

**Instituto Tecnológico de Cancún**

**Fundamentos de Telecomunicaciones**

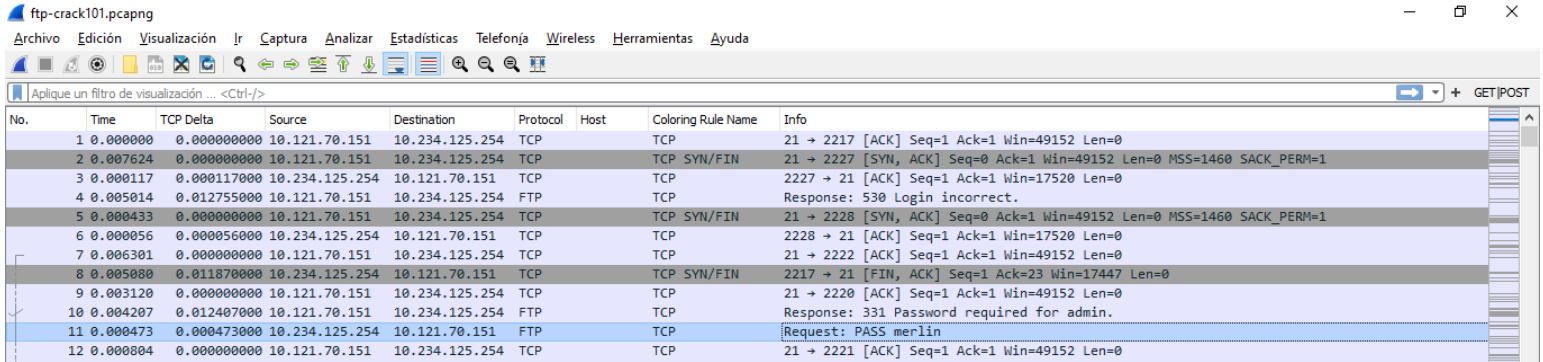
**Lab26 - Build a Coloring Rule to  
Highlight FTP User Names,  
Passwords, and More**

**Prof. Ismael Jiménez Sánchez**

**Alumno(a). Laury del Rosario Mex  
Martin**

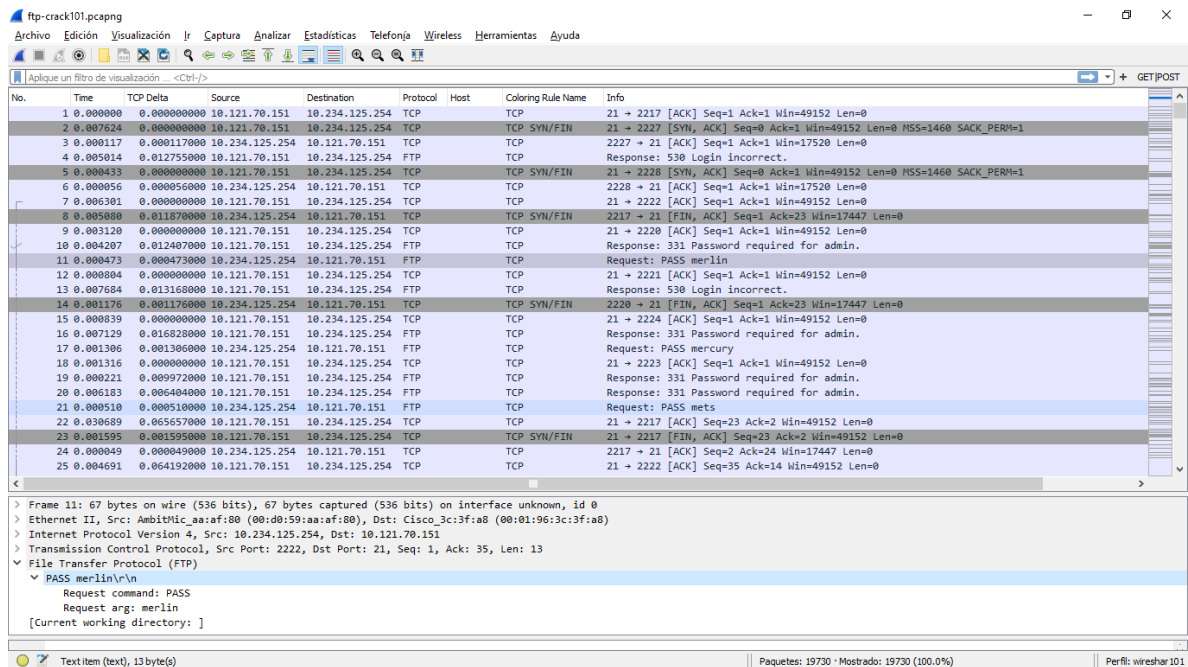
**Ciclo 2020-B**

En el paquete 11 se ve que hay un Request y una contraseña que es **Merlin** en la columna de información.



No.	Time	TCP Delta	Source	Destination	Protocol	Host	Coloring Rule Name	Info
1	0.000000	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2217 [ACK] Seq=1 Ack=1 Win=49152 Len=0
2	0.007624	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	21 → 2227 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
3	0.000117	0.000117000	10.234.125.254	10.121.70.151	TCP		TCP	2227 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.005014	0.012755000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 530 Login incorrect.
5	0.000433	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	21 → 2228 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
6	0.000056	0.000056000	10.234.125.254	10.121.70.151	TCP		TCP	2228 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
7	0.006301	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2222 [ACK] Seq=1 Ack=1 Win=49152 Len=0
8	0.005080	0.011870000	10.234.125.254	10.121.70.151	TCP		TCP SYN/FIN	2217 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0
9	0.003120	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2220 [ACK] Seq=1 Ack=1 Win=49152 Len=0
10	0.004207	0.012407000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
11	0.000473	0.000473000	10.234.125.254	10.121.70.151	FTP		TCP	Request: PASS merlin
12	0.000804	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2221 [ACK] Seq=1 Ack=1 Win=49152 Len=0

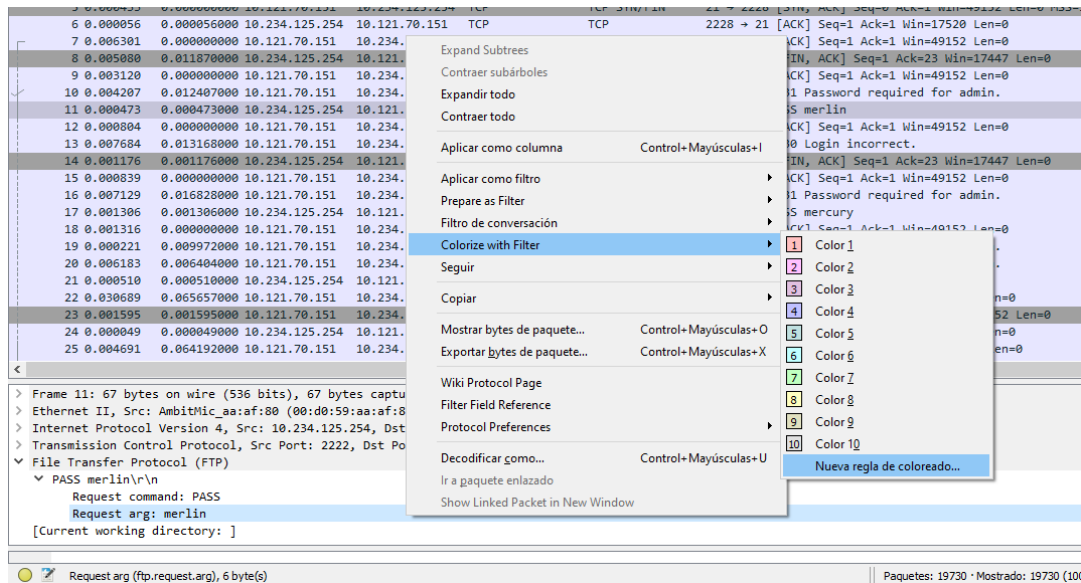
En los detalles del paquete 11 en la sección de FTP se observa dos tipos de request que son request command y request arg. Los vamos a poner un color diferente para poder diferenciarlos.



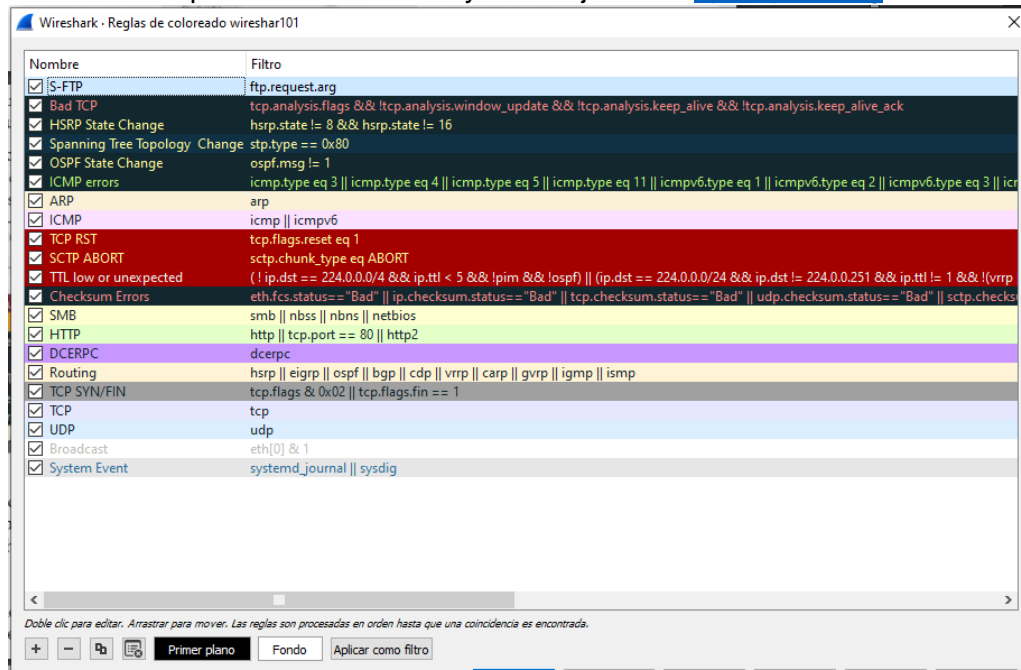
No.	Time	TCP Delta	Source	Destination	Protocol	Host	Coloring Rule Name	Info
1	0.000000	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2217 [ACK] Seq=1 Ack=1 Win=49152 Len=0
2	0.007624	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	21 → 2227 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
3	0.000117	0.000117000	10.234.125.254	10.121.70.151	TCP		TCP	2227 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.005014	0.012755000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 530 Login incorrect.
5	0.000433	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	21 → 2228 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
6	0.000056	0.000056000	10.234.125.254	10.121.70.151	TCP		TCP	2228 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
7	0.006301	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2222 [ACK] Seq=1 Ack=1 Win=49152 Len=0
8	0.005080	0.011870000	10.234.125.254	10.121.70.151	TCP		TCP SYN/FIN	2217 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0
9	0.003120	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2220 [ACK] Seq=1 Ack=1 Win=49152 Len=0
10	0.004207	0.012407000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
11	0.000473	0.000473000	10.234.125.254	10.121.70.151	FTP		TCP	Request: PASS merlin
12	0.000804	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2221 [ACK] Seq=1 Ack=1 Win=49152 Len=0
13	0.007684	0.013168000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 530 Login incorrect.
14	0.001176	0.001176000	10.234.125.254	10.121.70.151	TCP		TCP SYN/FIN	2220 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0
15	0.000839	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2224 [ACK] Seq=1 Ack=1 Win=49152 Len=0
16	0.007129	0.016828000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
17	0.001306	0.001306000	10.234.125.254	10.121.70.151	FTP		TCP	Request: PASS mercury
18	0.001316	0.000000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2223 [ACK] Seq=1 Ack=1 Win=49152 Len=0
19	0.000221	0.009972000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
20	0.000183	0.000404000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
21	0.000510	0.000510000	10.234.125.254	10.121.70.151	FTP		TCP	Request: PASS mets
22	0.030609	0.005657000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2217 [ACK] Seq=23 Ack=2 Win=49152 Len=0
23	0.001595	0.001595000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	2217 → 21 [FIN, ACK] Seq=23 Ack=2 Win=49152 Len=0
24	0.000049	0.000049000	10.234.125.254	10.121.70.151	TCP		TCP	2217 → 21 [ACK] Seq=2 Ack=24 Win=17447 Len=0
25	0.004691	0.004192000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2222 [ACK] Seq=35 Ack=14 Win=49152 Len=0

> Frame 11: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface unknown, id 0  
> Ethernet II, Src: AmbitWLC\_aa:af:80 (00:0b:59:aa:af:80), Dst: Cisco\_3c:f3:a8 (00:01:96:3c:f3:a8)  
> 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: ]

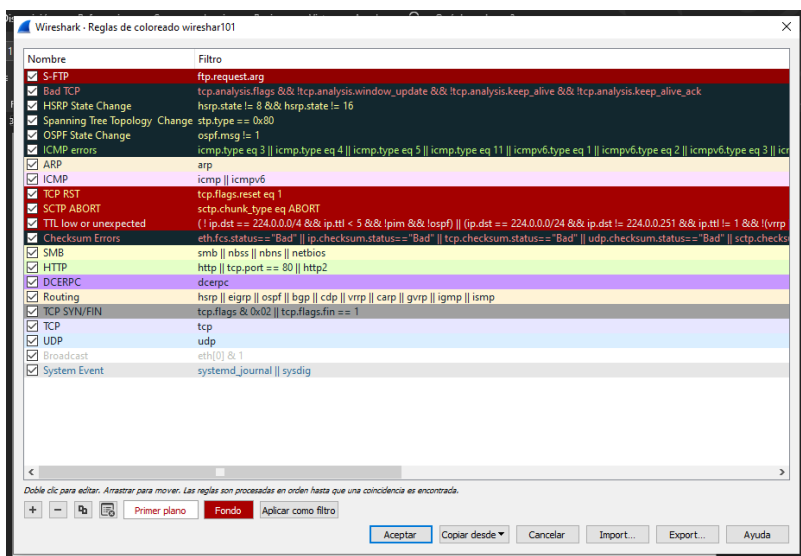
Damos clic derecho en request arg y seleccionamos colorized and filter | nueva regla de color.



Vamos a cambiar el nombre de la nueva regla como S-FTP y cambiamos el filtro eliminando la parte de == “merlin” y solo dejaremos [ftp.request.arg](#)



Le cambiaremos el color de fondo a rojo y el color de las letras en blanco.



Le damos clic en aceptar y ya estará listo.

