [SYN] Seq=0 Win= |
| 9 | 0.156745 | 0.156745... | 161.58.73.170 | 12.234.12.108 | TCP | 80 → 1125 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len= |
| 10 | 0.000079 | 0.000079... | 12.234.12.108 | 161.58.73.170 | TCP | 1125 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0 |
| 11 | 0.000291 | 0.000291... | 12.234.12.108 | 161.58.73.170 | HTTP | GET /stats HTTP/1.1 |
| 12 | 0.087260 | 0.087260... | 161.58.73.170 | 12.234.12.108 | TCP | 80 → 1125 [ACK] Seq=1 Ack=382 Win=49152 Len=0 |
| 13 | 0.010738 | 0.010738... | 161.58.73.170 | 12.234.12.108 | HTTP | HTTP/1.0 301 Moved Permanently (text/html) |
| 14 | 0.000076 | 0.000076... | 161.58.73.170 | 12.234.12.108 | TCP | 80 → 1125 [FIN, ACK] Seq=508 Ack=382 Win=49152 |
| 15 | 0.000037 | 0.000037... | 12.234.12.108 | 161.58.73.170 | TCP | 1125 → 80 [ACK] Seq=382 Ack=509 Win=64005 Len= |
| 16 | 0.000253 | 0.000253... | 12.234.12.108 | 161.58.73.170 | TCP | 1125 → 80 [FIN, ACK] Seq=382 Ack=509 Win=64005 |
| 17 | 0.158637 | 0.000000... | 12.234.12.108 | 161.58.73.170 | TCP | 1126 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 |
| 18 | 0.081801 | 0.081801... | 161.58.73.170 | 12.234.12.108 | TCP | 80 → 1126 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len= |

Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface unknown, id 0

- Interface id: 0 (unknown)
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 12, 2003 01:00:35.563117000 Hora estándar del Este (México)
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1045029635.563117000 seconds
- [Time delta from previous captured frame: 2.869444000 seconds]
- [Time delta from previous displayed frame: 2.869444000 seconds]
- [Time since reference or first frame: 13.502948000 seconds]
- Frame Number: 7
- Frame Length: 62 bytes (496 bits)
- Capture Length: 62 bytes (496 bits)
- [Frame is marked: False]
- [Frame is ignored: False]

```

0000 00 01 96 3c 3f 54 00 d0 59 aa af 80 08 00 45 00  ...<?T...Y.....E.
0010 00 30 0b a2 40 00 80 06 ea eb 0c ea 0c 6c a1 3a  .0..@... ..l.:
0020 49 aa 04 65 00 50 7c 57 24 f1 00 00 00 70 02  I..e.P|W$. ....p.
0030 fc 00 dc e6 00 00 02 04 05 b4 01 01 04 02      ....
  
```

net-lost-route.pcapng | Packets: 159 · Displayed: 159 (100.0%) | Profile: wireshark101