



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

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#26 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 5/Diciembre/2020

Horario: 5:00 pm – 6:00 pm

Laboratio N#26 – Cree una regla de colores para resaltar los nombres de usuario, las contraseñas y mas de FTP

Paso 1 – Abrimos ftp-crack101.pcapng. Y comenzamos a capturar en medio de varias comunicaciones FTP. En el frame 11 se puede observar “Request: PASS merlin”.

The image shows a Wireshark network traffic capture of the file ftp-crack101.pcapng. The main packet list pane displays several frames. Frame 11 is selected and highlighted in blue. It is an FTP request (command 'PASS') from source 10.234.125.254 to destination 10.121.70.151. The packet details pane for frame 11 shows the File Transfer Protocol (FTP) section expanded, displaying the request command 'PASS' and the request argument 'merlin'. The packet bytes pane shows the raw data of the packet, with the command and argument visible in the ASCII column.

No.	Time	TCP Delta	Info	Source	Destination
4	0.005014	0.012755000	Response: 530 Login incorrect.	10.121.70.151	10.234.125
5	0.000433	0.000000000	21 → 2228 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1	10.121.70.151	10.234.125
6	0.000056	0.000056000	2228 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0	10.234.125.254	10.121.70.
7	0.006301	0.000000000	21 → 2222 [ACK] Seq=1 Ack=1 Win=49152 Len=0	10.121.70.151	10.234.125
8	0.005080	0.011870000	2217 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0	10.234.125.254	10.121.70.
9	0.003120	0.000000000	21 → 2220 [ACK] Seq=1 Ack=1 Win=49152 Len=0	10.121.70.151	10.234.125
10	0.004207	0.012407000	Response: 331 Password required for admin.	10.121.70.151	10.234.125
11	0.000473	0.000473000	Request: PASS merlin	10.234.125.254	10.121.70.
12	0.000804	0.000000000	21 → 2221 [ACK] Seq=1 Ack=1 Win=49152 Len=0	10.121.70.151	10.234.125
13	0.007684	0.013168000	Response: 530 Login incorrect.	10.121.70.151	10.234.125
14	0.001176	0.001176000	2220 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0	10.234.125.254	10.121.70.

Frame Number: 11
Frame Length: 67 bytes (536 bits)
Capture Length: 67 bytes (536 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:ftp]
[Coloring Rule Name: TCP]

```
0000 00 01 96 3c 3f a8 00 d0 59 aa af 80 08 00 45 00 ...<?..Y...E
0010 00 35 36 44 40 00 80 06 ea 86 0a ea 7d fe 0a 79 -56D@... ..y
0020 46 97 08 ae 00 15 42 79 8f 49 4b 86 20 cd 50 18 F....By .IK. .P
0030 44 3d c4 c5 00 00 50 41 53 53 20 6d 65 72 6c 69 D=....PA SS merli
0040 6e 0d 0a n..
```

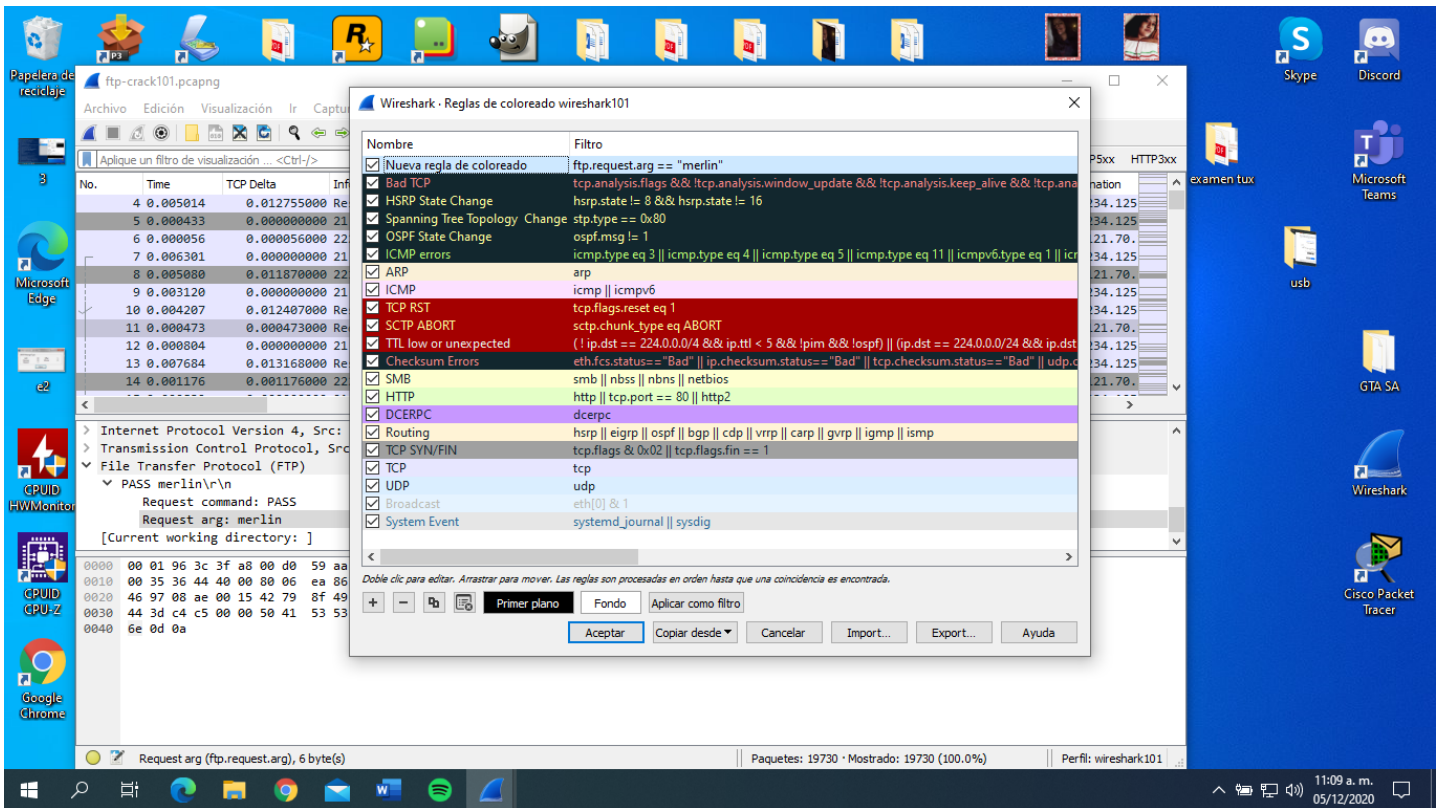
Paso 2 – En el panel de detalles del Frame11, expandimos la línea de protocolo la transferencia de archivos (FTP). Existen 2 secciones. Solicitar comando y Solicitar argumento.

The image shows the Wireshark packet details pane for frame 11. The 'File Transfer Protocol (FTP)' section is expanded, showing the 'PASS merlin\r\n' request. The 'Request command' is 'PASS' and the 'Request arg' is 'merlin'. The 'Current working directory' is empty. The packet bytes pane shows the raw data of the packet, with the command and argument visible in the ASCII column.

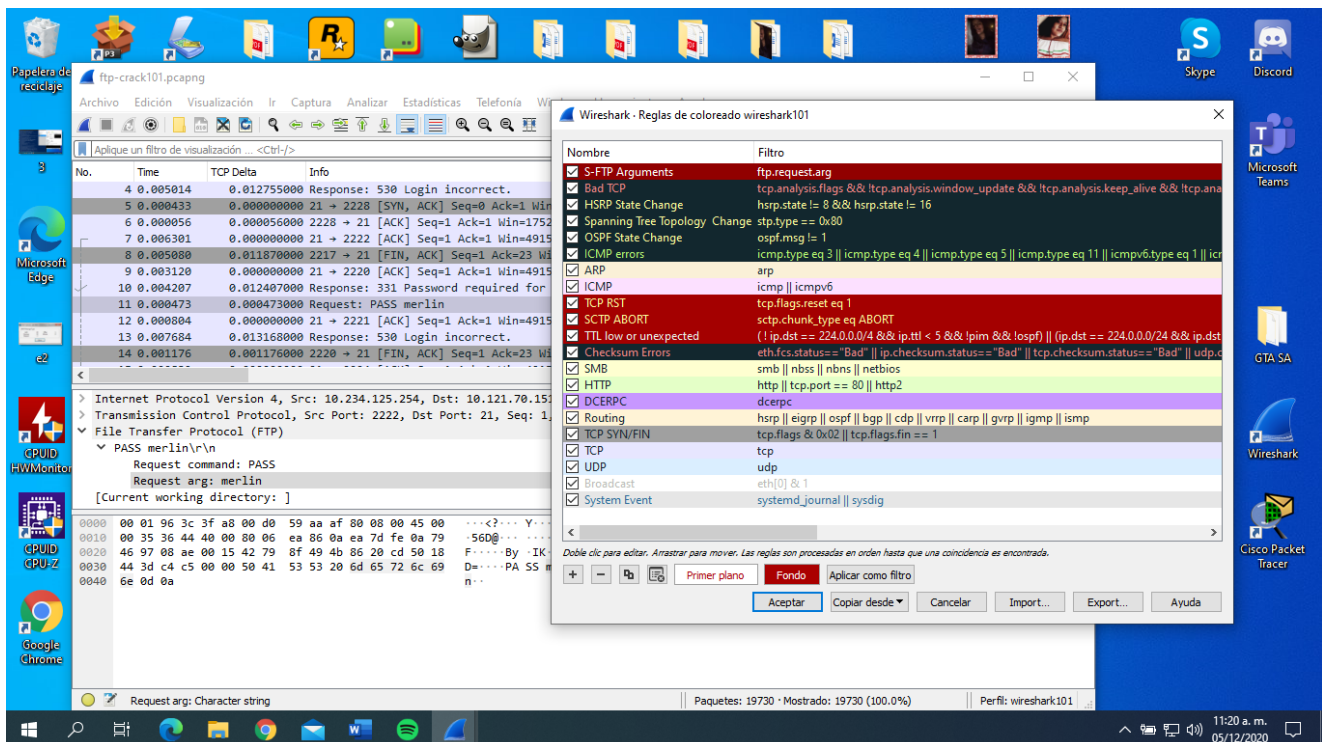
```
> Internet Protocol Version 4, Src: 10.234.125.254, Dst: 10.121.70.151
> Transmission Control Protocol, Src Port: 2222, Dst Port: 21, Seq: 1, Ack: 35, Len: 13
> File Transfer Protocol (FTP)
  PASS merlin\r\n
    Request command: PASS
    Request arg: merlin
    [Current working directory: ]
```

```
0000 00 01 96 3c 3f a8 00 d0 59 aa af 80 08 00 45 00 ...<?..Y...E
0010 00 35 36 44 40 00 80 06 ea 86 0a ea 7d fe 0a 79 -56D@... ..y
0020 46 97 08 ae 00 15 42 79 8f 49 4b 86 20 cd 50 18 F....By .IK. .P
0030 44 3d c4 c5 00 00 50 41 53 53 20 6d 65 72 6c 69 D=....PA SS merli
0040 6e 0d 0a n..
```

Paso 3 – Hacemos clic derecho en la línea Request arg y Seleccionar colorear con filtro | Nueva regla de coloración como se muestra.



Paso 4 - En la regla de coloración que aparece, nombre su regla de coloración “S-FTP Arguments” Edita el filtro a solo [ftp.request.arg](#)



Paso 5 – Hacemos clic en aceptar para cerrar las ventanas de las Reglas de coloración y luego nos desplazamos por el archivo de seguimiento para identificar el frame que coincida.

The screenshot shows a Windows desktop environment with various application icons on the left and right sides. The central window is Wireshark, displaying a packet capture file named 'ftp-crack101.pcapng'. The packet list pane shows a series of packets, with packet 21 selected. The packet details pane shows the structure of the selected packet, including the Internet Protocol Version 4, Transmission Control Protocol, and File Transfer Protocol (FTP) layers. The packet bytes pane shows the raw data of the selected packet.

No.	Time	TCP Delta	Info	Source	Destination
11	0.000473	0.000473000	Request: PASS merlin	10.234.125.254	10.121.70.151
12	0.000804	0.000000000	21 → 2221 [ACK] Seq=1 Ack=1 Win=49152 Len=0	10.121.70.151	10.234.125.254
13	0.007684	0.013168000	Response: 530 Login incorrect.	10.121.70.151	10.234.125.254
14	0.001176	0.001176000	2220 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0	10.234.125.254	10.121.70.151
15	0.000839	0.000000000	21 → 2224 [ACK] Seq=1 Ack=1 Win=49152 Len=0	10.121.70.151	10.234.125.254
16	0.007129	0.016828000	Response: 331 Password required for admin.	10.121.70.151	10.234.125.254
17	0.001306	0.001306000	Request: PASS mercury	10.234.125.254	10.121.70.151
18	0.001316	0.000000000	21 → 2223 [ACK] Seq=1 Ack=1 Win=49152 Len=0	10.121.70.151	10.234.125.254
19	0.000221	0.009972000	Response: 331 Password required for admin.	10.121.70.151	10.234.125.254
20	0.006183	0.006404000	Response: 331 Password required for admin.	10.121.70.151	10.234.125.254
21	0.000510	0.000510000	Request: PASS mets	10.234.125.254	10.121.70.151

Internet Protocol Version 4, Src: 10.234.125.254, Dst: 10.121.70.151
 Transmission Control Protocol, Src Port: 2222, Dst Port: 21, Seq: 1, Ack: 35, Len: 13
 File Transfer Protocol (FTP)
 PASS merlin\r\n
 Request command: PASS
 Request arg: merlin
 [Current working directory:]

0000 00 01 96 3c 3f a8 00 d0 59 aa af 80 08 00 45 00 ...?... Y...E-
 0010 00 35 36 44 40 00 00 06 ea 86 0a ea 7d fe 0a 79 :56D@... }...y
 0020 46 97 08 ae 00 15 42 79 8f 49 4b 86 20 cd 50 18 F...By...IK...P-
 0030 44 3d c4 c5 00 00 50 41 53 53 20 6d 65 72 6c 69 D...PA SS merli
 0040 6e 0d 0a n...

Request arg: Character string | Paquetes: 19730 · Mostrado: 19730 (100.0%) | Perfil: wireshark101