TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

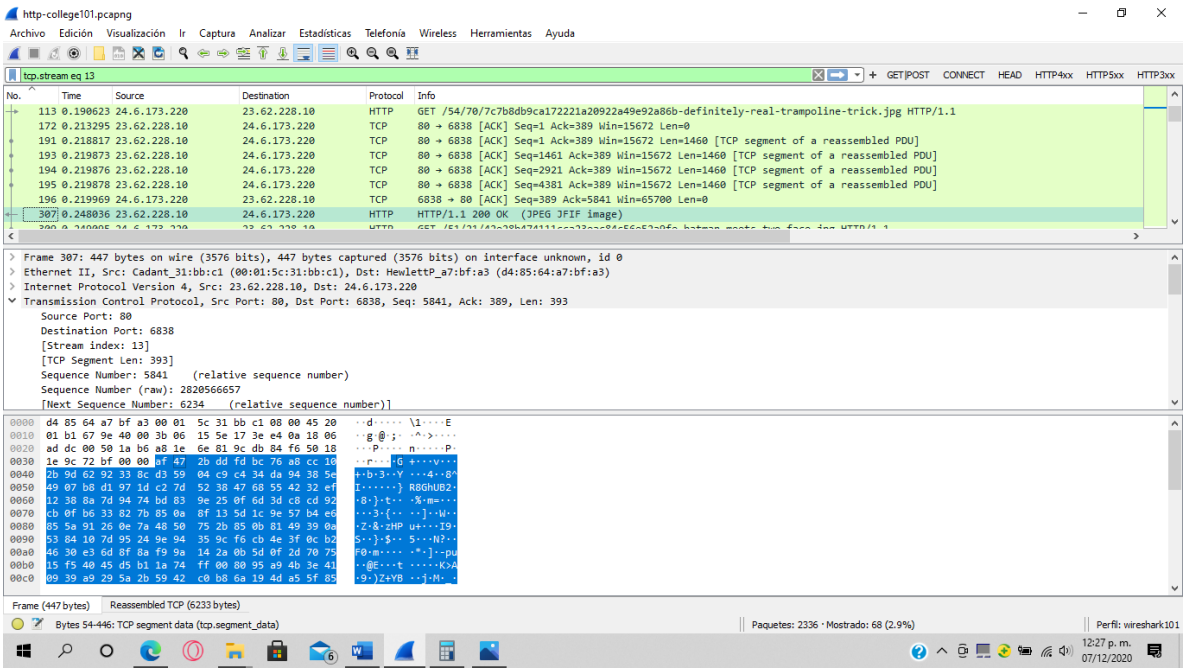
DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

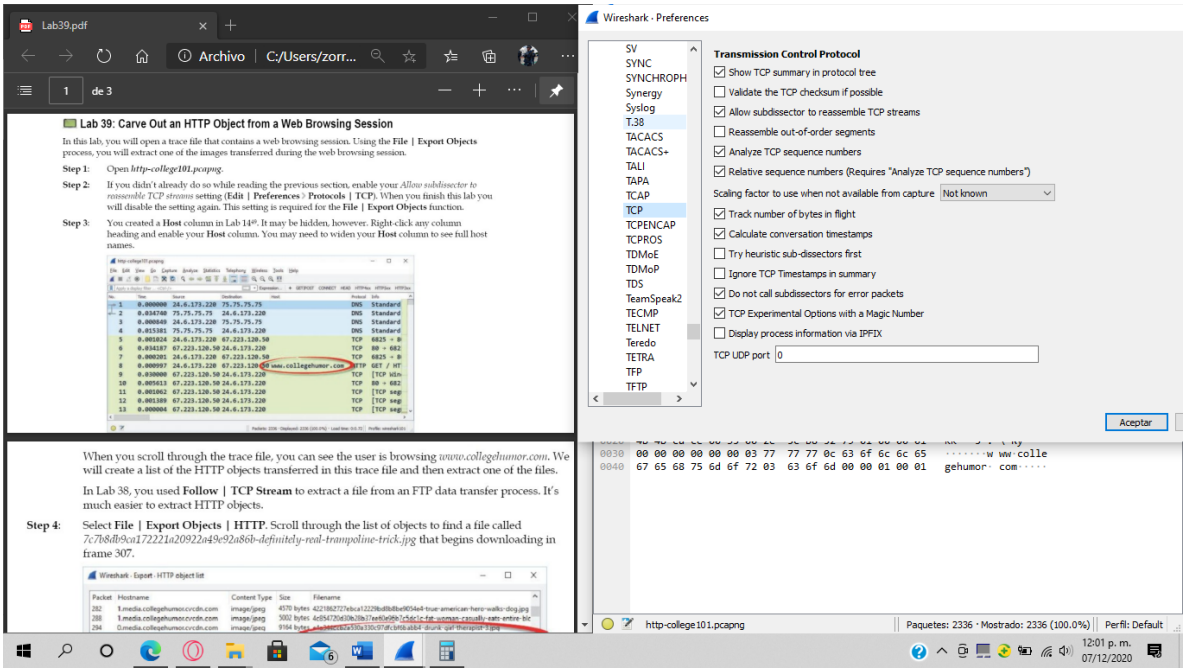
“LABORATORIO 39”

UNIDAD 3

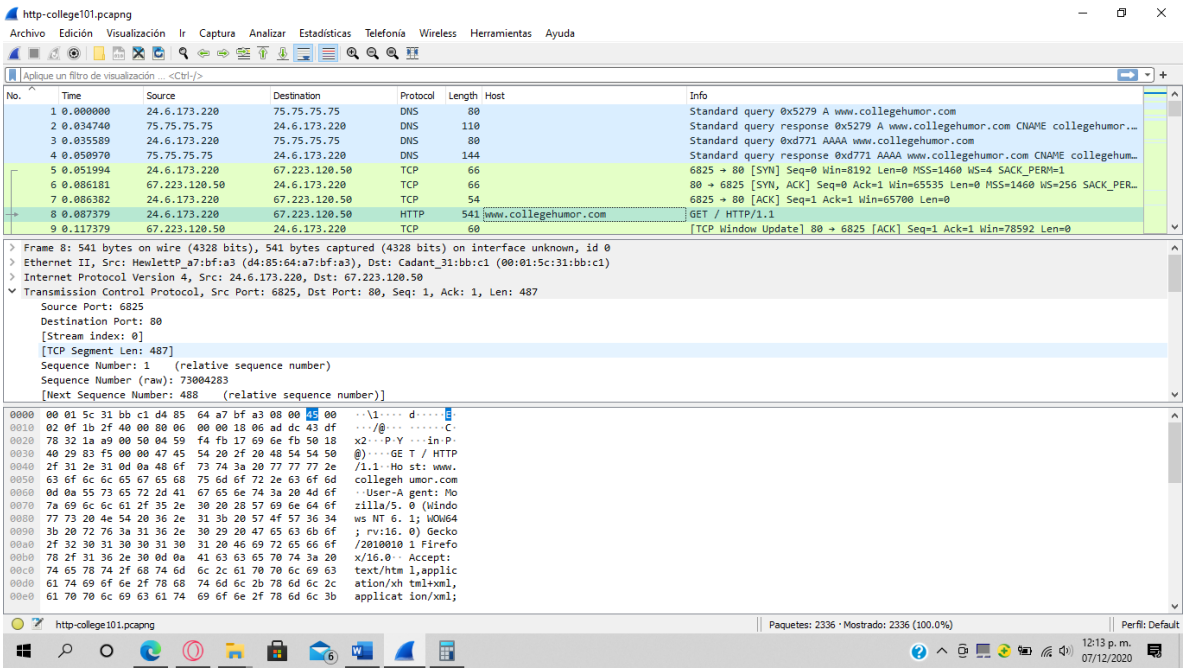
1)


http-college101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp.stream eq 13
No. Time Source Destination Protocol Info
113 0.190623 24.6.173.220 23.62.228.10 HTTP GET /54/70/7c7b8db9ca172221a20922a49e92a86b-definitely-real-trampoline-trick.jpg HTTP/1.1
172 0.213295 23.62.228.10 24.6.173.220 TCP 80 → 6838 [ACK] Seq=1 Ack=389 Win=15672 Len=0
191 0.218817 23.62.228.10 24.6.173.220 TCP 80 → 6838 [ACK] Seq=1 Ack=389 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
193 0.219873 23.62.228.10 24.6.173.220 TCP 80 → 6838 [ACK] Seq=1461 Ack=389 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
194 0.219876 23.62.228.10 24.6.173.220 TCP 80 → 6838 [ACK] Seq=2921 Ack=389 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
195 0.219878 23.62.228.10 24.6.173.220 TCP 80 → 6838 [ACK] Seq=4381 Ack=389 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
196 0.219969 24.6.173.220 23.62.228.10 TCP 6838 → 80 [ACK] Seq=389 Ack=5841 Win=65700 Len=0
307 0.248036 23.62.228.10 24.6.173.220 HTTP HTTP/1.1 200 OK (JPEG JFIF image)
Frame 307: 447 bytes on wire (3576 bits), 447 bytes captured (3576 bits) on interface unknown, id 0
Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
Internet Protocol Version 4, Src: 23.62.228.10, Dst: 24.6.173.220
Transmission Control Protocol, Src Port: 80, Dst Port: 6838, Seq: 5841, Ack: 389, Len: 393
Source Port: 80
Destination Port: 6838
[Stream index: 13]
[TCP Segment Len: 393]
Sequence Number: 5841 (relative sequence number)
Sequence Number (raw): 2820566657
[Next Sequence Number: 6234 (relative sequence number)]
Frame (447 bytes)
Reassembled TCP (6233 bytes)
Bytes 54-446: TCP segment data (tcp.segment_data)
Paquetes: 2336 · Mostrado: 68 (2.9%)
Perfil: wireshark101
12:27 p. m.
07/12/2020

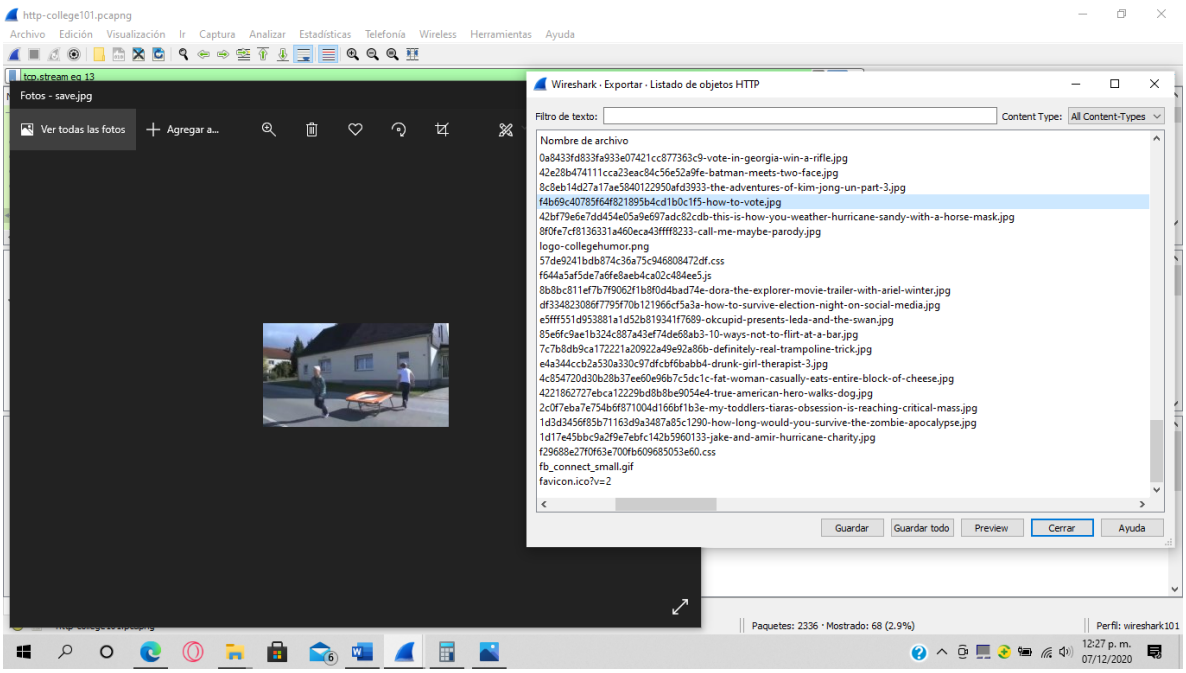
2)


Lab39.pdf
Archivo C:/Users/zorr...
1 de 3
Lab 39: Carve Out an HTTP Object from a Web Browsing Session
In this lab, you will open a trace file that contains a web browsing session. Using the File | Export Objects process, you will extract one of the images transferred during the web browsing session.
Step 1: Open http-college101.pcapng.
Step 2: If you didn't already do so while reading the previous section, enable your Allow subdissector to reassemble TCP streams setting (Edit | Preferences | Protocols | TCP). When you finish this lab you will disable the setting again. This setting is required for the File | Export Objects function.
Step 3: You created a Host column in Lab 14[9]. It may be hidden, however. Right-click any column heading and enable your Host column. You may need to widen your Host column to see full host names.
When you scroll through the trace file, you can see the user is browsing www.collegehumor.com. We will create a list of the HTTP objects transferred in this trace file and then extract one of the files.
In Lab 38, you used Follow | TCP Stream to extract a file from an FTP data transfer process. It's much easier to extract HTTP objects.
Step 4: Select File | Export Objects | HTTP. Scroll through the list of objects to find a file called 7c7b8db9ca172221a20922a49e92a86b-definitely-real-trampoline-trick.jpg that begins downloading in frame 307.
Wireshark · Preferences
Transmission Control Protocol
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
Analyze TCP sequence numbers
Relative sequence numbers (Requires "Analyze TCP sequence numbers")
Scaling factor to use when not available from capture Not known
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port 0
Aceptar
http-college101.pcapng
Paquetes: 2336 · Mostrado: 2336 (100.0%)
Perfil: Default
12:01 p. m.
07/12/2020

3)


http-college101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
No. Time Source Destination Protocol Length Host Info
1 0.000000 24.6.173.220 75.75.75.75 DNS 80 Standard query 0x5279 A www.collegehumor.com
2 0.034740 75.75.75.75 24.6.173.220 DNS 110 Standard query response 0x5279 A www.collegehumor.com CNAME collegehumor...
3 0.035589 24.6.173.220 75.75.75.75 DNS 80 Standard query 0xd771 AAAA www.collegehumor.com
4 0.050970 75.75.75.75 24.6.173.220 DNS 144 Standard query response 0xd771 AAAA www.collegehumor.com CNAME collegehum...
5 0.051994 24.6.173.220 67.223.120.50 TCP 66 6825 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6 0.086181 67.223.120.50 24.6.173.220 TCP 66 80 → 6825 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PER...
7 0.086382 24.6.173.220 67.223.120.50 TCP 54 6825 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8 0.087379 24.6.173.220 67.223.120.50 HTTP 541 www.collegehumor.com GET / HTTP/1.1
9 0.117379 67.223.120.50 24.6.173.220 TCP 60 [TCP Window Update] 80 → 6825 [ACK] Seq=1 Ack=1 Win=78592 Len=0
Frame 8: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface unknown, id 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 67.223.120.50
Transmission Control Protocol, Src Port: 6825, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
Source Port: 6825
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 487]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 73004283
[Next Sequence Number: 488 (relative sequence number)]
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 02 0f 1b 2f 40 00 80 06 00 00 18 06 ad dc 43 df
0020 78 32 1a a9 00 50 04 59 f4 fb 17 69 6e fb 50 18
0030 40 29 83 f5 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e
0050 63 6f 6c 6c 65 67 65 68 75 6d 6f 72 2e 63 6f 6d
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f
0070 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f
0080 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34
0090 3b 20 72 76 3a 31 36 2e 30 29 20 47 65 63 6b 6f
00a0 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f
00b0 78 2f 31 36 2e 30 0d 0a 41 63 63 65 70 74 3a 20
00c0 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63
00d0 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c
00e0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b
http-college101.pcapng
Paquetes: 2336 · Mostrado: 2336 (100.0%)
Perfil: Default
12:13 p. m.
07/12/2020

4)


http-college101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp.stream eq 13
Fotos - save.jpg
Ver todas las fotos
Agregar a...
Wireshark · Exportar · Listado de objetos HTTP
Filtro de texto:
Content Type: All Content-Types
Nombre de archivo
0a8433fd833fa933e07421cc877363c9-vote-in-georgia-win-a-rifle.jpg
42e28b474111cca23eac84c56e52a9fe-batman-meets-two-face.jpg
8c8eb14d27a17ae5840122950afd3933-the-adventures-of-kim-jong-un-part-3.jpg
f4b69c40785f64f821895b4cd1b0c1f5-how-to-vote.jpg
42bf79e6e7dd454e05a9e697adc82cdb-this-is-how-you-weather-hurricane-sandy-with-a-horse-mask.jpg
8f0fe7cf8136331a460eca43ffff8233-call-me-maybe-parody.jpg
logo-collegehumor.png
57de9241bdb874c36a75c946808472df.css
f644a5af5de7a6fe8aeb4ca02c484ee5.js
8b8bc811ef7b7f9062f1b8f0d4bad74e-dora-the-explorer-movie-trailer-with-ariel-winter.jpg
df334823086f7795f70b121966cf5a3a-how-to-survive-election-night-on-social-media.jpg
e5fff551d953881a1d52b819341f7689-okcupid-presents-leda-and-the-swan.jpg
85e6fc9ae1b324c887a43ef74de68ab3-10-ways-not-to-flirt-at-a-bar.jpg
7c7b8db9ca172221a20922a49e92a86b-definitely-real-trampoline-trick.jpg
e4a344ccb2a530a330c97dfcbf6babb4-drunk-girl-therapist-3.jpg
4c854720d30b28b37ee60e96b7c5dc1c-fat-woman-casually-eats-entire-block-of-cheese.jpg
4221862727ebca12229bd8b8be9054e4-true-american-hero-walks-dog.jpg
2c0f7eba7e754b6f871004d166bf1b3e-my-toddlers-tiaras-obsession-is-reaching-critical-mass.jpg
1d3d3456f85b71163d9a3487a85c1290-how-long-would-you-survive-the-zombie-apocalypse.jpg
1d17e45bbc9a2f9e7ebfc142b5960133-jake-and-amir-hurricane-charity.jpg
f29688e27f0f63e700fb609685053e60.css
fb_connect_small.gif
favicon.ico?v=2
Guardar
Guardar todo
Preview
Cerrar
Ayuda
Paquetes: 2336 · Mostrado: 68 (2.9%)
Perfil: wireshark101
12:27 p. m.
07/12/2020