

INSTITUTO TECNOLÓGICO DE CANCÚN

LEON QUEB MIGUEL ANGEL

ISMAEL JIMENEZ SANCHEZ

FUND. TELECOMUNICACIONES

HORARIO

17:00 – 18:00



## LABORATORIO 2 - WIRESHARK

### -Capturas

Capturing from Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

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

No.	Time	Source	Destination	Protocol	Length	Info
64	5.927960	13.107.6.171	192.168.0.6	TCP	60	443 → 62804 [ACK] Seq=606 Ack=12102 Win=64240 Len=0
65	5.927960	13.107.6.171	192.168.0.6	TCP	60	443 → 62804 [ACK] Seq=606 Ack=14992 Win=64240 Len=0
66	5.927960	13.107.6.171	192.168.0.6	TCP	60	443 → 62804 [ACK] Seq=606 Ack=15395 Win=63837 Len=0
67	5.962203	13.107.6.171	192.168.0.6	TLSv1	296	Application Data
68	6.002360	192.168.0.6	13.107.6.171	TCP	54	62804 → 443 [ACK] Seq=15395 Ack=848 Win=62875 Len=0
69	6.380827	162.159.134.234	192.168.0.6	TLSv1	169	Application Data
70	6.421981	192.168.0.6	162.159.134.234	TCP	54	62753 → 443 [ACK] Seq=1 Ack=815 Win=63287 Len=0
71	6.823793	192.168.0.6	13.107.6.171	TCP	1514	62804 → 443 [ACK] Seq=15395 Ack=848 Win=62875 Len=1460 [TCP segment of a reassembled PDU]
72	6.823793	192.168.0.6	13.107.6.171	TLSv1	1473	Application Data
73	6.823939	192.168.0.6	13.107.6.171	TCP	1514	62804 → 443 [ACK] Seq=18274 Ack=848 Win=62875 Len=1460 [TCP segment of a reassembled PDU]
74	6.823939	192.168.0.6	13.107.6.171	TLSv1	574	Application Data
75	6.914755	13.107.6.171	192.168.0.6	TCP	60	443 → 62804 [ACK] Seq=848 Ack=16855 Win=64240 Len=0
76	6.914755	13.107.6.171	192.168.0.6	TCP	60	443 → 62804 [ACK] Seq=848 Ack=18274 Win=62821 Len=0
77	6.914755	13.107.6.171	192.168.0.6	TCP	60	443 → 62804 [ACK] Seq=848 Ack=20254 Win=64240 Len=0
78	7.037760	13.107.9.156	192.168.0.6	TCP	60	443 → 62840 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 1: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF\_{9283F25F-F694-45A6-AC4E-3A7B3C8AD4F5}, id 0

> Ethernet II, Src: HonHaiPr\_03:c2:a4 (f4:b7:e2:03:c2:a4), Dst: IntelCor\_70:dc:2b (34:02:86:70:dc:2b)

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 1900, Dst Port: 1900

0000 34 02 86 70 dc 2b f4 b7 e2 03 c2 a4 08 00 45 40 4 - p + + + + +

0010 01 d4 52 fb 00 00 01 11 b4 71 c0 a8 00 0a ef ff - R + + + + +

0020 ff fa 07 6c 07 6c 01 c0 ec be 4e 4f 54 49 46 59 - 1 1 - - - NOTIFY

0030 20 2a 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 \* HTTP/ 1.1 - - - Hos

0040 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 35 t:239.25 5.255.25

0050 30 3a 31 39 30 30 0d 0a 4e 54 3a 75 75 69 64 3a 0:1900 - - - NT:uuid:

0060 30 66 64 32 62 39 35 66 2d 37 63 36 38 2d 34 31 0fd2b95f - 7c68-41

0070 30 64 2d 62 66 39 30 2d 66 32 64 66 66 62 66 64 0d-bf90- f2dffbfd

0080 32 63 64 37 0d 0a 4e 54 53 3a 73 73 64 70 3a 61 2cd7 - NT S:ssdp:a

0090 6c 69 76 65 0d 0a 4c 6f 63 61 74 69 6f 6e 6a 68 live - Lo cation:h

Wi-Fi: <live capture in progress> Paquetes: 286 - Mostrado: 286 (100.0%) Perfil: Default

Capturing from Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

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

No.	Time	Source	Destination	Protocol	Length	Info
78	7.037760	13.107.9.156	192.168.0.6	TCP	60	443 → 62840 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	7.172512	13.107.6.171	192.168.0.6	TLSv1	512	Application Data
80	7.172512	13.107.6.171	192.168.0.6	TLSv1	92	Application Data
81	7.172611	192.168.0.6	13.107.6.171	TCP	54	62804 → 443 [ACK] Seq=20254 Ack=1344 Win=64240 Len=0
82	7.449043	31.13.89.53	192.168.0.6	TLSv1	160	Application Data
83	7.491672	192.168.0.6	31.13.89.53	TCP	54	62781 → 443 [ACK] Seq=1 Ack=107 Win=63458 Len=0
84	8.513675	192.168.0.6	31.13.89.53	TCP	55	62918 → 443 [ACK] Seq=1 Ack=1 Win=63259 Len=1 [TCP segment of a reassembled PDU]
85	8.514693	192.168.0.6	192.168.0.7	TCP	171	62752 → 8009 [PSH, ACK] Seq=118 Ack=120 Win=63311 Len=117 [TCP segment of a reassembled PDU]
86	8.519424	192.168.0.7	192.168.0.6	TCP	173	8009 → 62752 [PSH, ACK] Seq=120 Ack=235 Win=65535 Len=119 [TCP segment of a reassembled PDU]
87	8.560423	192.168.0.6	192.168.0.7	TCP	54	62752 → 8009 [ACK] Seq=235 Ack=239 Win=63192 Len=0
88	8.589635	31.13.89.53	192.168.0.6	TCP	60	443 → 62918 [ACK] Seq=1 Ack=2 Win=65535 Len=0
89	10.517827	192.168.0.6	69.192.140.24	TCP	55	62807 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1 [TCP segment of a reassembled PDU]
90	10.517828	192.168.0.6	69.192.140.24	TCP	55	62805 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1 [TCP segment of a reassembled PDU]
91	10.517854	192.168.0.6	69.192.140.24	TCP	55	62806 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1 [TCP segment of a reassembled PDU]
92	10.517854	192.168.0.6	69.192.140.24	TCP	55	62808 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1 [TCP segment of a reassembled PDU]

> Frame 1: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF\_{9283F25F-F694-45A6-AC4E-3A7B3C8AD4F5}, id 0

> Ethernet II, Src: HonHaiPr\_03:c2:a4 (f4:b7:e2:03:c2:a4), Dst: IntelCor\_70:dc:2b (34:02:86:70:dc:2b)

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 1900, Dst Port: 1900

0000 34 02 86 70 dc 2b f4 b7 e2 03 c2 a4 08 00 45 40 4 - p + + + + +

0010 01 d4 52 fb 00 00 01 11 b4 71 c0 a8 00 0a ef ff - R + + + + +

0020 ff fa 07 6c 07 6c 01 c0 ec be 4e 4f 54 49 46 59 - 1 1 - - - NOTIFY

0030 20 2a 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 \* HTTP/ 1.1 - - - Hos

0040 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 35 t:239.25 5.255.25

0050 30 3a 31 39 30 30 0d 0a 4e 54 3a 75 75 69 64 3a 0:1900 - - - NT:uuid:

0060 30 66 64 32 62 39 35 66 2d 37 63 36 38 2d 34 31 0fd2b95f - 7c68-41

0070 30 64 2d 62 66 39 30 2d 66 32 64 66 66 62 66 64 0d-bf90- f2dffbfd

0080 32 63 64 37 0d 0a 4e 54 53 3a 73 73 64 70 3a 61 2cd7 - NT S:ssdp:a

0090 6c 69 76 65 0d 0a 4c 6f 63 61 74 69 6f 6e 6a 68 live - Lo cation:h

Wi-Fi: <live capture in progress> Paquetes: 1247 - Mostrado: 1247 (100.0%) Perfil: Default

Capturing from Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

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

No.	Time	Source	Destination	Protocol	Length	Info
3157	100.7597...	192.168.0.6	69.192.142.72	TCP	55	[TCP Keep-Alive] 62815 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1
3158	100.7777...	192.168.0.6	69.192.142.72	TCP	55	[TCP Keep-Alive] 62818 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1
3159	100.8146...	69.192.142.72	192.168.0.6	TCP	60	[TCP Keep-Alive ACK] 443 → 62817 [ACK] Seq=1 Ack=2 Win=63657 Len=0
3160	100.8225...	69.192.142.72	192.168.0.6	TCP	60	[TCP Keep-Alive ACK] 443 → 62815 [ACK] Seq=1 Ack=2 Win=63784 Len=0
3161	100.8261...	192.168.0.6	192.168.0.255	NBNS	92	Name query NB WPAD<00>
3162	100.8394...	69.192.142.72	192.168.0.6	TCP	60	[TCP Keep-Alive ACK] 443 → 62818 [ACK] Seq=1 Ack=2 Win=63657 Len=0
3163	101.0774...	192.168.0.6	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
3164	101.0785...	fe80::45a0:ab83:...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
3165	101.0803...	192.168.0.6	224.0.0.251	MDNS	70	Standard query 0x0000 AAAA wpad.local, "QM" question
3166	101.0817...	fe80::45a0:ab83:...	ff02::fb	MDNS	90	Standard query 0x0000 AAAA wpad.local, "QM" question
3167	101.0860...	192.168.0.6	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
3168	101.0880...	fe80::45a0:ab83:...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
3169	101.0891...	192.168.0.6	224.0.0.251	MDNS	70	Standard query 0x0000 AAAA wpad.local, "QM" question
3170	101.0902...	fe80::45a0:ab83:...	ff02::fb	MDNS	90	Standard query 0x0000 AAAA wpad.local, "QM" question
3171	101.5791...	192.168.0.6	192.168.0.255	NBNS	92	Name query NB WPAD<00>
3172	102.0393...	192.168.0.6	192.168.0.255	NBNS	92	Name query NB WPAD<00>
3173	102.0409...	192.168.0.6	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
3174	102.0419...	fe80::45a0:ab83:...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
3175	102.0428...	192.168.0.6	224.0.0.251	MDNS	70	Standard query 0x0000 AAAA wpad.local, "QM" question

> Frame 1: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF\_{9283F25F-F694-45A6-AC4E-3A7B3C8AD4F5}, id 0

> Ethernet II, Src: HonHaiPr\_03:c2:a4 (f4:b7:a2:03:c2:a4), Dst: IntelCor\_70:dc:2b (34:02:86:70:dc:2b)

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 1900, Dst Port: 1900

> Simple Service Discovery Protocol

Wireshark · All Addresses · Wi-Fi

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ All Addresses	139				0.0008	100%	0.1800	97.131
ff02::fb	90				0.0005	64.75%	0.1200	97.131
ff02::c	5				0.0000	3.60%	0.0200	0.000
ff02::1:3	44				0.0002	31.65%	0.0600	97.138
fe80::45a0:ab83:72ae:33dd	134				0.0007	96.40%	0.1800	97.131
fe80::1470:81f8:2debb891	5				0.0000	3.60%	0.0200	0.000

Wireshark · All Addresses · Wi-Fi

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ All Addresses	7898				0.0245	100%	1.1700	37.860
74.125.26.188	14				0.0000	0.18%	0.0200	36.042
69.192.142.72	306				0.0009	3.87%	0.7200	305.241
69.192.141.224	48				0.0001	0.61%	0.0900	305.243
69.192.140.63	18				0.0001	0.23%	0.0400	305.243
69.192.140.24	90				0.0003	1.14%	0.1500	305.345
52.96.103.50	2				0.0000	0.03%	0.0100	0.155
52.232.226.150	52				0.0002	0.66%	0.1100	92.118
52.184.215.140	29				0.0001	0.37%	0.1500	93.818
52.179.224.121	3				0.0000	0.04%	0.0200	230.514
52.177.166.224	8				0.0000	0.10%	0.0100	181.269
52.177.165.30	55				0.0002	0.70%	0.0800	209.006
52.114.159.34	23				0.0001	0.29%	0.0600	163.889
52.114.158.50	3				0.0000	0.04%	0.0100	19.421
52.114.132.23	4				0.0000	0.05%	0.0200	20.907
52.114.128.43	62				0.0002	0.79%	0.1200	308.665
52.113.195.132	1				0.0000	0.01%	0.0100	0.130
52.111.239.7	5				0.0000	0.06%	0.0400	30.837
52.111.239.4	149				0.0005	1.89%	0.0200	2.729
52.111.239.15	53				0.0002	0.67%	0.0600	37.316
52.109.8.30	1				0.0000	0.01%	0.0100	30.837
52.109.6.5	1				0.0000	0.01%	0.0100	18.925
52.109.6.39	1				0.0000	0.01%	0.0100	17.593
52.109.20.47	2				0.0000	0.03%	0.0100	31.451
52.109.2.52	1				0.0000	0.01%	0.0100	0.533
51.104.162.168	26				0.0001	0.33%	0.0800	164.461
40.90.23.153	60				0.0002	0.76%	0.2300	91.316