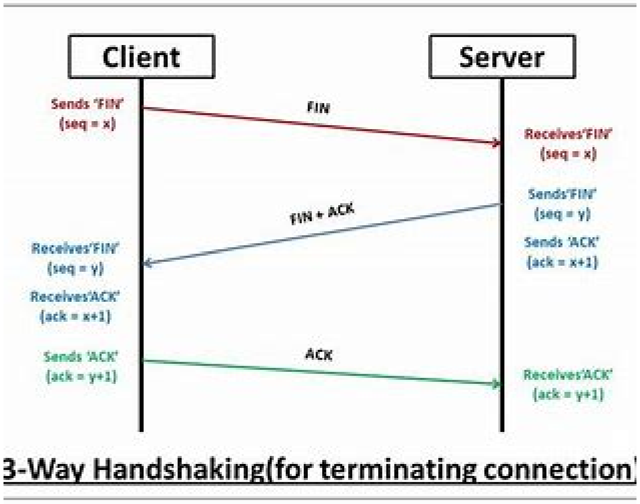
اليوم ان شاء الله بنكمل اخر جزئيه من النيتورك

by [(twitter.com/cyber6l)](twitter.com/cyber6l)

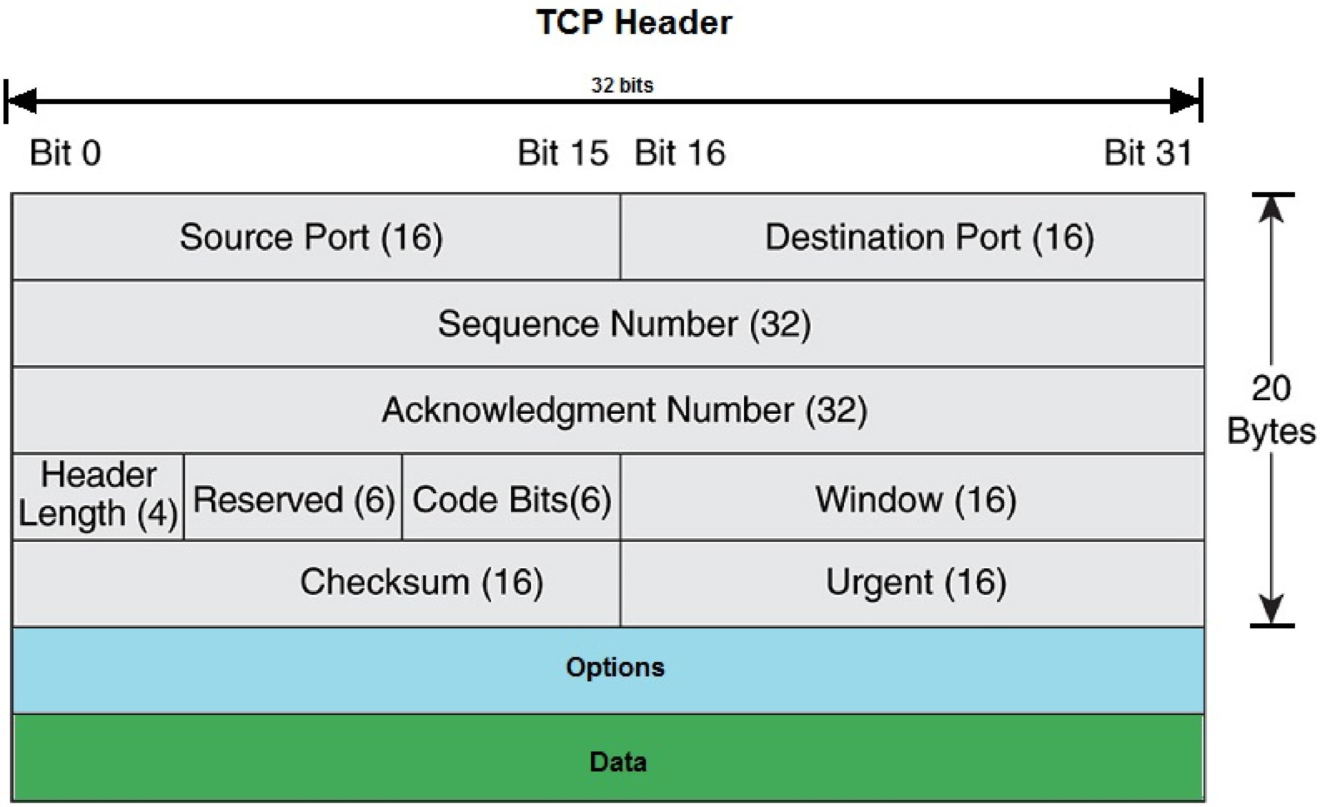
<< 2.4 DNS Traffic >>

```
TCP (Transmission Control Protocol) يتاكد لك ان الداتا وصلت بشكل صحيح من المرسل
الى المستقبل بدون فقدان قدرالامكان ويعالج لك الاخطاء ويأتمتها ويصححها ويرجعها
لك
عشان ما تنسى يستخدم TCP conducts a 3-way handshake
واقدر الخصها لك بهاذي الصوره
```

Suspicious TCP Traffic	**Normal TCP Traffic**
3-way handshake (SYN, SYN/ACK, ACK)	Excessive SYN packets (scanning)
Smart TCP attacks (usage of different flags)	
Single host to multiple ports or single host to multiple nodes (scanning)	



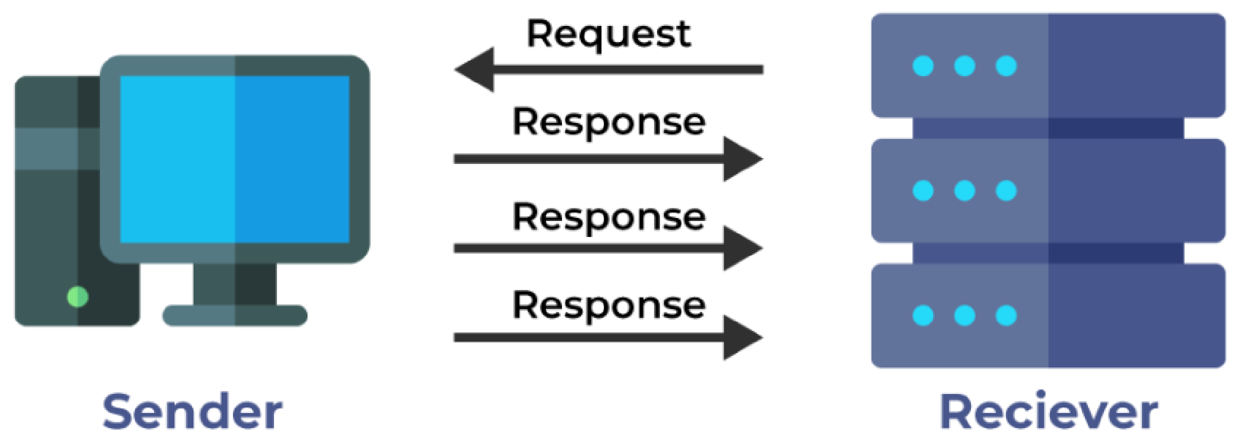
الهيدر عندي ب TCP So Complex



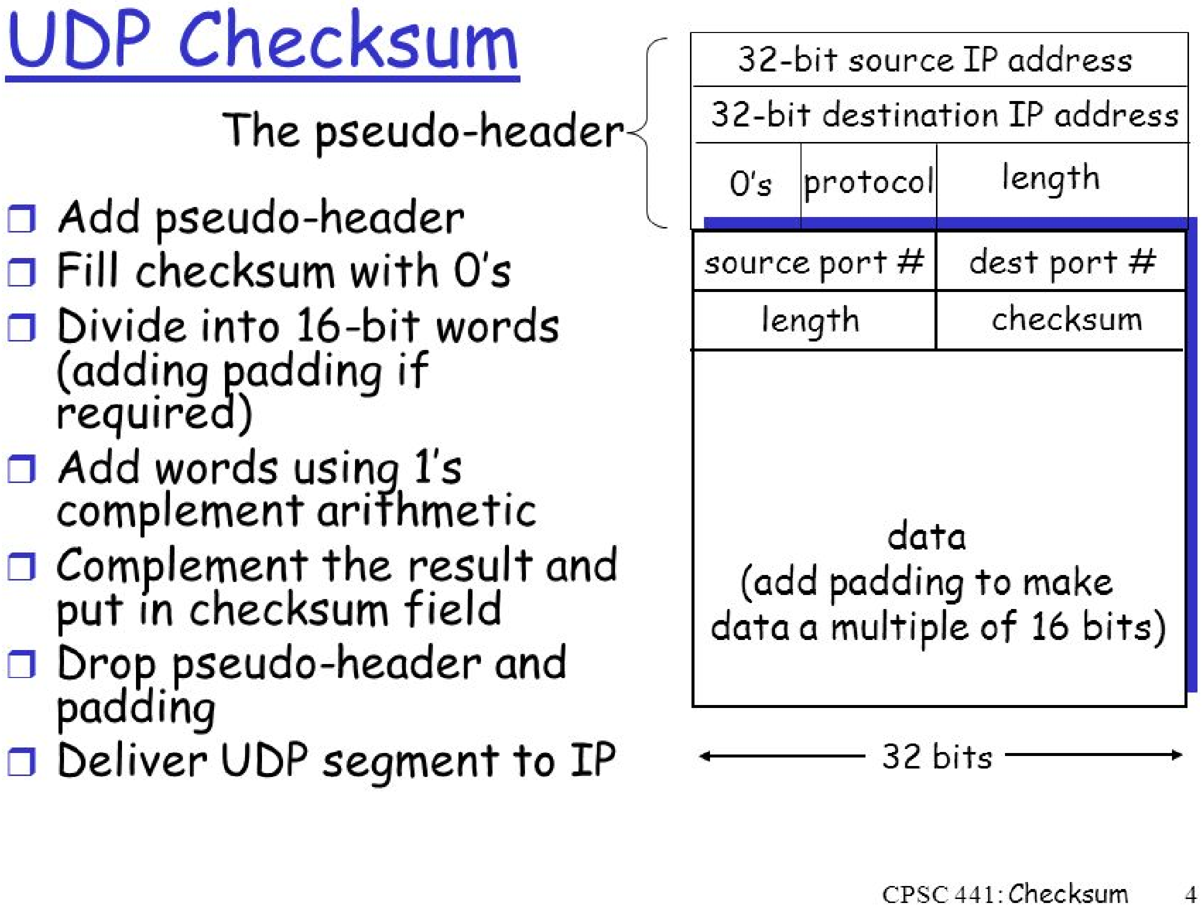
TCP Header

<table>
<tr><td colspan="3">Source Port (16)</td><td>Destination Port (16)</td></tr>
<tr><td colspan="4">Sequence Number (32)</td></tr>
<tr><td colspan="4">Acknowledgment Number (32)</td></tr>
<tr><td>Header Length (4)</td><td>Reserved (6)</td><td>Code Bits(6)</td><td>Window (16)</td></tr>
<tr><td colspan="3">Checksum (16)</td><td>Urgent (16)</td></tr>
<tr><td colspan="4">Options</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

```
UDP (User Datagram Protocol) Unlike TCP, it is an unreliable and connectionless
protocol. So, there is no need to establish a connection before data transfer
والاتصال برضو بتكون سيء زي البث لمن يقطع عليك و الخ
ومافي هاند تشك
```



الهيدر ب UDP so cute _



UDP Checksum

The pseudo-header

- ❒ Add pseudo-header
- ❒ Fill checksum with 0's
- ❒ Divide into 16-bit words (adding padding if required)
- ❒ Add words using 1's complement arithmetic
- ❒ Complement the result and put in checksum field
- ❒ Drop pseudo-header and padding
- ❒ Deliver UDP segment to IP

32-bit source IP address		
32-bit destination IP address		
0's	protocol	length
source port #		dest port #
length		checksum
data (add padding to make data a multiple of 16 bits)		

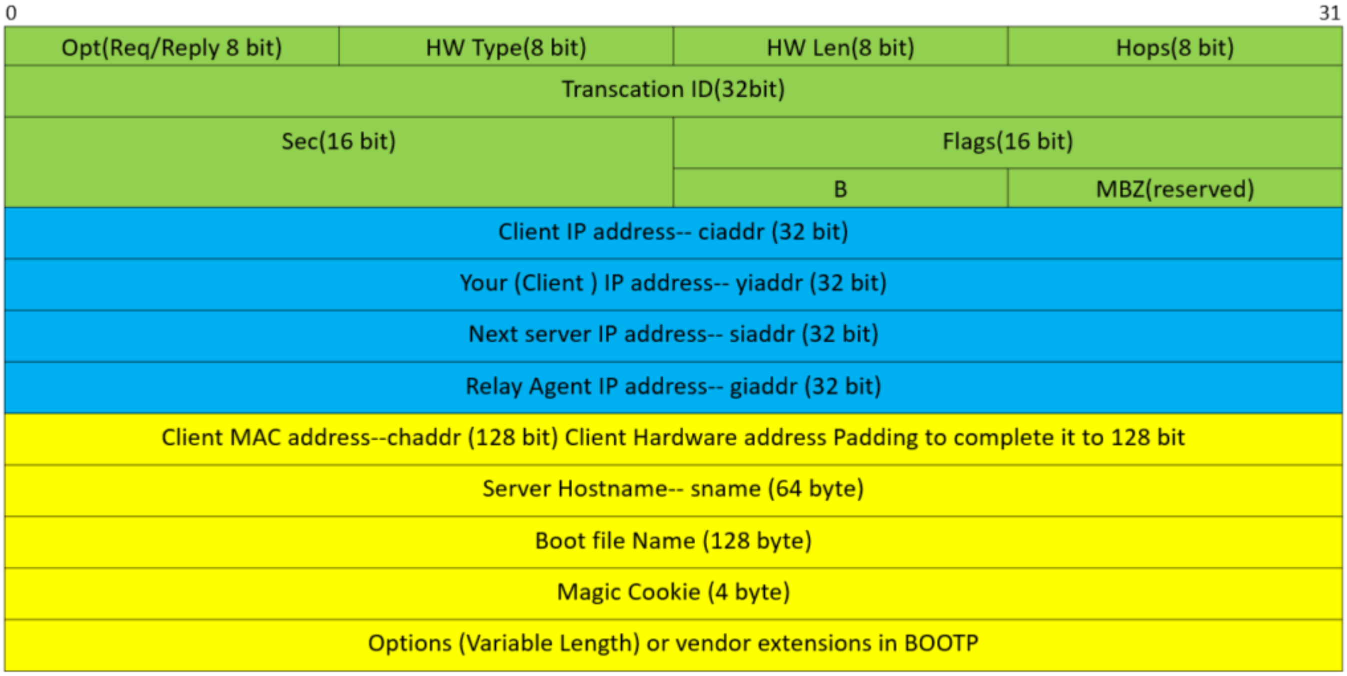
32 bits

CPSC 441: Checksum 4

وكذا خلصنا السكشن 4

<< 2.5 DHCP Traffic >>

```
وش فايدته وايش هو
DHCP (Dynamic Host Configuration Protocol) that assigns and manages IP addresses
for devices on a network, making it easier for them to connect and communicate
without manual configuration.
```



0			31
Opt(Req/Reply 8 bit)	HW Type(8 bit)	HW Len(8 bit)	Hops(8 bit)
Transcation ID(32bit)			
Sec(16 bit)		Flags(16 bit)	
		B	MBZ(reserved)
Client IP address-- ciaddr (32 bit)			
Your (Client) IP address-- yiaddr (32 bit)			
Next server IP address-- siaddr (32 bit)			
Relay Agent IP address-- giaddr (32 bit)			
Client MAC address--chaddr (128 bit) Client Hardware address Padding to complete it to 128 bit			
Server Hostname-- sname (64 byte)			
Boot file Name (128 byte)			
Magic Cookie (4 byte)			
Options (Variable Length) or vendor extensions in BOOTP			

Figure 1

- Automates IP address assignment.
- Furnishes additional details like DNS servers and gateway.
- Operates through the DORA process (DHCP Discover, DHCP Offer, DHCP Request, DHCP Acknowledgment).
- Relies on UDP with ports 67 for servers and 68 for clients.

Normal DHCP Behavior	Suspicious DHCP Activity
Dynamic allocation of IP addresses	Unusual or excessive IP address requests
Automatic configuration of network settings	Unauthorized DHCP servers
Timely renewal of IP leases	Frequent changes or disruptions in IP leases
Efficient management of network resources	Abnormal traffic patterns

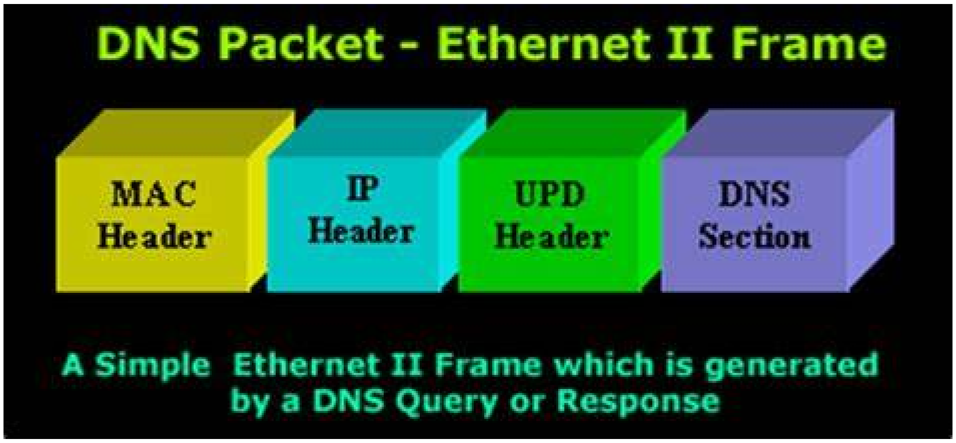
وخلصنا كان سكشن خفيف لطيف

<< 2.6 DNS Traffic >>

```
وش DNS, or Domain Name System, is a crucial internet infrastructure translating
user-friendly domain names like "[www.example.com] (http://www.example.com/)" into
numerical IP addresses, such as "192.168.1.1", allowing computers to locate and
communicate with each other.
```

- DNS is a query-response protocol
- DNS traffic normally uses UDP on port 53

• DNS traffic should go to DNS servers only


DNS Packet - Ethernet II Frame
MAC Header
IP Header
UPD Header
DNS Section
A Simple Ethernet II Frame which is generated by a DNS Query or Response

Normal DNS Traffic	Suspicious DNS Traffic
Port 53, UDP	UDP Traffic on port 53 but using TCP instead of UDP
Should only go to DNS Servers	DNS traffic not going to DNS Servers
Should see DNS Responses to DNS Queries	A lot of DNS Queries with no DNS responses or vice versa

```
The DNS Transaction ID is a 16-bit identifier in DNS queries, generated by the client to match responses. It aids in tracking and ensuring responses correspond to the correct queries
```

وخلصنا السكشن 6

<< 2.7 HTTP & HTTPS Traffic >>

```
about HTTP:
```

- HTTP traffic comprises requests and responses, forming messages.
- Clients make requests, and servers respond accordingly.
- HTTP responses contain a 3-digit status code indicating the outcome.
- Messages include a header and body, providing contextual and content information.
- HTTP employs various methods to perform operations.
- RFC 2616 defines 8 HTTP methods.
- Web servers may restrict certain methods based on permissions.

Normal HTTP Traffic	Suspicious HTTP Traffic
Typically uses port 80 for unsecured HTTP	Unusual or excessive requests on non-standard ports
Clients make legitimate requests	Frequent requests for sensitive resources
Responses include standard 3-digit codes	Unexpected or uncommon status codes
Message headers and bodies are standard	Unusual or irregular message structures
Follows standard HTTP methods	Use of uncommon or unauthorized HTTP methods

```
about HTTPS (Hypertext Transfer Protocol Secure):
```

In a nutshell:

- **Encryption:** Safeguards data with encryption, ensuring privacy.
- **Authentication:** Certificates verify the legitimacy of the website, preventing impersonation.
- **Data Integrity:** Ensures data remains unchanged during transmission, preventing tampering.
- **SSL/TLS Protocols:** Utilizes Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for secure connections.
- **Port 443:** Typically uses port 443, distinguishing it from unsecured HTTP traffic.
- **Green Padlock:** Browser displays a padlock for a secure connection, building user confidence.
- **SEO Boost:** HTTPS contributes to better search engine rankings.
- **Trust:** Establishes trust for secure online transactions, enhancing user confidence.

Normal HTTPS Traffic	Suspicious HTTPS Traffic
Encrypted data transmission	Unusual or excessive encrypted traffic
Authentication through digital certificates	Invalid or suspicious digital certificates
Standard HTTPS ports (e.g., 443)	Traffic on non-standard HTTPS ports
Secure communication with known servers	Connections to untrusted or malicious servers
Valid SSL/TLS protocols	Use of outdated or insecure SSL/TLS protocols

اللابات ان شاء الله بتكون موجوده بقناه سطام

We have finished the network section