



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

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Captura de tráfico Laboratorio 2

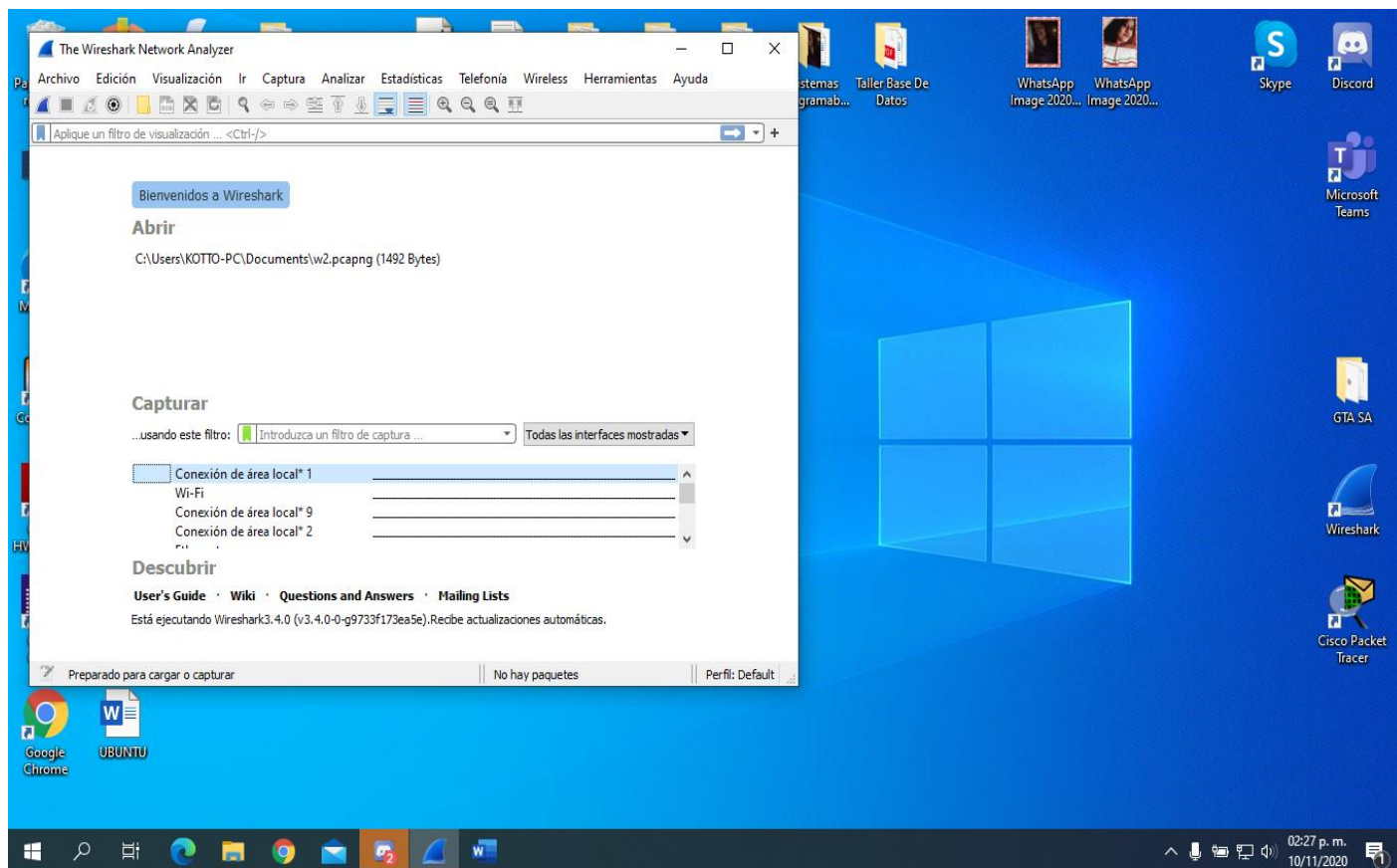
Alumno: Vargas Rodríguez Javier Jesús

Maestro: Ismael Jiménez Sánchez

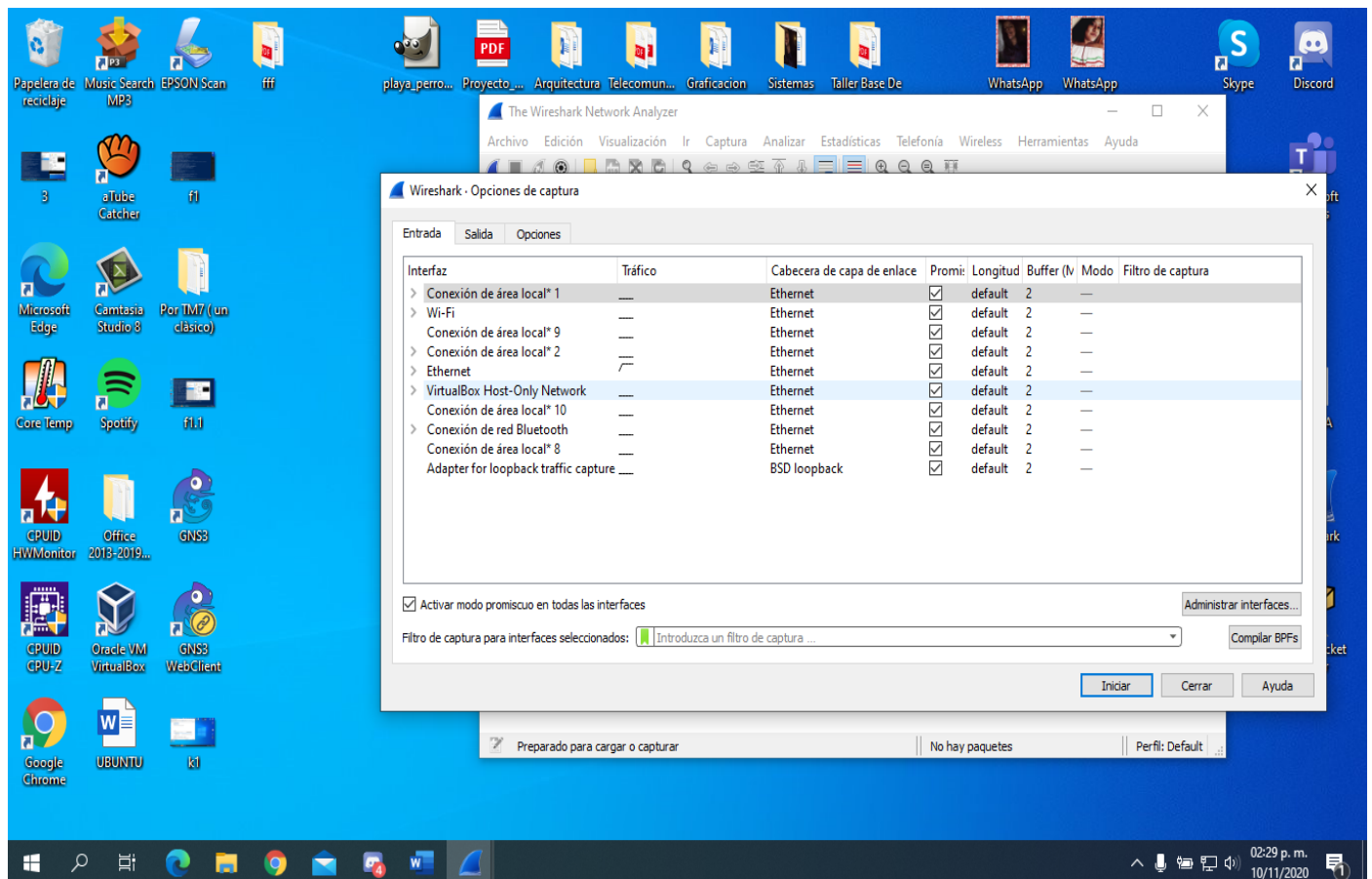
Fecha De Entrega: 10/Noviembre/2020

Horario: 5:00 pm – 6:00 pm

Para poder capturar nuestro trafico en la red, lo primero que debemos hacer es abrir Wireshark y automaticamente nos mostrara las redes a la que nosotros deseemos poder ver su trafico.



Ahora solo nos toca seleccionar en la opción que nos muestra con el Nombre de Captura de Datos y nos aparecerán todas las conexiones que se tienen ligadas. En algunos casos estos nos muestran ningún flujo de paquete de datos.



Ya en lo ultimo que seleccionemos, en mi caso le di “Ethernet” me empezara a mostrar el flujo de los datos de esa conexión y se ira mostrando en la pantalla.

Capturing from Ethernet

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
58	15.714328	162.159.130.233	192.168.100.45	TCP	66	443 → 49867 [ACK] Seq=1 Ack=2 Win=68 Len=0 SLE=1 SRE=2
59	15.874088	192.168.100.45	172.107.230.118	UDP	50	65358 → 50001 Len=8
60	15.917985	172.107.230.118	192.168.100.45	UDP	60	50001 → 65358 Len=8
61	15.961519	192.168.100.45	162.159.130.235	TLSv1.2	115	Application Data
62	15.999984	172.107.230.118	192.168.100.45	RTCP	94	Receiver Report
63	16.042317	162.159.130.235	192.168.100.45	TLSv1.2	111	Application Data
64	16.087243	192.168.100.45	162.159.130.235	TCP	54	49803 → 443 [ACK] Seq=123 Ack=115 Win=509 Len=0
65	16.235845	CloudNet_19:eb:63	Broadcast	ARP	60	Who has 192.168.100.29? Tell 192.168.100.11
66	16.958980	SamsungE_60:2a:e4	Broadcast	ARP	60	Who has 192.168.100.1? Tell 192.168.100.58
67	16.998928	172.107.230.118	192.168.100.45	RTCP	94	Receiver Report
68	17.237773	CloudNet_19:eb:63	Broadcast	ARP	60	Who has 192.168.100.29? Tell 192.168.100.11
69	17.852506	192.168.100.2	192.168.100.255	UDP	119	9431 → 9431 Len=77
70	17.998915	172.107.230.118	192.168.100.45	RTCP	94	Receiver Report
71	18.526099	192.168.100.45	172.107.230.118	RTCP	102	Sender Report
72	18.998902	172.107.230.118	192.168.100.45	RTCP	94	Receiver Report
73	19.973552	SamsungE_60:2a:e4	Broadcast	ARP	60	Who has 192.168.100.1? Tell 192.168.100.58
74	19.999728	172.107.230.118	192.168.100.45	RTCP	94	Receiver Report
75	20.186080	192.168.100.11	192.168.100.255	UDP	86	57621 → 57621 Len=44

> Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{E955E6FB-DAA6-484D-99DC-432AF20DEFF8}, id 0

> Ethernet II, Src: HuaweiTe_ed:72:9e (68:4a:ae:ed:72:9e), Dst: HewlettP_e6:ef:5a (b0:5a:da:e6:ef:5a)

> Internet Protocol Version 4, Src: 172.107.230.118, Dst: 192.168.100.45

> User Datagram Protocol, Src Port: 50001, Dst Port: 65358

> Real-time Transport Control Protocol (Receiver Report)

```

0000 b0 5a da e6 ef 5a 68 4a ae ed 72 9e 08 00 45 20  .Z...ZhJ...r...E
0010 00 50 2e 0e 40 00 35 11 5f b7 ac 6b e6 76 c0 a8  .P..@.5...k.v...
0020 64 2d c3 51 ff 4e 00 3c 83 62 81 c9 00 07 00 03  d-.Q.N<..b.....
0030 2e 96 e4 53 65 16 7a 7b cf a9 9d c8 0c 93 1f 4a  .Se.z{.....J
0040 64 04 75 88 8e 9b 4f 2b 53 b1 af 44 e2 40 5f 6d  d-u...O+ S...D.@_m
0050 5d af fc 98 77 5c 0c 98 20 e5 f9 01 00 00      ]...w\... ..

```

Ethernet: <live capture in progress> Paquetes: 77 · Mostrado: 77 (100.0%) Perfil: Default