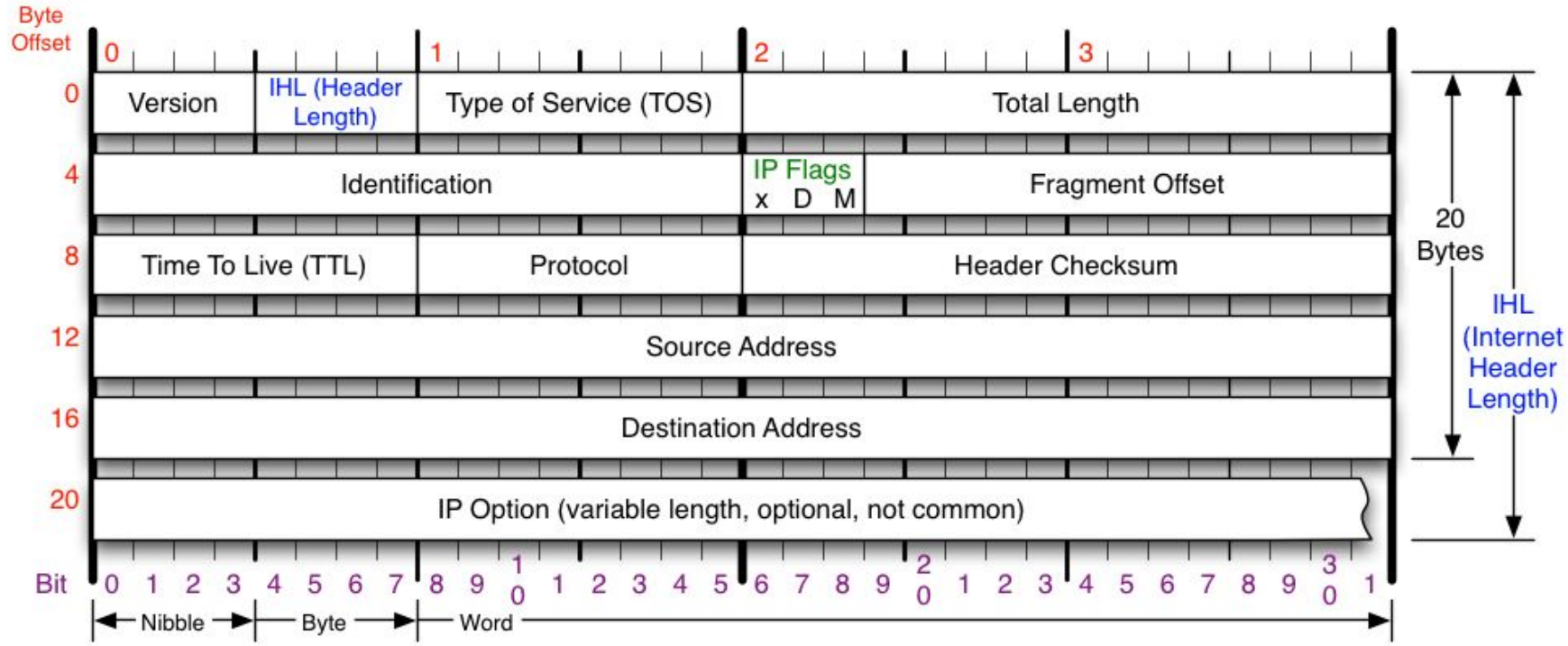
BASIC NETWORK PROTOCLS EXPLAINING BY TRAFFIC ANALYZING

IP

Internet

Protocol

IPv4 Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Ip_TASK:

You have HEX representation of IP-header:

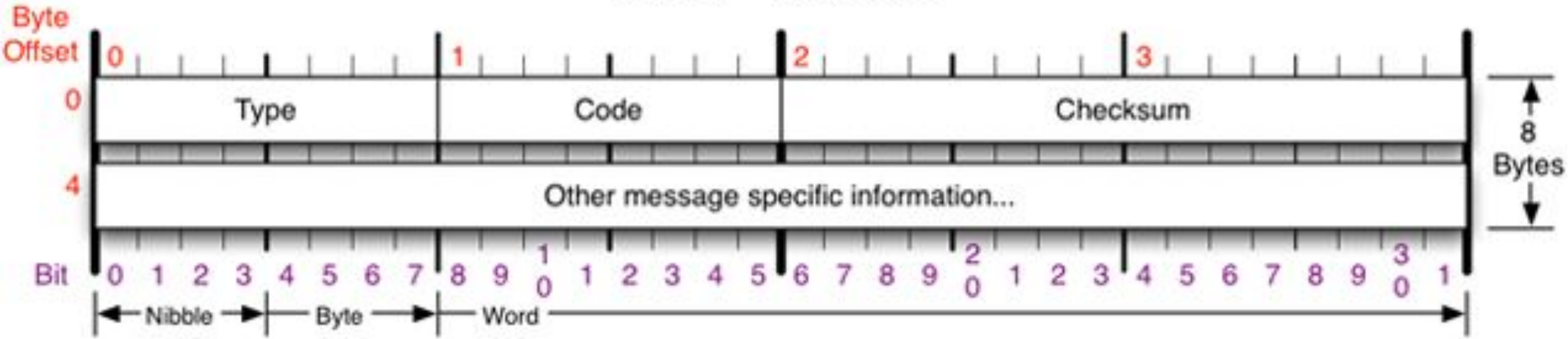
45 00 03 e4 b5 d0 20 00 40 01 9b 44 02 01 01 02 02 01 01 01

Find out and present in human-readable format:

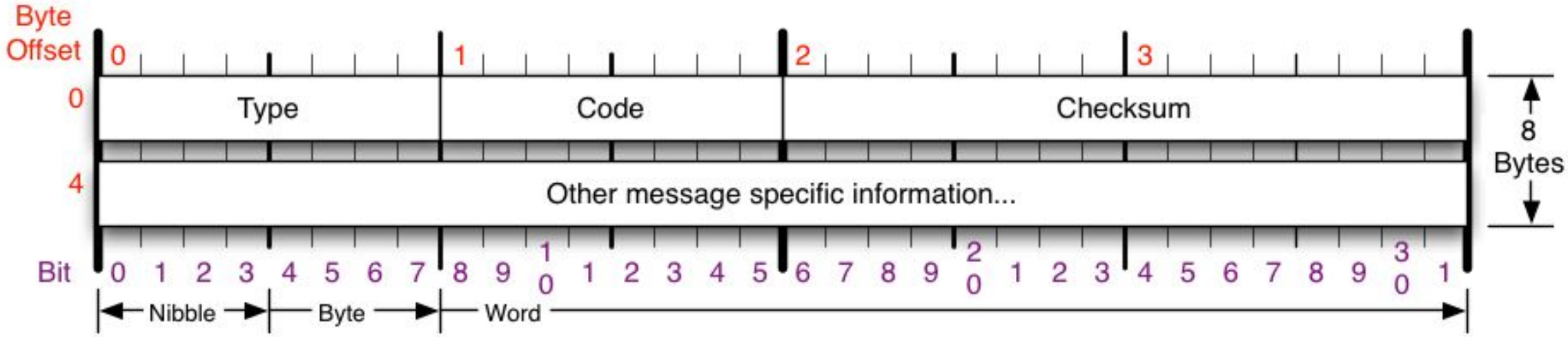
1. Internet Protocol version
2. Header length
3. Total length (Header length + Data)
4. TTL
5. Next level (transport) protocol
6. Source address
7. Destinations address

ICMP
Internet Control Message Protocol

ICMP Header


Byte Offset
0
4
0
1
2
3
Type
Code
Checksum
Other message specific information...
8 Bytes
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word

ICMP Header



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS

Type	Code/Name
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection

Type	Code/Name
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation needed and DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect datagram for the Network
	1	Redirect datagram for the host
	2	Redirect datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem	0	Pointer indicates error
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

icmp_TASK:

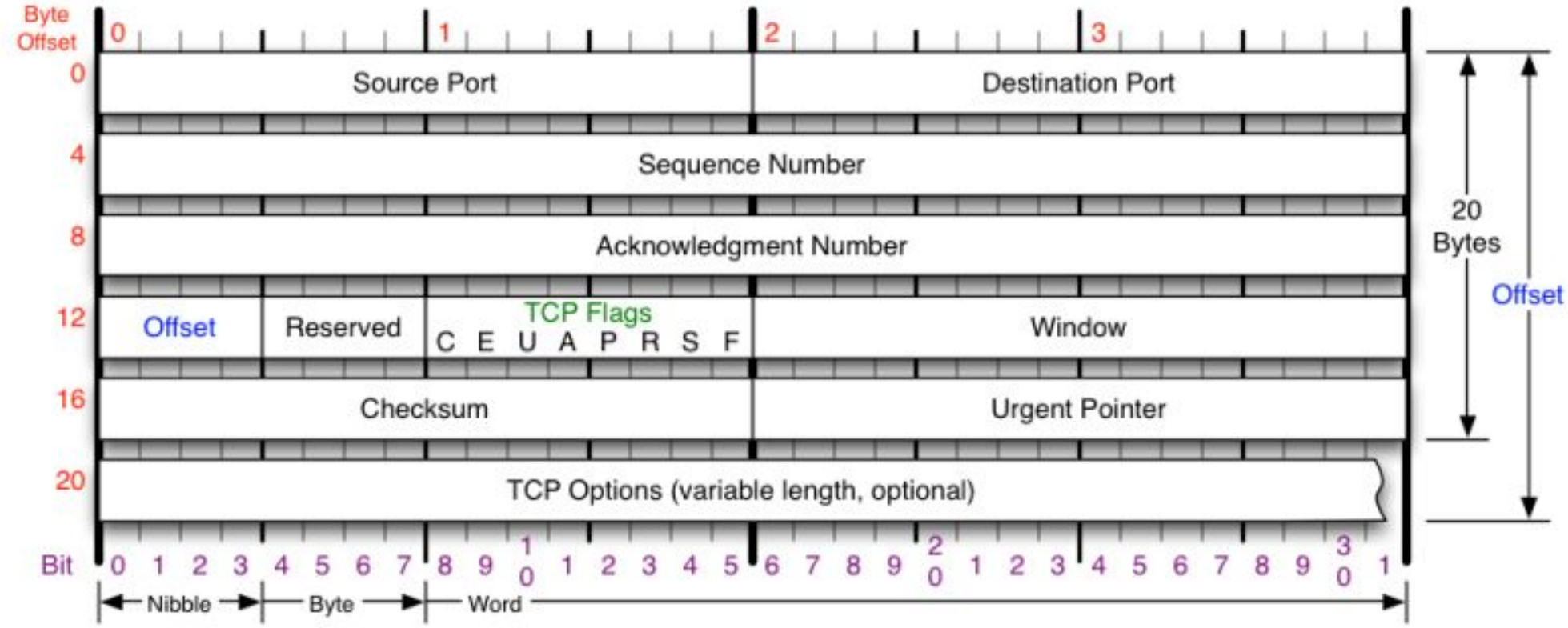
1. Open Wireshark and start sniffing on WLAN interface
2. Use filtering bar to display only ICMP traffic
3. Try to ping https://www.webpagetest.org/.

Analyze what is going on?

4. Try to tracert https://www.webpagetest.org/.

Analyze what is going on?

TCP
Transmission Control
Protocol



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

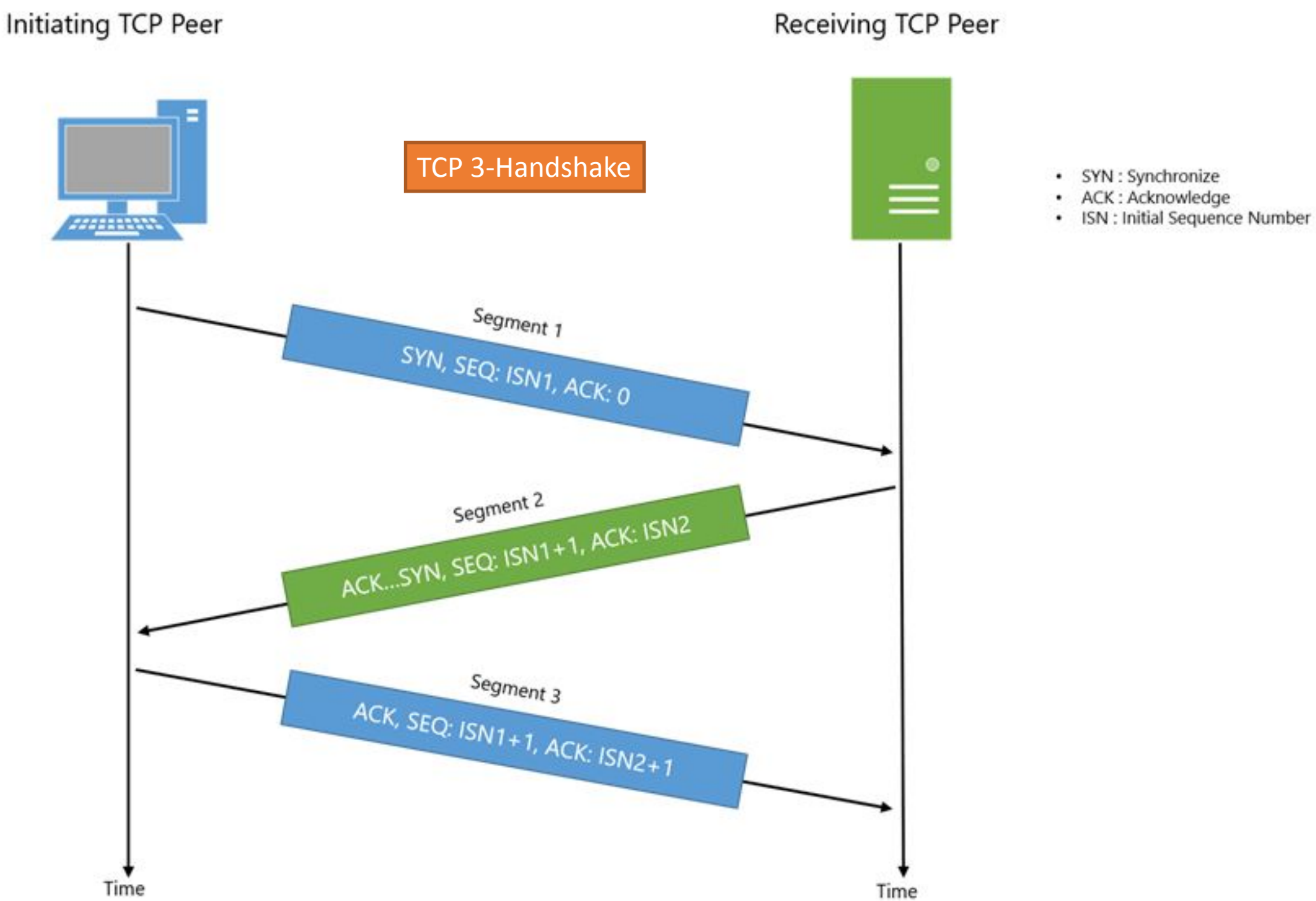
RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Флаги (управляющие биты)

- **SYN** — синхронизация номеров последовательности
- **ACK** — поле *«Номер подтверждения»* задействовано
- **PSH** — инструктирует получателя протолкнуть данные, накопившиеся в приёмном буфере, в приложение пользователя
- **FIN** — указывает на завершение соединения
- **RST** — оборвать соединения, сбросить буфер (очистка буфера)

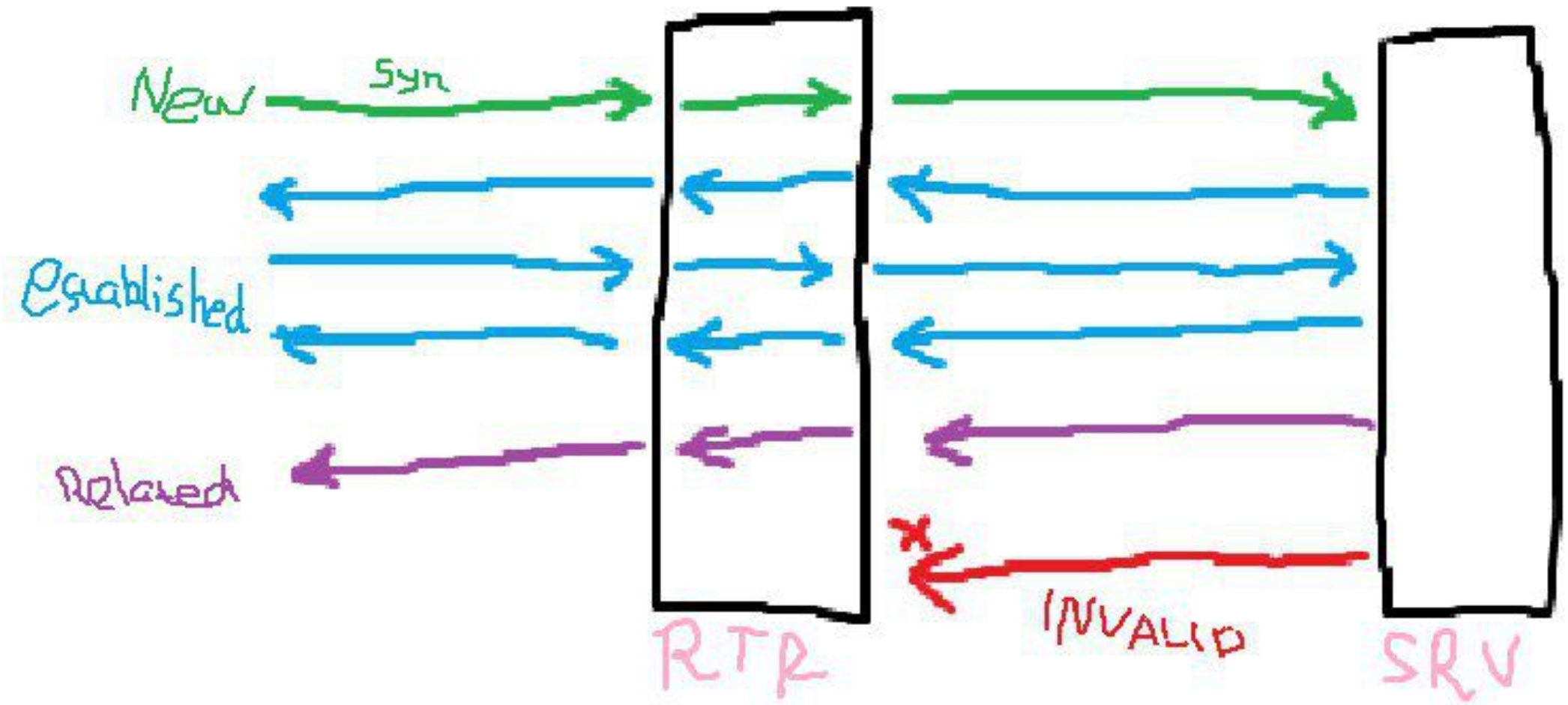
- **URG** — поле *«Указатель важности»* задействовано (англ. *Urgent pointer field is significant*)


Initiating TCP Peer
Receiving TCP Peer
TCP 3-Handshake
SYN : Synchronize
ACK : Acknowledge
ISN : Initial Sequence Number
Segment 1
SYN, SEQ: ISN1, ACK: 0
Segment 2
ACK...SYN, SEQ: ISN1+1, ACK: ISN2
Segment 3
ACK, SEQ: ISN1+1, ACK: ISN2+1
Time
Time

tcp_TASK:

1. Open Wireshark and start sniffing on WLAN interface
2. Use filter bar to display only TCP traffic
3. Send GET request to http://google.com. Analyze the TCP-session establishment process (use **curl** tool from bash or powershell)

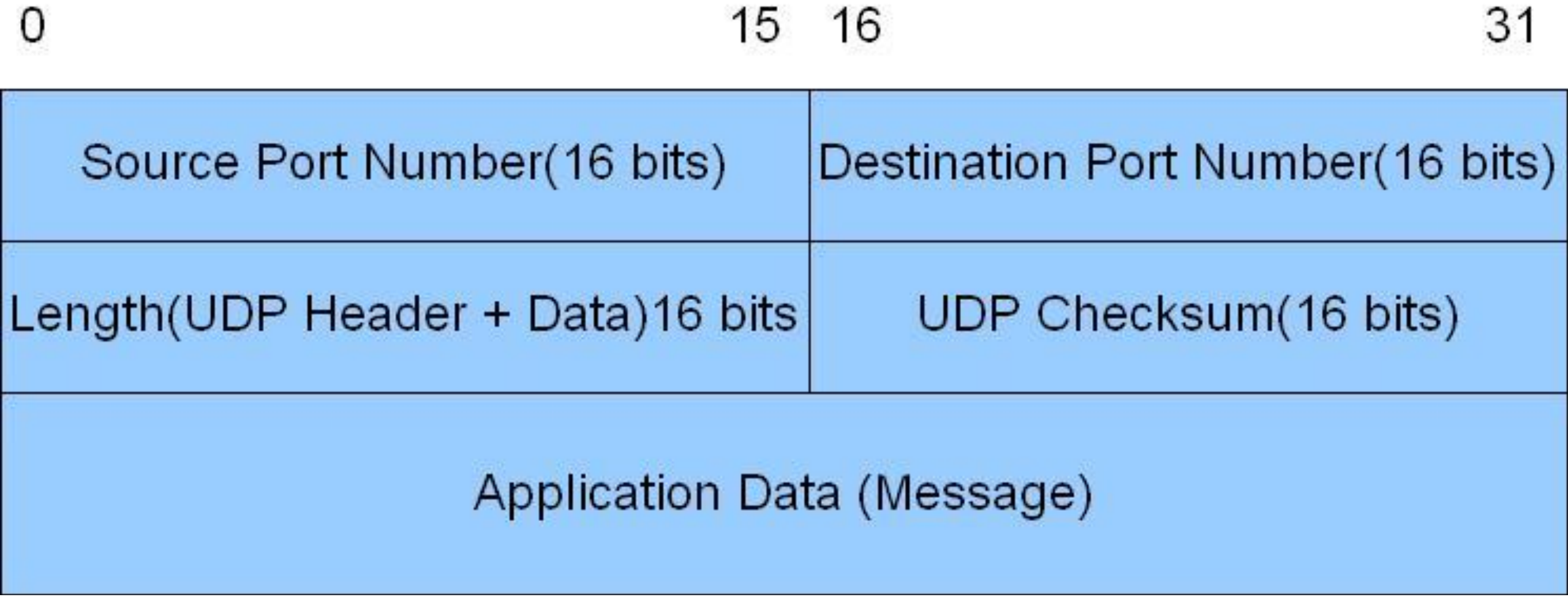
Connection types



tls_TASK:

1. Use filter bar to display only TCP traffic
2. Send GET request to http[s]://google.com. (use **curl** tool from bash or **powershell**)
3. Delete all filters. Analyze, where is HTTP protocol?

UDP
User Datagram
Protocol


0
15
16
31
Source Port Number(16 bits)
Destination Port Number(16 bits)
Length(UDP Header + Data)16 bits
UDP Checksum(16 bits)
Application Data (Message)

UDP usage

- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real time applications

udp_TASK:

1. Open Wireshark and start sniffing on WLAN interface
2. Use filtering bar to display only udp traffic
3. Let`s disscused: How many ports are exist?
4. Try scanning all ports at https://www.webpagetest.org.
5. Which ports were discovered and which are open?