Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

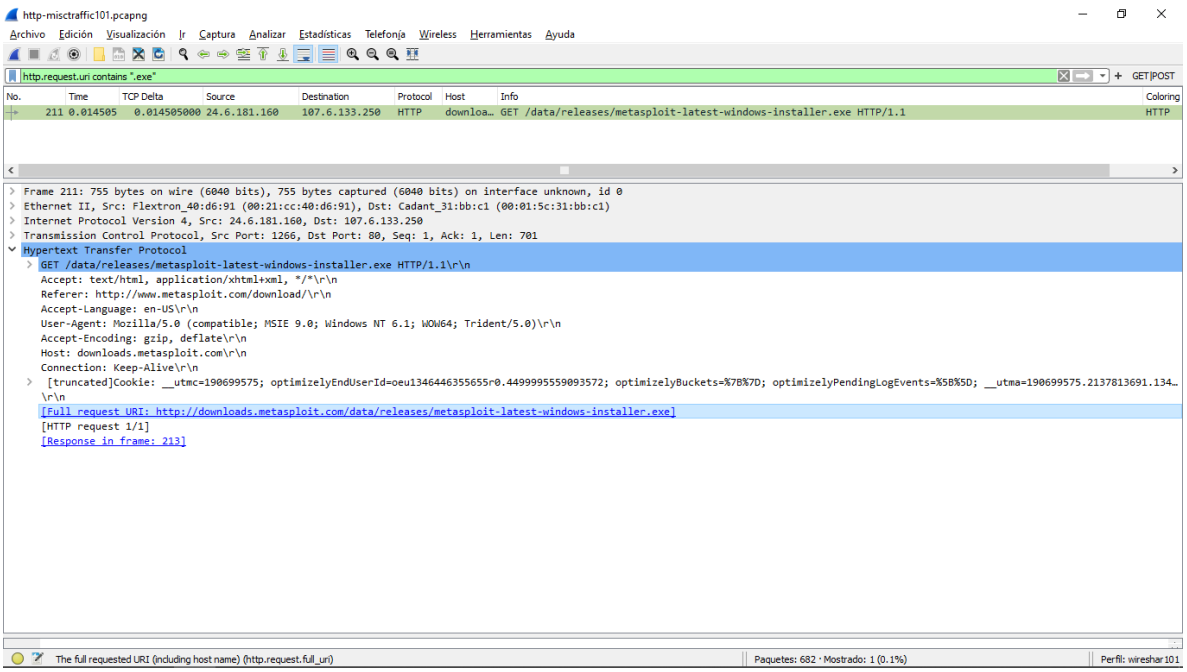
Lab29 - Export a Single TCP Conversation

Prof. Ismael Jiménez Sánchez

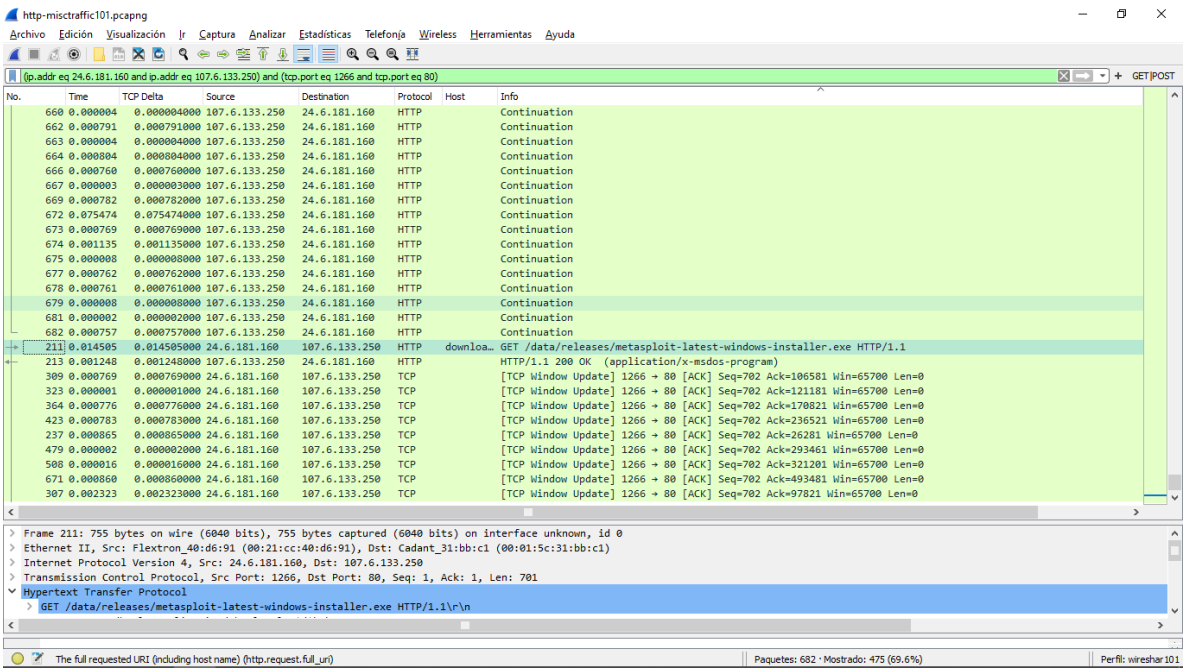
Alumno(a). Laury del Rosario Mex Martin

Ciclo 2020-B

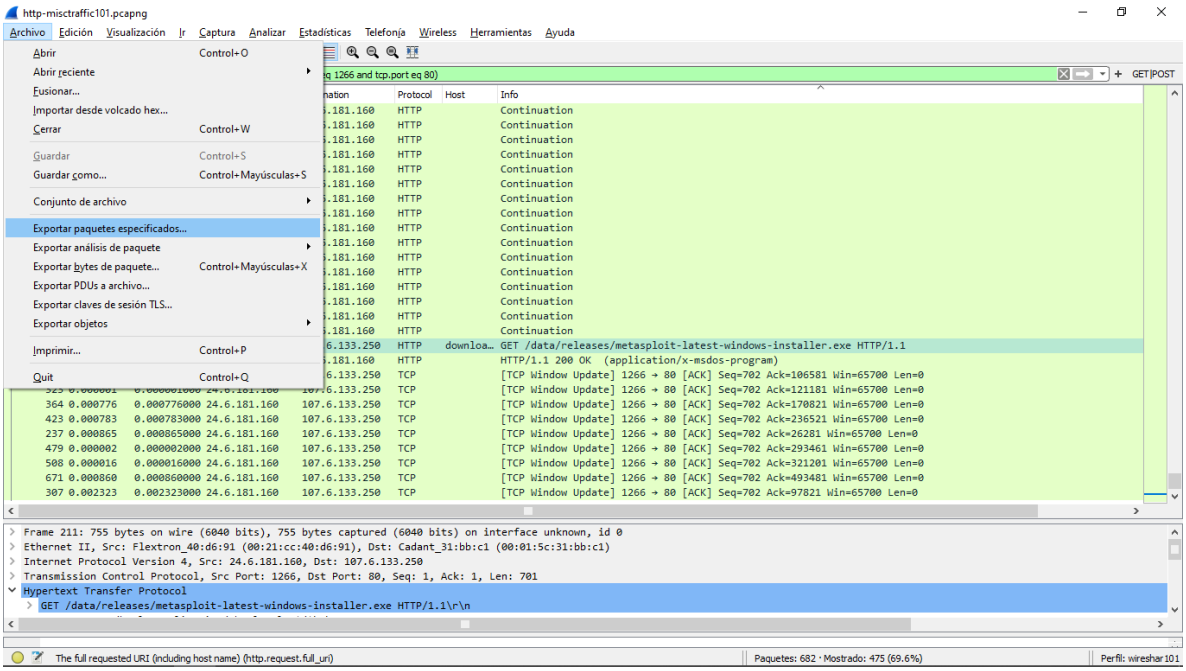
En este lab buscaremos paquetes que contengan .exe en los Request de HTTP usaremos el filtro http.request.uri contains “.exe”. Y podemos visualizar en el frame 211 que hay uno.



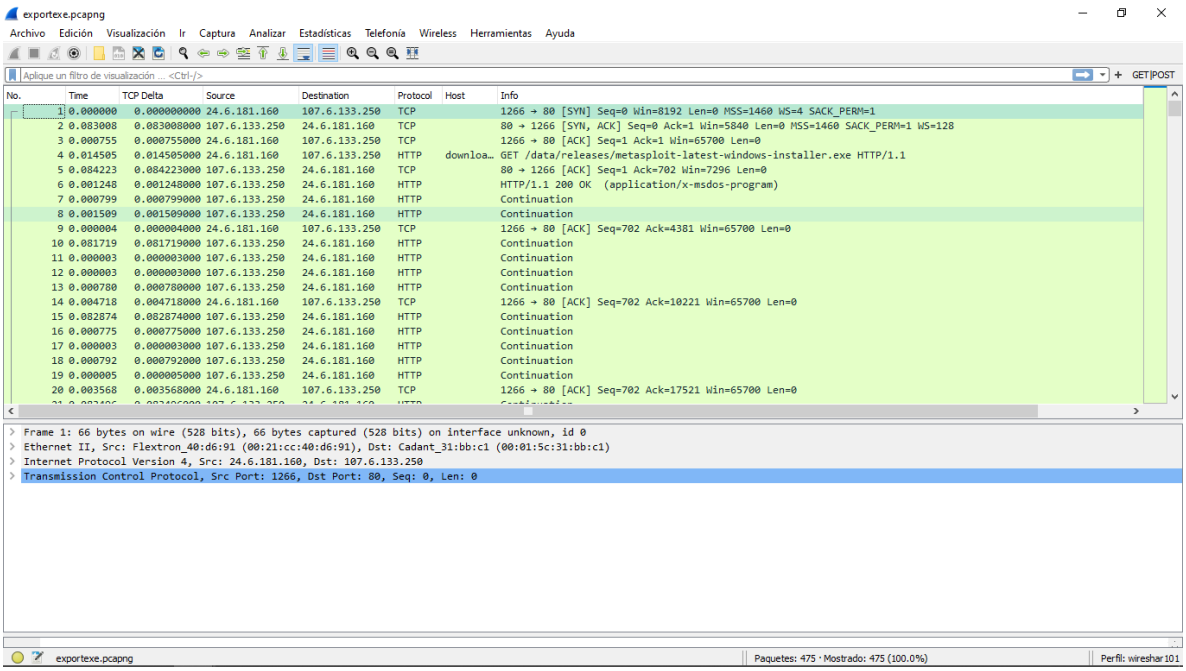
Seleccionamos el paquete y le damos clic en conversation Filter | TCP y aparecerá en la barra de filtros de display y nos indicará que hay 475 paquetes de este archivo.



Y vamos a guardar la conversación de los paquetes que separamos con el filtro de la siguiente manera File | Export Specified Packets.



Lo guardaremos como exporexe.pcapng, al abrir la captura nos aparece solamente los paquetes que se seleccionaron con el filtro



Esto nos ayuda a saber qué fue lo que realmente descargo o visualizo esta usuario si en el lugar está permitido este tipo de cosas para sancionar y para tener una evidencia de esto, y por parte de usuarios maliciosos les permite extraer los archivo o descargas de una captura.