

Wireshark Lab #3: IP

Suyi Liu, Yuan Jing Vincent Yan

April 8, 2017

Problem 1

42	2017-04-08 15:35:57.889921	192.168.0.105	98.139.183.24	UDP	70	35913 → 3
43	2017-04-08 15:35:57.891031	192.168.0.1	192.168.0.105	ICMP	98	Time-to-l
44	2017-04-08 15:35:57.891723	2601:14d:4000:3c56...	2001:558:feed::1	DNS	104	Standard
45	2017-04-08 15:35:57.897691	2001:558:feed::1	2601:14d:4000:3c56...	DNS	104	Standard
▶ Frame 42: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0						
▶ Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)						
▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24						

As shown, the private IP address is 192.168.0.105. (By the way, the public IP address is 66.249.76.29)

Problem 2

- ▶ Flags: 0x00
- Fragment offset: 0
- ▶ Time to live: 1
- Protocol: UDP (17)
- Header checksum: 0x52b6 [validation disabled]
- [Header checksum status: Unverified]

The value in the upper layer protocol field is 17 (UDP).

Problem 3

- 0101 = Header Length: 20 bytes (5)
- ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56

20 bytes are in the IP header. 36 bytes are in the payload of the IP datagram. Since the total length of the packet is 56 bytes, the payload is $56 - 20 = 36$ bytes.

Problem 4

▶ Flags: 0x00	
Fragment offset: 0	
▶ Time to live: 1	
Protocol: UDP (17)	
Header checksum: 0x52b6 [validation disabled]	
[Header checksum status: Unverified]	
0000	50 c7 bf 29 91 f0 80 e6 50 1e 24 f2 08 00 45 00 P.).... P.\$...E.
0010	00 38 8c 4a 00 00 01 11 52 b6 c0 a8 00 69 62 8b .8.J.... R....ib.

This IP datagram has not been fragmented, because by examining the packet we see that the fragmentation offset is 0 and the flag bit set to 0, indicating that this is the one and only fragment.

Problem 5

50	2017-04-08	15:35:57.910505	192.168.0.105	98.139.183.24
48	2017-04-08	15:35:57.908991	192.168.0.105	98.139.183.24
46	2017-04-08	15:35:57.908118	192.168.0.105	98.139.183.24
42	2017-04-08	15:35:57.889921	192.168.0.105	98.139.183.24
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x8c4a (35914) Flags: 0x00 Fragment offset: 0 ▶ Time to live: 1 Protocol: UDP (17) Header checksum: 0x52b6 [validation disabled] [Header checksum status: Unverified] Source: 192.168.0.105 Destination: 98.139.183.24 [Source GeoIP: Unknown]				

50	2017-04-08	15:35:57.910505	192.168.0.105	98.139.183.24	UDP
48	2017-04-08	15:35:57.908991	192.168.0.105	98.139.183.24	UDP
46	2017-04-08	15:35:57.908118	192.168.0.105	98.139.183.24	UDP
42	2017-04-08	15:35:57.889921	192.168.0.105	98.139.183.24	UDP
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x8c4d (35917) Flags: 0x00 Fragment offset: 0 ▶ Time to live: 2 Protocol: UDP (17) Header checksum: 0x51b3 [validation disabled] [Header checksum status: Unverified] Source: 192.168.0.105 Destination: 98.139.183.24					

As shown, identification and header checksum always change from one datagram to the next. The time-to-live field actually changes every three datagrams, due to the way *traceroute* works.

Problem 6

64	2017-04-08	15:35:58.034888	192.168.0.105	98.139.183.24	UDP	70	35913 → 33443	Len=
62	2017-04-08	15:35:58.024278	192.168.0.105	98.139.183.24	UDP	70	35913 → 33442	Len=
58	2017-04-08	15:35:57.988018	192.168.0.105	98.139.183.24	UDP	70	35913 → 33441	Len=
56	2017-04-08	15:35:57.977529	192.168.0.105	98.139.183.24	UDP	70	35913 → 33440	Len=
54	2017-04-08	15:35:57.968052	192.168.0.105	98.139.183.24	UDP	70	35913 → 33439	Len=

▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0x8c50 (35920)

► Flags: 0x00

Fragment offset: 0

► Time to live: 3

Protocol: UDP (17)

Header checksum: 0x50b0 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.105

Destination: 98.139.183.24

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

70	2017-04-08	15:35:58.095351	192.168.0.105	98.139.183.24	UDP			
66	2017-04-08	15:35:58.052553	192.168.0.105	98.139.183.24	UDP			
64	2017-04-08	15:35:58.034888	192.168.0.105	98.139.183.24	UDP			
62	2017-04-08	15:35:58.024278	192.168.0.105	98.139.183.24	UDP			
58	2017-04-08	15:35:57.988018	192.168.0.105	98.139.183.24	UDP			
56	2017-04-08	15:35:57.977529	192.168.0.105	98.139.183.24	UDP			

▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0x8c53 (35923)

► Flags: 0x00

Fragment offset: 0

► Time to live: 4

Protocol: UDP (17)

Header checksum: 0x4fad [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.105

Destination: 98.139.183.24

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

As shown, Fields that stay constant:

Version(IPv4 as always), Header Length(20 bytes), Differentiated Services Field(always same type of service), Potocol(all of them are UDP packets), Source IP(sending from same IP address), Destination IP(sending to same IP address)

Fields must stay constant:

Version(IPv4 as always), Header Length(20 bytes), Differentiated Services Field(always same type of service), Potocol(all of them are UDP packets), Source IP(sending from same IP address), Destination IP(sending to same IP address)

Fields must change:

Identification(Different packet have different IDs), Time to live(Traceroute pro-

gram increments TTL), Header checksum(since headers must change)

Problem 7

76	2017-04-08	15:35:58.145578	192.168.0.105	98.139.183.24	UDP
74	2017-04-08	15:35:58.132730	192.168.0.105	98.139.183.24	UDP
70	2017-04-08	15:35:58.095351	192.168.0.105	98.139.183.24	UDP
66	2017-04-08	15:35:58.052553	192.168.0.105	98.139.183.24	UDP
64	2017-04-08	15:35:58.034888	192.168.0.105	98.139.183.24	UDP
▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24					
0100 = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 56					
Identification: 0x8c54 (35924)					
-- -- --					

76	2017-04-08	15:35:58.145578	192.168.0.105	98.139.183.24	UDP
74	2017-04-08	15:35:58.132730	192.168.0.105	98.139.183.24	UDP
70	2017-04-08	15:35:58.095351	192.168.0.105	98.139.183.24	UDP
66	2017-04-08	15:35:58.052553	192.168.0.105	98.139.183.24	UDP
64	2017-04-08	15:35:58.034888	192.168.0.105	98.139.183.24	UDP
▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24					
0100 = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 56					
Identification: 0x8c55 (35925)					

76	2017-04-08	15:35:58.145578	192.168.0.105	98.139.183.24	UDP
74	2017-04-08	15:35:58.132730	192.168.0.105	98.139.183.24	UDP
70	2017-04-08	15:35:58.095351	192.168.0.105	98.139.183.24	UDP
66	2017-04-08	15:35:58.052553	192.168.0.105	98.139.183.24	UDP
64	2017-04-08	15:35:58.034888	192.168.0.105	98.139.183.24	UDP
▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24					
0100 = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 56					
Identification: 0x8c56 (35926)					

The pattern: the values in the Identification field of the IP datagram increases over time.

Problem 8

32	2017-04-08	15:35:51.791018	192.168.0.1	192.168.0.105	ICMP	74	Destination unreachable (Port unreachable)
34	2017-04-08	15:35:52.293519	192.168.0.1	192.168.0.105	ICMP	74	Destination unreachable (Port unreachable)
43	2017-04-08	15:35:57.891031	192.168.0.1	192.168.0.105	ICMP	98	Time-to-live exceeded (Time to live exceeded)
47	2017-04-08	15:35:57.908915	192.168.0.1	192.168.0.105	ICMP	98	Time-to-live exceeded (Time to live exceeded)
49	2017-04-08	15:35:57.910405	192.168.0.1	192.168.0.105	ICMP	98	Time-to-live exceeded (Time to live exceeded)
121	2017-04-08	15:36:02.802303	192.168.0.1	192.168.0.105	ICMP	74	Destination unreachable (Port unreachable)

▶ Source: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
 Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)

▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x9031 (36913)

▶ Flags: 0x00
 Fragment offset: 0
 Time to live: 64
 Protocol: ICMP (1)

For the first ICMP TTL-exceeded reply,
 Identification field: 36913; TTL field: 64

Problem 9

The Identification field changes for the ICMP TTL-exceeded replies because the identification field must be unique, unless they are fragments of a single large IP datagram.

The TTL field remains unchanged since TTL field by the first hop router are always set the same.

Problem 10

[Question: Find the first ICMP Echo...]

332	2017-04-08	15:36:38.376612	192.168.0.105	52.73.131.128	TCP	54	57446 → 4
337	2017-04-08	15:36:45.296792	192.168.0.105	98.139.183.24	IPv4	1514	Fragmented
• 338	2017-04-08	15:36:45.296793	192.168.0.105	98.139.183.24	UDP	534	35928 → 3
340	2017-04-08	15:36:45.302877	192.168.0.105	98.139.183.24	IPv4	1514	Fragmented
341	2017-04-08	15:36:45.302878	192.168.0.105	98.139.183.24	UDP	534	35928 → 3
343	2017-04-08	15:36:45.305085	192.168.0.105	98.139.183.24	IPv4	1514	Fragmented
344	2017-04-08	15:36:45.305086	192.168.0.105	98.139.183.24	UDP	534	35928 → 3

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)

▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1500
 Identification: 0x8c59 (35929)

▶ Flags: 0x01 (More Fragments)
 Fragment offset: 0

Yes, this message has been fragmented, since its flag bit is set to 1.

Problem 11

[Question: Print out the first fragment...]

```
337 2017-04-08 15:36:45.296792 192.168.0.105 98.139.183.24 IPv4 1514
Fragmented IP protocol (proto=UDP 17, off=0, ID=8c59) [Reassembled in #338]
Frame 337: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 8, 2017 15:36:45.296792000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1491680205.296792000 seconds
[Time delta from previous captured frame: 0.000917000 seconds]
[Time delta from previous displayed frame: 0.000917000 seconds]
[Time since reference or first frame: 62.180074000 seconds]
Frame Number: 337
Frame Length: 1514 bytes (12112 bits)
Capture Length: 1514 bytes (12112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:data]
[Coloring Rule Name: TTL low or unexpected]
[Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst ==
224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))]
Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x8c59 (35929)
Flags: 0x01 (More Fragments)
Fragment offset: 0
Time to live: 1
Protocol: UDP (17)
Header checksum: 0x2d03 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.105
Destination: 98.139.183.24
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Reassembled IPv4 in frame: 338
Data (1480 bytes)
```

In the IP header, a flag bit of 1 indicates that the datagram been fragmented. A fragmentation offset of 0 indicates that this is the first fragment. This IP datagram is 1500 bytes long, including the header.

Problem 10

[Question: Print out the second fragment...]

```
338 2017-04-08 15:36:45.296793 192.168.0.105 98.139.183.24 UDP 534
35928 → 33435 Len=1972
Frame 338: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 8, 2017 15:36:45.296793000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1491680205.296793000 seconds
[Time delta from previous captured frame: 0.000001000 seconds]
[Time delta from previous displayed frame: 0.000001000 seconds]
[Time since reference or first frame: 62.180075000 seconds]
Frame Number: 338
Frame Length: 534 bytes (4272 bits)
Capture Length: 534 bytes (4272 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: TTL low or unexpected]
[Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst ==
224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))]
Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 520
Identification: 0x8c59 (35929)
Flags: 0x00
Fragment offset: 1480
Time to live: 1
Protocol: UDP (17)
Header checksum: 0x501e [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.105
Destination: 98.139.183.24
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[2 IPv4 Fragments (1980 bytes): #337(1480), #338(500)]
User Datagram Protocol, Src Port: 35928, Dst Port: 33435
Data (1972 bytes)
```

In the IP header, fragmentation offset of 1480 indicates that this is not the first datagram fragment. There are no more fragments, since the flag bit is set to 0 here.

Problem 11

[Question: What fields change in the IP header...]

As shown in the previous print outs, total length, offset, flags, and header checksum fields change in the IP header between the first and second fragment.

Problem 12

919	2017-04-08	15:38:08.995686	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
920	2017-04-08	15:38:08.995687	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
921	2017-04-08	15:38:08.995687	192.168.0.105	98.139.180.149	UDP	554	35946 → 33435 Len=3472
925	2017-04-08	15:38:09.013495	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
926	2017-04-08	15:38:09.013496	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
927	2017-04-08	15:38:09.013496	192.168.0.105	98.139.180.149	UDP	554	35946 → 33436 Len=3472

▼ Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)

► Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)

► Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.180.149

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0x8c6b (35947)

► Flags: 0x01 (More Fragments)

Fragment offset: 0

► Time to live: 1

Protocol: UDP (17)

Header checksum: 0x2f74 [validation disabled]

919	2017-04-08	15:38:08.995686	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
920	2017-04-08	15:38:08.995687	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
921	2017-04-08	15:38:08.995687	192.168.0.105	98.139.180.149	UDP	554	35946 → 33435 Len=3472
925	2017-04-08	15:38:09.013495	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
926	2017-04-08	15:38:09.013496	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
927	2017-04-08	15:38:09.013496	192.168.0.105	98.139.180.149	UDP	554	35946 → 33436 Len=3472

▼ Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)

► Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)

► Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.180.149

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0x8c6b (35947)

► Flags: 0x01 (More Fragments)

Fragment offset: 1480

► Time to live: 1

Protocol: UDP (17)

Header checksum: 0x2ebb [validation disabled]

•	919	2017-04-08	15:38:08.995686	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
•	920	2017-04-08	15:38:08.995687	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
↑	921	2017-04-08	15:38:08.995687	192.168.0.105	98.139.180.149	UDP	554	35946 → 33435 Len=3472
	925	2017-04-08	15:38:09.013495	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
	926	2017-04-08	15:38:09.013496	192.168.0.105	98.139.180.149	IPv4	1514	Fragmented IP protocol (proto
	927	2017-04-08	15:38:09.013496	192.168.0.105	98.139.180.149	UDP	554	35946 → 33435 Len=3472
▼	Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)							
	► Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)							
	► Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)							
	Type: IPv4 (0x0800)							
▼	Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.180.149							
	0100 = Version: 4							
 0101 = Header Length: 20 bytes (5)							
	► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
	Total Length: 540							
	Identification: 0x8c6b (35947)							
	► Flags: 0x00							
	Fragment offset: 2960							
	► Time to live: 1							
	Protocol: UDP (17)							
	Header checksum: 0x51c2 [validation disabled]							

As shown above, 3 fragments were created from the original datagram.

Problem 13

Please look at the screenshots from **Problem 12** for reference. Fragmentation offset, flag bit(changes between the second last fragment and the last one), header checksum and total length(changes between the second last fragment and the last one) change among the fragments.