ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 10: Layer 3 Attacks

Outline

- IP Fragmentation
- IP Fragementation Attacks
- Ping of Death
- Teardrop
- Memory DoS

IP Header

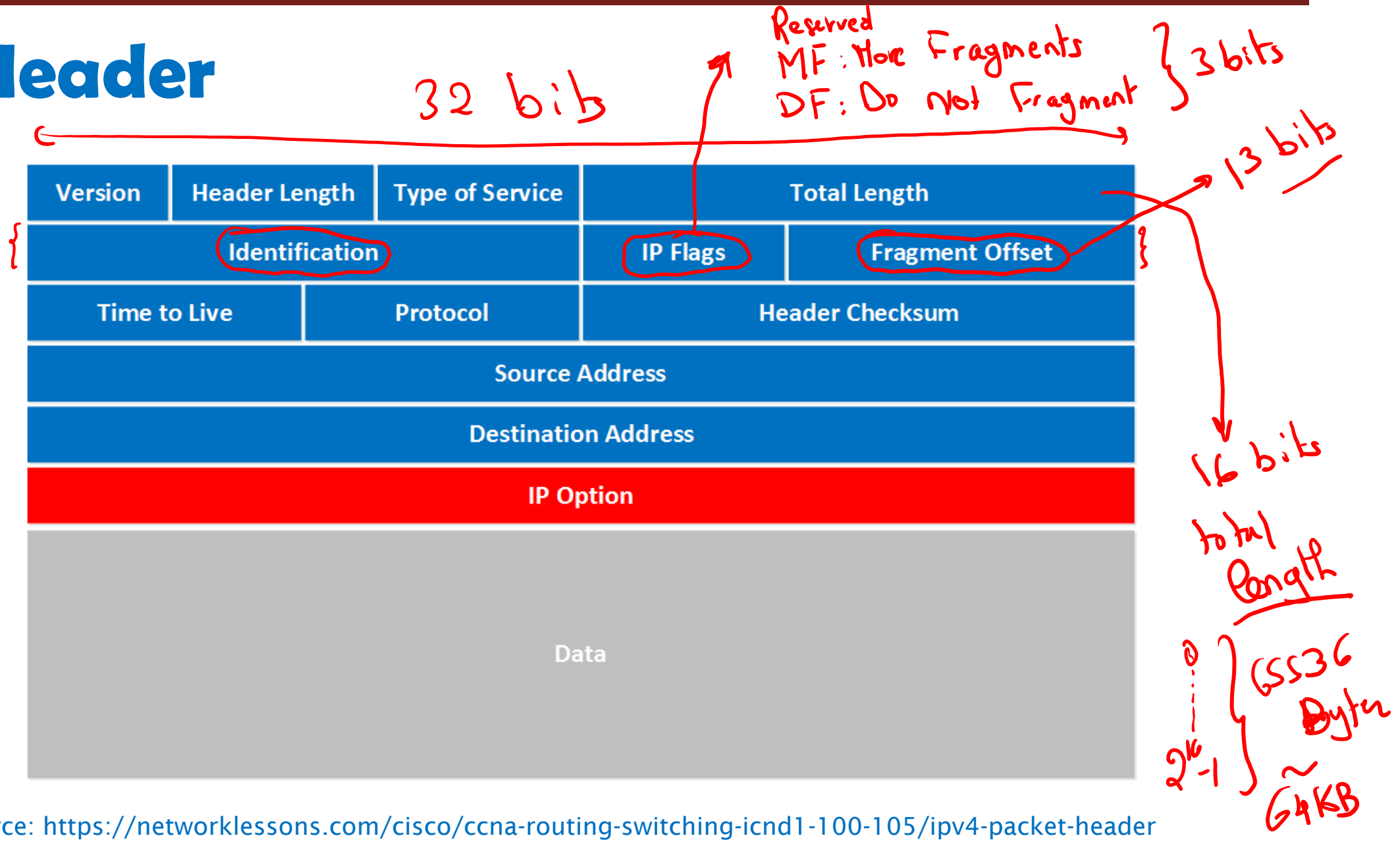


Image source: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ipv4-packet-header

Fragmentation: Why?

Hardware Limits / Physical World Limits

Recall from Ethernet Frames discussion

- Maximum Transmission Unit (MTU)
- $46 \leq MTU \leq 1500$ bytes

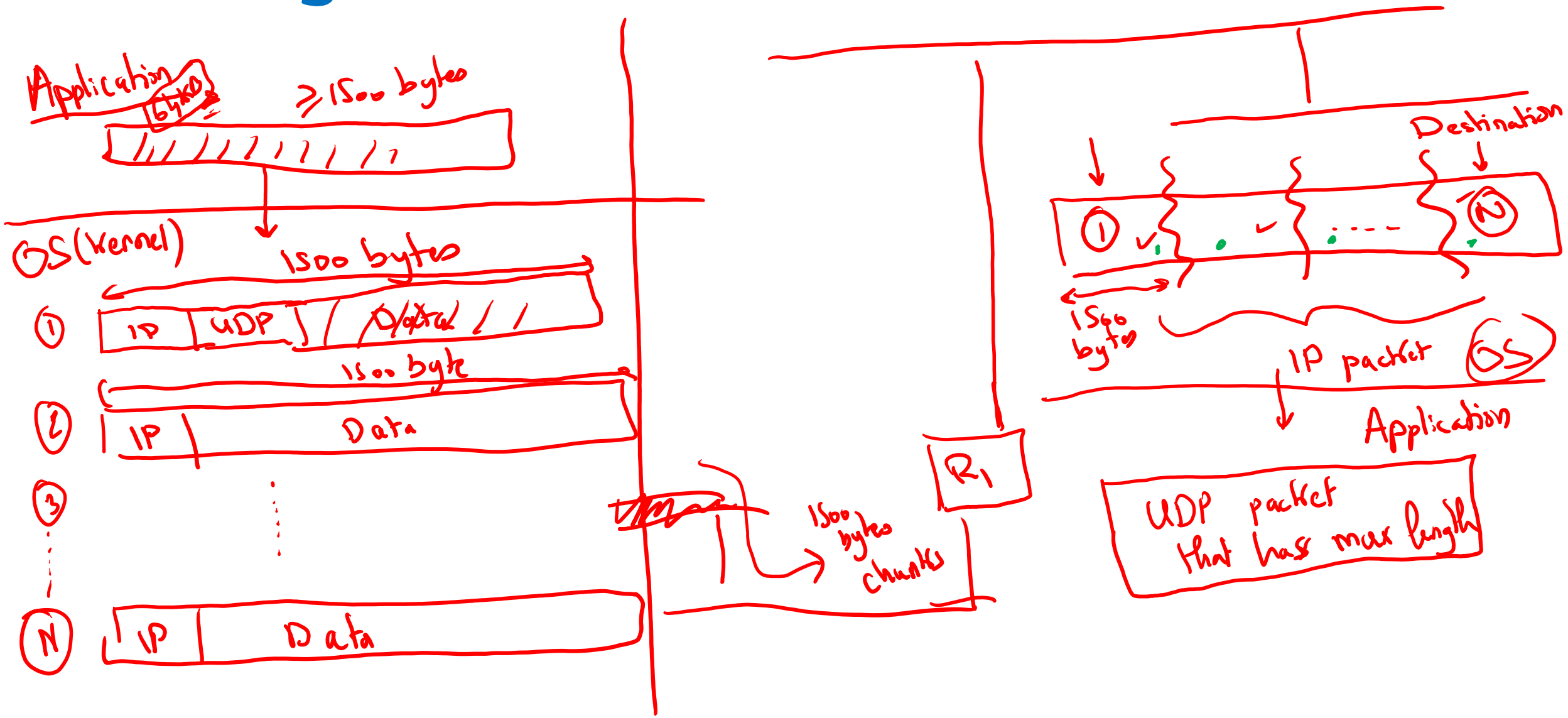
Detect Collisions

Hard limit on how big a packet can be

↳ ≥ 1500 : Fragment (IP. fragmentation)

File 3 MB
≈ 3×10^6 Bytes

IP Fragmentation

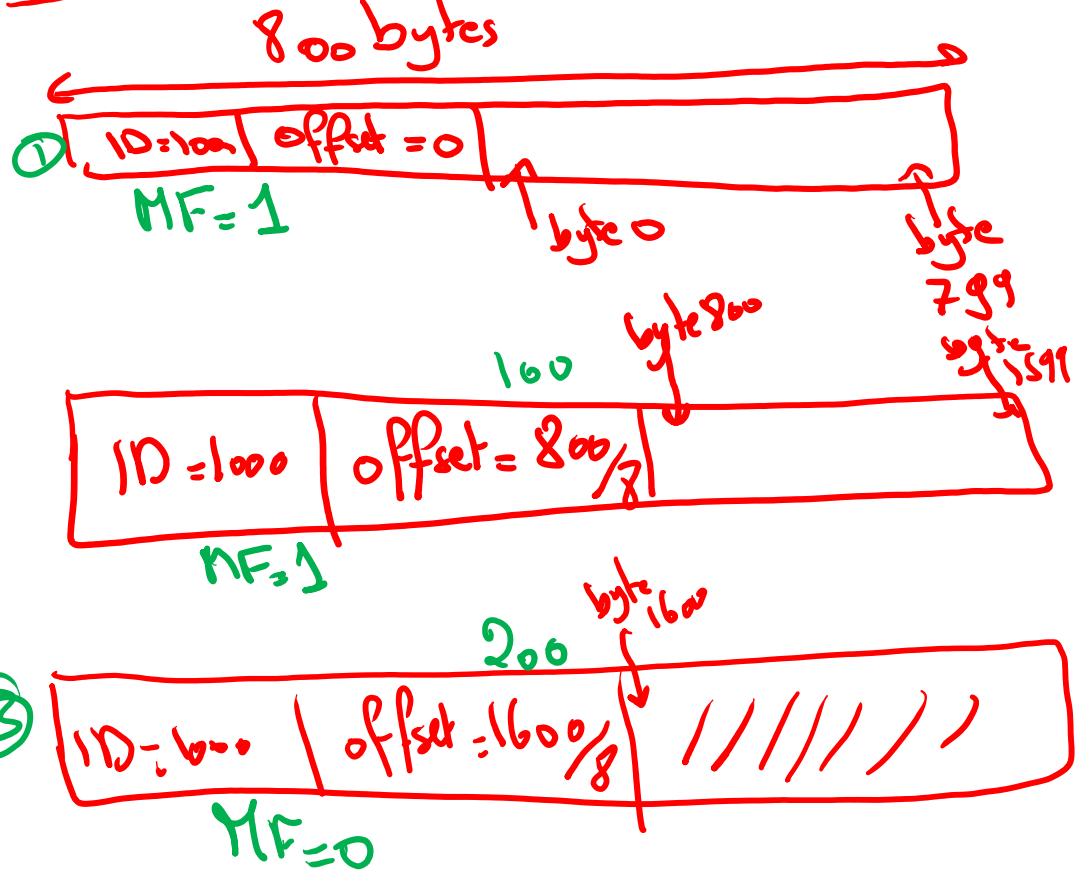


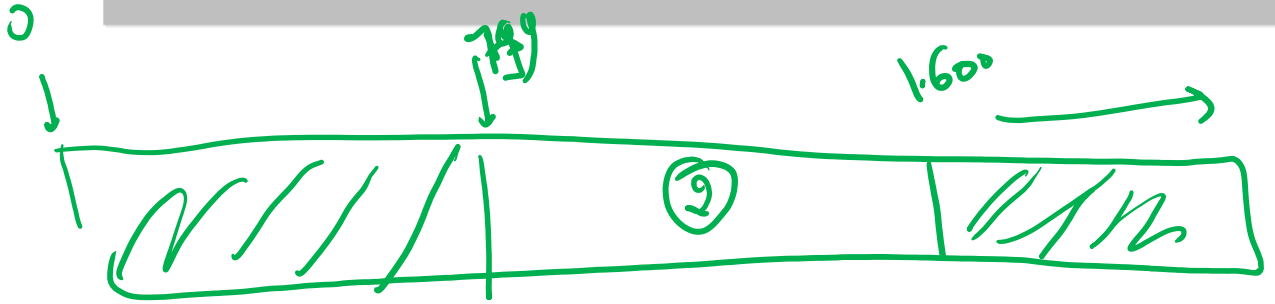
Fragmentation Offsets

Version	Header Length	Type of Service	Total Length
Identification		IP Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
IP Option			
Data			

multiple of 8 — 16 bits — 000 — 13 bit byte offset of the first byte w.r.t the packet total length

MTU = 800 Bytes (1600+ change)bytes





Fragmentation Demo

`send_fragments.py`

Rules

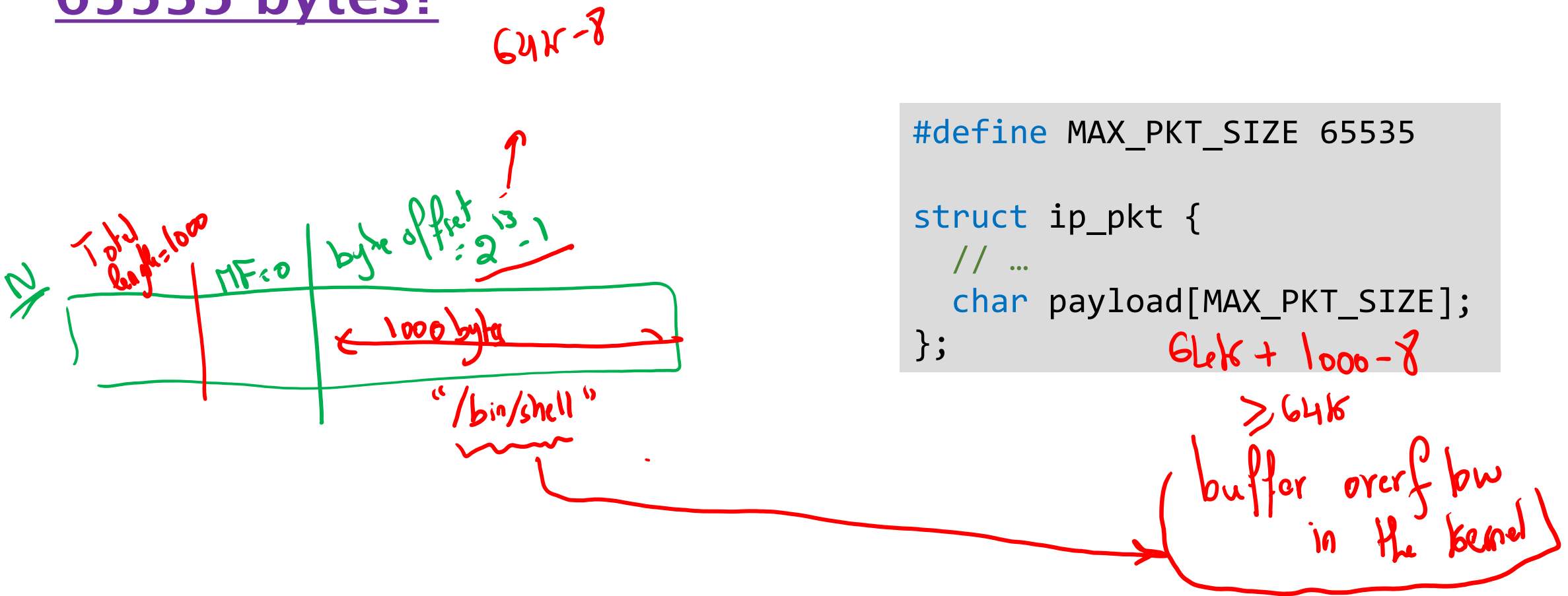
- Protocols are just rules
- Note everyone follows rules
- Packets are created artifacts

Questions

- Can you create a packet that **is larger than** 65535 bytes?
- Can you create **abnormal conditions** using packet offsets and payload sizes?
- Can you use a small amount of bandwidth to **tie up a target's resources**?

Ping of Death Attack

Q1: Can you create a packet that is larger than 65535 bytes?



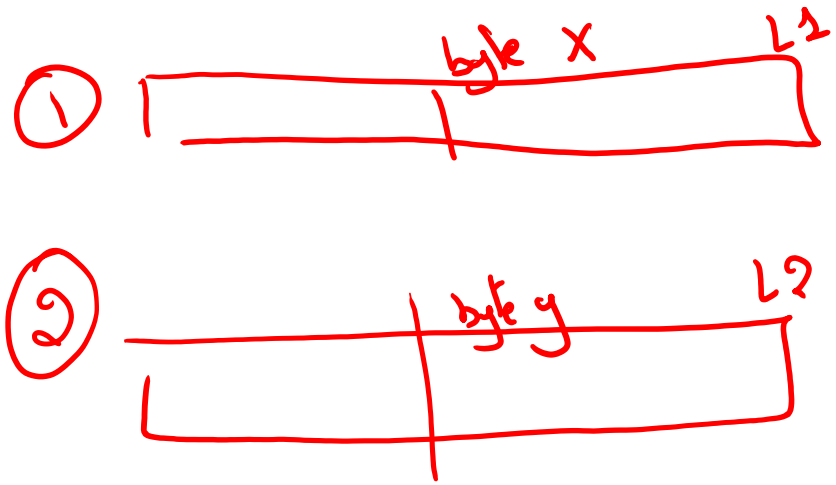

```
#define MAX_PKT_SIZE 65535

struct ip_pkt {
  // …
  char payload[MAX_PKT_SIZE];
};
```

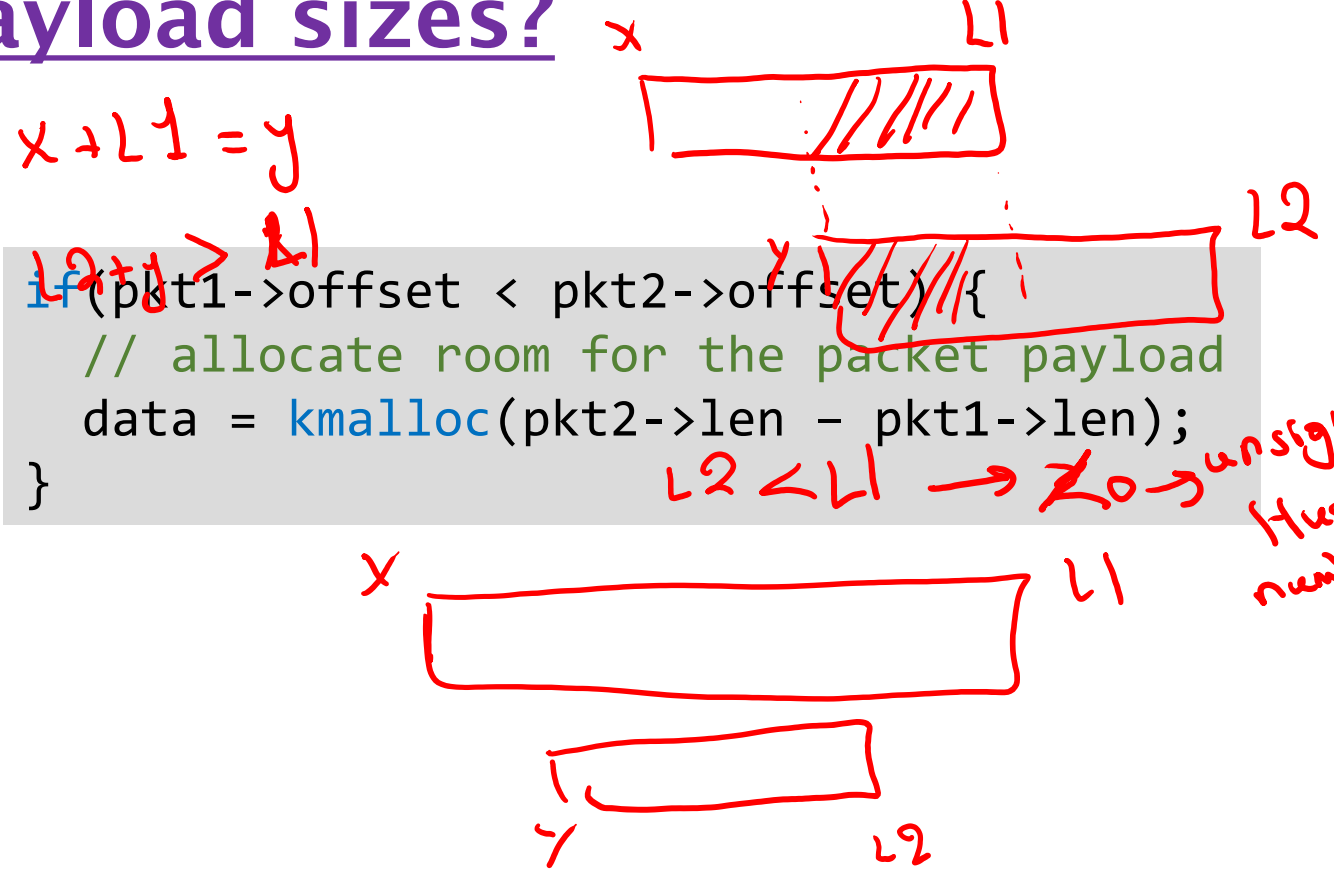
Still there


Windows “Ping of Death” bug revealed – patch now!
14 OCT 2020
24
Microsoft, Vulnerability

The Teardrop Attack

Q2: Can you create abnormal conditions using packet offsets and payload sizes?





Memory DoS using IP Fragments

Q3: Can you use a small amount of bandwidth to tie up a target's resources?