



“Secretaría De La Educación Superior”
“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#18 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

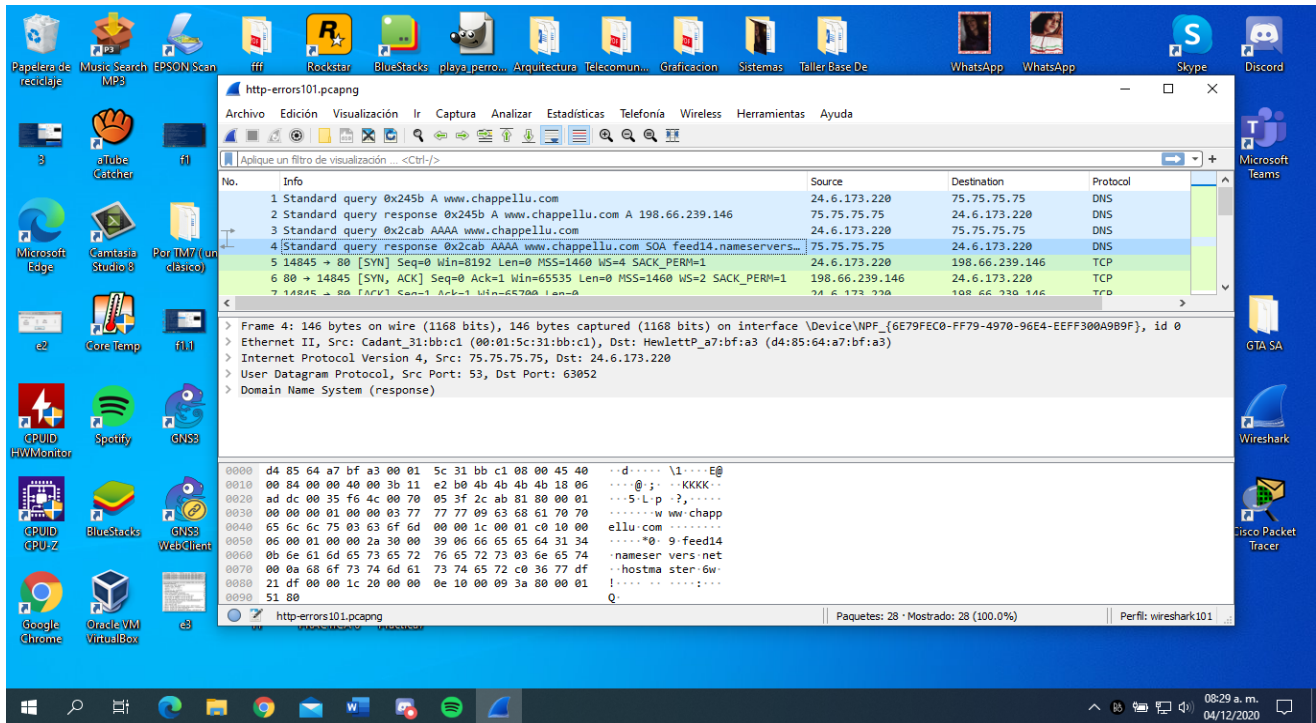
Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 4/Diciembre/2020

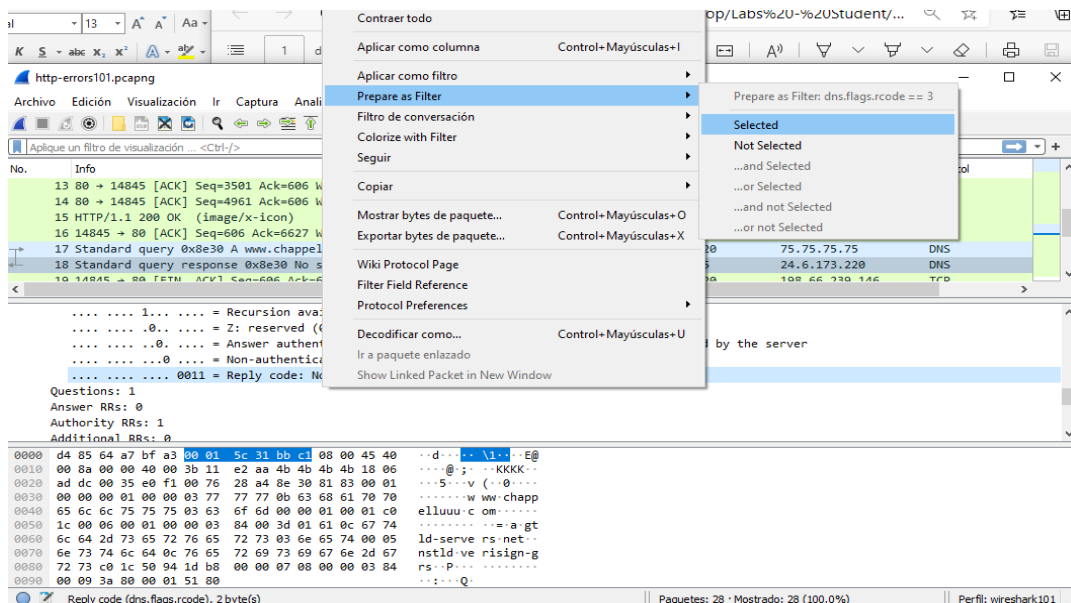
Horario: 5:00 pm – 6:00 pm

Laboratio N#18 – Filtro de errores de nombre DNS o respuestas HTTP 404.

Paso 1 – Abrimos el archivo http-errors101.pcapng. Nos desplazamos en la columna de información para ver los problemas de inicio de sesión de navegación web.



Paso 2 – Abrimos el Frame 18. Este viene siendo una respuesta de error de DNS y así podemos ver los campos o los subárboles de DNS.



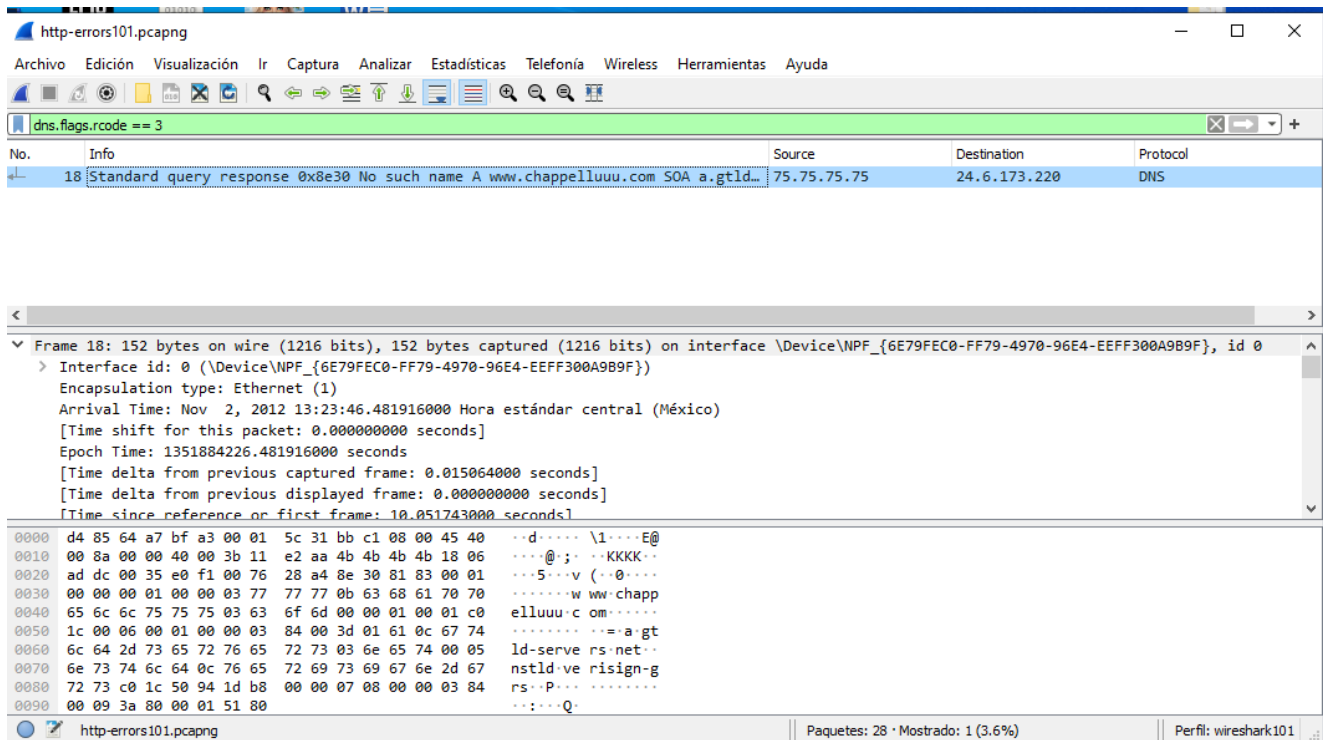
Paso 3 – Ahora vamos a seleccionar el Frame 9. Esta es una respuesta HTTP 404. Expandimos la sección HTTP del paquete, Hacemos clic derecho en la línea de código del estado, seleccionamos preparar un filtro y seleccionado. Y en el área de filtro debe de mostrar lo siguiente.
(dns.flags.rcode==3) || (http.response.code==404).

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Diseño', 'Disposición', 'Referencias', 'Correspondencia', 'Revisar', 'Vista', and 'Ayuda'. Below the menu is a toolbar with various icons for file operations, editing, and analysis. The main window is divided into three panes: 'Paquetes' (Packets), 'Detalles' (Details), and 'Bytes' (Bytes).

In the 'Paquetes' pane, a list of captured packets is shown. Packet 9 is highlighted, showing it is an 'HTTP/1.1 404 Not Found (text/html)' response. A filter is applied to the capture, displayed as 'dns.flags.rcode == 3' in the filter bar. A right-click context menu is open over the filter bar, with the 'Prepare as Filter' option selected. The menu also includes options like 'Expand Subtrees', 'Contraer subárboles', 'Expandir todo', 'Contraer todo', 'Aplicar como columna', 'Aplicar como filtro', 'Filtro de conversación', 'Colorize with Filter', 'Seguir', 'Copiar', 'Mostrar bytes de paquete...', 'Exportar bytes de paquete...', 'Wiki Protocol Page', 'Filter Field Reference', 'Protocol Preferences', 'Decodificar como...', 'Ir a paquete enlazado', and 'Show Linked Packet in New Window'.

The 'Detalles' pane shows the expanded details of the selected packet. It displays the 'Hypertext Transfer Protocol' section, indicating the response code is '404 Not Found'. The 'Bytes' pane shows the raw data of the packet in hexadecimal and ASCII format.

Paso 4 – Hacemos clic en aplicar.



The screenshot shows the Wireshark interface with a filter applied: `dns.flags.rcode == 3`. The packet list shows a single packet (No. 18) of type "Standard query response 0x8e30 No such name A www.chappelluuu.com SOA a.gtld...". The packet details pane shows the following information:

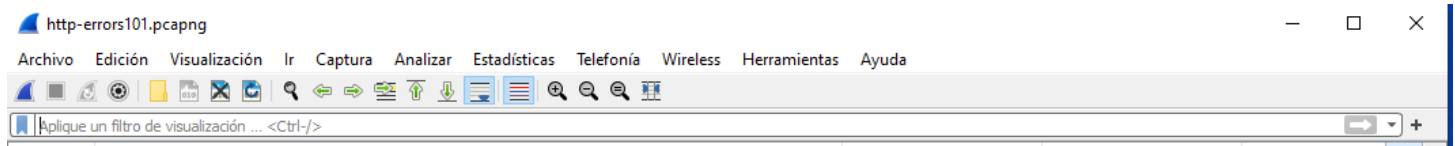
- Interface id: 0 (\Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F})
- Encapsulation type: Ethernet (1)
- Arrival Time: Nov 2, 2012 13:23:46.481916000 Hora estándar central (México)
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1351884226.481916000 seconds
- [Time delta from previous captured frame: 0.015064000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 10.051743000 seconds]

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

```
0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 40 ..d.... \1....E@
0010 00 8a 00 00 40 00 3b 11 e2 aa 4b 4b 4b 18 06 ....@;...KKKK..
0020 ad dc 00 35 e0 f1 00 76 28 a4 8e 30 81 83 00 01 ...5...v (-0....
0030 00 00 00 01 00 00 03 77 77 77 0b 63 68 61 70 70 .....w ww.chapp
0040 65 6c 6c 75 75 03 63 6f 6d 00 00 01 00 01 c0 elluuu.c om.....
0050 1c 00 06 00 01 00 00 03 84 00 3d 01 61 0c 67 74 .....==a.gt
0060 6c 64 2d 73 65 72 76 65 72 73 03 6e 65 74 00 05 ld-serve rs.net..
0070 6e 73 74 6c 64 0c 76 65 72 69 73 69 67 6e 2d 67 nstld.ve risign-g
0080 72 73 c0 1c 50 94 1d b8 00 00 07 08 00 00 03 84 rs.P.....
0090 00 09 3a 80 00 01 51 80 .....Q.
```

The status bar at the bottom indicates: Paquetes: 28 · Mostrado: 1 (3.6%) | Perfil: wireshark101

Paso 5 – Hacemos clic en borrar el filtro.



The screenshot shows the Wireshark interface with the filter bar cleared. The filter bar now displays: `Aplique un filtro de visualización ... <Ctrl-/>`. The status bar at the bottom indicates: Paquetes: 28 · Mostrado: 1 (3.6%) | Perfil: wireshark101