

Capture UDP packets and with the help of the captured UDP Packets.

a. analyses UDP DHCP Packets

b. analyses UDP DNS Packets

Analysis of UDP DHCP Packets:

- DHCP is used for ip configuration

Dhcp Request

```
> Frame 46: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits)
> Ethernet II, Src: AzureWav_95:a1:61 (80:91:33:95:a1:61), Dst: TendaTec_7
✓ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 344
    Identification: 0x000f (15)
    > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xb7cc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.104
    Destination Address: 192.168.0.1
✓ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 324
    Checksum: 0x2eac [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    > [Timestamps]
    UDP payload (316 bytes)
✓ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x35e601ca
    Seconds elapsed: 0
    > Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.0.104
    Your (client) IP address: 0.0.0.0
```

```

> Frame 46: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits)
> Ethernet II, Src: AzureWav_95:a1:61 (80:91:33:95:a1:61), Dst: TendaTec_
v Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 344
    Identification: 0x000f (15)
    > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xb7cc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.104
    Destination Address: 192.168.0.1
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 324
    Checksum: 0x2eac [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    > [Timestamps]
    UDP payload (316 bytes)
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x35e601ca
    Seconds elapsed: 0
    > Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.0.104
    Your (client) IP address: 0.0.0.0

```

From the above pictures we can know the DHCP configuration. Source and Destination Ports and IP here source and destination has static port (67,68). And various other information regarding DHCP request.

DHCP ACK

```
> Frame 47: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{1D4E0B16-3097-4
> Ethernet II, Src: TendaTec_71:8d:d8 (50:2b:73:71:8d:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
√ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 576
        Identification: 0x0000 (0)
    > Flags: 0x00
        Fragment Offset: 0
        Time to Live: 64
        Protocol: UDP (17)
        Header Checksum: 0xb804 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.1
        Destination Address: 255.255.255.255
√ User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 556
    Checksum: 0x1d1f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    > [Timestamps]
        UDP payload (548 bytes)
√ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x35e601ca
    Seconds elapsed: 0
    > Bootp flags: 0x8000, Broadcast flag (Broadcast)
        Client IP address: 192.168.0.104
        Your (client) IP address: 192.168.0.104
        Next server IP address: 0.0.0.0
```

```
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x35e601ca  
Seconds elapsed: 0  
➤ Bootp flags: 0x8000, Broadcast flag (Broadcast)  
Client IP address: 192.168.0.104  
Your (client) IP address: 192.168.0.104  
Next server IP address: 0.0.0.0  
Relay agent IP address: 0.0.0.0  
Client MAC address: AzureWav_95:a1:61 (80:91:33:95:a1:61)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
▼ Option: (53) DHCP Message Type (ACK)  
    Length: 1  
    DHCP: ACK (5)  
▼ Option: (54) DHCP Server Identifier (192.168.0.1)  
    Length: 4  
    DHCP Server Identifier: 192.168.0.1  
▼ Option: (51) IP Address Lease Time  
    Length: 4  
    IP Address Lease Time: (86400s) 1 day  
▼ Option: (1) Subnet Mask (255.255.255.0)  
    Length: 4  
    Subnet Mask: 255.255.255.0  
▼ Option: (3) Router  
    Length: 4  
    Router: 192.168.0.1  
▼ Option: (6) Domain Name Server  
    Length: 4  
    Domain Name Server: 192.168.0.1  
▼ Option: (0) Padding  
    Padding: 00000000000000000000000000000000000000000000000000000000000000000000000000000000...  
▼ Option: (255) End  
    Option End: 255
```

Basically, DHCP is used for providing an automatic IP address to Hosts which want to connect to a network

Analyses UDP DNS Packets

- *Dns server is used to resolve the domain name into IP*

```

v Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x0012 (18)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xb8df [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.104
    Destination Address: 192.168.0.1
v User Datagram Protocol, Src Port: 63699, Dst Port: 53
  Source Port: 63699
  Destination Port: 53
  Length: 46
  Checksum: 0x6ba0 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 15]
  > [Timestamps]
    UDP payload (38 bytes)
v Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
v Queries
  > 8.8.8.8.in-addr.arpa: type PTR, class IN
    [Response In: 142]
```

In the above image we can find the source and Destination IP and ports

But here source Ip is dynamic. And we can also find the query..

And various other details regarding the DNS request

✓ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 122

Identification: 0x19dc (6620)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 64

Protocol: UDP (17)

Header Checksum: 0xdedd [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.1

Destination Address: 192.168.0.104

✓ User Datagram Protocol, Src Port: 53, Dst Port: 63699

Source Port: 53

Destination Port: 63699

Length: 102

Checksum: 0xd96e [unverified]

[Checksum Status: Unverified]

[Stream index: 15]

> [Timestamps]

UDP payload (94 bytes)

✓ Domain Name System (response)

Transaction ID: 0x0002

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 2

✓ Queries

> 8.8.8.8.in-addr.arpa: type PTR, class IN

✓ Answers

> 8.8.8.8.in-addr.arpa: type PTR, class IN, dns.google

> Additional records

[\[Request In: 141\]](#)

In the DNS Standard query response we can see the information regarding the request sent by my machine and Various other information regarding the request and response..