



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

## **Ingeniería en Sistemas Computacionales**

**Materia:** Fundamentos de Telecomunicaciones

**Tema:** Laboratorio N#14 Wireshark

**Alumno:** Vargas Rodríguez Javier Jesús

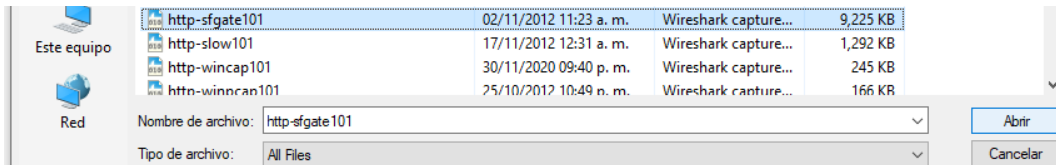
**Maestro:** Ismael Jiménez Sánchez

***Fecha De Entrega: 3/Diciembre/2020***

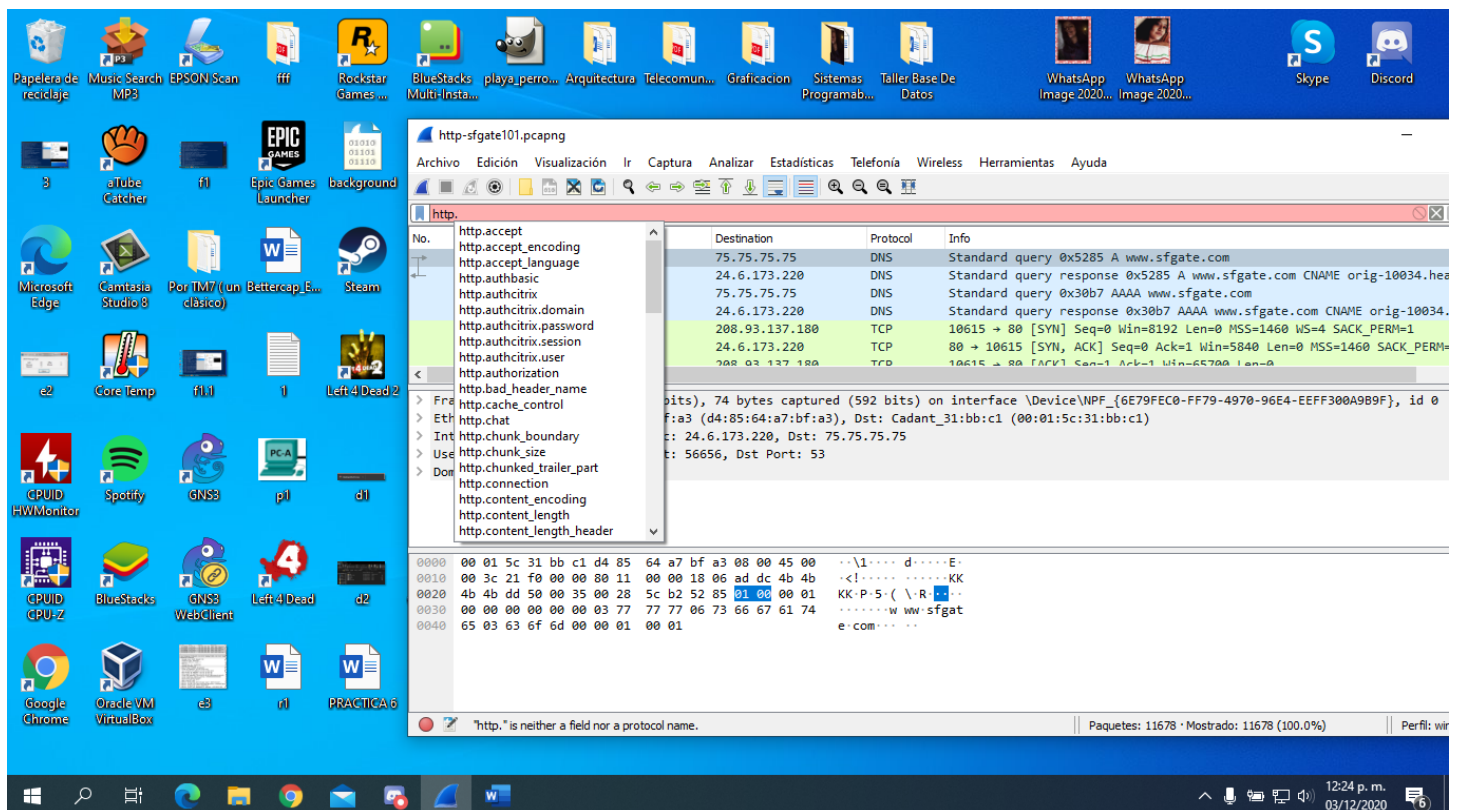
Horario: 5:00 pm – 6:00 pm

## Laboratio N#14 – Use autocompletar para encontrar trafico a un servidor HTTP especifico

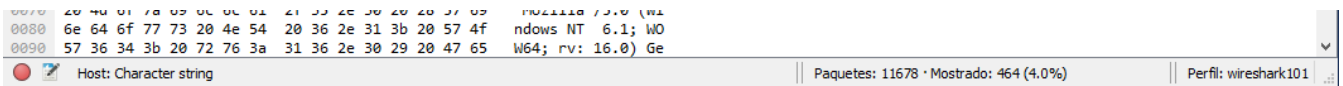
Paso 1 – Abrimos el archivo http-sfgate101.pcapng Miramos el rastreo para tener una idea del trafico. Debemos de ver mucho trafico DNS y HTTP en este archivo de seguimiento.



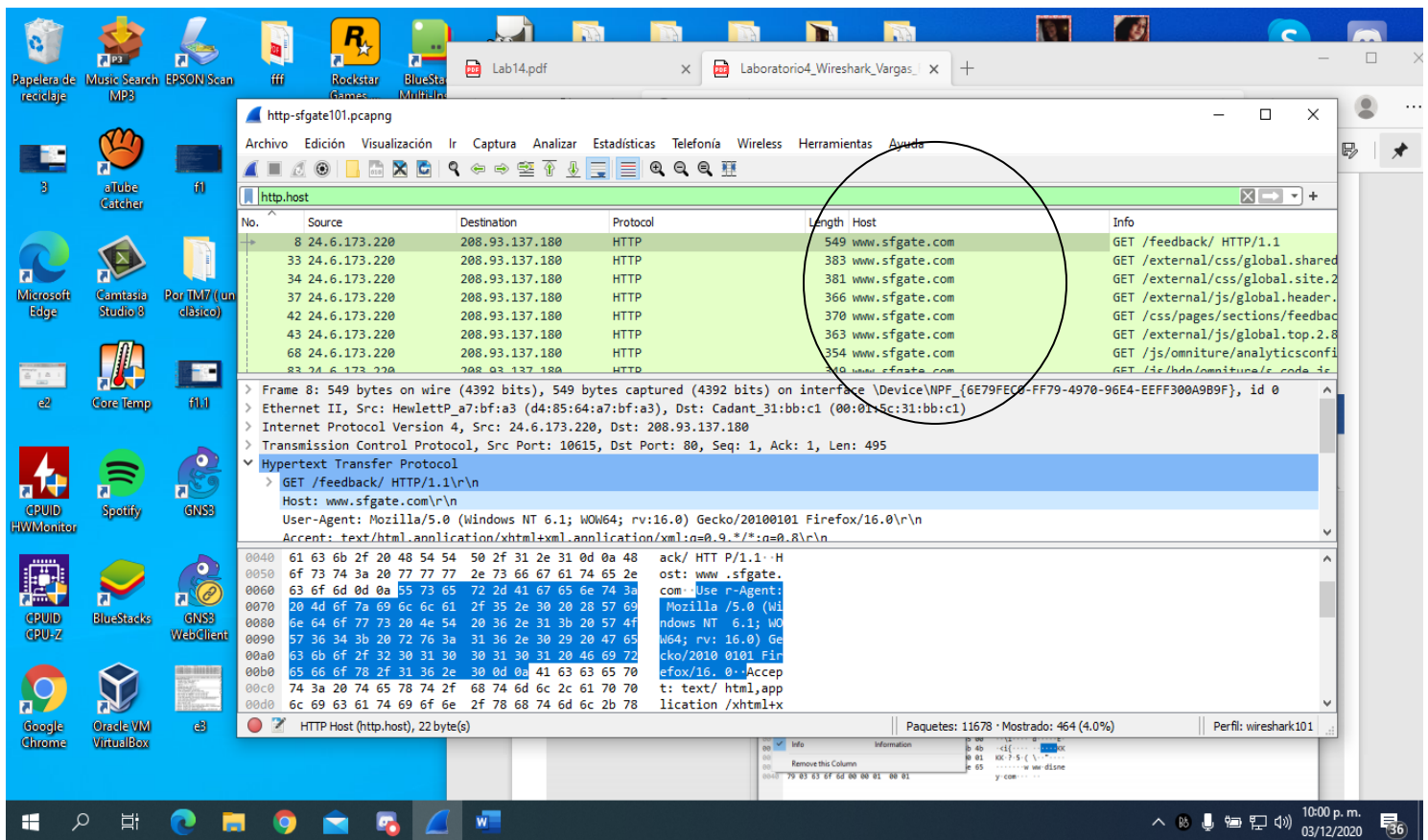
Paso 2 – Usaremos la función de autocompletar para comenzar el filtro de visualización, en el área de visualización escriba http.(incluido el punto). Aparecerá un menú desplegable que enumera todos los filtros con el http.patern.



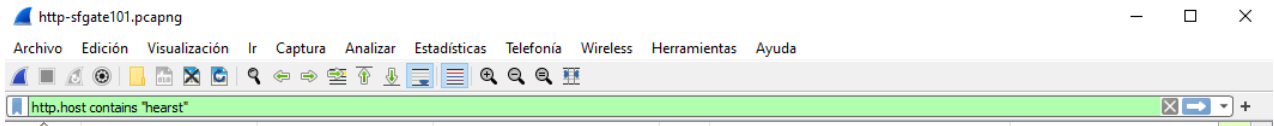
Paso 3 – Usaremos esta lista para averiguar a que host HTTP se esta accediendo en este archivo de seguimiento. Hacemos clic en el botón aplicar y debe indicar que son 464 paquetes.



Paso 4 – Hay que agregar una columna para que podamos ver fácilmente que hosts fueron contactados. Hacemos clic con el botón derecho en el campo de host y seleccionamos aplicar como columna.



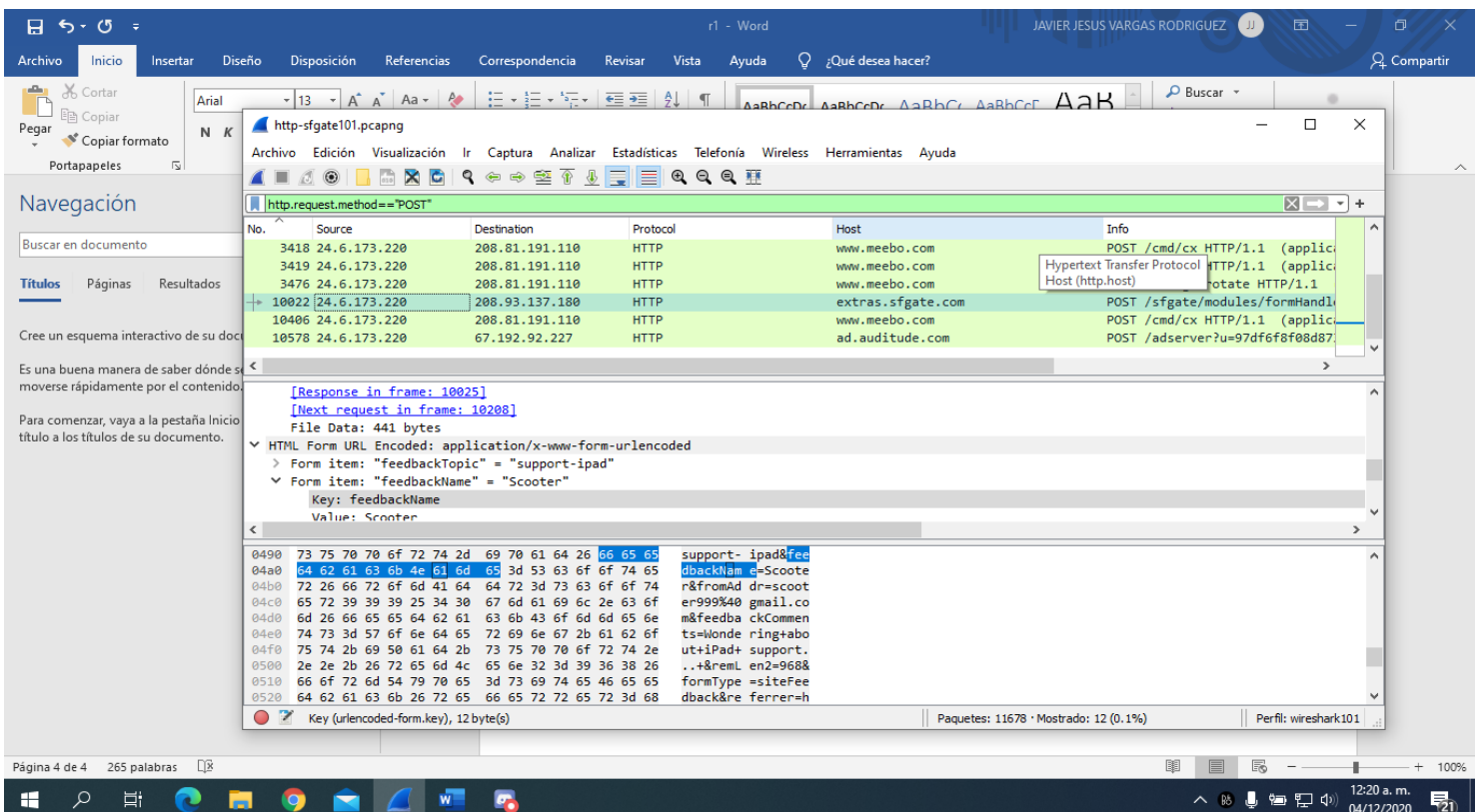
Paso 5 – Desplace por el archivo de seguimiento para ver los numerosos host que se solicitaron. Escriba en el área del filtro de pantalla para expandir su filtro de pantalla a http.host contains "hearst".



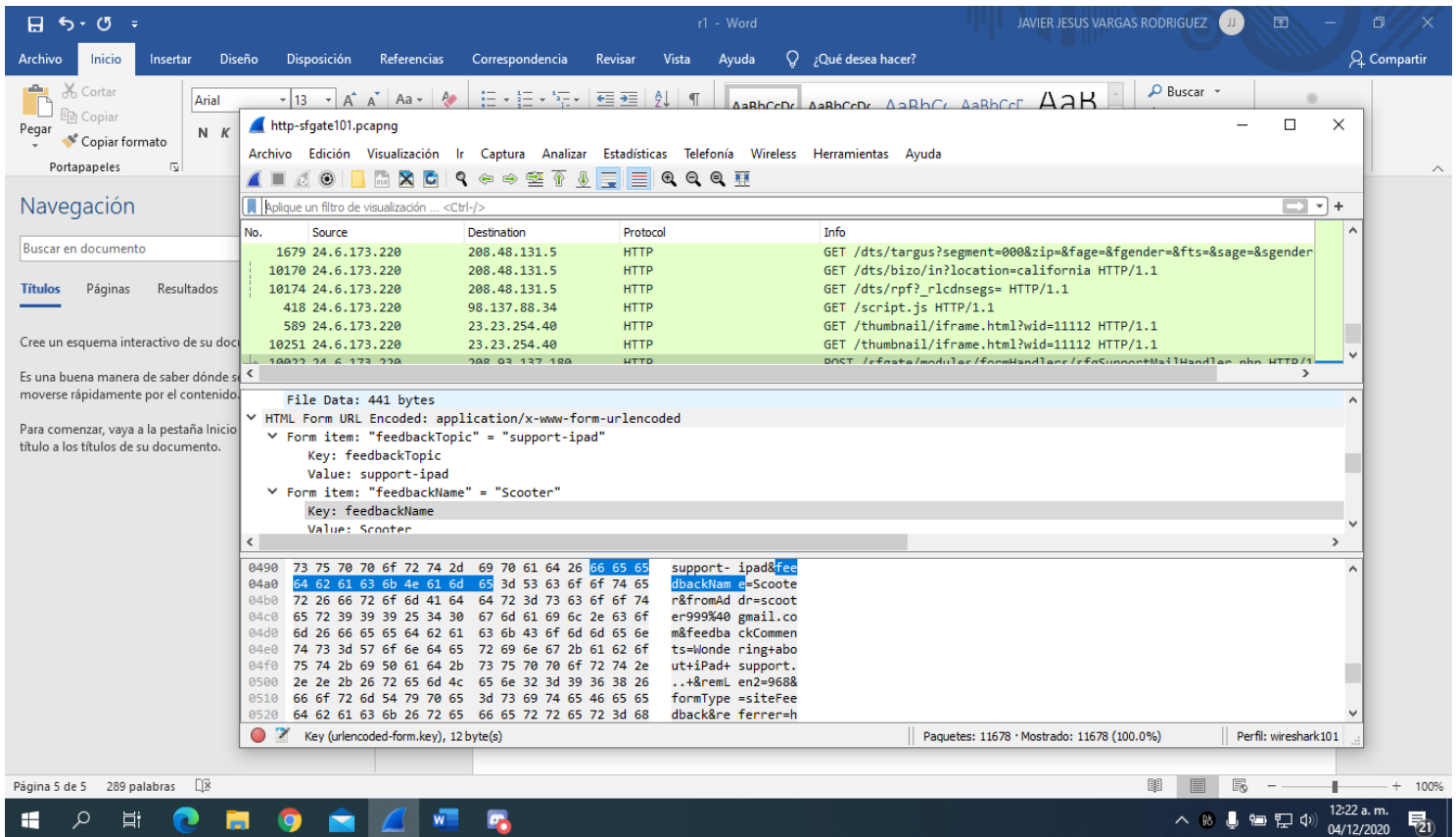
Paso 6 – Primero examinamos la sección HTTP de cualquier paquete en el panel Detalles del paquete. Hay que asegurarnos que la sección de HTTP esta ampliada. Y solo deben de alcanzar a verse 12 paquetes.



Paso 7 - Nos desplazamos por los 12 paquetes para buscar alguna referencia a extras.sfgate.com en la columna host.



Paso 8 – Hacemos clic en el botón derecho de la columna HOST y anulamos la selección de esa columna de la lista para ocultarla y así es como debería de quedar ahora.



The screenshot shows a Windows desktop with a Microsoft Word document open in the background. In the foreground, the Wireshark network protocol analyzer is running, displaying a packet capture from the file 'http-sfgate101.pcapng'. The main packet list pane shows several HTTP GET requests. The packet list is as follows:

No.	Source	Destination	Protocol	Info
1679	24.6.173.220	208.48.131.5	HTTP	GET /dts/targus?segment=000&zip=&fage=&fgender=&fts=&sage=&sgender=
10170	24.6.173.220	208.48.131.5	HTTP	GET /dts/bizo/in?location=california HTTP/1.1
10174	24.6.173.220	208.48.131.5	HTTP	GET /dts/rpf?_rlcdnsegs= HTTP/1.1
418	24.6.173.220	98.137.88.34	HTTP	GET /script.js HTTP/1.1
589	24.6.173.220	23.23.254.40	HTTP	GET /thumbnail/iframe.html?wid=11112 HTTP/1.1
10251	24.6.173.220	23.23.254.40	HTTP	GET /thumbnail/iframe.html?wid=11112 HTTP/1.1

The packet list pane is filtered by 'Host'. The packet details pane for the selected packet (No. 10251) shows the following structure:

- File Data: 441 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "feedbackTopic" = "support-ipad"
    - Key: feedbackTopic
    - Value: support-ipad
  - Form item: "feedbackName" = "Scooter"
    - Key: feedbackName
    - Value: Scooter

The raw data pane shows the hexadecimal and ASCII representation of the packet data, including the form data and the 'feedbackName' key-value pair.