

Assignment 7

The image shows a computer screen with two windows. On the left is Wireshark, displaying a network traffic capture on the 'http.stream eq 15' interface. The packet list pane shows a series of TCP and HTTP packets. Packet 183 is highlighted, showing a SYN packet from source IP 18.254.30.9 to destination IP 23.222.5.89. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) layers. The packet bytes pane shows the raw hex and ASCII data.

On the right is a Microsoft Word document titled 'Document1 - Word'. The document content includes the name 'Nicholas Robertson' and the title 'Assignment 7'. Below this, there is a numbered list with one item: '1. The URL that I used was www.steampower.com and it's IP address is 23.222.5.89'. The document is displayed in a dark theme.

At the bottom of the screen, the Windows taskbar is visible, showing the system tray with the date and time '12:07 PM 11/9/2023'.

1.

```

GET /appinfo/1240440/sha/a5f93fd85485c99ef112f540fbac40007470ae0c.txt.gz HTTP/1.1
Host: clientconfig.akamai.steamstatic.com
Accept: text/html,*/*;q=0.9
accept-encoding: gzip,identity,*;q=0
accept-charset: ISO-8859-1,utf-8,*;q=0.7
user-agent: Valve/Steam HTTP Client 1.0

```

```

HTTP/1.1 200 OK
Content-Type: application/gzip
Content-Length: 38426
Last-Modified: Sat, 20 Jan 2018 01:00:00 GMT
Cache-Control: max-age=1209214
Date: Thu, 09 Nov 2023 16:55:07 GMT
Connection: keep-alive

```

```

.....[.%u. .+.)...fZfEr./.'....$. . hrz^.NeFe.*2"...
c4....%...%... ..&!.$ . ....B.+L !,..p...s. ....L...q....Z.
..k.y.....o|.%.K...K...y...=...?...x.h.`_...6...{:z...l.%.....I...pp
....wS ....m..R...W...{.....6.j.....zQ...j_n..W...f...X.....{...C)..._t..
...p...9{...+...=<.:?:{t...Wlz.n01.z...R^.....jb.....gz...G...8.....k.i
..?.....?:?...m...w...{W...F.....%Rr..^...s/.W_i...y.B.%xq36G..7.....3.
.."......^.....`st.....g.....~.....ON.n...~....._.....G'.O..G7.....5
.;?{.
_9.|...5.n.6.....t?N..7.....+.....'.....z...h.....z:..o.j.%;c.....;...
...h.8..IO~a~.....^x.7.....?.....W.....~.....n.Gg'.
..'.....?}|6....9...=;8>..^../\|.}a.....|.Omx<z.....O}.{a.....
...|jw~v...gz...>.....7_9...{.....v.....?.....7...{..y...'.=.....p.
..|.....?.....> d...<c.....d..cq}l...G.....y.]._..Ww/.N8=...D..@.R.s...|d...
..Wk...y...z.W..._=:>b.?Z.w.7.....c/=..}/=<x.9y...w.spz.E...gw..._.....f...?..W
0'.;g..U"/||].7..0.....~.....*..i.....K.w;>;>...?..Q..g.v.....w^=.
.w.....[.....hz.f]...1 ;s...w7.YE... ....8o?^.....==.d..
.^..S.9<
.87...+)...].F/=..0,...?. ...t.....2.8.. ...?....Gm_..N.qp...;...7*>z.....
.I..^..|.;...=.9.%g..._.....{...6W/..$.C...Kz..|.^.{.g'.x.r...wyx...}._|OAb
..g.....[#{V.[.t... S>}.m...G'Ov.K..._...O...X~.@.'E.....=.].a.k?.i.....C\
..w..~.}W.j.5..8.>..Eh.....G..~g..|.N.._9;8;?}.....[...R.Q.%V.Q..#.z.....?
M.....U">".?..d.?..mxB9~T.....=.....Q}.....Z.....z3>3...^.....a.....rv~|.
.w.;]!..j..{...M>.Z/.....
.y.c...Gw.s<..W~..W.....&..E..>...+or...6..`..+p..t..9..._...l.d...9....En...t.
J...9..._Y...{...r.Wk.^.....=...l.....9>.....#.sq]}?.....//.".....w...
.P...(.w ..0.B...).8....y.+..r...g.../...#_z..].7.....T.....<P.]V..C..
.P?p_o_z..7.....^.....|.....{.0<.{...^}=.x~.+Z.....8<8;}.G...
..k.b.7.....x..7~.5.....7.....G?v~.3.. ....\d.N.^...Ov...W...Xa
..j^..o{..."}|_..|sp.a[.0....._.....w./.....<..Ok..d.....g.....?z...0...
..>...<Q=V...xZ...U...t...:..6G.x.WC
Q. ....=?.#.?.>...~.R.8>..'..nN..<.H4..?<F./.....>CJ...wv|<k....
...
..p_.../...o...8...8...V<. .x..^.../_.../.....K$.#...l.%y...|.IBz....|
.x_..... ..%.J.p.....py...e..wV.....]...mN...].E:.....
W.+sD...2...j2).j.%..c)...C.6<.'>...x3...zcK...s.{.C...e.d.3..v.t...0.
8.<..D...&...>..zSk..~.S7N...l..Pb...L~...).]...C...u1u.....".....+..Py...^;..z..x.=
(...Z;..X....0
S~.....5.Tk.Wh...E.....i.....!gn_.R.....m{.b...;...#)A.o.^..Z.....].i..0
.....U..k4...R2.PC.....8.....v...&.....a...rK<u...y.U.....f...4....._u
...2.6...b?..
5g_kj...../5.S.&.....[.g.....3}.].1?..0..u+...M...O..rre...>..v.Sg.
.]q
..#.6..N.&u..N..k?%WZ.>.._l.>8...o..C0.{=...q..T.....i.#7u...9.....[.o.1B..

```

1 client pkt, 28 server pkts, 1 turn.

Entire conversation (38 kB) Show data as ASCII Stream 15

Find:

The URL that I used was www.steampower.com and it's IP address is 23.222.5.89

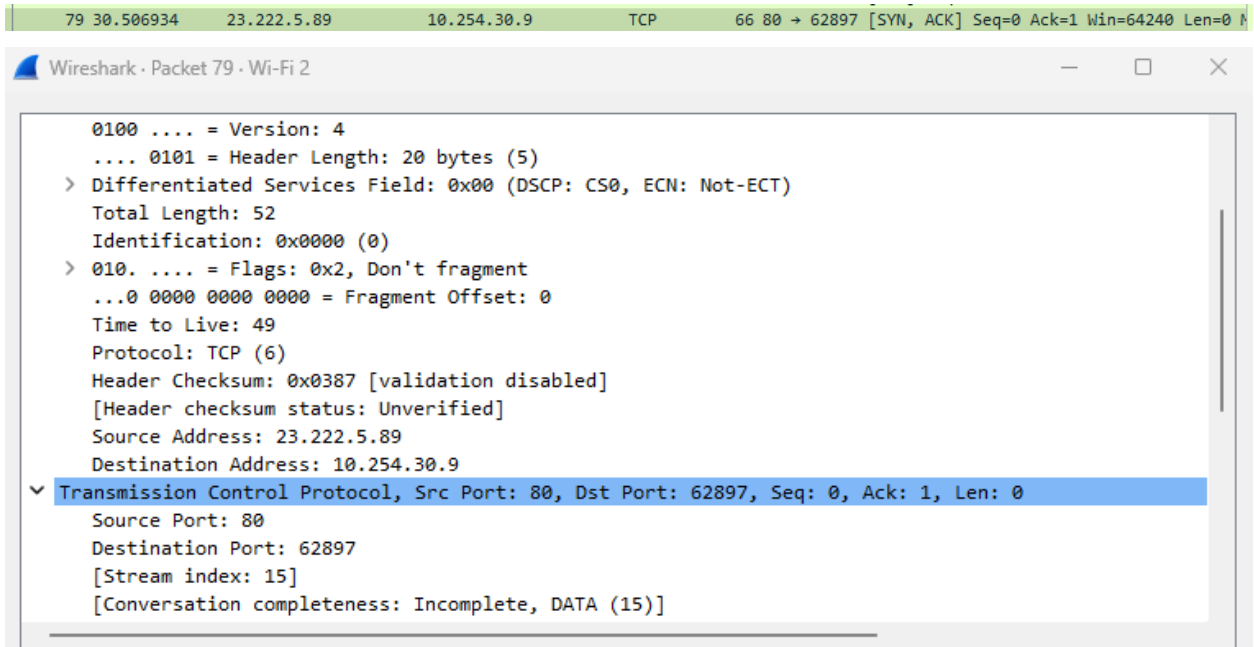
1b.

No.	Time	Source	Destination	Protocol	Length	Info
75	30.498949	10.254.30.9	23.222.5.89	TCP	66	62897 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=


```
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.254.30.9
Destination Address: 23.222.5.89
Transmission Control Protocol, Src Port: 62897, Dst Port: 80, Seq: 0, Len: 0
Source Port: 62897
Destination Port: 80
[Stream index: 15]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3424393636
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
```

The source IP address is 10.254.30.9 and the destination IP address is 23.222.5.89. The source Port is 62897, the destination port is 80, and the header checksum says 0x0000 [Validation disabled] [Header checksum status: Unverified].

1c.



The source IP address for the SYN/ACK packet is 23.222.5.89 and the destination IP address is 10.254.30.9. The source port number is 80 and the destination port number is 62897, and the header checksum is 0x0387 [validation disabled] [Header checksum status: Unverified].

1d.

The image shows a Wireshark packet capture window for a packet on the Wi-Fi 2 interface. The packet number is 80, with source IP 10.254.30.9 and destination IP 23.222.5.89. The protocol is TCP, and it is an acknowledgment (ACK) segment with sequence number 1, acknowledgment number 1, and window size 131584. The length of the segment is 0 bytes. The packet details pane shows the following information:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 40
- Identification: 0x3c07 (15367)
- Flags: 0x2, Don't fragment
- Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.254.30.9
- Destination Address: 23.222.5.89
- Transmission Control Protocol, Src Port: 62897, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
- Source Port: 62897
- Destination Port: 80
- [Stream index: 15]
- [Conversation completeness: Incomplete, DATA (15)]

The packet bytes pane shows the raw data of the packet:

```
0000 00 00 0c 07 ac 01 f8 9e 94 af 14 69 08 00 45 00 .....i..E.
0010 00 28 3c 07 40 00 80 06 00 00 0a fe 1e 09 17 de .(<@.....
0020 05 59 f5 b1 00 50 cc 1c 19 a5 3a c8 6b 4a 50 10 .Y...P...:kJP.
0030 02 02 46 58 00 00 ..FX..
```

At the bottom of the window, there is a checkbox labeled "Show packet bytes" which is checked. There are also "Close" and "Help" buttons.

The source IP address of the packet that acknowledges the SYN/ACK segment is 10.254.30.9 and the destination IP address is 23.222.5.89. The source port number is

62897 and the destination port number is 80, and the header checksum is 0x0000 [validation disabled] [Header checksum status: Unverified].

The image shows a Wireshark capture window titled "*Wi-Fi 2". The main pane displays a list of 24 network packets. The selected packet (No. 1) is a TCP segment from source 10.254.30.9 to destination 10.254.53.211, with source port 63330 and destination port 7680. The header checksum is 0x0000, and the status is "Unverified".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.254.30.9	10.254.53.211	TCP	66	63330 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.847621	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
3	0.973030	162.254.192.74	10.254.30.9	UDP	190	27018 → 65040 Len=148
4	1.034247	10.254.30.9	162.254.192.74	UDP	238	65040 → 27018 Len=196
5	1.173224	162.254.192.74	10.254.30.9	UDP	190	27018 → 65040 Len=148
6	1.220834	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
7	1.344703	10.254.30.9	172.253.63.132	TCP	55	63309 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP se
8	1.353110	172.253.63.132	10.254.30.9	TCP	66	443 → 63309 [ACK] Seq=1 Ack=2 Win=271 Len=0 SLE=1 S
9	1.371977	162.254.192.74	10.254.30.9	UDP	206	27018 → 65040 Len=164
10	1.468411	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
11	1.624089	162.254.192.74	10.254.30.9	UDP	206	27018 → 65040 Len=164
12	1.717483	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
13	1.877931	162.254.192.74	10.254.30.9	UDP	206	27018 → 65040 Len=164
14	1.969978	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
15	2.072340	162.254.192.74	10.254.30.9	UDP	174	27018 → 65040 Len=132
16	2.122885	162.254.192.74	10.254.30.9	UDP	206	27018 → 65040 Len=164
17	2.161643	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
18	2.171423	162.254.192.74	10.254.30.9	UDP	174	27018 → 65040 Len=132
19	2.273180	162.254.192.74	10.254.30.9	UDP	190	27018 → 65040 Len=148
20	2.286759	10.254.30.9	162.254.192.74	UDP	1242	65040 → 27018 Len=1200
21	2.286901	10.254.30.9	162.254.192.74	UDP	850	65040 → 27018 Len=808
22	2.422699	162.254.192.74	10.254.30.9	UDP	254	27018 → 65040 Len=212
23	2.537088	10.254.30.9	162.254.192.74	UDP	190	65040 → 27018 Len=148
24	2.672337	162.254.192.74	10.254.30.9	UDP	206	27018 → 65040 Len=164

The detailed view of the selected packet (Frame 1) shows the following structure:

- Ethernet II, Src: IntelCor_af:14:69 (f8:9e:94:af:14:69), Dst: IntelCor_dd:ea:78 (c4:23:60:dd:ea:78)
- Internet Protocol Version 4, Src: 10.254.30.9, Dst: 10.254.53.211
 - Version: 4
 - Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC)
 - Total Length: 52
 - Identification: 0xd815 (55317)
 - Flags: 0x2, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 128
 - Protocol: TCP (6)
 - Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified]
 - Source Address: 10.254.30.9
 - Destination Address: 10.254.53.211
- Transmission Control Protocol, Src Port: 63330, Dst Port: 7680
 - Source Port: 63330
 - Destination Port: 7680
 - [Stream index: 0]
 - [Conversation completeness: Incomplete, SYN_SENT (1)]
 - [TCP Segment Len: 0]

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

2.

