

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

**Lab33 - Detect Suspicious Protocols or
Applications**

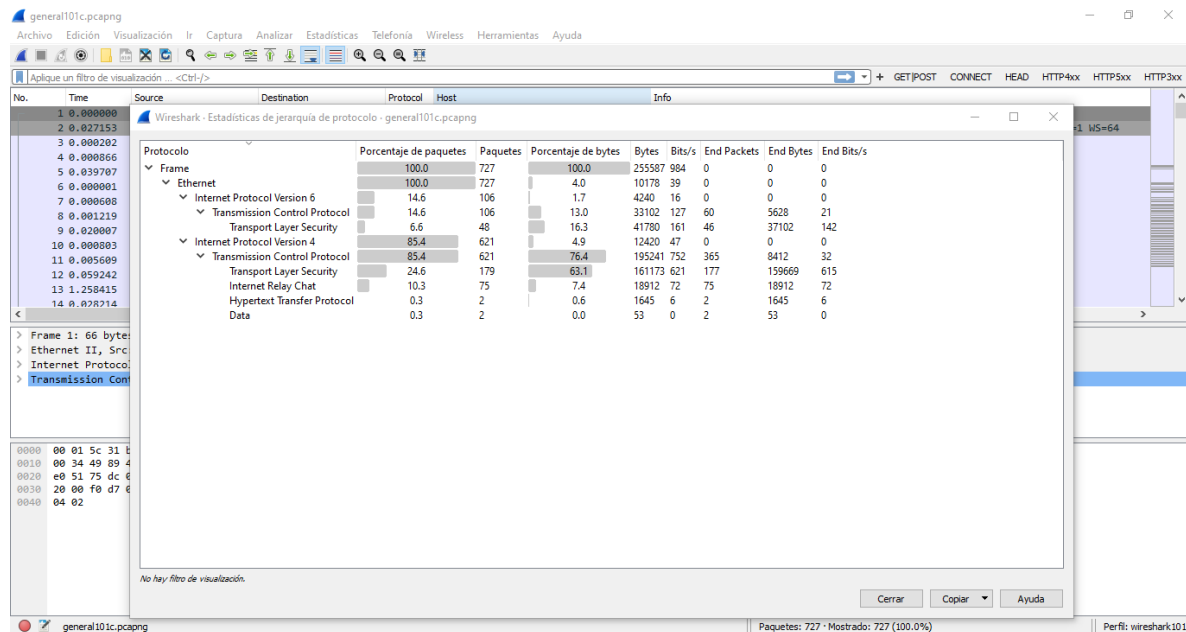
Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

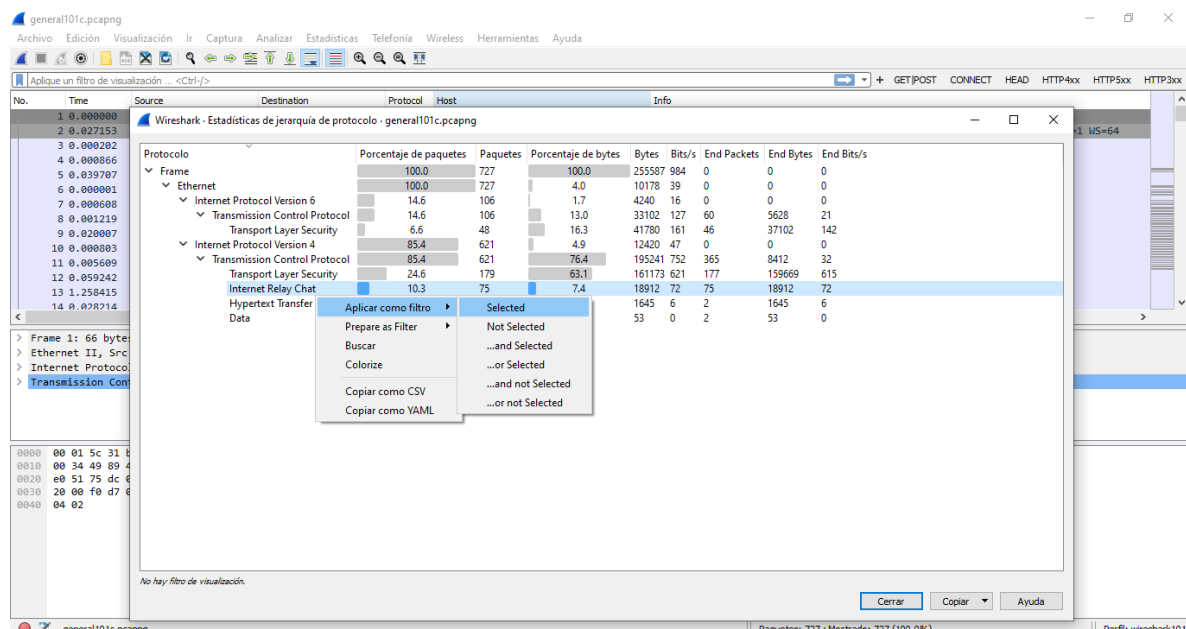
Lab33 - Detect Suspicious Protocols or Applications

1 Abrimos el archivo general101c.pcapng

2 Seleccionamos Estadísticas>Protocol Hierarchy y podemos observar que Internet Relay Chat y Data están debajo de la sección TCP



3 Click derecho en Internet Relay Chat y seleccionamos Apply as Filter>Selected



Podemos observar en el panel de detalles la comunicación que tiene.

general101c.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

GET/POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

No.	Time	Source	Destination	Protocol	Info
566	0.004936	24.6.173.220	67.220.66.111	IRC	Request (CAP)
569	0.001637	67.220.66.111	24.6.173.220	IRC	Response (NOTICE) (NOTICE)
570	0.000129	24.6.173.220	67.220.66.111	IRC	Request (NICK) (USER)
579	0.000001	67.220.66.111	24.6.173.220	IRC	Response (NOTICE)
581	0.073444	67.220.66.111	24.6.173.220	IRC	Response (NOTICE) (CAP)
583	0.006803	24.6.173.220	67.220.66.111	IRC	Request (CAP)
584	0.038451	67.220.66.111	24.6.173.220	IRC	Response (CAP)
585	0.000348	24.6.173.220	67.220.66.111	IRC	Request (CAP)
586	0.026163	67.220.66.111	24.6.173.220	IRC	Response (PING)
587	0.000459	24.6.173.220	67.220.66.111	IRC	Request (PONG)
588	0.027775	67.220.66.111	24.6.173.220	IRC	Response (001) (002) (003) (004) (005) (005) (042) (251) (252)
589	0.001404	67.220.66.111	24.6.173.220	IRC	Response (ne) (254) (255) (265) (266) (250) (375) (372) (372) (372) (372) (372) (372)
591	0.000843	67.220.66.111	24.6.173.220	IRC	Response (=====) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372)
592	0.000002	67.220.66.111	24.6.173.220	IRC	Response (-----) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372)
593	0.000002	67.220.66.111	24.6.173.220	IRC	Response (-----)

> Frame 566: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface unknown, id 0
> Ethernet II, Src: HewlettP_a7:bfa3 (d4:85:04:a7:bfa3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 67.220.66.111
> Transmission Control Protocol, Src Port: 30209, Dst Port: 6667, Seq: 1, Ack: 1, Len: 7
> Internet Relay Chat

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1....d.....E-
0010 00 2f 4a e6 40 00 00 06 00 00 18 06 ad dc 43 dc ./3 @... ..C-
0020 42 6f 76 01 1a 00 05 2f 87 5e c8 50 c2 e4 50 18 8ov.../..P..P-
0030 40 29 4c 4f 00 00 43 41 50 20 4c 53 0a @)LO..CA P L\$-

general101c.pcapng Paquetes: 727 · Mostrado: 75 (10.3%) Perfil: wireshark101