“Secretaria De La Educación Superior”

“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#37 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

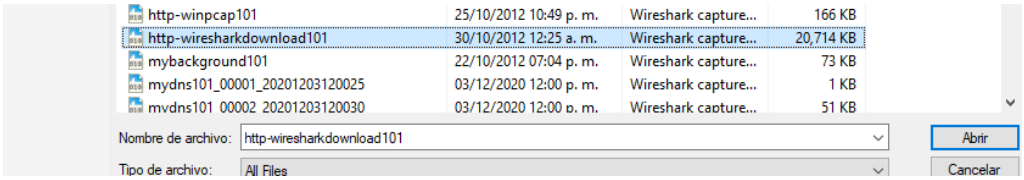
Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 6/Diciembre/2020

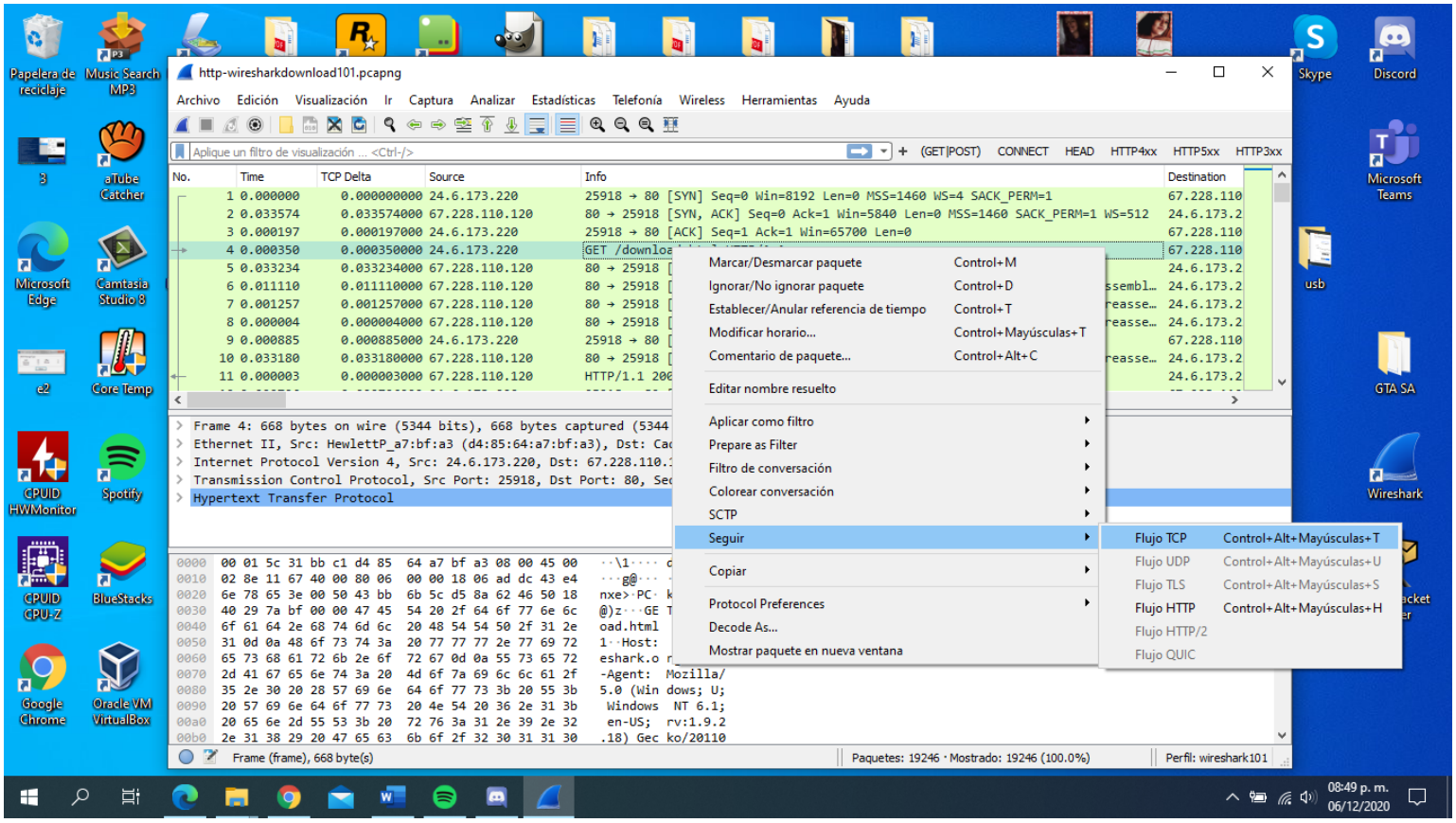
Horario: 5:00 pm – 6:00 pm

Laboratio N#37 – Usamos el reensamblaje para encontrar el mensaje HTTP oculto en un sitio web.

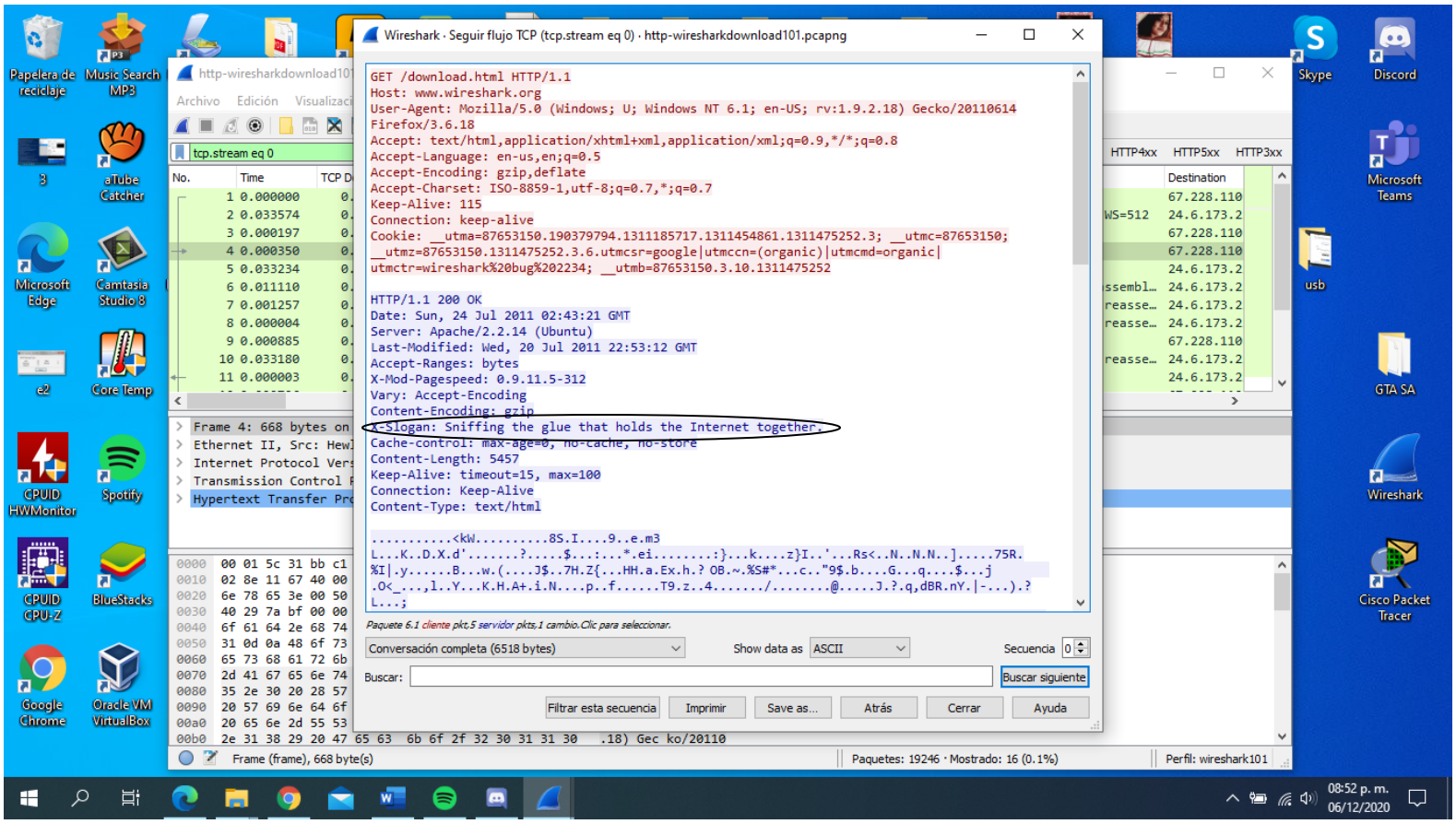
Paso 1 – Abrimos el archivo http-wiresharkdownload101.pcapng



Paso 2 – Los primeros 3 paquetes TCP para la conexión del servidor web. El frame 4 es el cliente. Solicitud GET para la pagina download.html. Haga clic con el botón derecho en el Frame 4 y seleccionar Seguir | Secuencia TCP

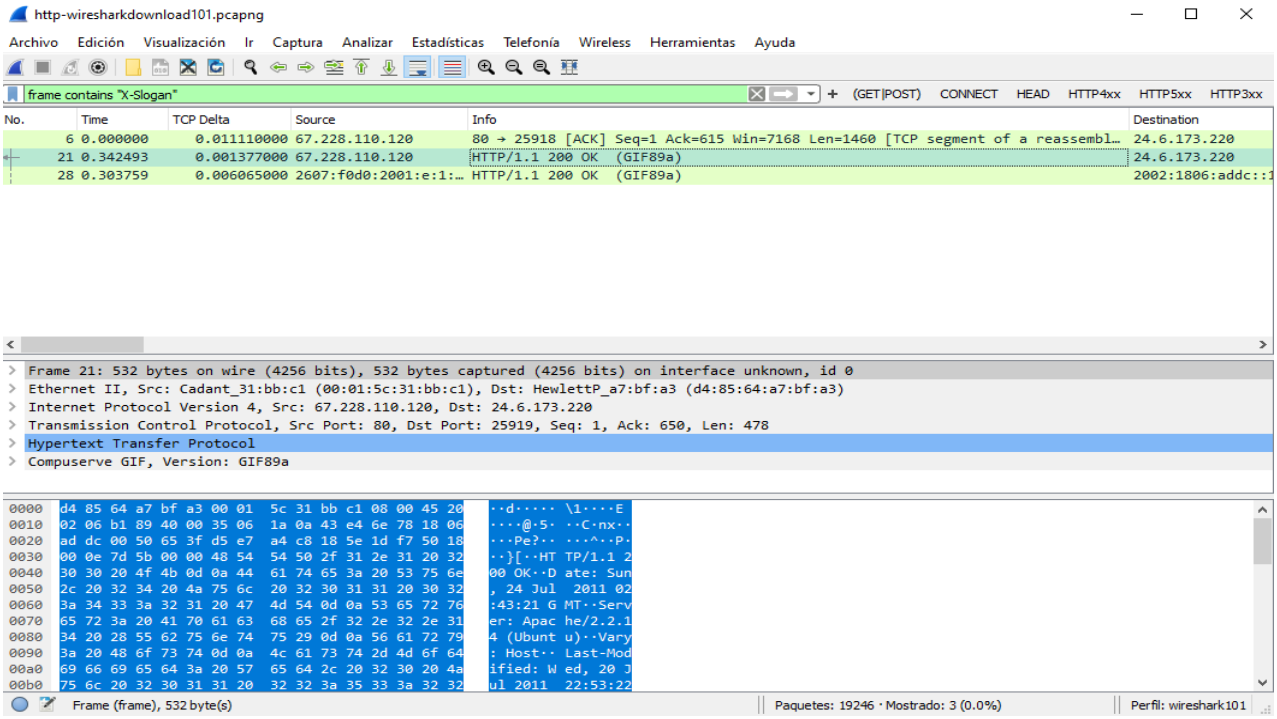


Paso 3 – Wireshark muestra la conversación sin los encabezados Ethernet, IP o TCP. Desplazarse por el Stream para buscar el mensaje oculto Gerald Combs, creador de wireshark se encuentra en el servidor y comienza con X-SLOGAN.

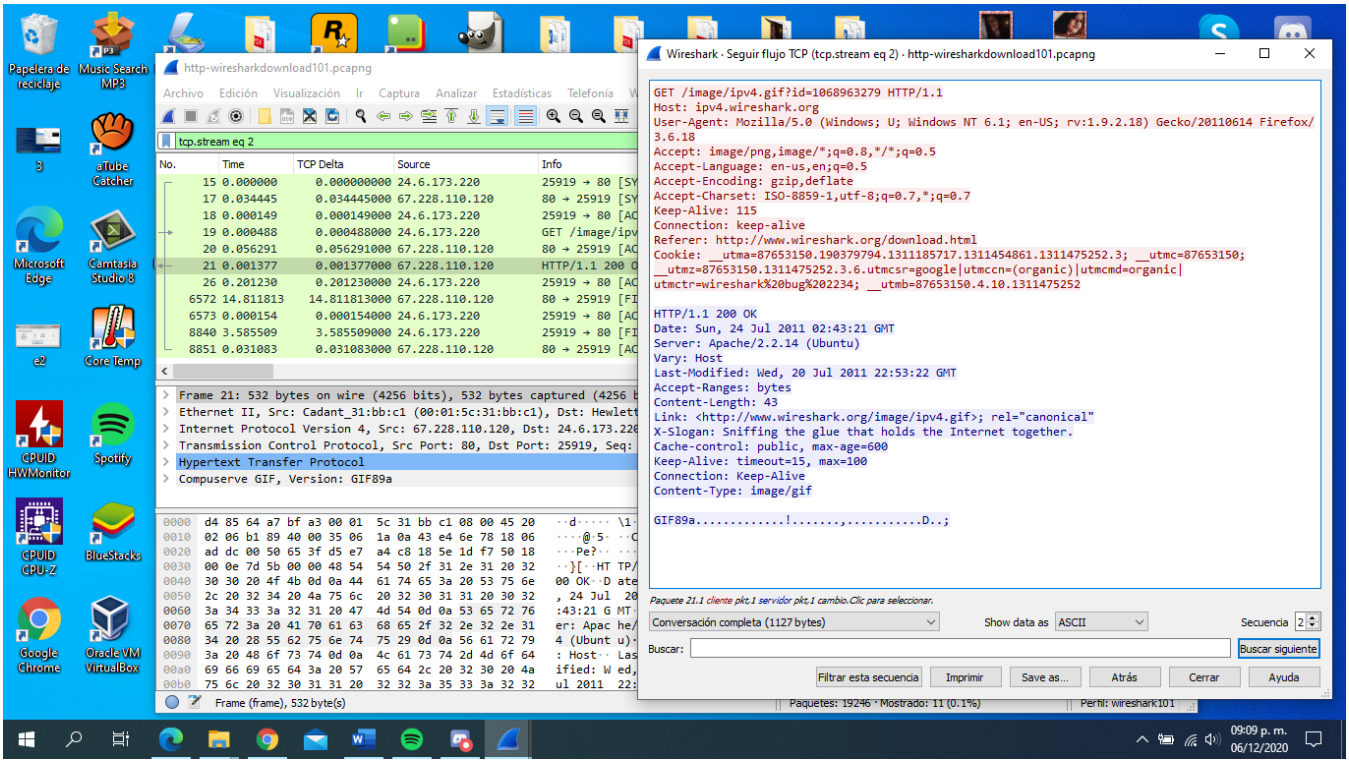


Paso 4 – Este no es el único mensaje oculto en la sesión de navegación web, ahora que conocemos el mensaje comienza con “ X – Slogan”.

Hacemos clic en el botón cerrar y luego en el botón borrar para eliminar el filtro TCP.



Paso 5 - Hacemos clic derecho en los otros 2 frames desplazados y seleccionamos Seguir | Secuencia TCP para examinar encabezados HTTP entre Host.



Paso 6 – Hacemos clic en cerrar la ventana cuando se haya terminado de ver las corrientes.