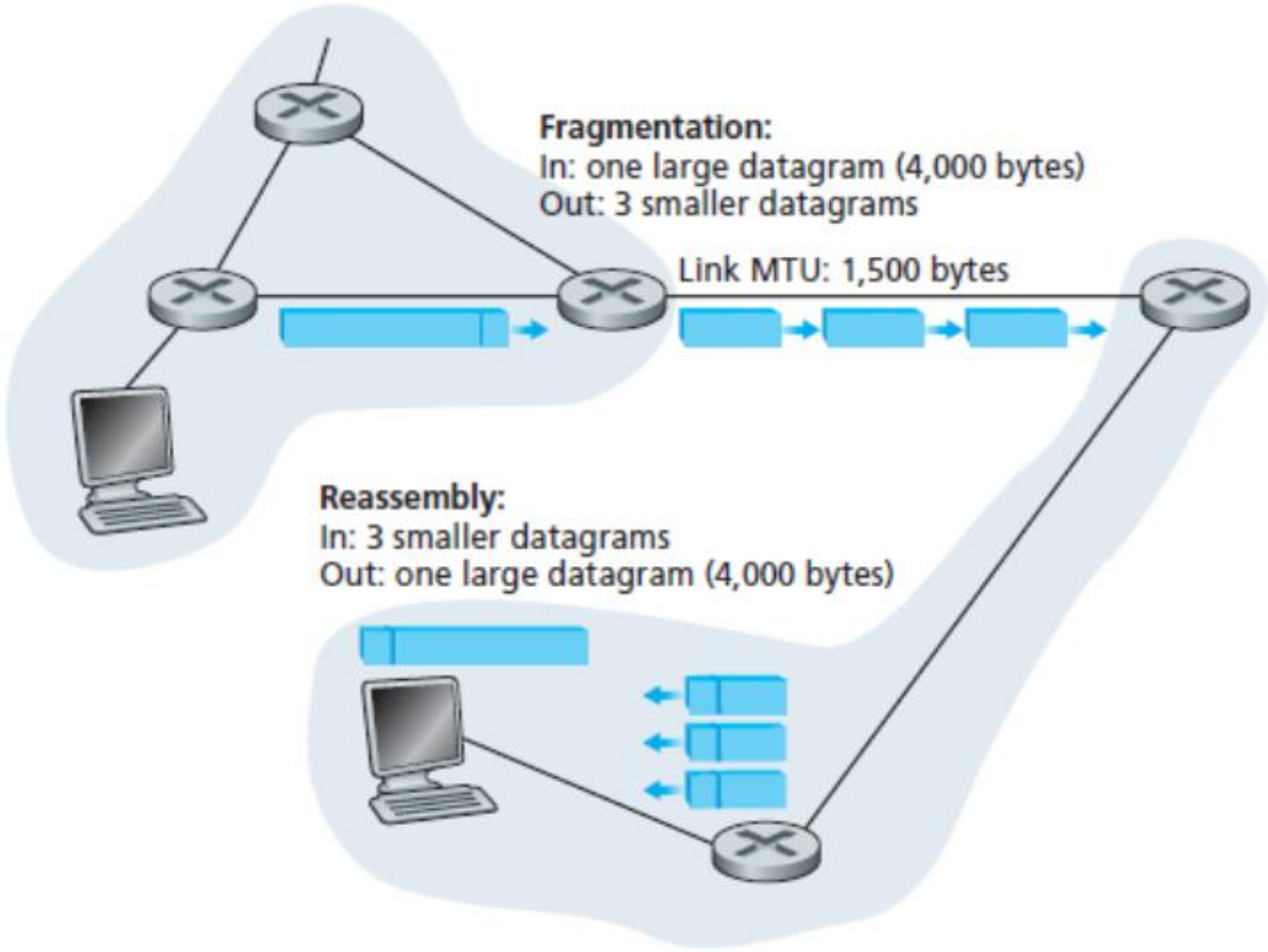
Tutorial 8: More hints on P3

IP Datagram Fragmentation



Datagram Fragment

- How to find the fragments of the same datagram?

  Check for the ID field of the IP header
- How to find the last fragment of a datagram?

  Flag = 0 and offset != 0

Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

RTT for Fragments

- According to RFC 792, for fragmented datagrams,

only one “TTL exceeds” message will be returned

For example,

the source sends Frag 1, Frag2, Frag 3 (of the same datagram, ID: 3000) with timesteps t1; t2; t3, respectively.

Later, the source receives one “ICMP TTL exceeded” message (ID: 3000). The timestamp is T.

Then the RTTs are calculated as: T − t1, T − t2, T − t3.

Packet Match

- For Linux traces, use the source port number in the UDP packets
- For windows traces, match the sequence number between ICMP echo and ICMP error message
- Why different?

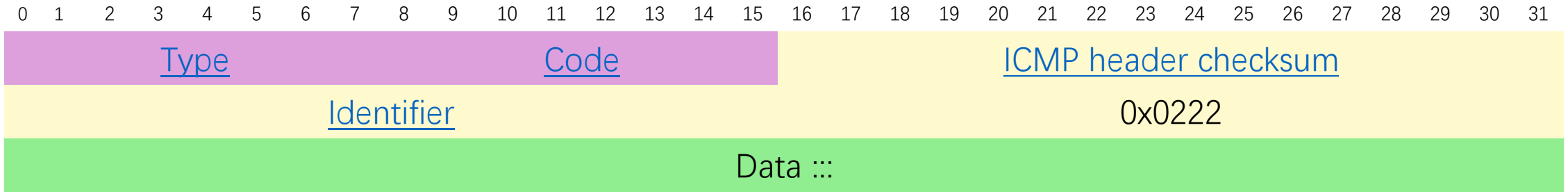
Linux and Windows implements traceroute in different ways:

Unix/Linux uses UDP packets

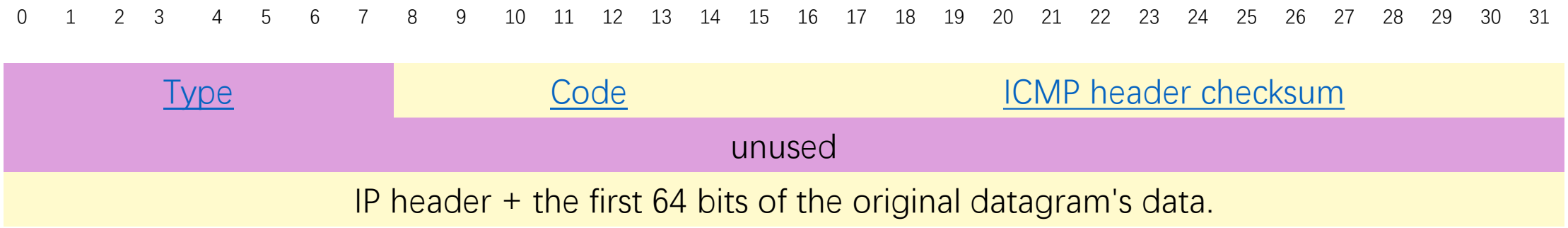
Windows uses ICMP packets

Using win_trace2 for an example,

The first frame is the ICMP type 8, Echo request message:

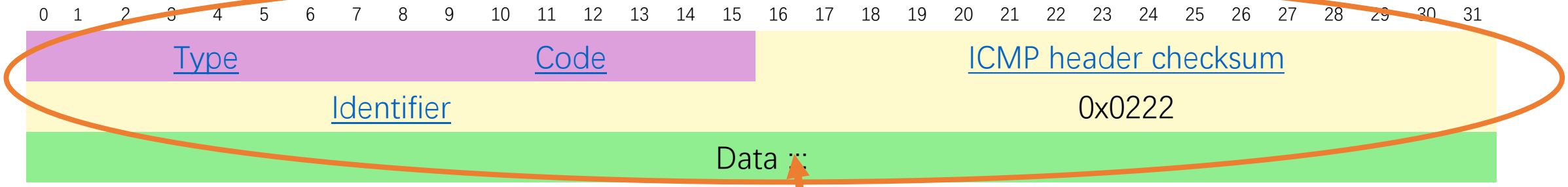


The 2nd frame is the ICMP type 11, Time exceeded message:

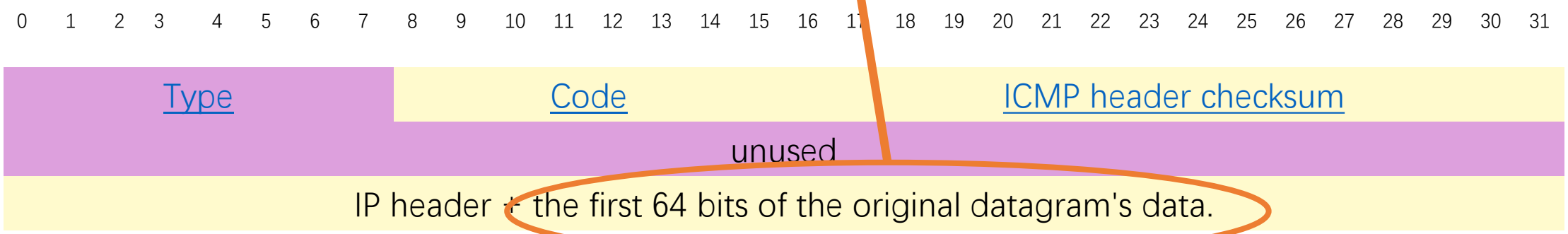


Using win_trace2 for an example,

The first frame is the ICMP type 8, Echo request message:



The 2nd frame is the ICMP type 11, Time exceeded message:



Other Questions

- Why do multiple routers return an error message for UDP with same TTL in a trace file

Multiple UDP message with the same TTL hits different routers due to load balance.

In this case, list the routers with the same orders that they appear in the trace file.

- You may find packets with TCP and DNS protocols, which can be ignored in this assignment except for ICMP and UDP.