

# 2. Network Traffic & Flow Analysis

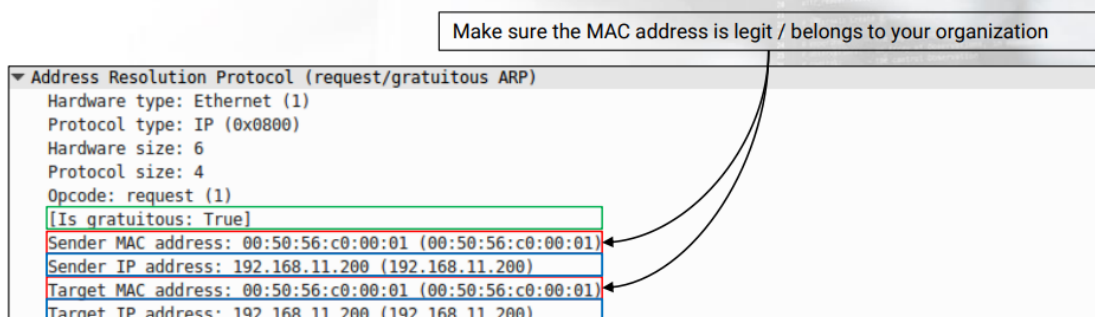
## Data Link Layer

### Ethernet 802.3

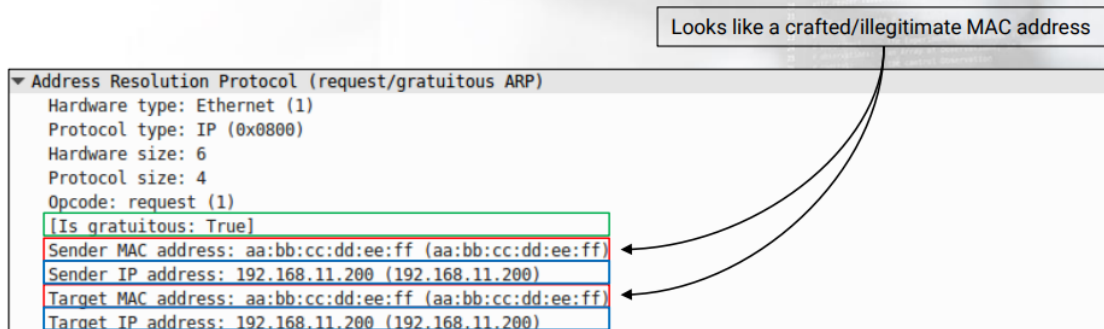
#### ARP Attacks & Detection

- The so-called gratuitous ARP requests and responses are also possible, and they are usually abused by attackers.
- **Gratuitous ARP request:** It is a request packet where **the source and destination IP are set with the IP of the machine** that is issuing the packet and the **destination MAC is the broadcast address**.
- Gratuitous ARP may be useful to detect IP conflict or simply inform other hosts/switches of a MAC address in the network, but attackers can also use these packets to mount **ARP poisoning attacks**.

#### Normal Gratuitous ARP



# Attacker-crafted Gratuitous ARP



- **Gratuitous ARP reply:** It is an ARP reply that has been sent **without being requested**. (usually malicious)

## Tips regarding normal and suspicious ARP traffic.

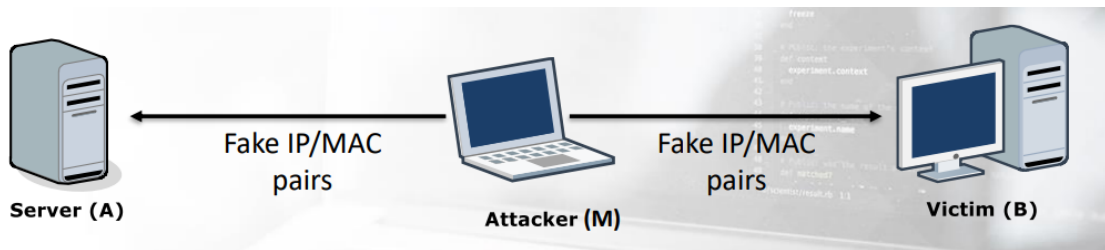
- **Normal:** ARP broadcasts are normal from both clients and servers, including network devices at a reasonable flow.
- **Suspicious:** Tens, hundreds, or even thousands of ARP broadcast messages within a small time window

No.	Time	Source	Destination	Protocol	Length	Info
15	61.162590056	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.1? Tell 172.16.5.67
16	61.164533730	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.2? Tell 172.16.5.67
17	61.166589500	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.3? Tell 172.16.5.67
18	61.171696684	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.4? Tell 172.16.5.67
19	61.173595193	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.5? Tell 172.16.5.67
20	61.175482595	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.6? Tell 172.16.5.67
21	61.177434405	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.7? Tell 172.16.5.67
22	61.179428423	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.8? Tell 172.16.5.67
23	61.181401311	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.9? Tell 172.16.5.67
24	61.183387692	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.10? Tell 172.16.5.67
25	61.185470650	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.11? Tell 172.16.5.67
26	61.187379238	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.12? Tell 172.16.5.67
27	61.189625522	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.13? Tell 172.16.5.67
28	61.191455492	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.14? Tell 172.16.5.67
29	61.193387656	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.15? Tell 172.16.5.67
30	61.195423342	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.16? Tell 172.16.5.67
31	61.197387752	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.17? Tell 172.16.5.67
32	61.199389322	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.18? Tell 172.16.5.67
33	61.201395568	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.19? Tell 172.16.5.67
34	61.203388474	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.20? Tell 172.16.5.67

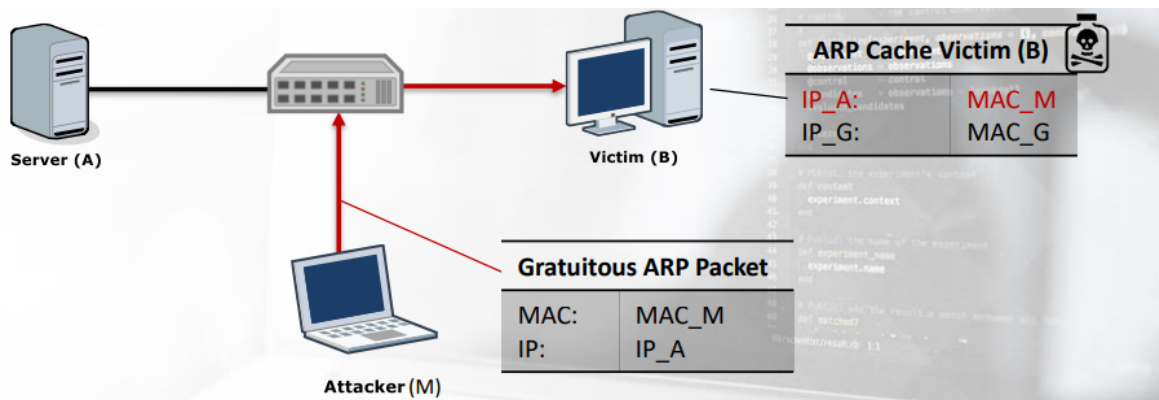
## ARP poisoning (between two communication peers into a local network)

- ARP poisoning can be exploited to add fake information between
  - The following are the steps for a successful attack (**ARP Poisoning**):
1. **M** would pretend to be **B to A**: it will send a **gratuitous ARP reply** with the pair: **IP\_B->MAC\_M**

2. **M** would pretend to be **A to B**: it will send a **gratuitous ARP reply** with the pair: **IP\_A->MAC\_M**



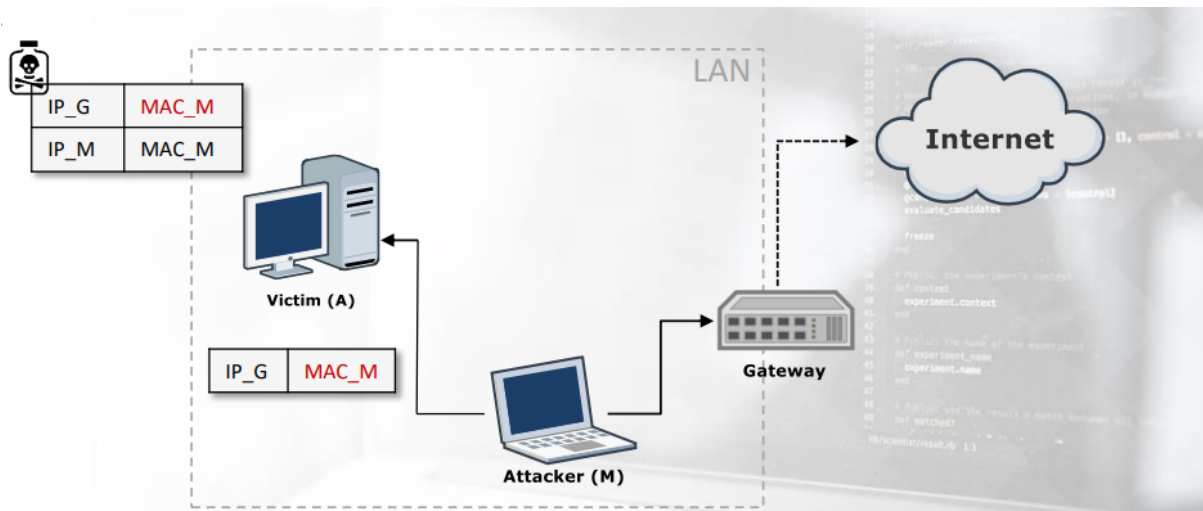
- Because of the **TTL** in hosts **ARP caches**, an attacker would need to send these packets at intervals lower than the timeout (usually every **30** seconds is a good choice).
- Once the gratuitous ARP packet is sent, B's ARP cache gets poisoned with the entry: **IP\_A->MAC\_M**. Next time B wants to send a packet to A, it will be forwarded to M. (The same thing happens against A.)



- Another gratuitous ARP with correct values would restore the correct values after the sniffing is completed

## ARP poisoning (between local host and remote host )

- When a host in a LAN wants to send packets to hosts outside the LAN, it uses the **default gateway**.
- The default gateway MAC address must be used to **forward** the packet along with the correct IP address configured by the administrator or given by DHCP.
- The use of ARP poisoning in this scenario leads to a **MITM attack from local to remote**.



The following describes the steps that take place in the previous scenario:

1. **Host A wants to send packets to the Internet.** It already has the IP of the gateway (IP\_G), and it needs the associated MAC address.
2. M can use a **gratuitous ARP reply** to advertise itself as the default gateway: **binds IP\_G with his own (MAC\_M).**
3. All the traffic meant to leave the LAN will pass **through M(the attacker)**, which will then redirect it to the real gateway.

## ARP Spoofing Prevention

1. Using Static ARP
  - not a feasible approach into large and always-changing networks
2. Tools like **arpwatch** can detect but not stop such attacks
3. **Switches** usually feature protections against ARP spoofing (Port Security)

## 2.4.6.1 Checking the ARP Cache

You can check the ARP cache of your host by typing:

- `arp -a` on Windows.
- `arp` on \*nix operating systems
- `ip neighbour` on Linux

```
</>
$ ip neighbour
192.168.17.202 dev eth0 lladdr d0:d4:12:e1:ef:5a STALE
192.168.17.1 dev eth0 lladdr 00:50:7f:78:fc:40 STALE
192.168.17.99 dev eth0 lladdr 00:d0:4b:92:2d:89 STALE
192.168.17.14 dev eth0 lladdr 60:a4:4c:a8:be:5b STALE
192.168.17.18 dev eth0 lladdr 20:cf:30:c7:ad:ae STALE
192.168.17.30 dev eth0 lladdr 20:cf:30:ea:22:13 STALE
192.168.17.66 dev eth0 lladdr a4:ee:57:e8:2e:0b STALE
192.168.17.254 dev eth0 lladdr c8:4c:75:a4:79:a6 REACHABLE
192.168.17.12 dev eth0 lladdr 60:a4:4c:a8:bd:1a STALE
192.168.17.19 dev eth0 lladdr 54:04:a6:a0:6e:ad STALE
192.168.17.24 dev eth0 lladdr bc:5f:f4:ef:63:51 STALE
```

## MAC Flooding

- switches store the MAC address to physical switch port pairing in their **Content Addressable Memory (CAM)** table.
  - <MAC address - port number - TTL>.
- **MAC flooding is meant to fill the CAM table of the switch.**
- When the space in the CAM is **filled** with fake MAC addresses, the **switch cannot learn new MAC addresses** so it forces switches to behave like a **hub** and then **forward frames on all the ports**.

## MAC Flooding Prevention

- **port security** (restrict the association of a port with a single source MAC address)
- Additionally, there are switches that can be configured in such a way so that acting like a hub is prohibited.

## 802.11 Wireless (layer 2) header

The types of 802.11 packets are:

- **Management:** Connectivity between hosts at layer 2 is based upon those packets.
  - Authentication packets

- Association packets
  - **Beacon** packets
  - **Control**: Delivery of packets is enabled by those packets. Congestion is also “regulated” by them.
    - Request-to-send packets
    - Clear-to-send packets
  - **Data**: Those packets are the actual data containers. They are the only packet kind that can be passed from the wireless to the wired network.
- 
- **Beacon packets** are broadcasted from a wireless access point to inform other listening wireless clients of its existence and its connection requirements.

**Beacon frame capture**

The 802.11 management frame header contains information such as:

- **Timestamp**: Packet transmission time
- **Beacon Interval**: Beacon packet retransmission time
- **Capabilities Information**: Hardware capabilities of the AP
- **SSID parameter set**: Network name broadcasted by the AP
- **Supported Rates**: Data transfer rates supported by the AP
- **DS Parameter set**: Channel on which the AP operates

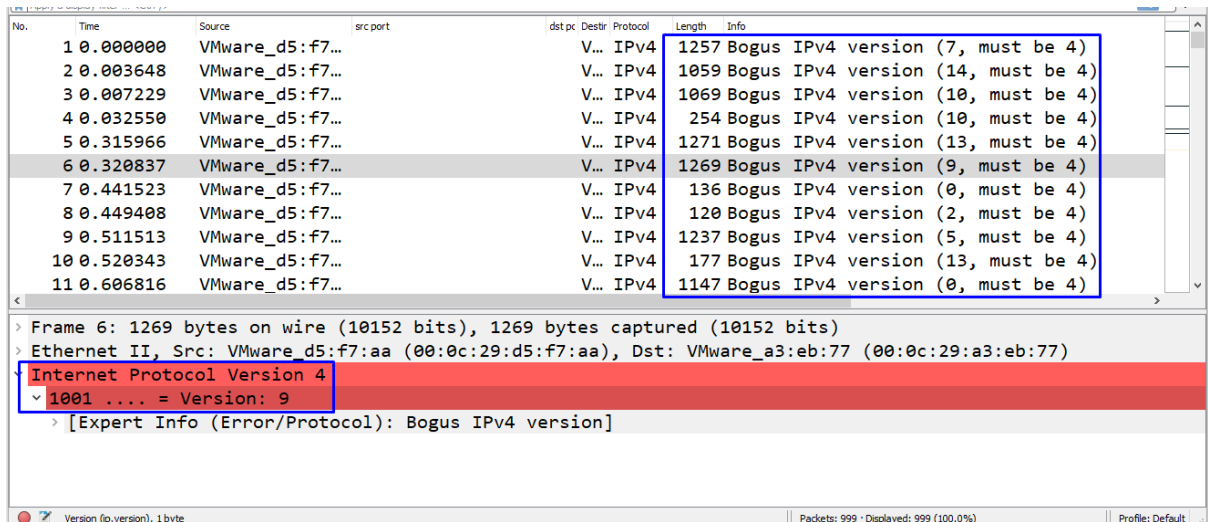
```

▶ Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
  ▼ IEEE 802.11 Beacon frame, Flags: .....
    Type/Subtype: Beacon frame (0x0008)
    Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: D-Link_0b:22:ba (00:13:46:0b:22:ba)
    Source address: D-Link_0b:22:ba (00:13:46:0b:22:ba)
    BSS Id: D-Link_0b:22:ba (00:13:46:0b:22:ba)
    .... .. 0000 = Fragment number: 0
    0101 0100 1000 .... = Sequence number: 1352
  ▼ IEEE 802.11 wireless LAN management frame
    ▼ Fixed parameters (12 bytes)
      Timestamp: 0x000000001685a181
      Beacon Interval: 0.102400 [Seconds]
      ▶ Capabilities Information: 0x0431
    ▼ Tagged parameters (96 bytes)
      ▶ Tag: SSID parameter set: ██████████
      ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 12, 24, 36, [Mbit/sec]
      ▶ Tag: DS Parameter set: Current Channel: 11
      ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
      ▶ Tag: ERP Information
      ▶ Tag: Extended Supported Rates 9, 18, 48, 54, [Mbit/sec]
      ▶ Tag: Vendor Specific: AtherosC: Advanced Capability
      ▶ Tag: Vendor Specific: AtherosC: Unknown
      ▶ Tag: Vendor Specific: AtherosC: eExtended Range
      ▶ Tag: Vendor Specific: GlobalSu
          
```

## IP Layer Attacks with each header

### IDS/Firewall Evasion (**invalid IP version**)

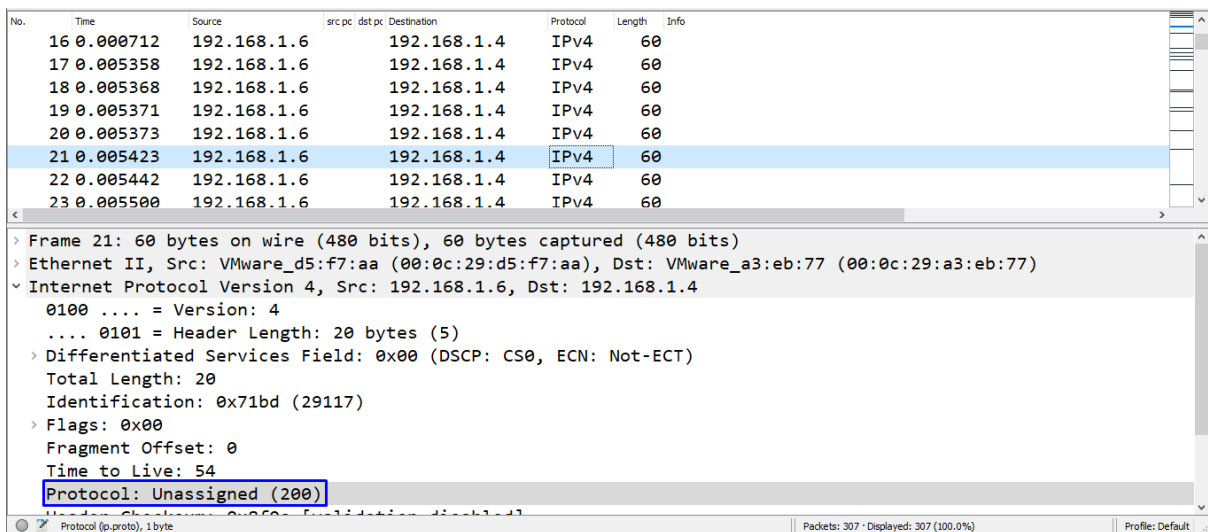
- Oftentimes, attackers check the reactions of firewalls and IDS by crafting and sending datagrams with an **invalid IP version**

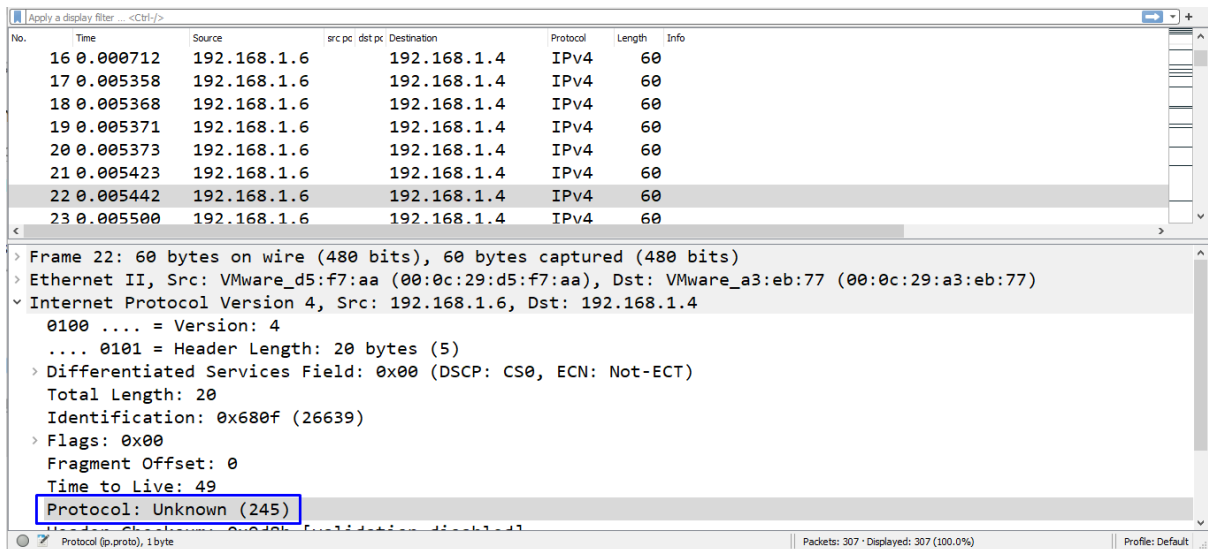


## Stealthy Nmap Scan (changing the IPv4 Protocol Number.)

<https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>

- The venerable Nmap network scanner leverages this to perform IP protocol scanning against a given target.
- This type of scanning is also a stealthier way to identify a live host.





## Source & Destination IP Addresses

- There are three golden detection rules that are related to this set of IPv4 header fields.
1. **Incoming traffic** to your network should obviously have a **Source IP Address that doesn't belong to your network address space**. If it does, it is most probably **crafted**.
  2. **Outgoing traffic** from your network should obviously have a **Source IP Address that belongs to your network address space**. If it doesn't, there is most probably a misconfiguration or the address is **spoofed**.
  3. Private network addresses or the loopback mode address also require your attention

## Fragmentation (abused for IDS/IPS evasion purposes)

- Fragmentation is the action of **dividing a packet** whose size is greater than the Maximum Transmission Unit (MTU)
- it can be performed by a **router** or the sending **host** itself.
- Each fragment's IP header contains fields and values that facilitate **reassembling** the original packet at the destination.
- When it comes to fragmented packets, IDS/IPS must act just if they were the **destination host**, in terms of **packet reassembling**. This is for obvious reasons, IDS/IPS need the **whole packet in order to inspect it**

- attackers can introduce difficulties in the reassembling procedure by the IDS/IPS, such as:
  - Crafted fragmented packets with **identical offsets** but **different payloads**
  - Crafted packets arriving with a **great time difference**
- For the IDS/IPS to safely perform such packet reassembling and inspection, it should act just like the destination host does. (wait as long as the destination does for a fragment to arrive)
- IP packet exceeding the 65535 bytes limit of data via a ping command (**ping-of-death**)

## IPv6

### IPv6 Tunneling

- It is a known fact that attackers have been using tunnelbased IPv6 transition mechanisms for hide communication and stealthy exfiltration over an IPv4-only or dual-stack network.

```

Apply a display filter ... <Ctrl-/>
No.    Time           Source                src port    dst port    Destination          Protocol  Length
---    -
6 9.829544    fe80::ffff:ffff:f...  55519      teredo      ff02::2              ICMP...   103
7 9.956850    fe80:0:7274:696e:...  teredo     55519      fe80::ffff:ff...    ICMP...   159

> Frame 7: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
> Ethernet II, Src: VMware_e1:a9:f8 (00:50:56:e1:a9:f8), Dst: VMware_60:22:18 (00:0c:29:60:2...
> Internet Protocol Version 4, Src: 83.170.6.76, Dst: 192.168.73.148
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 145
    Identification: 0x7a20 (31264)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x5c09 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 83.170.6.76
    Destination Address: 192.168.73.148
  > User Datagram Protocol, Src Port: teredo (3544), Dst Port: 55519 (55519)
  > Teredo IPv6 over UDP tunneling
    > Teredo Authentication header
      Client identifier length: 0
      Authentication value length: 0
      Nonce value: 58b1b73fc3d0859b
      Confirmation byte: 00
    > Teredo Origin Indication header
  > Internet Protocol Version 6, Src: fe80:0:7274:696e:8000:dd8:ac55:f9b3, Dst: fe80::ffff:fff...
    0110 .... = Version: 6
    > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 0000 = Flow Label: 0x000000
    Payload Length: 56
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80:0:7274:696e:8000:dd8:ac55:f9b3
  
```

## Network Discovery Attacks

- Attackers ultimately want to introduce incorrect IPv6 host address/link layer pairings; this can be achieved via two (2) distinct ways:
  - An attacker on the same local network can tamper with a returned **Neighbor Advertisement (NA)** spoofing an address, after a **Neighbor Solicitation (NS)** request is sent; this is the equivalent of **ARP poisoning in IPv4**.
  - An attacker can also craft an **NS** request containing the fake IPv6 host address/link layer pairing. Listening neighbors will introduce this not requested pairing in their neighbor cache; this is the equivalent of **abused Gratuitous ARP in IPv4**.
- Other Network Discovery attacks include:
- Causing a **DoS**, by spoofing an **NA response**, informing the NS request sender that the target host resides at a non-existing link address. The same can be

achieved by abusing the Neighbor Unreachable Protocol to send a spoofed NA response informing that communication with the target is not possible.

- Causing a **DoS**, by spoofing an **NS response**, informing that the address is taken. Recall the Duplicate Address Detection procedure. DAD could be abused multiple times to prevent a host from being assigned an address.
  - Executing a **man-in-the-middle attack**, by spoofing an RA, informing the host that sent the RS message that the attacker's host is the router.
  - Those, are only a subset of the attacks that can be executed against an IPv6 implementation. For more, please refer to the following resources:
    1. <https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf>
    2. <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Schaefer-Workshop-Slides.pdf>
    3. [https://www.tno.nl/media/3274/testing\\_the\\_security\\_of\\_ipv6\\_implementations.pdf](https://www.tno.nl/media/3274/testing_the_security_of_ipv6_implementations.pdf)
- 

## Transport Layer Attacks

### ▼ TCP - UDP Theoretical

## Transport layer (segments/datagrams)

the transport layer is the link between the application layer and the lower layers that are responsible for network transmission.

### Transport Layer Responsibilities:

1. Tracking Individual Conversations
2. Segmenting Data and Reassembling Segments
3. Add Header Information
4. Identifying the Applications
5. Conversation Multiplexing
  - a. the transport layer uses segmentation and multiplexing to enable different communication conversations to be interleaved on the same network.

## the benefits of dividing the data into segments :

- **Increases speed** - Because a large data stream is segmented into packets, large amounts of data can be sent over the network without tying up a communications link. This allows many different conversations to be interleaved on the network called multiplexing.
- **Increases efficiency** - If a single segment fails to reach its destination due to a failure in the network or network congestion, only that segment needs to be retransmitted instead of resending the entire data stream.
- TCP is responsible for sequencing the individual segments.

## TCP & UDP

### TCP

- Transmission Control Protocol. Enables reliable communication between processes running on separate hosts and provides reliable, acknowledged transmissions that confirm successful delivery. (segments) (Connection-Oriented=must first establish a connection between the sender and the receiver)

TCP provides reliability and flow control using these basic operations:

- Number and track data segments transmitted to a specific host from a specific application
- Acknowledge received data
- Retransmit any unacknowledged data after a certain amount of time
- Sequence data that might arrive in wrong order
- Send data at an efficient rate that is acceptable by the receiver

# TCP Header Fields



The table identifies and describes the ten fields in a TCP header.

TCP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Sequence Number	A 32-bit field used for data reassembly purposes.
Acknowledgment Number	A 32-bit field used to indicate that data has been received and the next byte expected from the source.
Header Length	A 4-bit field known as "data offset" that indicates the length of the TCP segment header.
Reserved	A 6-bit field that is reserved for future use.
Control bits	A 6-bit field that includes bit codes, or flags, which indicate the purpose and function of the TCP segment.
Window size	A 16-bit field used to indicate the number of bytes that can be accepted at one time.
Checksum	A 16-bit field used for error checking of the segment header and data.
Urgent	A 16-bit field used to indicate if the contained data is urgent.

The six **control bits** flags are as follows:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination

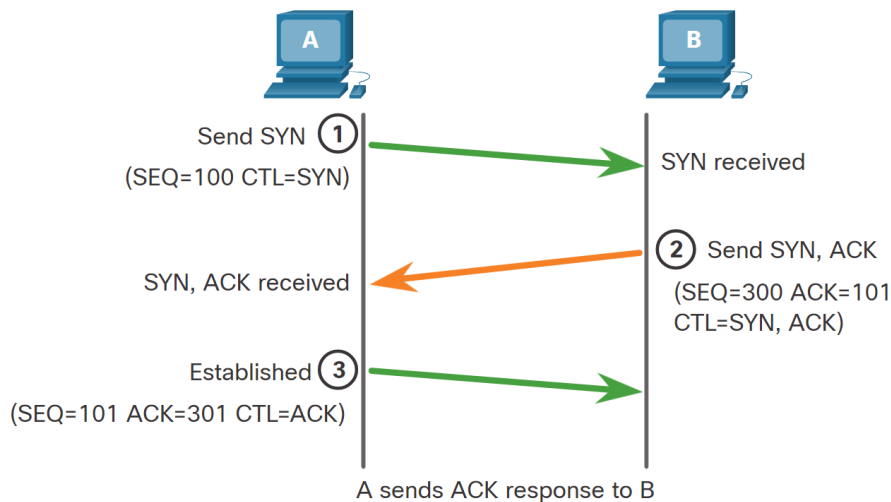
## TCP Server Processes

- Each application process running on a server is configured to use a port number.
- The port number is either automatically assigned or configured manually by a system administrator.
- An individual server cannot have two services assigned to the same port number within the same transport layer services.

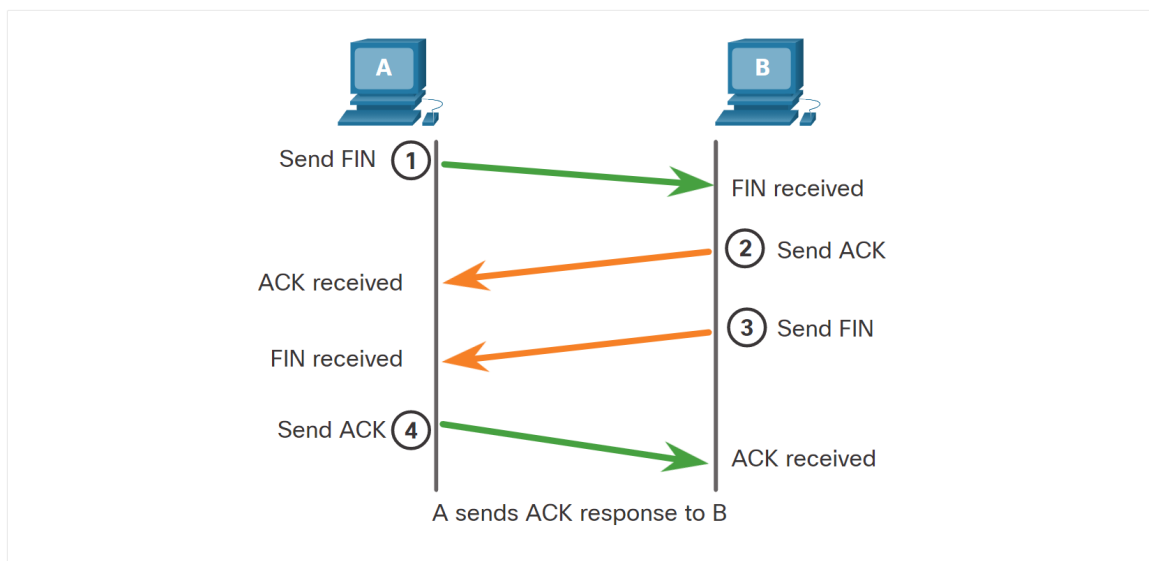
- There can be many ports open simultaneously on a server, one for each active server application.

## TCP Connection Establishment (3-way Handshake)

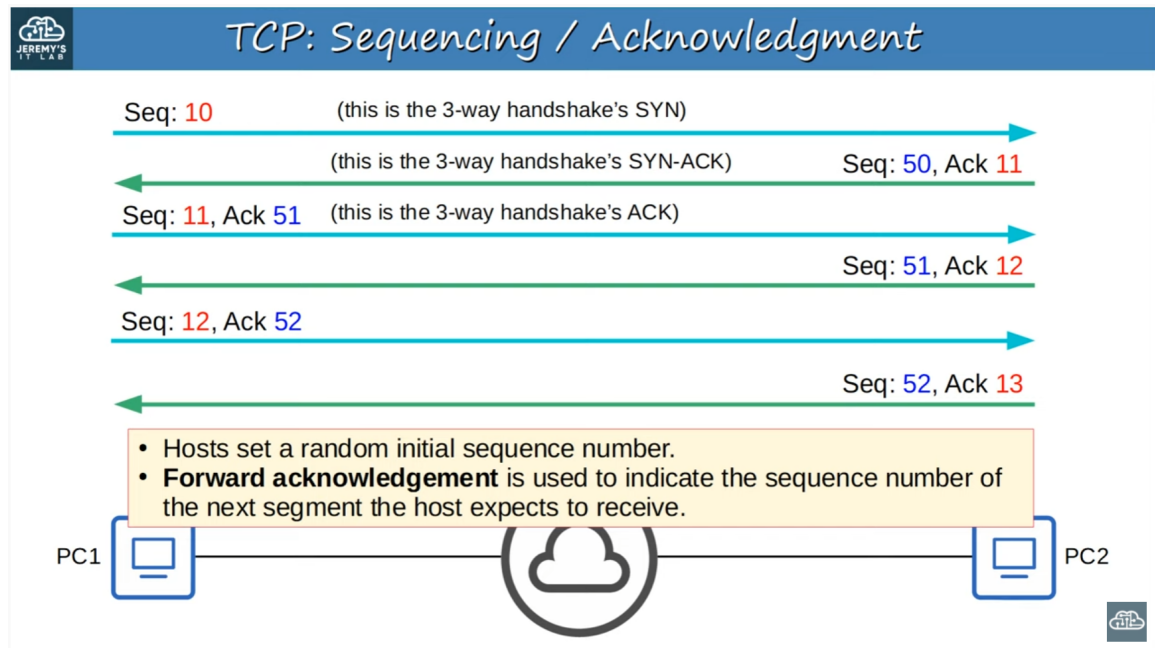
- It establishes that the destination device is present on the network.
- It verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use.
- It informs the destination device that the source client intends to establish a communication session on that port number.



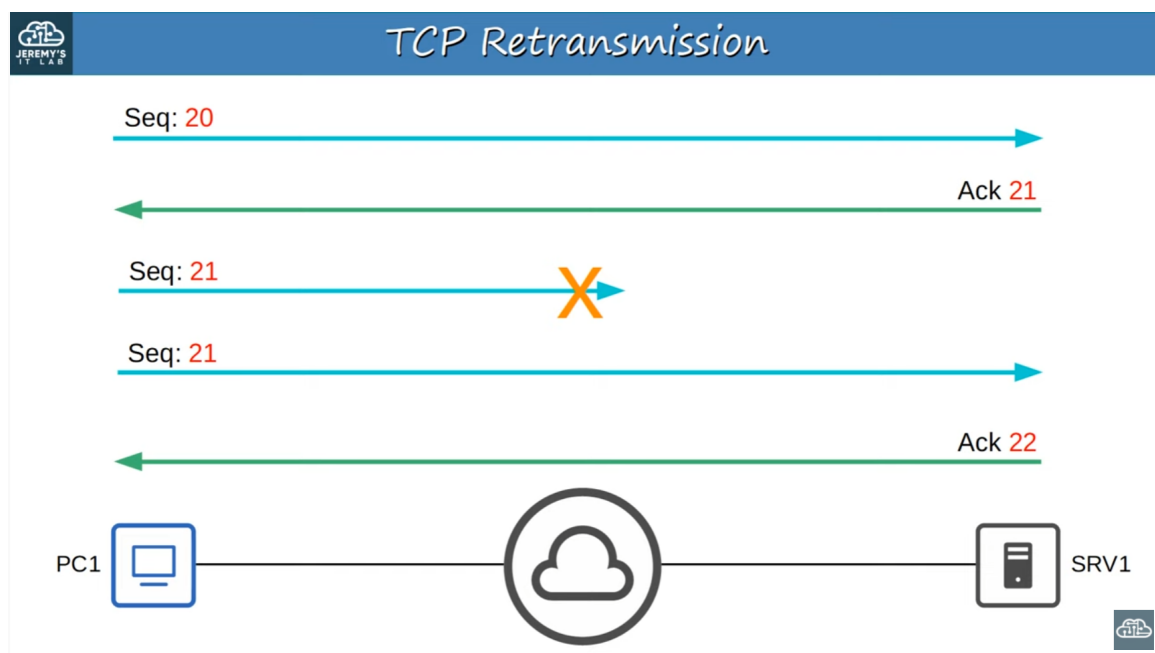
## Session Termination ( 4-way Handshake)



## TCP Reliability – Sequence Numbers and Acknowledgements



## TCP Retransmission



## TCP Flow Control - Window Size (Watch)

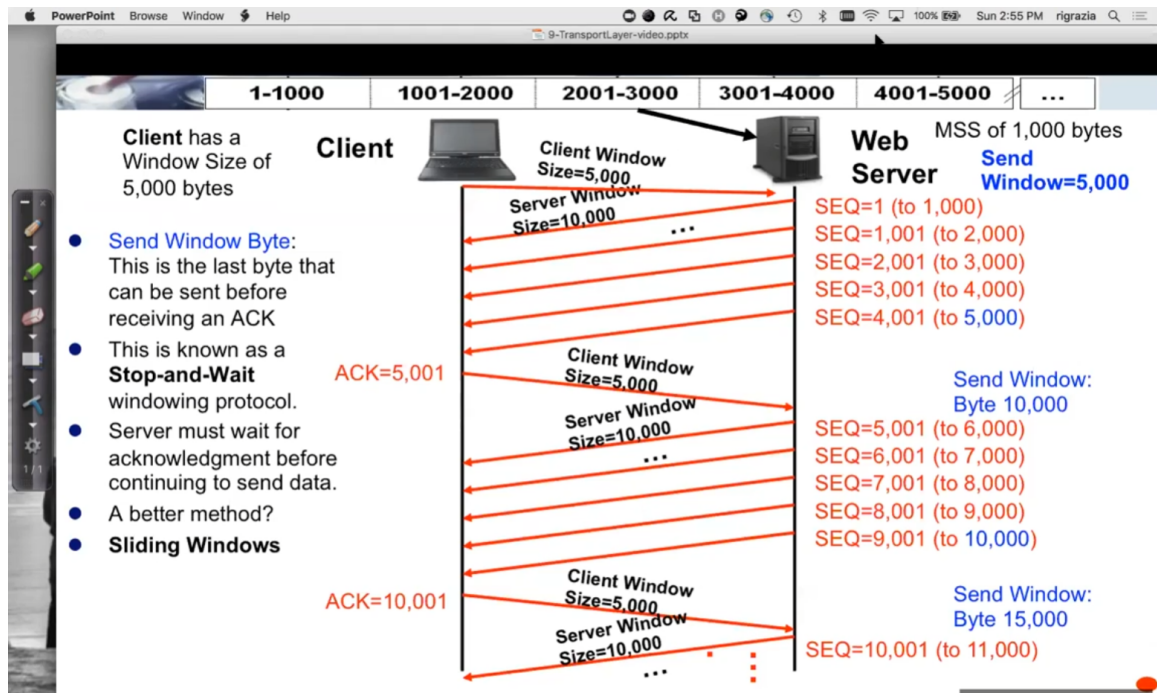
## TCP Flow Control: Window Size

- Acknowledging every single segment, no matter what size, is inefficient.
- The TCP header's **Window Size** field allows more data to be sent before an acknowledgment is required.
- A 'sliding window' can be used to dynamically adjust how large the window size is.

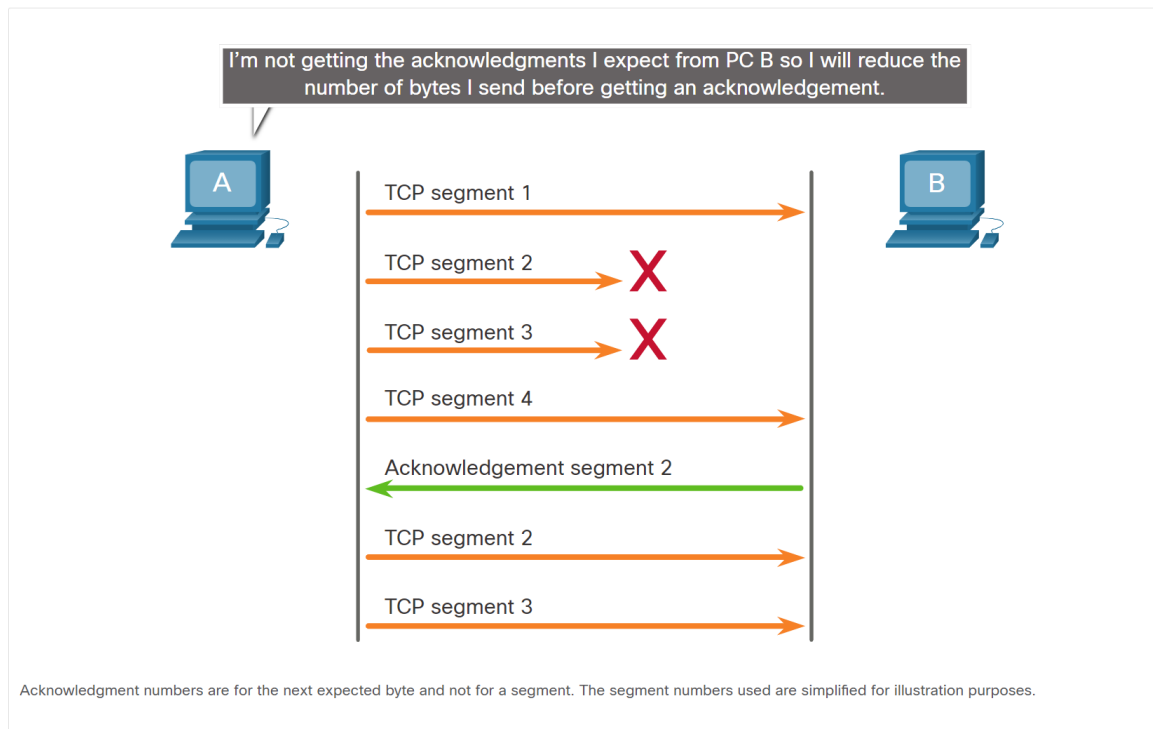


In all of these examples, I used very simple sequence numbers. In real situations, the sequence numbers get much larger and do not increase by 1 with each message. For the CCNA, just understand the concepts and don't worry about the exact numbers.

## MSS= Maximum Segment Size



## TCP Congestion Control



## UDP

- User Datagram Protocol. Enables a process running on one host to send packets to a process running on another host. However, UDP does not confirm successful datagram transmission. (**datagram**) (Connectionless)

- UDP does not provide reliability or flow control
- it does not require an established connection
- UDP is also known as a best-effort delivery protocol because there is no acknowledgment
- Live video and voice applications can tolerate some data loss with minimal or no noticeable effect, and are perfectly suited to UDP.

## UDP Header Fields



The table identifies and describes the four fields in a UDP header.

UDP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Length	A 16-bit field that indicates the length of the UDP datagram header.
Checksum	A 16-bit field used for error checking of the datagram header and data.

### Socket:

- The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket.
- The socket is used to identify the server and service being requested by the client
- The socket on a web server might be **192.168.1.7:80**
- these two sockets combine to form a socket pair: 192.168.1.5:1099, 192.168.1.7:80
  - Sockets enable multiple processes, running on a client, to distinguish themselves from each other, and multiple connections to a server process to be distinguished from each other.

### Suspicious TCP Traffic

1. **Excessive SYN** packets (scanning)
2. Usage of different **flags**
3. **Single host to multiple ports** or single host to **multiple nodes** (scanning)
4. **Source Port Abnormalities :**
  - **Privileged (server) ports [1-1023]** ← Should remain unchanged during the entire connection
  - **Unprivileged (client)/ephemeral ports [1023-65535]** ← Chosen only for **one connection**. Can be chosen again after the connection closes.

No.	Time	Source	Destination	src port	dst port	Protocol	Length
1	0.000000	192.168.1.6	192.168.1.2	36901	ms-wbt-server	TCP	58
3	0.000366	192.168.1.6	192.168.1.2	36901	smtp	TCP	58
4	0.000432	192.168.1.6	192.168.1.2	36901	ms-wbt-server	TCP	54
5	0.000671	192.168.1.6	192.168.1.2	36901	epmap	TCP	58
6	0.000906	192.168.1.6	192.168.1.2	36901	mysql	TCP	58
7	0.000973	192.168.1.6	192.168.1.2	36901	netbios-ssn	TCP	58
8	0.001115	192.168.1.6	192.168.1.2	36901	sunrpc	TCP	58
9	0.001821	192.168.1.6	192.168.1.2	36901	imap	TCP	58
12	0.002144	192.168.1.6	192.168.1.2	36901	epmap	TCP	54
13	0.002149	192.168.1.6	192.168.1.2	36901	netbios-ssn	TCP	54
14	0.002297	192.168.1.6	192.168.1.2	36901	pftp	TCP	58
15	0.002404	192.168.1.6	192.168.1.2	36901	https	TCP	58
16	0.002467	192.168.1.6	192.168.1.2	36901	imaps	TCP	58
17	0.005389	192.168.1.6	192.168.1.2	36901	rtsp	TCP	58
18	0.005502	192.168.1.6	192.168.1.2	36901	h323hostcall	TCP	58
19	0.005565	192.168.1.6	192.168.1.2	36901	http-alt	TCP	58
20	0.005663	192.168.1.6	192.168.1.2	36901	ftp	TCP	58

> Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)  
 > Ethernet II, Src: VMware\_d5:f7:aa (00:0c:29:d5:f7:aa), Dst: HewlettP\_c4:7b:f4 (d4:85:64:  
 > Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.2  
 > Transmission Control Protocol, Src Port: 36901 (36901), Dst Port: ms-wbt-server (3389),

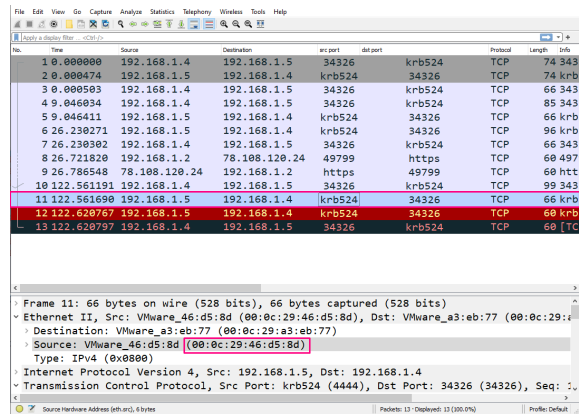
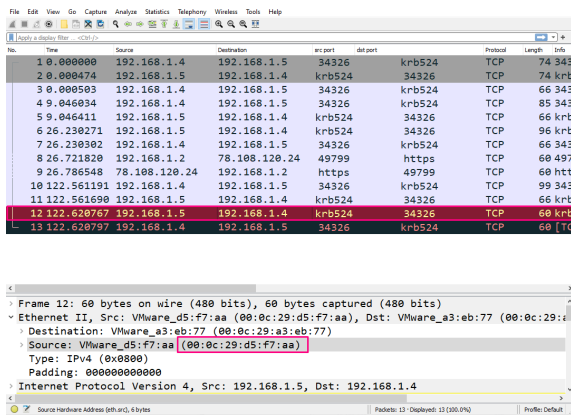
- If you carefully look at packets , you will notice that the host 192.168.1.6 uses the same source port (36901) for multiple connection attempts to different ports of the remote host. This is abnormal.

## 5. Sequence Number Prediction & SYN Scanning

- One of the ways using which the venerable **Nmap** tool tries to perform **OS fingerprinting**, is by examining the Initial **Sequence Numbers (ISNs)** generated by the target host (after connections are being attempted to a listening port).
- Each TCP/IP stack (and subsequently each OS) features **its own way of generating Initial Sequence Numbers**.
- Nmap repeatedly used the **ISN** from the scanning host, while scanning **the different ports of the remote host**.
  - **Unique ISNs should be used**, when attempting to connect to **different ports of a remote host**.



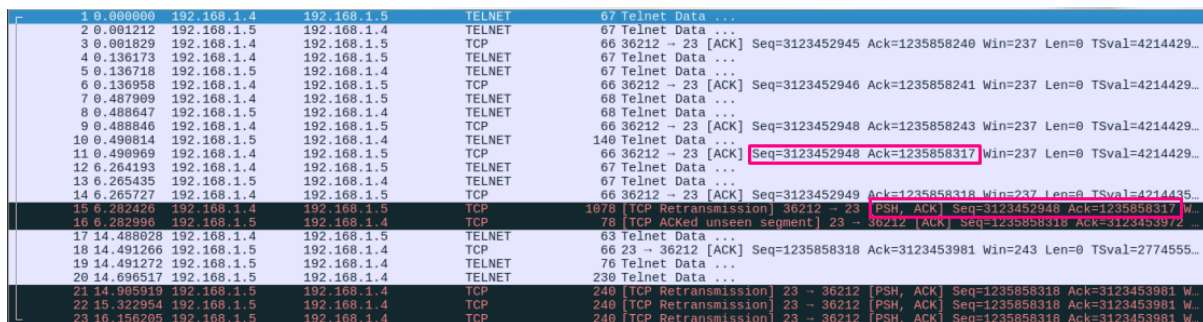
- Source & Destination IP
- “correct” Sequence Number



- the attacker spoofed the src ip and sent a TCP RST packet to the server ti cut the connection.

## 7. TCP Session Hijacking

- TCP is defenseless against “packet injection” attacks.
- An attacker could choose to hijack a whole TCP session, instead of executing a simple TCP RST attack. (requires the same prior knowledge as the TCP RST attack.)



- Telnet offers no encryption and thus, we can see every command the client issued and every result returned by the server in clear text.
- Let’s analyze packet #15.
  - TCP Retransmission is displayed because the sequence number and the acknowledgement number of this packet are the same as the ones in packet #11.

- The MAC address of the client (192.168.1.4) in packet #15 (**attacker**) is different than the MAC address that is included in all previous packets related to this host.
- It looks like an attacker has taken over (hijacked) the whole Telnet session.
- This is also apparent in packet #17, that includes the MAC address of the attacker and the command the attacker issued (uname -a)
- The server has no defense mechanism to detect that the Telnet session is hijacked and sends the output of the uname -a command back to the 192.168.1.4 client.

```

.....uname
uname -a
Linux kali 4.13.0-kali1-amd64 #1 SMP Debian 4.13.10-1kali2 (2017-11-08) x86_64 GNU/Linux
.]0;administrator@kali: ~.[01;31madministrator@kali.[00m:.[01;34m~.[00m$

```

## 8. TCP Timestamps Option

the TCP Timestamps options can be abused in order to:

1. Determine the **patch level of a system**, through uptime analysis
2. Perform **host identification** using clock skew
3. Identify how a target **DMZ is structured**

<https://www.scip.ch/en/?labs.20150305>

## 9. Leveraging TCP Option Support & Ordering

- TCP/IP stacks, support a subset of the available TCP options and also, perform TCP option storing in their own unique order. Nmap leverages the above (and other things), in order to perform **OS fingerprinting**.

<https://nmap.org/nmap-fingerprinting-article.txt>

# UDP-based attacks

DNS Command & Control, DNS exfiltration (to be discussed)

---

## ICMP Abuse

1. **ICMP Echo Request (8)**

- To map live hosts
- most sites nowadays disallow inbound and/or outbound ICMP echo requests.

## 2. ICMP Address Mask Request(17)/Reply(18)

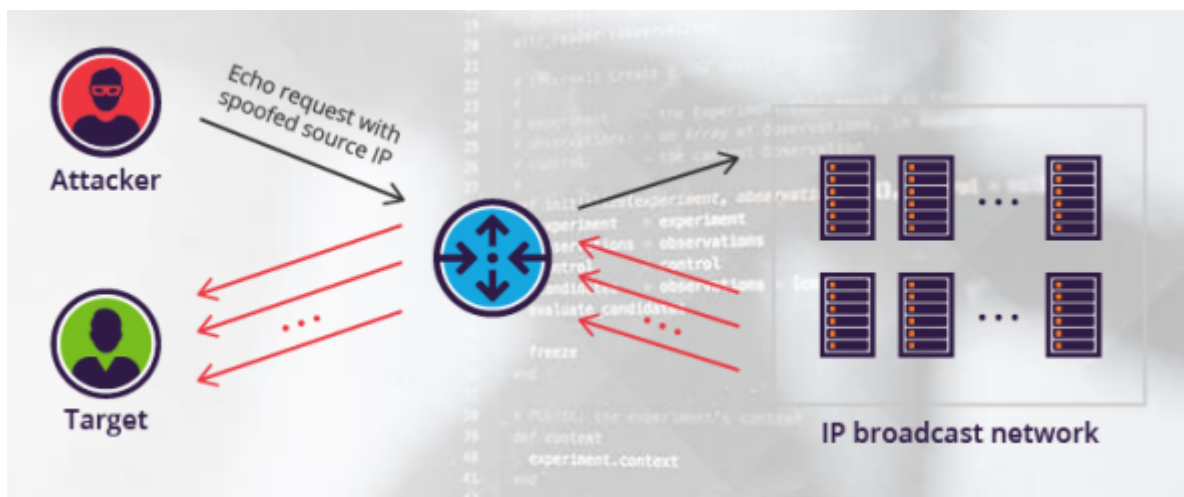
- can be used to identify a target host's subnet mask.

## 3. ICMP Timestamp Request(13)/Reply (14)

- can be used to obtain **timestamps** from remote systems.
- used in zero days attack to see if the system got patched

## 4. Smurf Attack(DDoS)

- is executed as follows:
  1. the attacker sends fake echo requests to an intermediate ip broadcast network with a spoofed src ip of the target
  2. the requests is transmitted to all of the network hosts on the network
  3. all hosts on the network will send an ICMP echo reply to the target server causing it to get down



## 5. ICMP Tunneling

- ICMP can be misused to create a **covert channel of communication**. This can be achieved through ill-intended ICMP tunneling
- Numerous ICMP tunneling solutions exists, but attackers seem to prefer the **ptunnel** one.



table so that it uses the shortest path.

- such ICMP redirect packets can be forged by an attacker and make the sender host redirect its packet to an **attacker-controlled** or non-existing destination.

The image shows a Wireshark packet capture. The top part is a packet list table with columns for No., Time, Source, Destination, Protocol, and Length. It shows a series of ICMP Redirect packets (Type 5, Code 1) from 10.100.13.1 to 10.100.13.126. The bottom part is a packet details pane for the selected packet (No. 3), showing Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (Type 5, Code 1, Gateway address: 10.100.13.20).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	72:9b:2f:a0:90:...	Broadcast	ARP	60	Who has 10.100.13.126? Tell 10.100.13.20
2	0.000022	Vmware_a1:cb:34	72:9b:2f:a0:90:91	ARP	42	10.100.13.126 is at 00:50:56:a1:cb:34
3	0.251032	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
4	0.333845	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
5	0.397539	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
6	0.468985	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
7	0.555181	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
8	0.637849	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
9	0.722346	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
10	0.811009	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
11	0.900367	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)
12	0.968061	10.100.13.1	10.100.13.126	ICMP	82	Redirect (Redirect for host)

Frame 3: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)  
Ethernet II, Src: 72:9b:2f:a0:90:91 (72:9b:2f:a0:90:91), Dst: Vmware\_a1:cb:34 (00:50:56:a1:cb:34)  
Internet Protocol Version 4, Src: 10.100.13.1, Dst: 10.100.13.126  
Internet Control Message Protocol  
Type: 5 (Redirect)  
Code: 1 (Redirect for host)  
Checksum: 0x3dfe [correct]  
[Checksum Status: Good]  
Gateway address: 10.100.13.20  
Internet Protocol Version 4, Src: 10.100.13.126, Dst: 10.23.56.100  
Transmission Control Protocol, Src Port: 55555, Dst Port: 80

- A large number of ICMP Redirect packets exist.
- In those packets the router instructs the client **10.100.13.126** to make a change in its routing table to use
- the gateway 10.100.13.20 for all subsequent packets. At this moment, you should check if the gateway 10.100.13.20 is a legitimate gateway.
- If you filter the whole capture file, based on the MAC address of the router (**10.100.13.1**) [eth.src==72:9b:2f:a0:90:91], you will notice that this MAC address is associated with the **10.100.13.20** machine.
- Even though it is not clearly visible in the capture file, every HTTP request can now be sniffed by the 10.100.13.20 host, as a result of the ICMP Redirect attack.

## Application Layer

### Network Basic Input/Output System NetBIOS

- a set of protocols developed in for Windows only in order to provide services for the session layer

#### NetBIOS provides three services :

1. **(NBNS)** Name service (works over **UDP** port **137**) for **name registration** and **name to IP** address resolution.

- a. it was later replaced by **DNS**
- 2. **(NBDS) Datagram** distribution service (works over **UDP** port **138**) for **service announcements** by clients and servers.
- 3. **(NBSS) Session** service (works over **TCP** port **139**) for **session negotiation between hosts**. This is used for **accessing files, opening directories**, and so on.
- There are additional protocols such as Server Message Block (**SMB**)

## SMB

- a protocol that is used for browsing directories, copying files, accessing services such as printers, and several other operations over the network
- SMB runs on top of the **session layer** protocols such as **NetBIOS** as originally designed
  - can also run directly over **TCP** port **445**
- Common Internet File System (**CIFS**) is a form, or flavor, of SMB.

## Detection

- **SMB works in a client-server model**
- Code **0** means **STATUS\_OK**, which implies that everything works fine and there is no problem. Any other code should be examined.

203.12.106.10	SMB	93	NT Trans Response, FID: 0x0001, NT NOTIFY, Error: STATUS_CANCELLED
203.12.106.10	SMB	478	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
203.12.106.10	SMB	93	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
203.12.106.10	SMB	478	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
203.12.106.10	SMB	93	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
203.12.106.10	SMB	478	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
203.12.106.10	SMB	93	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
203.12.106.14	SMB	93	Trans2 Response, GET_DFS_REFERRAL, Error: STATUS_NO_SUCH_DEVICE
203.12.106.14	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED

- **NULL session** : **anonymous** and passwordless **authentication**, if allowed it could be used to execute various **RPC** calls and subsequently perform information gathering or user enumeration.

TCP	57500 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=969964135 TSecr=
TCP	445 → 57500 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSva
TCP	57500 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=969964135 TSecr=1641308
SMB	Negotiate Protocol Request
SMB	Negotiate Protocol Response
TCP	57500 → 445 [ACK] Seq=54 Ack=118 Win=29312 Len=0 TSval=969964135 TSecr=1641308
SMB	Session Setup AndX Request, User anonymous
SMB	Session Setup AndX Response
SMB	Tree Connect AndX Request, Path: \\192.168.57.105\IPC\$
SMB	Tree Connect AndX Response
SMB	NT Create AndX Request, FID: 0x4000, Path: \samr
SMB	NT Create AndX Response, FID: 0x4000
DCERPC	Bind: call_id: 1094795585, Fragment: Single, 1 context items: SAMR V1.0 (32bit NDR
SMB	Write AndX Response, FID: 0x4000, 72 bytes
SMB	Read AndX Request, FID: 0x4000, 2048 bytes at offset 0
DCERPC	Bind_ack: call_id: 1094795585, Fragment: Single, max_xmit: 2048 max_recv: 2048, 1
SAMR	Connect4 request
SMB	Write AndX Response, FID: 0x4000, 84 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	Connect4 response
SAMR	EnumDomains request
SMB	Write AndX Response, FID: 0x4000, 52 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	EnumDomains response
SAMR	LookupDomain request, User-PC[Long frame (2 bytes)]
SMB	Write AndX Response, FID: 0x4000, 80 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	LookupDomain response
SAMR	OpenDomain request
SMB	Write AndX Response, FID: 0x4000, 76 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	OpenDomain response
SAMR	QueryDisplayInfo request
SMB	Write AndX Response, FID: 0x4000, 60 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	QueryDisplayInfo response
SAMR	Close request
SMB	Write AndX Response, FID: 0x4000, 44 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	Close response
SAMR	Close request
SMB	Write AndX Response, FID: 0x4000, 44 bytes
SMB	Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR	Close response
SMB	Tree Disconnect Request
SMB	Tree Disconnect Response
SMB	Logoff AndX Request
SMB	Logoff AndX Response
TCP	57500 → 445 [FIN, ACK] Seq=1943 Ack=2587 Win=35328 Len=0 TSval=969964141 TSecr=164

## MSRPC

- RPC (Remote Procedure Call) mechanism allows an application to seamlessly invoke remote procedures, as if these procedures were executed locally
- MSRPC is the Microsoft implementation of the **DCE RPC** mechanism.
- **File operations** utilize **SMB/CIFS**, whereas **administrative operations**, **resource management** operations etc. utilize **MSRPC**.

### There are multiple MSRPC implementations:

- RPC over **SMB**
- DCOM (RPC **directly over TCP/UDP**) [TCP/UDP port 135]

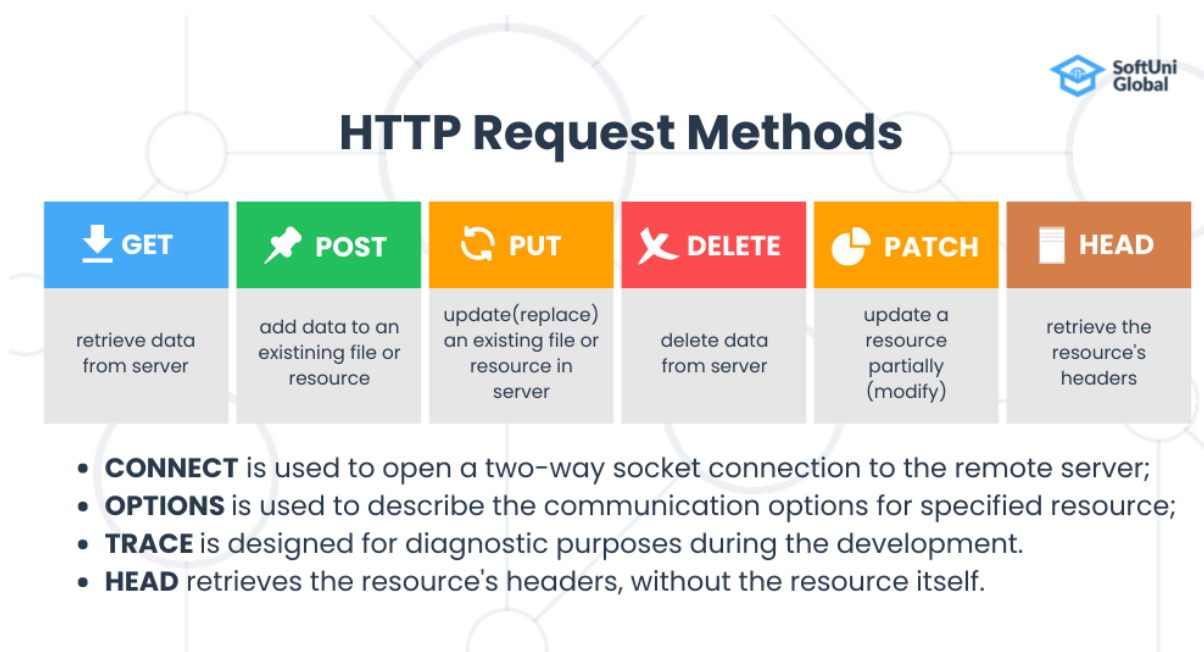
No.	Time	Source	Destination	src port	dst port	Protocol	Length	Info
129	13.162956	192.168.52.61	192.168.52.10	49168	135	TCP	66	66 49168 → 135 [SYN] Seq=1270918437 Win=8192
130	13.163090	192.168.52.10	192.168.52.61	135	49168	TCP	66	66 135 → 49168 [SYN, ACK] Seq=582498090 Ack=
131	13.163230	192.168.52.61	192.168.52.10	49168	135	TCP	54	54 49168 → 135 [ACK] Seq=1270918438 Ack=5824
132	13.165417	192.168.52.61	192.168.52.10	49168	135	DCERPC	214	214 Bind: call_id: 2, Fragment: Single, 3 con
133	13.165587	192.168.52.10	192.168.52.61	135	49168	DCERPC	162	162 Bind_ack: call_id: 2, Fragment: Single, m
134	13.165875	192.168.52.61	192.168.52.10	49168	135	EPM	210	210 Map request, DRSUAPI, 32bit NDR
135	13.166136	192.168.52.10	192.168.52.61	135	49168	EPM	206	206 Map response, DRSUAPI, 32bit NDR
167	13.369138	192.168.52.61	192.168.52.10	49168	135	TCP	54	54 49168 → 135 [ACK] Seq=1270918754 Ack=5824
195	16.136993	192.168.52.61	192.168.52.10	49168	135	EPM	210	210 Map request, DRSUAPI, 32bit NDR
196	16.137415	192.168.52.10	192.168.52.61	135	49168	EPM	206	206 Map response, DRSUAPI, 32bit NDR
230	16.333563	192.168.52.61	192.168.52.10	49168	135	TCP	54	54 49168 → 135 [ACK] Seq=1270918910 Ack=5824

Frame 130: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 > Ethernet II, Src: RealtekU\_0a:70:f7 (52:54:00:0a:70:f7), Dst: RealtekU\_c6:63:ca (52:54:00:c6:63:ca)  
 > Internet Protocol Version 4, Src: 192.168.52.10, Dst: 192.168.52.61  
 > Transmission Control Protocol, Src Port: epmap (135), Dst Port: 49168 (49168), Seq: 582498090, Ack: 1270918438, Len: 0

- RPC over HTTP or HTTPS [TCP/UDP port 593]

## HTTP

- HTTP uses methods to perform various operations.
  - Not all methods will be permitted by web server.



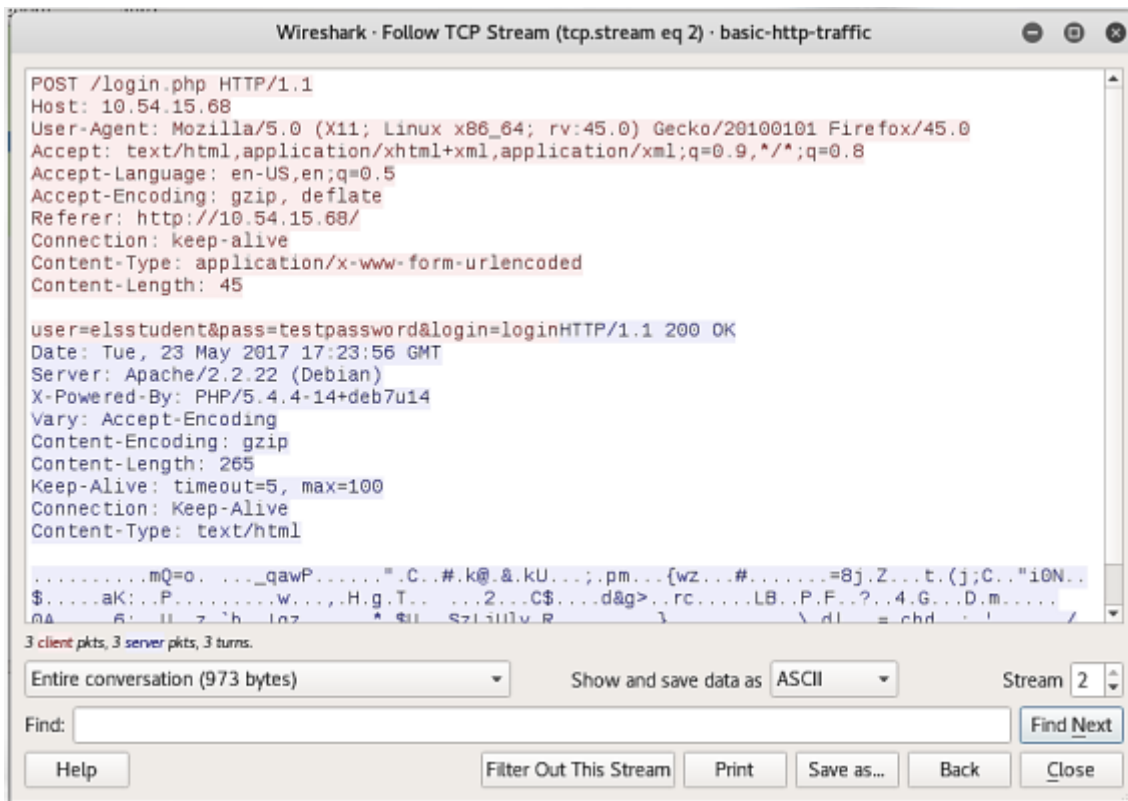
## Normal vs Suspicious HTTP Traffic

Normal HTTP Traffic	Suspicious HTTP Traffic
Port 80, TCP Port 8080, TCP (used as alternate) Port 8088, TCP (used as alternate)	Malicious binaries (backdoors), scripts, <u>web shells</u> , etc. will use this port because typically in all corporate environments the port is open.
<u>Plaintext</u> traffic	If the traffic is <u>encrypted</u> then most likely it's being used for malicious traffic. Malicious traffic can be in plaintext as well.
Web server typically in FQDN format.	Server will point to an <u>IP address</u> instead of FQDN format.

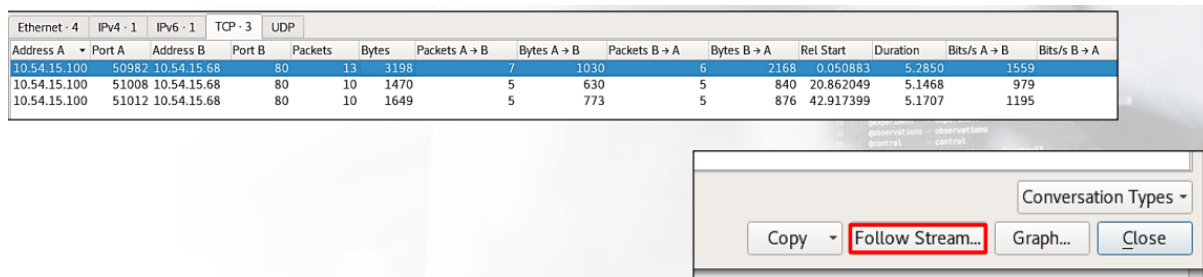
### Normal HTTP Traffic example:

Time	Source	Destination	Protocol	Length	Info
3 0.0508829...	10.54.15...	10.54.15...	TCP	74	50982 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK
5 0.0965761...	10.54.15...	10.54.15...	TCP	74	80 → 50982 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MS
6 0.0966111...	10.54.15...	10.54.15...	TCP	66	50982 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2
7 0.0968141...	10.54.15...	10.54.15...	HTTP	347	GET / HTTP/1.1
8 0.1469519...	10.54.15...	10.54.15...	TCP	66	80 → 50982 [ACK] Seq=1 Ack=282 Win=15552 Len=0 TSval=
9 0.1809993...	10.54.15...	10.54.15...	HTTP	654	HTTP/1.1 200 OK (text/html)

- We are seeing 6 packets (4 relating to TCP and 2 relating to HTTP).
  - Packets **3-6** is the **TCP Handshake**. HTTP relies on TCP for reliability.
  - Packet **7** we notice a **HTTP method (GET)**.
  - Packet **9** we notice a **HTTP response code (200 OK)**.
  - port **80** is used
- we can see the content of the HTTP Stream with **Follow** -> **Follow TCP Stream**



- or **Select Statistics -> Conversations** Under the **TCP** tab in Conversations we can see there are 3 TCP Streams. From here we can select a stream and choose Follow Stream from bottom right corner.



## Malicious HTTP Traffic Example

- The attacker is attempting sql injection manually

Source	Destination	Protocol	Length	Info
10.124.211.200	10.124.211.96	HTTP	373	GET /newsdetails.php?id=26%27 HTTP/1.1
10.124.211.96	10.124.211.200	TCP	1391	[TCP segment of a reassembled PDU]
10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1258 Ack=6640 Win=44800 Len=0 TSval=127992 TSecr=224575
10.124.211.96	10.124.211.200	HTTP	68	HTTP/1.1 200 OK (text/html)
10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1258 Ack=6642 Win=44800 Len=0 TSval=127992 TSecr=224575
10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [FIN, ACK] Seq=6642 Ack=1258 Win=18768 Len=0 TSval=225826 TSecr=127992
10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [FIN, ACK] Seq=1258 Ack=6643 Win=44800 Len=0 TSval=129243 TSecr=225826
10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [ACK] Seq=6643 Ack=1259 Win=18768 Len=0 TSval=225842 TSecr=129243
10.124.211.200	10.124.211.96	TCP	74	33022 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=129973 TSecr=0
10.124.211.96	10.124.211.200	TCP	74	80 → 33022 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=226572 TSecr=0
10.124.211.200	10.124.211.96	TCP	66	33022 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=129989 TSecr=226572
10.124.211.200	10.124.211.96	HTTP	389	GET /newsdetails.php?id=26%20and%201=1;--%20- HTTP/1.1
10.124.211.96	10.124.211.200	TCP	66	80 → 33022 [ACK] Seq=1 Ack=324 Win=15552 Len=0 TSval=226590 TSecr=129989
10.124.211.96	10.124.211.200	TCP	84	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
10.124.211.200	10.124.211.96	TCP	78	[TCP Window Update] 33022 → 80 [ACK] Seq=324 Ack=1 Win=30336 Len=0 TSval=130008 TSecr=0
10.124.211.96	10.124.211.200	TCP	1391	[TCP Out-Of-Order] 80 → 33022 [ACK] Seq=1 Ack=324 Win=15552 Len=1325 TSval=226591 TSecr=0
10.124.211.200	10.124.211.96	TCP	66	33022 → 80 [ACK] Seq=324 Ack=1344 Win=33280 Len=0 TSval=130008 TSecr=226591
10.124.211.96	10.124.211.200	TCP	66	80 → 33022 [FIN, ACK] Seq=324 Ack=1344 Win=33280 Len=0 TSval=131258 TSecr=226591
10.124.211.200	10.124.211.96	TCP	66	80 → 33022 [ACK] Seq=1344 Ack=324 Win=15552 Len=0 TSval=227842 TSecr=130008
10.124.211.96	10.124.211.200	TCP	66	33022 → 80 [ACK] Seq=325 Ack=1345 Win=33280 Len=0 TSval=227842 TSecr=227842
10.124.211.200	10.124.211.96	TCP	66	80 → 33022 [ACK] Seq=1345 Ack=325 Win=15552 Len=0 TSval=227852 TSecr=131258
10.124.211.96	10.124.211.200	TCP	74	33024 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=131888 TSecr=0
10.124.211.200	10.124.211.96	TCP	74	80 → 33024 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=228481 TSecr=0
10.124.211.96	10.124.211.200	TCP	66	33024 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=131898 TSecr=228481
10.124.211.200	10.124.211.96	HTTP	389	GET /newsdetails.php?id=26%20and%201=2;--%20- HTTP/1.1
10.124.211.96	10.124.211.200	TCP	66	80 → 33024 [ACK] Seq=1 Ack=324 Win=15552 Len=0 TSval=228492 TSecr=131899
10.124.211.96	10.124.211.96	HTTP	1285	HTTP/1.1 200 OK (text/html)
10.124.211.200	10.124.211.96	TCP	66	33024 → 80 [ACK] Seq=324 Ack=1220 Win=32128 Len=0 TSval=131910 TSecr=228493
10.124.211.200	10.124.211.96	TCP	66	33024 → 80 [FIN, ACK] Seq=324 Ack=1220 Win=32128 Len=0 TSval=133160 TSecr=228493

- By further inspection in packet #20, we see that the **User-Agent** is **Firefox** and the OS is **Linux**

```

▶ Frame 20: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits)
▶ Ethernet II, Src: 1a:3a:46:bf:43:91 (1a:3a:46:bf:43:91), Dst: Vmware_a1:4e:f0 (00:50:56:a1:4e:f0)
▶ Internet Protocol Version 4, Src: 10.124.211.200, Dst: 10.124.211.96
▶ Transmission Control Protocol, Src Port: 33020, Dst Port: 80, Seq: 951, Ack: 5315, Len: 307
▼ Hypertext Transfer Protocol
  ▶ GET /newsdetails.php?id=26%27 HTTP/1.1\r\n
    Host: 10.124.211.96\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://10.124.211.96/newsdetails.php?id=26%27]
    [HTTP request 4/4]
    [Prev request in frame: 15]
    [Response in frame: 23]

```

- Strangely, packet #56, and the packet after that, packet #73, don't seem to contain any SQL injection queries. Maybe he quit?

Time	Source	Destination	Protocol	Length	Info
56.34.163959	10.124.211.200	10.124.211.96	HTTP	266	GET /newsdetails.php?id=1 HTTP/1.1
57.34.169322	10.124.211.96	10.124.211.200	TCP	74	80 → 33028 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=230739 TSecr=134145 WS=4
58.34.169364	10.124.211.200	10.124.211.96	TCP	66	33028 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=134156 TSecr=230739
59.34.180457	10.124.211.200	10.124.211.96	TCP	74	33030 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=134158 TSecr=0 WS=128
60.34.202983	10.124.211.96	10.124.211.200	TCP	66	80 → 33026 [ACK] Seq=1 Ack=201 Win=15552 Len=0 TSval=230747 TSecr=134154
61.34.206414	10.124.211.96	10.124.211.200	TCP	1391	[TCP segment of a reassembled PDU]
62.34.206432	10.124.211.200	10.124.211.96	TCP	66	33026 → 80 [ACK] Seq=201 Ack=1326 Win=32128 Len=0 TSval=134165 TSecr=230748
63.34.206495	10.124.211.96	10.124.211.200	HTTP	82	HTTP/1.1 200 OK (text/html)
64.34.206501	10.124.211.200	10.124.211.96	TCP	66	33026 → 80 [ACK] Seq=201 Ack=1342 Win=32128 Len=0 TSval=134165 TSecr=230748
65.34.206508	10.124.211.96	10.124.211.200	TCP	66	80 → 33026 [FIN, ACK] Seq=1342 Ack=201 Win=15552 Len=0 TSval=230748 TSecr=134154
66.34.207131	10.124.211.200	10.124.211.96	TCP	66	33026 → 80 [FIN, ACK] Seq=201 Ack=1343 Win=32128 Len=0 TSval=134165 TSecr=230748
67.34.218945	10.124.211.96	10.124.211.200	TCP	74	80 → 33030 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=230751 TSecr=134158 WS=4
68.34.218972	10.124.211.200	10.124.211.96	TCP	66	33030 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=134168 TSecr=230751
69.34.230922	10.124.211.200	10.124.211.96	TCP	74	33032 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=134171 TSecr=0 WS=128
70.34.249217	10.124.211.96	10.124.211.200	TCP	66	80 → 33026 [ACK] Seq=1343 Ack=202 Win=15552 Len=0 TSval=230759 TSecr=134165
71.34.269905	10.124.211.96	10.124.211.200	TCP	74	80 → 33032 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=230764 TSecr=134171 WS=4
72.34.269934	10.124.211.200	10.124.211.96	TCP	66	33032 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=134181 TSecr=230764
73.35.126264	10.124.211.200	10.124.211.96	HTTP	266	GET /newsdetails.php?id=1 HTTP/1.1
74.35.126569	10.124.211.96	10.124.211.200	TCP	74	33034 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=134395 TSecr=0 WS=128
75.35.166226	10.124.211.96	10.124.211.200	TCP	66	80 → 33028 [ACK] Seq=1 Ack=201 Win=15552 Len=0 TSval=230988 TSecr=134395
76.35.166267	10.124.211.96	10.124.211.200	TCP	66	80 → 33034 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=230988 TSecr=134395 WS=4
77.35.166341	10.124.211.200	10.124.211.96	TCP	66	33034 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=134405 TSecr=230988
78.35.166806	10.124.211.96	10.124.211.200	TCP	1391	[TCP segment of a reassembled PDU]
79.35.166835	10.124.211.200	10.124.211.96	TCP	66	33028 → 80 [ACK] Seq=201 Ack=1326 Win=32128 Len=0 TSval=134405 TSecr=230988
80.35.166826	10.124.211.96	10.124.211.200	HTTP	82	HTTP/1.1 200 OK (text/html)
81.35.166943	10.124.211.200	10.124.211.96	TCP	66	33028 → 80 [ACK] Seq=201 Ack=1342 Win=32128 Len=0 TSval=134405 TSecr=230988
82.35.166962	10.124.211.96	10.124.211.200	TCP	66	80 → 33028 [FIN, ACK] Seq=1342 Ack=201 Win=15552 Len=0 TSval=230988 TSecr=134395
83.35.170154	10.124.211.200	10.124.211.96	TCP	66	33028 → 80 [FIN, ACK] Seq=201 Ack=1343 Win=32128 Len=0 TSval=134406 TSecr=230988

- taking a closer look we found out that The User-Agent for this HTTP GET Request is **Sqlmap**. So the attacker didn't quit, he **escalated**.

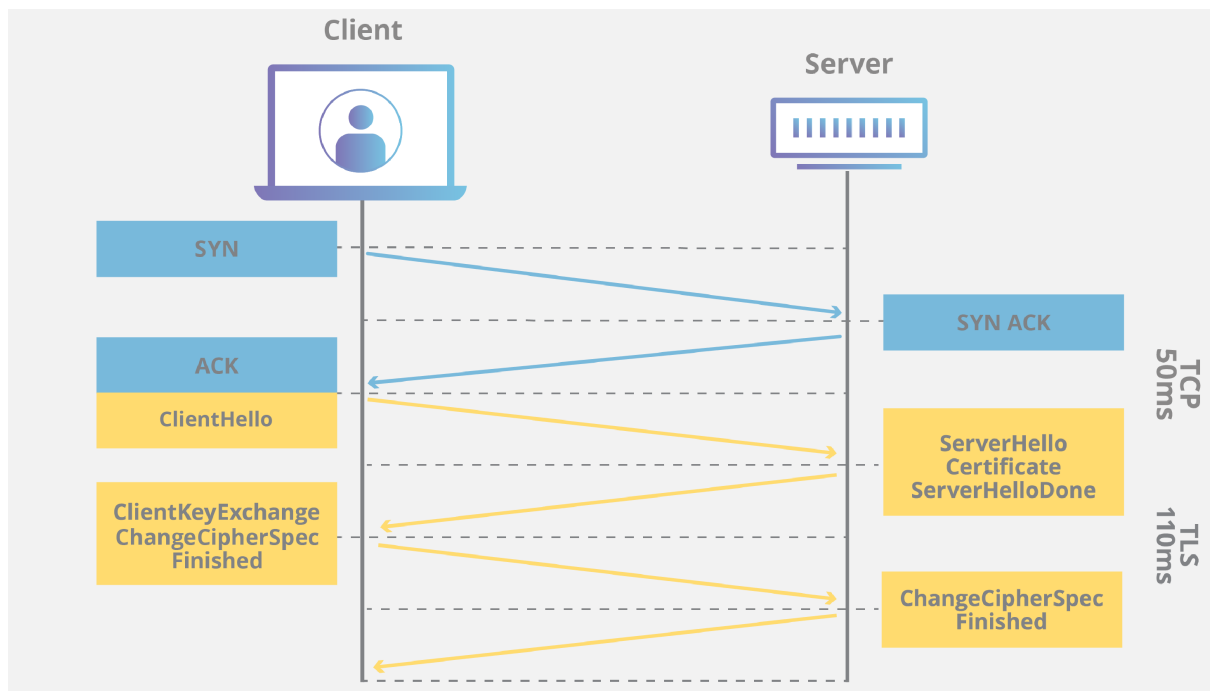
```

▶ Frame 56: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits)
▶ Ethernet II, Src: 1a:3a:46:bf:43:91 (1a:3a:46:bf:43:91), Dst: Vmware_a1:4e:f0 (00:50:56:a1:4e:f0)
▶ Internet Protocol Version 4, Src: 10.124.211.200, Dst: 10.124.211.96
▶ Transmission Control Protocol, Src Port: 3307, Dst Port: 80, Seq: 1, Ack: 1, Len: 200
▼ Hypertext Transfer Protocol
  ▶ GET /newsdetails.php?id=1 HTTP/1.1\r\n
    Accept-Encoding: gzip,deflate\r\n
    Host: 10.124.211.96\r\n
    Accept: */*\r\n
    User-Agent: sqlmap/1.1.4#stable (http://sqlmap.org)\r\n
    Connection: close\r\n
  Cache-Control: no-cache\r\n
  \r\n
  [Full request URI: http://10.124.211.96/newsdetails.php?id=1]
  [HTTP request 1/1]
  [Response in frame: 63]

```

## HTTPS

- HTTPS also establishes a **handshake** similar to TCP but more **complicated**. Below is a brief summary:
  - Both the client and the server need to agree on the **protocol version**.
  - Both the client and the server need to select **cryptographic algorithms**.
  - **Optionally authenticate** to each other.
  - Use **public key encryption techniques** to establish secure communications.



## Normal vs Suspicious HTTPS Traffic

Normal HTTPS Traffic	Suspicious HTTPS Traffic
Port 443, TCP Port 8443, TCP (used as alternate)	Malicious binaries (backdoors), scripts, web shells, etc. will use this port because typically in all corporate environments the port is open.
Encrypted traffic	If the traffic is not encrypted and Secure Sockets Layer packet details are empty within packet details then that will fall under suspicious.
Web server typically in FQDN format.	Server will point to an IP address instead of FQDN format.

## Normal HTTPS Traffic

- the Secure Sockets Layer portion of the packet details should not be empty
- in **Client Hello packet**. We see the following:
  - Content Type = Handshak
  - Handshake Protocol: Client Hello
  - Version: TLS 1.2
  - Cipher Suites (11 suites)
  - Compression Method (1 method)

```

▶ Frame 25: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits)
▶ Ethernet II, Src: 26:11:59:88:53:02 (26:11:59:88:53:02), Dst: Vmware_a1:61:66 (00:50:56:a1:61:66)
▶ Internet Protocol Version 4, Src: 10.54.15.100, Dst: 10.54.15.15
▶ Transmission Control Protocol, Src Port: 45114, Dst Port: 443, Seq: 1, Ack: 1, Len: 167
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 162
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 158
    Version: TLS 1.2 (0x0303)
    ▶ Random
    Session ID Length: 0
    Cipher Suites Length: 22
  ▼ Cipher Suites (11 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
    Compression Methods Length: 1
  ▼ Compression Methods (1 method)
    Compression Method: null (0)
    Extensions Length: 95
    ▶ Extension: renegotiation_info
    ▶ Extension: elliptic_curves
    ▶ Extension: ec_point_formats
    ▶ Extension: SessionTicket TLS
    ▶ Extension: next_protocol_negotiation
    ▶ Extension: Application Layer Protocol Negotiation
    ▶ Extension: status_request
    ▶ Extension: signature_algorithms

```

- in the server's response, Server Hello packet

```

▶ Frame 27: 1391 bytes on wire (11128 bits), 1391 bytes captured (11128 bits)
▶ Ethernet II, Src: Vmware_a1:f4:d0 (00:50:56:a1:f4:d0), Dst: 26:11:59:88:53:02 (26:11:59:88:53:02)
▶ Internet Protocol Version 4, Src: 10.54.15.15, Dst: 10.54.15.100
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 45114, Seq: 1, Ack: 168, Len: 1325
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 61
    ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 57
      Version: TLS 1.2 (0x0303)
      ▼ Random
        GMT Unix Time: May 23, 2017 13:27:38.000000000 EDT
        Random Bytes: 2000d7125ade0022e9441d5121c77b5e3cb88e6b5fd2242e...
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 17
        ▶ Extension: renegotiation_info
        ▶ Extension: ec_point_formats
        ▶ Extension: SessionTicket TLS
      ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 1011
        ▼ Handshake Protocol: Certificate
          Handshake Type: Certificate (11)
          Length: 1007
          Certificates Length: 1004
          ▼ Certificates (1004 bytes)
            Certificate Length: 1001
            ▼ Certificate: 308203e5308202cda003020102020900d98303cf87501375... (pkcs-9-at-emailAddress=e
              ▼ signedCertificate
                version: v3 (2)
                serialNumber: -277336875566807947
                ▶ signature (sha1WithRSAEncryption)
                ▶ issuer: rdnSequence (0)
                ▶ validity
                ▶ subject: rdnSequence (0)
                ▶ subjectPublicKeyInfo
                ▶ extensions: 3 items
                ▶ algorithmIdentifier (sha1WithRSAEncryption)
                Padding: 0
                encrypted: 2326c8138a9c0a09ff804ee8e6909cae6f34ae00cf343ae9...

```

- Here we see the **Server Key Exchange** which will be followed by the **Client Key Exchange** packet. (step #3 in the establishment of an SSL/TLS session)

▶ Frame 29: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)  
 ▶ Ethernet II, Src: Vmware\_a1:f4:d0 (00:50:56:a1:f4:d0), Dst: 26:11:59:88:53:02 (26:11:59:88:53:02)  
 ▶ Internet Protocol Version 4, Src: 10.54.15.15, Dst: 10.54.15.100  
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 45114, Seq: 1326, Ack: 168, Len: 104  
 ▶ [2 Reassembled TCP Segments (338 bytes): #27(243), #29(95)]  
 ▼ Secure Sockets Layer  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: **Server Key Exchange**  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 333  
   ▼ Handshake Protocol: Server Key Exchange  
     Handshake Type: Server Key Exchange (12)  
     Length: 329  
   ▼ EC Diffie-Hellman Server Params  
     Curve Type: named\_curve (0x03)  
     Named Curve: secp256r1 (0x0017)  
     Pubkey Length: 65  
     Pubkey: 04401daa41bf0a036acffe3ce86c112c109af374b2ef1326...  
   ▼ Signature Hash Algorithm: 0x0401  
     Signature Hash  
     Signature Length: 8f3e65...

▶ Frame 31: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits)  
 ▶ Ethernet II, Src: 26:11:59:88:53:02 (26:11:59:88:53:02), Dst: Vmware\_a1:61:66 (00:50:56:a1:61:66)  
 ▶ Internet Protocol Version 4, Src: 10.54.15.100, Dst: 10.54.15.15  
 ▶ Transmission Control Protocol, Src Port: 45114, Dst Port: 443, Seq: 168, Ack: 1430, Len: 126  
 ▼ Secure Sockets Layer  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: **Client Key Exchange**  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 70  
   ▼ Handshake Protocol: Client Key Exchange  
     Handshake Type: Client Key Exchange (16)  
     Length: 66  
   ▼ EC Diffie-Hellman Client Params  
     Pubkey Length: 65  
     Pubkey: 04496c4e42312aa0f1b9855834438ee5d7f9774553bfc5e...  
   ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
     Content Type: Change Cipher Spec (20)  
     Version: TLS 1.2 (0x0303)  
     Length: 1  
     Change Cipher Spec Message  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 40  
   ▼ Handshake Protocol: Hello Request  
     Handshake Type: Hello Request (0)  
     Length: 0  
   ▼ Handshake Protocol: Hello Request  
     Handshake Type: Hello Request (0)  
     Length: 0

- This is the last packet and the handshake between the server and client is now complete.

```

▶ Frame 34: 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits)
▶ Ethernet II, Src: Vmware_a1:f4:d0 (00:50:56:a1:f4:d0), Dst: 26:11:59:88:53:02 (26:11:59:88:53:02)
▶ Internet Protocol Version 4, Src: 10.54.15.15, Dst: 10.54.15.100
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 45114, Seq: 1430, Ack: 604, Len: 258
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket ←
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 202
    ▼ Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 198
      ▼ TLS Session Ticket
        Session Ticket Lifetime Hint: 300
        Session Ticket Length: 192
        Session Ticket: c87ec842e1a7e7c2fd503729435f618d50f9e59487ae8647...
  ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message ←
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message

```

- The rest of the packets between these two devices will now be **encrypted**.
- The traffic is unreadable, but if this is internal traffic within our corporate environment, then, it is feasible to decrypt this traffic using the **private key** from the internal server.

```

▶ Frame 35: 770 bytes on wire (6160 bits), 770 bytes captured (6160 bits)
▶ Ethernet II, Src: Vmware_a1:f4:d0 (00:50:56:a1:f4:d0), Dst: 26:11:59:88:53:02 (26:11:59:88:53:02)
▶ Internet Protocol Version 4, Src: 10.54.15.15, Dst: 10.54.15.100
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 45114, Seq: 1688, Ack: 604, Len: 704
▼ Secure Sockets Layer
  ▶ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
  ▶ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
  ▶ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 32
    Encrypted Application Data: bb006752c8e53aef6bb13c15ff590c829883685da8b96e44...

```

## Malicious HTTPS Traffic Example

- we can use this filter `ssl.record.content_type == 22` in order to get the **SSL/TLS handshakes**

No.	Time	Source	Destination	src port	dst port	Protocol	Length	Info
1	0.000000	215.255.186.158	251.217.119.1...	55726	https	TLSv1	364	Client Hello
2	0.040015	215.255.186.158	251.217.119.1...	55731	https	TLSv1	364	Client Hello
14	0.543463	215.255.186.158	251.217.119.1...	55733	https	TLSv1.2	364	Client Hello
17	0.545287	215.255.186.158	251.217.119.1...	55734	https	TLSv1.2	364	Client Hello
22	0.764012	215.255.186.158	251.217.119.1...	55369	https	TLSv1	364	Client Hello
23	0.850374	251.217.119.170	215.255.186.1...	https	55734	TLSv1.2	1514	Server Hello
26	0.850399	251.217.119.170	215.255.186.1...	https	55734	TLSv1.2	645	Certificate, Server Key E
31	0.851933	215.255.186.158	251.217.119.1...	55734	https	TLSv1.2	192	Client Key Exchange, Chan
33	0.908004	215.255.186.158	251.217.119.1...	55681	https	TLSv1	364	Client Hello
34	0.952042	215.255.186.158	251.217.119.1...	55723	https	TLSv1	364	Client Hello
36	1.016351	251.217.119.170	215.255.186.1...	https	55734	TLSv1.2	292	New Session Ticket, Chang
42	1.222375	251.217.119.170	215.255.186.1...	https	55733	TLSv1.2	1514	Server Hello
45	1.222428	251.217.119.170	215.255.186.1...	https	55733	TLSv1.2	645	Certificate, Server Key E
50	1.223959	215.255.186.158	251.217.119.1...	55733	https	TLSv1.2	192	Client Key Exchange, Chan
53	1.387800	251.217.119.170	215.255.186.1...	https	55733	TLSv1.2	292	New Session Ticket, Chang
59	1.534411	215.255.186.158	251.217.119.1...	55736	https	TLSv1.2	364	Client Hello
62	1.541089	215.255.186.158	251.217.119.1...	55737	https	TLSv1	364	Client Hello

> Frame 1: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits)  
 > Ethernet II, Src: 06:94:a7:35:af:33 (06:94:a7:35:af:33), Dst: 06:7e:64:b6:bc:3f (06:7e:64:b6:bc:3f)  
 > Internet Protocol Version 4, Src: 215.255.186.158, Dst: 251.217.119.170  
 > Transmission Control Protocol, Src Port: 55726 (55726), Dst Port: https (443), Seq: 1215393884, Ack: 3100448357,  
 > Transport Layer Security

- When it comes to SSL/TLS handshakes, you should remember two things:
  - Each SSL/TLS handshake is effectively a **new connection** (consuming resources)
  - SSL/TLS handshakes are quite **CPU intensive operations** (server-side)
- The number of new Client Hello messages is **abnormal**.
- it looks like we are dealing with a **TLS Renegotiation Attack** (DoS attack against the TLS layer)

## SMTP (Simple Mail Transfer Protocol)

### How SMTP works ?

- It's the protocol responsible for sending emails
- SMTP is a text-based protocol, meaning that it relies on **exchanging ASCII based strings** as **commands** between the **server** and the **client**.

HELO	Sent by a client to identify itself, usually with a domain name.
MAIL FROM	Identifies the sender of the message; used in the form MAIL FROM:.
RCPT TO	Identifies the message recipients; used in the form RCPT TO:.
VERFY	Verifies that a mailbox is available for message delivery;.

- The SMTP server starts the conversation, once the **TCP three-way handshake is completed**, by sending its banner, containing the server's name and version.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			TCP	62	1077->25 [SYN] Seq=0 win=16384 Len=0 MS
2	0.000000			TCP	62	25->1077 [SYN, ACK] Seq=0 Ack=1 Win=175
3	0.020029			TCP	60	1077->25 [ACK] Seq=1 Ack=1 win=17520 Le
4	0.020029			SMTP	158	S: 220 [REDACTED]
5	0.030043			SMTP	67	C: EHLO Client
6	0.190274			TCP	54	25->1077 [ACK] Seq=105 Ack=14 Win=17507
7	0.420605			SMTP	290	S: 250 Server Hello [REDACTED]   25
8	0.430619			SMTP	66	C: AUTH LOGIN
9	0.430619			SMTP	72	S: 334 vXNlcm5hbWU6
10	0.430619			SMTP	64	C: User: [REDACTED]
11	0.430619			SMTP	72	S: 334 UGFzc3dvcmQ6
12	0.430619			SMTP	64	C: Pass: [REDACTED]
13	0.440634			SMTP	91	S: 235 2.7.0 Authentication successful

## Malicious SMTP Traffic Example

- The lack of proper security configuration may also allow the attacker to connect to the SMTP server and **manually enumerate** the users on that server using the **VERFY**, **EXPN** or **RCPT TO** commands.
- User enumeration may be used as part of a **social engineering attack** or as a first step of a brute force attack against account passwords on that server.

## DNS (Domain Name System)

- resolves **names** to **IP addresses**.
- DNS is a **query-response** protocol.
- DNS traffic normally uses **UDP** on port **53**.
- DNS traffic should go to **DNS servers only**.

## Normal vs Malicious DNS Traffic

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

## Normal DNS Traffic

No.	Time	Source	Destination	Protocol	Length	Info
16	26.200151138	172.16.5.100	172.16.5.10	DNS	83	Standard query 0xde40 PTR 5.5.16.172.in-addr.arpa
19	26.272980431	172.16.5.10	172.16.5.100	DNS	127	Standard query response 0xde40 PTR 5.5.16.172.in-addr.arpa PTR wkst-techsupport.sportsfoo.com
41	56.605405613	172.16.5.100	172.16.5.10	DNS	94	Standard query 0xa620 PTR 5.5.16.172.in-addr.arpa OPT
42	56.639661726	172.16.5.10	172.16.5.100	DNS	138	Standard query response 0xa620 PTR 5.5.16.172.in-addr.arpa PTR wkst-techsupport.sportsfoo.com OPT

- 4 packets: 2 packets for DNS Queries and 2 for DNS Responses.

```

Frame 16: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
  Ethernet II, Src: b2:fe:ed:db:02:32 (b2:fe:ed:db:02:32), Dst: Vmware_a1:a4:5f (00:50:56:a1:a4:5f)
  Internet Protocol Version 4, Src: 172.16.5.100, Dst: 172.16.5.10
  User Datagram Protocol, Src Port: 42653, Dst Port: 53
  Domain Name System (query)
    [Response In: 19]
    Transaction ID: 0xde40
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      5.5.16.172.in-addr.arpa: type PTR, class IN
        Name: 5.5.16.172.in-addr.arpa
        [Name Length: 23]
0000  00 50 56 a1 a4 5f b2 fe  ed db 02 32 08 00 45 00  .PV... ..2..E.
0010  00 45 ae 11 00 00 40 11  6a 08 ac 10 05 64 ac 10  .E...@. j...d..
0020  05 0a a6 9d 00 35 00 31  2d 00 de 40 01 00 00 01  .....5.1 ..@....
0030  00 00 00 00 00 00 01 35  01 35 02 31 36 03 31 37  .....5 .5.16.17
0040  32 07 69 6e 2d 61 64 64  72 04 61 72 70 61 00 00  2.in-add r.arpa..
0050  0c 00 01
  
```

- this is a **UDP** packet and it's using an expected port, **53**.

```
▶ Frame 19: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
▶ Ethernet II, Src: Vmware_a1:a4:5f (00:50:56:a1:a4:5f), Dst: b2:fe:ed:db:02:32 (b2:fe:ed:db:02:32)
▶ Internet Protocol Version 4, Src: 172.16.5.10, Dst: 172.16.5.100
▶ User Datagram Protocol, Src Port: 53, Dst Port: 42653
▼ Domain Name System (response)
  [Request In: 16]
  [Time: 0.072829293 seconds]
  Transaction ID: 0xde40
  ▶ Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ 5.5.16.172.in-addr.arpa: type PTR, class IN
      Name: 5.5.16.172.in-addr.arpa
      [Name Length: 23]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
  ▼ Answers
    ▼ 5.5.16.172.in-addr.arpa: type PTR, class IN, wkst-techsupport.sportsfoo.com
      Name: 5.5.16.172.in-addr.arpa
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
      Time to live: 3600
      Data length: 32
      Domain Name: wkst-techsupport.sportsfoo.com
```

- This is the DNS Response to the DNS Query in packet looks normal

## Malicious DNS Traffic

- **DNS Zone Transfers** : a way to replicate DNS databases across a group of DNS servers.
- **DNS tunnels**