

Q1. What is the host name?

A: DESKTOP-H800JIR

```
C:\Users\User>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-H800JIR
```

Q2. What is the physical (data-link) address?

A: 98-EE-CB-64-ED-A8

```
Ethernet adapter 乙太網路 13:

Connection-specific DNS Suffix . : hitronhub.home
Description . . . . . : Realtek PCIe GbE Family Controller #6
Physical Address. . . . . : 98-EE-CB-64-ED-A8
```

Q3. What is the IP address?

A: 192.168.0.167

```
IPv4 Address. . . . . : 192.168.0.167(Preferred)
```

Q4. What is the IP address of the default gateway?

A: 192.168.0.1

```
Default Gateway . . . . . : 192.168.0.1
```

Q5. Locate the DNS query and response messages for the Web page:www.ntut.edu.tw. Are they sent over UDP or TCP?

A: UDP

No.	Time	Source	Destination	Protocol	Length	Info
2260	10.345329	192.168.0.167	192.168.0.1	DNS	75	Standard query 0x718b A www.ntut.edu.tw

```
> Frame 2260: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{44144D08-D1F4-4489-B4...}
> Ethernet II, Src: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8), Dst: HitronTe_19:32:72 (60:6c:63:19:32:72)
v Internet Protocol Version 4, Src: 192.168.0.167, 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: 61
    Identification: 0x97cc (38860)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.167
    Destination Address: 192.168.0.1
```

Q6. What is the destination port for the DNS query message? What is the source port of DNS response message?

A: DNS query message destination port: 53

```
2260 10.345329 192.168.0.167 192.168.0.1 DNS 75 Standard query 0x718b A www.ntut.edu.tw
> Frame 2260: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{44144D08-D1F4-4489-B45D-A
> Ethernet II, Src: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8), Dst: HitronTe_19:32:72 (60:6c:63:19:32:72)
> Internet Protocol Version 4, Src: 192.168.0.167, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 58846, Dst Port: 53
```

A: DNS response message source port: 53

```
2287 10.428756 192.168.0.1 192.168.0.167 DNS 91 Standard query response 0x718b A www.ntut.edu.tw A 140.124.13.105
> Frame 2287: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{44144D08-D1F4-4489-B45D-A
> Ethernet II, Src: HitronTe_19:32:72 (60:6c:63:19:32:72), Dst: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.167
> User Datagram Protocol, Src Port: 53, Dst Port: 58846
```

Q7. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

A: 192.168.0.1, same as my local DNS server

```
2260 10.345329 192.168.0.167 192.168.0.1 DNS 75 Standard query 0x718b A www.ntut.edu.tw
Select Command Prompt
> ipconfig
DNS Servers . . . . . : 192.168.0.1
```

Q8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

A: 1 answer

```
2287 10.428756 192.168.0.1 192.168.0.167 DNS 91 Standard query response 0x718b A www.ntut.edu.tw A 140.124.13.105
> Frame 2287: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{44144D08-D1F4-4489-B45D
> Ethernet II, Src: HitronTe_19:32:72 (60:6c:63:19:32:72), Dst: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.167
> User Datagram Protocol, Src Port: 53, Dst Port: 58846
v Domain Name System (response)
  Transaction ID: 0x718b
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  v Answers
    v www.ntut.edu.tw: type A, class IN, addr 140.124.13.105
      Name: www.ntut.edu.tw
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 600 (10 minutes)
      Data length: 4
      Address: 140.124.13.105
[Request In: 2260]
[Time: 0.083427000 seconds]
```