

Kirollous Ramzy Assad
Lab 8

Question 1

nat-inside-wireshark-trace1-1 (2).pcapng

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

> Frame 4: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth1, id 0
> Ethernet II, Src: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c), Dst: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7)
v Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 382
 Identification: 0x6296 (25238)
 > 010. = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: TCP (6)
 Header Checksum: 0x64dc [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.10.11
 Destination Address: 138.76.29.8
 [Stream index: 0]
 > Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
 > Hypertext Transfer Protocol

0000 08 00 27 82 36 d7 08 00 27 89 c7 7c 08 00 45 00 ...6... ..E
0010 01 7e 62 96 40 00 40 06 64 dc 08 08 00 8a 4c ...b@-@- d...L
0020 1d 00 d2 a4 00 50 a2 b5 4a 2b 99 71 bd 0e 00 18 ...P...J+q...
0030 01 f6 1b ea 00 00 01 01 08 0a 13 3c 6d 6d 2f d1<mm/.
0040 9f 2e 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ...GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 31 33 38 2e 37 36 2e 32 ...Host: 138.76.2
0060 39 2e 38 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 9.8 Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0080 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 1; Ubuntu u; Linux
0090 20 78 38 36 5f 36 34 3b 20 72 76 3a 37 35 2e 30 x86_64; rv:75.0
00a0 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31) Gecko/ 20100101
00b0 20 46 69 72 65 66 6f 78 2f 37 35 2e 30 0d 0a 41 Firefox /75.0-A
00c0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html
00d0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht
00e0 6d 6c 2b 78 6d 6c 2c 61 70 78 6c 69 63 61 74 69 ml+xml,a pplicati
00f0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima
0100 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e ge/webp, */q=0.
0110 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 8-Accep t-Langua
0120 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 ge: en-U S,en;q=0
0130 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 .5-Accep t-Encod
0140 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 ing: gzi p, defla
0150 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 te-Conn ection:
0160 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 keep-ali ve- Upgr
0170 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Inse cure-Reqr
0180 75 65 73 74 73 3a 20 31 0d 0a 0d 0a uests: 1

Source Address: 192.168.10.11

Destination Address: 138.76.29.8

http						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

> Frame 4: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth1, id 0		0000	08 00 27 82 36 d7 08 00	27 89 c7 7c 08 00 45 00	--'6... '... ...E-
> Ethernet II, Src: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c), Dst: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7)		0010	01 7e 62 96 40 00 40 06	64 dc c0 a8 0a 0b 8a 4c	--b:@: d:-----L
> Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8		0020	1d 08 d2 a4 00 50 a2 b5	4a 2b 99 71 bd 0e 80 18P..J+:q....
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330		0030	01 76 1b ea 00 00 01 01	08 0a 13 3c 6d 6d 2f d1<img/
Source Port: 53924		0040	9f 2e 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1
Destination Port: 80		0050	0d 0a 48 6f 73 74 3a 20	31 33 38 2e 37 36 2e 32	--Host: 138.76.2
[Stream index: 0]		0060	39 2e 38 0d 0a 55 73 65	72 2d 41 67 65 6e 74 3a	9.8-Use r-Agent:
[Stream Packet Number: 4]		0070	20 4d 6f 7a 69 6c 6c 61	2f 35 2e 30 20 28 58 31	Mozilla /5.0 (X1
> [Conversation completeness: Complete, WITH_DATA (31)]		0080	31 3b 20 55 62 75 6e 74	75 3b 20 4c 69 6e 75 78	1; Ubuntu; Linux
[TCP Segment Len: 330]		0090	20 78 38 36 5f 36 34 3b	20 72 76 3a 37 35 2e 30	x86_64; rv:75.0
Sequence Number: 1 (relative sequence number)		00a0	29 20 47 65 63 6b 6f 2f	32 30 31 30 30 31 30 31) Gecko/ 20100101
Sequence Number (raw): 2729789995		00b0	20 46 69 72 65 66 6f 78	2f 37 35 2e 30 0d 0a 41	Firefox /75.0..A
[Next Sequence Number: 331 (relative sequence number)]		00c0	63 63 65 70 74 3a 20 74	65 78 74 2f 68 74 6d 6c	cept: t ext/html
Acknowledgment Number: 1 (relative ack number)		00d0	2c 61 70 70 6c 69 63 61	74 69 6f 6e 2f 78 68 74	, applica tion/xht
Acknowledgment number (raw): 2574368014		00e0	6d 6c 2b 78 6d 6c 2c 61	70 70 6c 69 63 61 74 69	ml+xml;q a pplicati
1000 = Header Length: 32 bytes (8)		00f0	6f 6e 2f 78 6d 6c 3b 71	3d 30 2e 39 2c 69 6d 61	on/xml;q =0.9, ima
Flags: 0x018 (PSH, ACK)		0100	67 65 2f 77 65 62 70 2c	2a 2f 2a 3b 71 3d 30 2e	ge/webb, +/;iq=0.
Window: 502		0110	30 0d 0a 41 63 63 65 70	74 2d 4c 61 6e 67 75 61	8 Accep t-Langua
[Calculated window size: 64256]		0120	67 65 3a 20 65 6e 2d 55	53 2c 65 6e 3b 71 3d 30	ge: en-U S,en;q=0
[Window size scaling factor: 128]		0130	2e 35 0d 0a 41 63 63 65	70 74 2d 45 6e 63 6f 64	.5..Acce pt-Encod
Checksum: 0x1bea [unverified]		0140	69 6e 67 3a 20 67 7a 69	70 2c 20 64 65 66 6c 61	ing: gzi p, defla
[Checksum Status: Unverified]		0150	74 65 0d 0a 43 6f 6e 6e	65 63 74 69 6f 6e 3a 20	te Connec tion:
		0160	6b 65 65 70 2d 61 6c 69	76 65 0d 0a 55 70 67 72	keep-ali ve Upgr
		0170	61 64 65 2d 49 6e 73 65	63 75 72 65 2d 52 65 71	ade-Inse cure-Req
		0180	75 65 73 74 73 3a 20 31	0d 0a 0d 0a	uests: 1

Source Port: 53924
Destination Port: 80

Question 2

Time = 0.27362245

QUESTION 3

http						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

> Frame 6: Packet, 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, id 0		0010	02 57 6c 7c 40 00 3e 06	5c 1d 8a 4c 1d 08 c0 a8	-Wl@-> \.L.4..
> Ethernet II, Src: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7), Dst: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c)		0020	0a 0b 00 50 d2 a4 99 71	bd 0e a2 b5 4b 75 80 18	--P...q ...Ku..
> Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11		0030	01 fb 2c 58 00 00 01 01	08 0a 2f d1 9f 4b 13 3c	...X...../...K<
0100 = Version: 4		0040	6d 6d 48 54 54 50 2f 31	2e 31 20 32 30 30 20 4f	mmHTTP/1 .1 200 0
.... 0101 = Header Length: 20 bytes (5)		0050	4b 0d 0a 44 61 74 65 3a	20 4d 6f 6e 2c 20 32 39	K..Date: Mon, 29
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		0060	20 4d 61 72 20 32 30 32	31 20 30 33 3a 35 30 3a	Mar 202 1 03:50:
Total Length: 599		0070	32 37 20 47 4d 54 0d 0a	53 65 72 76 65 72 3a 20	27 GMT.. Server:
Identification: 0x6c7c (27772)		0080	41 70 61 63 68 65 2f 32	2e 34 2e 34 31 20 28 55	Apache/2 .4.41 (U
> 010. = Flags: 0x2, Don't fragment		0090	62 75 6e 74 75 29 0d 0a	4c 61 73 74 2d 4d 6f 64	buntu).. Last-Mod
...0 0000 0000 0000 = Fragment Offset: 0		00a0	69 66 69 65 64 3a 20 54	75 65 2c 20 31 32 20 4a	ified: T ue, 12 J
Time to Live: 62		00b0	61 6e 20 32 30 32 31 20	31 38 3a 35 35 3a 30 34	an 2021 18:55:04
Protocol: TCP (6)		00c0	20 47 4d 54 0d 0a 45 54	61 67 3a 20 22 31 33 37	GMT..ET ag: "137
Header Checksum: 0x5c1d [validation disabled]		00d0	2d 35 62 38 62 38 38 66	38 34 35 32 61 61 2d 67	-5b8b88f 8452aa-q
[Header checksum status: Unverified]		00e0	7a 69 70 22 0d 0a 41 63	63 65 70 74 2d 52 61 6e	zip"..Ac cept-Ran
Source Address: 138.76.29.8		00f0	67 65 73 3a 20 62 79 74	65 73 0d 0a 56 61 72 79	ges: byt es..Vary
Destination Address: 192.168.10.11		0100	3a 20 41 63 63 65 70 74	2d 45 6e 63 6f 64 69 6e	: Acce pt-Encodin
[Stream index: 0]		0110	67 0d 0a 43 6f 6e 74 65	6e 74 2d 45 6e 63 6f 64	g..Conte nt-Encod
> Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547		0120	69 6e 67 3a 20 67 7a 69	70 0d 0a 43 6f 6e 74 65	ing: gzi p..Conte
> Hypertext Transfer Protocol		0130	6e 74 2d 4c 65 6e 67 74	68 3a 20 32 31 30 0d 0a	nt-Lengt h: 210..
> Line-based text data: text/html (12 lines)		0140	4b 65 65 70 2d 41 6c 69	76 65 3a 20 74 69 6d 65	Keep-Alt ves: time
		0150	6f 75 74 3d 35 2c 20 6d	61 78 3d 31 30 30 0d 0a	out=5, m ax=100..
		0160	43 6f 6e 6e 65 63 74 69	6f 6e 3a 20 4b 65 65 70	Connecti on: Keep
		0170	2d 41 6c 69 76 65 0d 0a	43 6f 6e 74 65 6e 74 2d	-Alive..Conten t-
		0180	54 79 70 65 3a 20 74 65	78 74 2f 68 74 6d 6c 0d	Type: te xt/html..
		0190	0a 0d 0a 1f 8b 08 00 00	00 00 00 00 03 5d 50 d1JP..
		01a0	8a 02 31 0c 7c 76 bf 22	fe c0 89 af 47 29 08 22	--1{v"G)"

Source Address: 138.76.29.8
Destination Address: 192.168.10.11

http						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

Frame 0: Packet, 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, in 0		0010	02 57 6c 7c 40 00 3e 06	5c 1d 8a 4c 1d 08 c0 a8	Wl@> \..L..
> Ethernet II, Src: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7), Dst: PCSSystemtec_B9:c7:7c (08:00:27:89:c7:7c)		0020	0a 0b 00 50 d2 a4 99 71	bd 0e a2 b5 4b 75 80 18	..P...q...Ku..
> Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11		0030	01 fb 2c 58 00 00 01 01	08 0a 2f d1 9f 4b 13 3c	..X....../..K<
Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547		0040	6d 6d 48 54 50 2f 31	2e 31 20 32 30 30 20 4f	mHTTP/1.1 200 O
Source Port: 80		0050	4b 0d 0a 44 61 74 65 3a	20 4d 6f 6e 2c 20 32 39	K -Date: Mon, 29
Destination Port: 53924		0060	20 4d 61 72 20 32 30 32	31 20 30 33 3a 35 30 3a	Mar 202 1 03:50:
[Stream index: 0]		0070	32 37 20 47 4d 54 0d 0a	53 65 72 76 65 72 3a 20	27 GMT.. Server:
[Stream Packet Number: 6]		0080	41 70 61 63 68 65 2f 32	2e 34 2e 34 31 20 28 55	Apache/2.4.41 (U
> [Conversation completeness: Complete, WITH_DATA (31)]		0090	62 75 6e 74 75 29 0d 0a	4c 61 73 74 2d 4d 6f 64	buntu).. Last-Mod
[TCP Segment Len: 547]		00a0	69 66 69 65 64 3a 20 54	75 65 2c 20 31 32 20 4a	ified: Tue, 12 J
Sequence Number: 1 (relative sequence number)		00b0	61 6e 20 32 30 32 31 20	31 38 3a 35 35 3a 30 34	an 2021 18:55:04
Sequence Number (raw): 2574368014		00c0	20 47 4d 54 0d 0a 45 54	61 67 3a 20 22 31 33 37	GMT..ET ag: "137
[Next Sequence Number: 548 (relative sequence number)]		00d0	2d 35 62 38 62 38 38 66	38 34 35 32 61 61 2d 67	-Sub808f 8452aa-q
Acknowledgment Number: 331 (relative ack number)		00e0	7a 69 70 22 0d 0a 41 63	63 65 70 74 2d 52 61 6e	zip"..Ac cept-Rah
Acknowledgment Number (raw): 2729790325		00f0	67 65 73 3a 20 62 79 74	65 73 0d 0a 56 61 72 79	ges: byt es..Vary
1000 = Header Length: 32 bytes (8)		0100	3a 20 41 63 63 65 70 74	2d 45 6e 63 6f 64 69 6e	: Accept -Encodin
Flags: 0x018 (PSH, ACK)		0110	67 0d 0a 43 6f 6e 74 65	6e 74 2d 45 6e 63 6f 64	g..Conte nt-Encod
Window: 507		0120	69 6e 67 3a 20 67 7a 69	70 0d 0a 43 6f 6e 74 65	ing: gz1 p..Conte
[Calculated window size: 64896]		0130	6e 74 2d 4c 65 6e 67 74	68 3a 20 32 31 30 0d 0a	nt-Length h: 210..
Window size scaling factor: 128		0140	4b 65 65 70 2d 41 6c 69	76 65 3a 20 74 69 6d 65	Keep-Ali ve: time
Checksum: 0x2c58 (unverified)		0150	6f 75 74 3d 35 2c 20 6d	61 78 3d 31 30 30 0d 0a	out=5, m ax=100..
[Checksum Status: Unverified]		0160	43 6f 6e 6e 65 63 74 69	6f 6e 3a 20 4b 65 65 70	Connecti on: Keep
		0170	2d 41 6c 69 76 65 0d 0a	43 6f 6e 74 65 6e 74 2d	-Alive.. Content-
		0180	54 79 70 65 3a 20 74 65	78 74 2f 68 74 6d 6c 0d	Type: te xt/html-
		0190	0a 0d 0a 1f 8b 08 00 00	00 00 00 00 03 5d 50 d1[P.
		01a0	8a 02 31 0c 7c 76 bf 22	fe c0 89 af 47 29 08 22	..1lv."G)"

Source Port: 80

Destination Port: 53924

Part B

Question 4

Time =0.027356291

Question 5

The image shows a Wireshark packet capture analysis of an HTTP GET request. The packet list at the top shows four packets, with packet 4 selected. The packet details pane on the left shows the structure of the selected packet, and the packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

Frame 4: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface 0

- Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: 138.76.29.8 (08:00:27:43:65:cd)
- Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
 - Total Length: 382
 - Identification: 0x6296 (25238)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 63
 - Protocol: TCP (6)
 - Header Checksum: 0x2492 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 10.0.1.254
 - Destination Address: 138.76.29.8
 - [Stream index: 0]
- Transmission Control Protocol, Src Port: 53924, Dst Port: 80
 - Window Size: 65535
 - Sequence Number: 100000000
 - Initial Sequence Number: 100000000
 - Window Scale: 0
 - Checksum: 0x2492 [validation disabled]
 - [Checksum status: Unverified]
 - Urgent Pointer: 0
 - Options: (len=0) [No Options]
- Hypertext Transfer Protocol

Source Address (ip.src), 4 bytes

Packets: 19 · Displayed: 4 (21.1%)

Profile: Default

Source Address: 10.0.1.254

Destination Address: 138.76.29.8

nat-outside-wireshark-trace1-1.pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

> Frame 4: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface 0
> Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: 10.0.1.254 (08:00:27:43:65:cd)
> Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
> Transmission Control Protocol, Src Port: 53924, Dst Port: 80

Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 4]
> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 330]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2729789995
[Next Sequence Number: 331 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2574368014
1000 = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
Window: 502
[Calculated window size: 64256]

0020 1d 08 d2 a4 00 50 a2 b5 4a 2b 99 71 bd 0e 80 18 ...
0030 01 f6 da 9f 00 00 01 01 08 0a 13 3c 6d 6d 2f d1 ...
0040 9f 2e 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ...G
0050 0d 0a 48 6f 73 74 3a 20 31 33 38 2e 37 36 2e 32 ...H
0060 39 2e 38 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 9.8
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mo
0080 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 1;
0090 20 78 38 36 5f 36 34 3b 20 72 76 3a 37 35 2e 30 x8
00a0 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31) G
00b0 20 46 69 72 65 66 6f 78 2f 37 35 2e 30 0d 0a 41 Fi
00c0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c cce
00d0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,ap
00e0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+
00f0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/
0100 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e ge/
0110 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 8..
0120 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 ge:
0130 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 .5.
0140 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 ing
0150 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 te.
0160 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 kee
0170 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade

Source Port (tcp.srcport), 2 bytes Packets: 19 · Displayed: 4 (21.1%) Profile: Default

Source Port: 53924
Destination Port: 80

Question 6

- Source IP changed
- Source port did NOT change
- Destination IP unchanged
- Destination port unchanged

Question 7

NAT does **not** modify HTTP payload data.

Question 8

- IP Header Checksum
- TTL may also change (decremented by router)

Question 9

Time = 0.03625966

Question 10

nat-outside-wireshark-trace1-1.pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

> Frame 6: Packet, 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface 0
> Ethernet II, Src: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74), Dst: 10.0.1.254 (08:00:27:22:fd:74)
v Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
 Total Length: 599
 Identification: 0x6c7c (27772)
 > 010. = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 63
 Protocol: TCP (6)
 Header Checksum: 0x19d3 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 138.76.29.8
 Destination Address: 10.0.1.254
 [Stream index: 0]
v Transmission Control Protocol, Src Port: 80, Dst Port: 5353
 Source Port: 80

Packet (613 bytes) Uncompressed entity body (311 bytes)

Source Address (ip.src), 4 bytes Packets: 19 · Displayed: 4 (21.1%) Profile: Default

Source Address: 138.76.29.8

Destination Address: 10.0.1.254

nat-outside-wireshark-trace1-1.pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

Frame 6: Packet, 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface 0
 Ethernet II, Src: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74), Dst: 10.0.1.254 (08:00:00:00:00:00)
 Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254
 Transmission Control Protocol, Src Port: 80, Dst Port: 53924
 Source Port: 80
 Destination Port: 53924
 [Stream index: 0]
 [Stream Packet Number: 6]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 547]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 2574368014
 [Next Sequence Number: 548 (relative sequence number)]
 Acknowledgment Number: 331 (relative ack number)
 Acknowledgment number (raw): 2729790325
 1000 = Header Length: 32 bytes (8)
 Flags: 0x018 (PSH, ACK)
 Window: 507
 [Calculated window size: 64896]
 Destination Address (ip.dst), 4 bytes

0010 02 57 6c 7c 40 00 3f 06 19 d3 8a 4c 1d 08 0a 00
 0020 01 fe 00 50 d2 a4 99 71 bd 0e a2 b5 4b 75 80 18
 0030 01 fb eb 0d 00 00 01 01 08 0a 2f d1 9f 4b 13 3c
 0040 6d 6d 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f
 0050 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 39
 0060 20 4d 61 72 20 32 30 32 31 20 30 33 3a 35 30 3a
 0070 32 37 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20
 0080 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55
 0090 62 75 6e 74 75 29 0d 0a 4c 61 73 74 2d 4d 6f 64
 00a0 69 66 69 65 64 3a 20 54 75 65 2c 20 31 32 20 4a
 00b0 61 6e 20 32 30 32 31 20 31 38 3a 35 35 3a 30 34
 00c0 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 33 37
 00d0 2d 35 62 38 62 38 38 66 38 34 35 32 61 61 2d 67
 00e0 7a 69 70 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e
 00f0 67 65 73 3a 20 62 79 74 65 73 0d 0a 56 61 72 79
 0100 3a 20 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e
 0110 67 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e 63 6f 64
 0120 69 6e 67 3a 20 67 7a 69 70 0d 0a 43 6f 6e 74 65
 0130 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 31 30 0d 0a
 0140 4b 65 65 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65

Packet (613 bytes) Uncompressed entity body (311 bytes)

Packets: 19 · Displayed: 4 (21.1%) Profile: Default

Source Port: 80

Destination Port: 53924

Part C

Question 11

Source IP = 138.76.29.8

Destination IP = 192.168.10.11

Source Port = 80

Destination Port = 53924