



TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

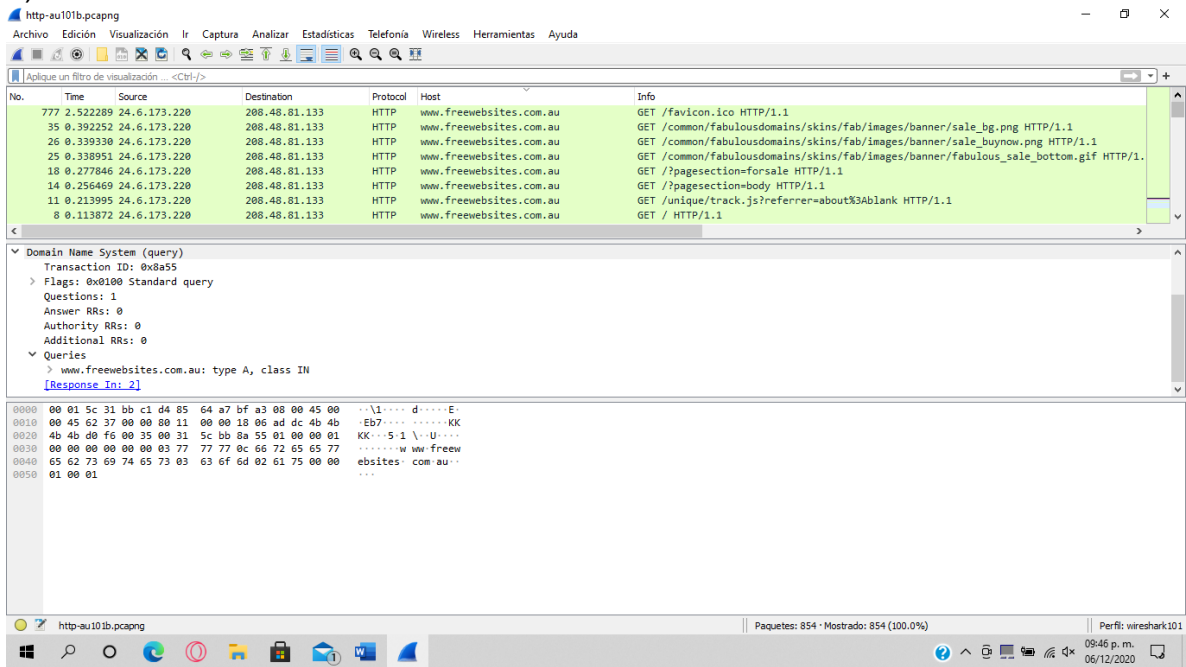
DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“LABORATORIO 29”

UNIDAD 3

1)



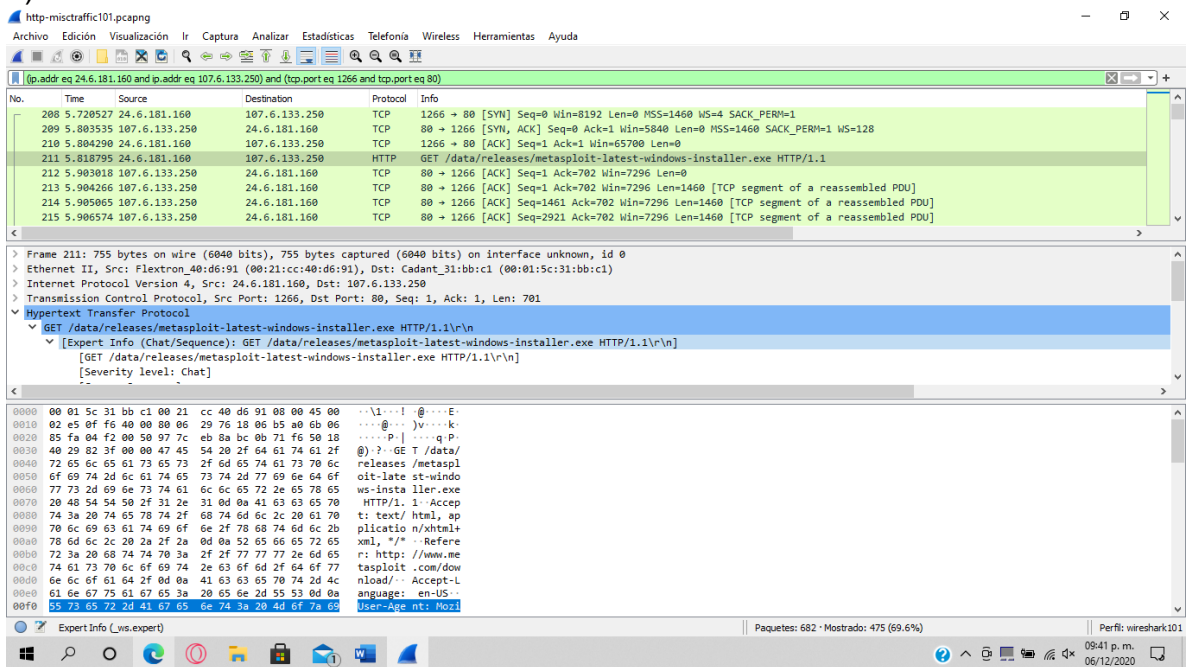
Wireshark capture of HTTP traffic. The packet list shows a GET request for /favicon.ico. The packet details pane shows the Domain Name System (query) section, indicating a query for www.freewebsites.com.au. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Host	Info
777	2.522289	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /favicon.ico HTTP/1.1
35	0.392252	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /common/fabulousdomains/skins/fab/images/banner/sale_bg.png HTTP/1.1
26	0.339330	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /common/fabulousdomains/skins/fab/images/banner/sale_buynow.png HTTP/1.1
25	0.338951	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /common/fabulousdomains/skins/fab/images/banner/fabulous_sale_bottom.gif HTTP/1.1
18	0.277846	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /?pageaction=forsale HTTP/1.1
14	0.256469	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /?pageaction=body HTTP/1.1
11	0.213995	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET /unique/track.js?referrer=about%3Ablank HTTP/1.1
8	0.113872	24.6.173.220	208.48.81.133	HTTP	www.freewebsites.com.au	GET / HTTP/1.1

Domain Name System (query)
Transaction ID: 0x8a55
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries:
www.freewebsites.com.au: type A, class IN
[Response In: 2]

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ...1... d...E:
0010 00 45 62 37 00 00 00 11 00 00 18 06 ad dc 4b 4b ...Eb7... ..K:
0020 4b 4b 00 f6 00 35 00 31 5c bb 8a 55 01 00 00 01 KK...5 1 \-U...
0030 00 00 00 00 00 03 77 77 77 0c 66 72 65 77w w freew
0040 65 62 73 69 74 65 73 03 63 6f 6d 02 61 75 00 00 ebsites .com.au..
0050 01 00 01 ...

2)



Wireshark capture of HTTP traffic. The packet list shows a GET request for /data/releases/metasploit-latest-windows-installer.exe. The packet details pane shows the Hypertext Transfer Protocol section, indicating a GET request for /data/releases/metasploit-latest-windows-installer.exe. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Info
208	5.720527	24.6.181.160	107.6.133.250	TCP	1266 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
209	5.803535	107.6.133.250	24.6.181.160	TCP	80 → 1266 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
210	5.804290	24.6.181.160	107.6.133.250	TCP	1266 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
211	5.818795	24.6.181.160	107.6.133.250	HTTP	GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1
212	5.903018	107.6.133.250	24.6.181.160	TCP	80 → 1266 [ACK] Seq=1 Ack=702 Win=7296 Len=0
213	5.904266	107.6.133.250	24.6.181.160	TCP	80 → 1266 [ACK] Seq=1 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
214	5.905065	107.6.133.250	24.6.181.160	TCP	80 → 1266 [ACK] Seq=1461 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
215	5.906574	107.6.133.250	24.6.181.160	TCP	80 → 1266 [ACK] Seq=2921 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]

Frame 211: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface unknown, id 0
Ethernet II, Src: Flextron_40:d6:91 (00:21:cc:40:d6:91), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.181.160, Dst: 107.6.133.250
Transmission Control Protocol, Src Port: 1266, Dst Port: 80, Seq: 1, Ack: 1, Len: 701
Hypertext Transfer Protocol
GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1\r\n
[GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1\r\n
[Severity level: Chat]

0000 00 01 5c 31 bb c1 00 21 cc 40 d6 91 00 00 45 00 ...1...1 -@...E:
0010 02 e5 0f f6 40 00 00 06 29 76 18 06 b5 a0 6b 06 ...@... v...k:
0020 85 fa 04 f2 00 50 97 7c eb 8a bc 0b 71 f6 50 18P. | ...q P:
0030 40 29 82 3f 00 00 47 45 54 20 2f 64 61 74 61 2f @) ? -GE T /data/
0040 72 65 6c 65 61 73 65 79 2f 6d 65 74 61 73 70 6c releases /metasp
0050 6f 69 74 2d 6c 61 74 65 73 74 2d 77 69 6e 64 6f oit-late st-windo
0060 77 73 2d 69 6e 73 74 61 6c 6c 65 72 2e 65 78 65 ws-insta ller.exe
0070 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 HTTP/1.1 -Accep
0080 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
0090 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
00a0 78 6d 6c 2c 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 xml, */* -Refere
00b0 72 3a 20 68 74 70 3a 2f 2f 77 77 77 2e 6d 65 rs: http: //www.me
00c0 74 61 73 70 6c 6f 69 74 2e 63 6f 6d 2f 64 6f 77 tasloit .com/dow
00d0 6e 6c 6f 61 64 2f 0d 0a 41 63 63 65 70 74 2d 4c nload/- Accept-L
00e0 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 0d 0a anguage: en-US
00f0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 78 65 User-Age nt: Mozil

3)

