INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

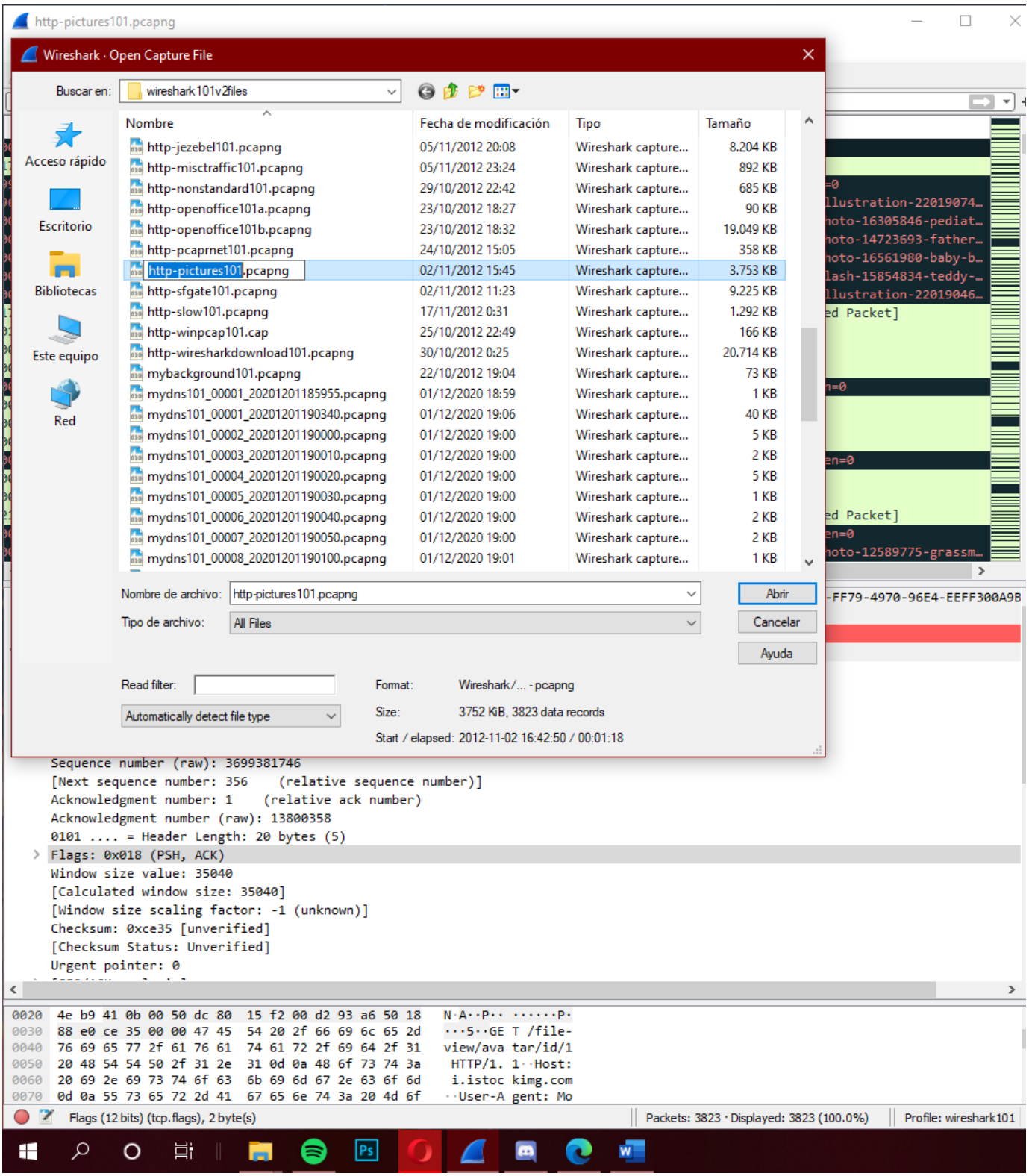
Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio

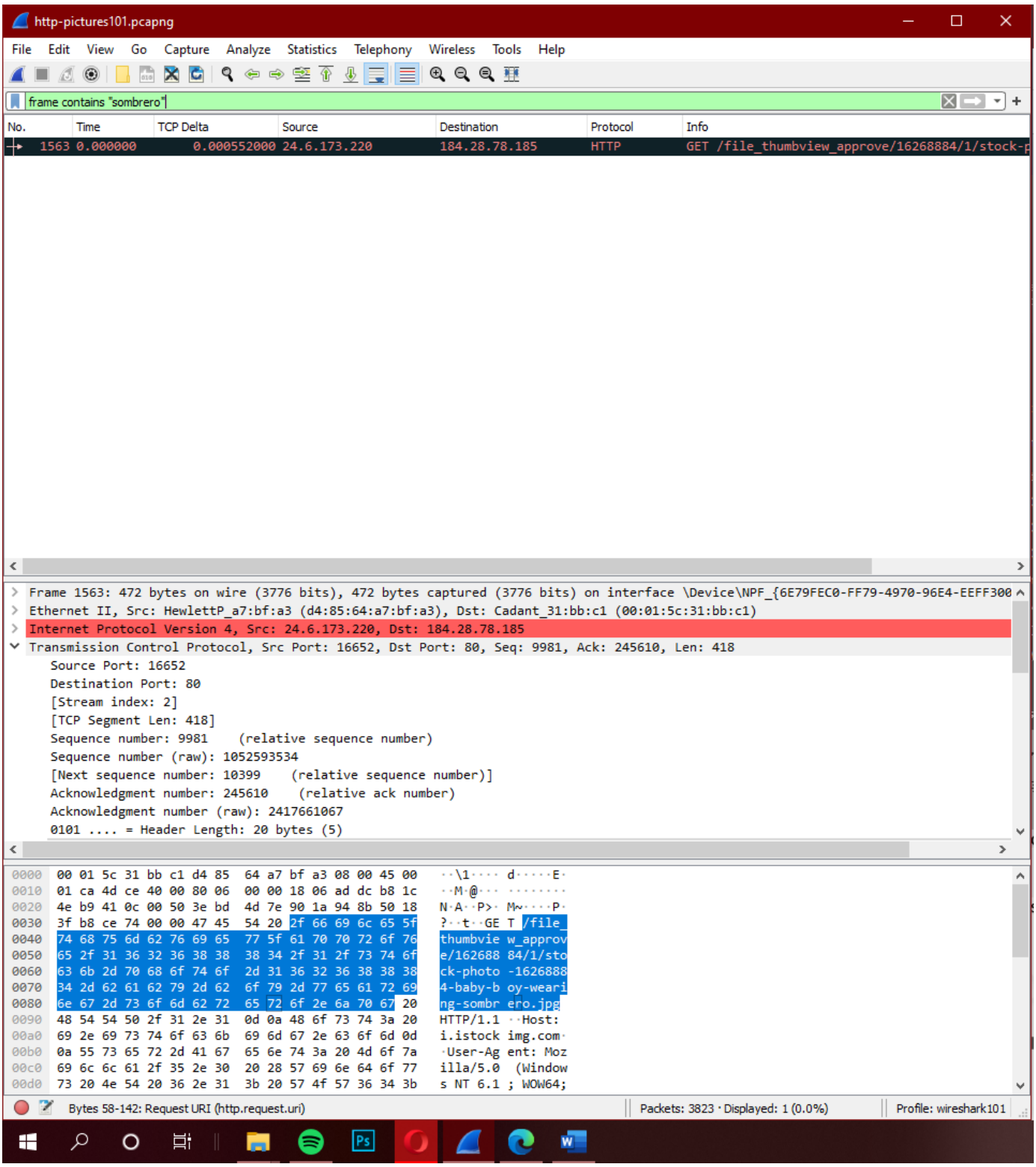
Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

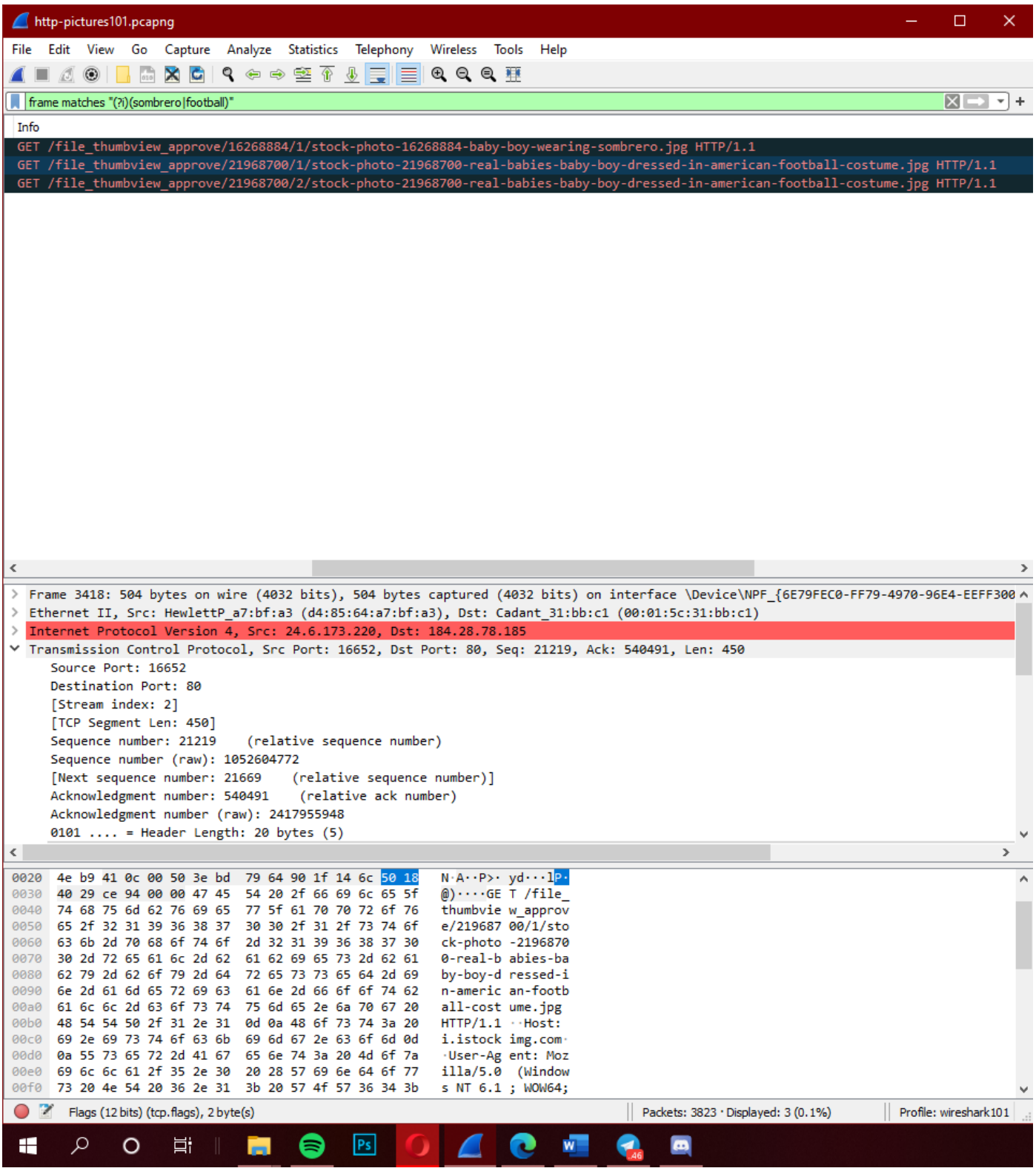
Lab21- Filter to Locate a Set of Key Words in a Trace File



Paso 2:


http-pictures101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame contains "sombrero"
No. Time TCP Delta Source Destination Protocol Info
1563 0.000000 0.000552000 24.6.173.220 184.28.78.185 HTTP GET /file_thumbview_approve/16268884/1/stock-p
Frame 1563: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300
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: 184.28.78.185
Transmission Control Protocol, Src Port: 16652, Dst Port: 80, Seq: 9981, Ack: 245610, Len: 418
Source Port: 16652
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 418]
Sequence number: 9981 (relative sequence number)
Sequence number (raw): 1052593534
[Next sequence number: 10399 (relative sequence number)]
Acknowledgment number: 245610 (relative ack number)
Acknowledgment number (raw): 2417661067
0101 .... = Header Length: 20 bytes (5)
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ··\1···· d·····E·
0010 01 ca 4d ce 40 00 80 06 00 00 18 06 ad dc b8 1c ··M·@··· ········
0020 4e b9 41 0c 00 50 3e bd 4d 7e 90 1a 94 8b 50 18 N·A··P>· M~····P·
0030 3f b8 ce 74 00 00 47 45 54 20 2f 66 69 6c 65 5f ?··t··GE T /file_
0040 74 68 75 6d 62 76 69 65 77 5f 61 70 70 72 6f 76 thumbvie w_approv
0050 65 2f 31 36 32 36 38 38 38 34 2f 31 2f 73 74 6f e/162688 84/1/sto
0060 63 6b 2d 70 68 6f 74 6f 2d 31 36 32 36 38 38 38 ck-photo -1626888
0070 34 2d 62 61 62 79 2d 62 6f 79 2d 77 65 61 72 69 4-baby-b oy-weari
0080 6e 67 2d 73 6f 6d 62 72 65 72 6f 2e 6a 70 67 20 ng-sombr ero.jpg
0090 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
00a0 69 2e 69 73 74 6f 63 6b 69 6d 67 2e 63 6f 6d 0d i.istock img.com·
00b0 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a ·User-Ag ent: Moz
00c0 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window
00d0 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b s NT 6.1 ; WOW64;
Bytes 58-142: Request URI (http.request.uri)
Packets: 3823 · Displayed: 1 (0.0%)
Profile: wireshark101

Paso 3:


http-pictures101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame matches "(?i)(sombrero|football)"
Info
GET /file_thumbview_approve/16268884/1/stock-photo-16268884-baby-boy-wearing-sombrero.jpg HTTP/1.1
GET /file_thumbview_approve/21968700/1/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1
GET /file_thumbview_approve/21968700/2/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1
Frame 3418: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300
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: 184.28.78.185
Transmission Control Protocol, Src Port: 16652, Dst Port: 80, Seq: 21219, Ack: 540491, Len: 450
Source Port: 16652
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 450]
Sequence number: 21219 (relative sequence number)
Sequence number (raw): 1052604772
[Next sequence number: 21669 (relative sequence number)]
Acknowledgment number: 540491 (relative ack number)
Acknowledgment number (raw): 2417955948
0101 .... = Header Length: 20 bytes (5)
0020 4e b9 41 0c 00 50 3e bd 79 64 90 1f 14 6c 50 18 N·A··P>· yd···lP·
0030 40 29 ce 94 00 00 47 45 54 20 2f 66 69 6c 65 5f @)····GE T /file_
0040 74 68 75 6d 62 76 69 65 77 5f 61 70 70 72 6f 76 thumbvie w_approv
0050 65 2f 32 31 39 36 38 37 30 30 2f 31 2f 73 74 6f e/219687 00/1/sto
0060 63 6b 2d 70 68 6f 74 6f 2d 32 31 39 36 38 37 30 ck-photo -2196870
0070 30 2d 72 65 61 6c 2d 62 61 62 69 65 73 2d 62 61 0-real-b abies-ba
0080 62 79 2d 62 6f 79 2d 64 72 65 73 73 65 64 2d 69 by-boy-d ressed-i
0090 6e 2d 61 6d 65 72 69 63 61 6e 2d 66 6f 6f 74 62 n-americ an-footb
00a0 61 6c 6c 2d 63 6f 73 74 75 6d 65 2e 6a 70 67 20 all-cost ume.jpg
00b0 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
00c0 69 2e 69 73 74 6f 63 6b 69 6d 67 2e 63 6f 6d 0d i.istock img.com·
00d0 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a ·User-Ag ent: Moz
00e0 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window
00f0 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b s NT 6.1 ; WOW64;
Flags (12 bits) (tcp.flags), 2 byte(s)
Packets: 3823 · Displayed: 3 (0.1%)
Profile: wireshark101