

電腦網路作業: Wireshark Lab: DNS

S1154041 邱立宇

1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in?

Ans: 103.21.124.10

2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

Ans: hntpl.hinet.net

3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

Ans: non-authoritative

```
C:\Windows\system32>nslookup www.iitb.ac.in.  
伺服器: hntpl.hinet.net 2  
Address: 168.95.192.1  
  
未經授權的回答: 3  
名稱: www.iitb.ac.in  
Address: 103.21.124.10 1
```

4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?

Ans: (1) dns1.iitb.ac.in (2) nslookup dns1.iitb.ac.in

```
C:\Windows\system32>nslookup -type=NS www.iitb.ac.in.  
伺服器: dns.hinet.net  
Address: 168.95.192.1  
  
iitb.ac.in  
primary name server = dns1.iitb.ac.in 4.2  
responsible mail addr = postmaster.iitb.ac.in  
serial = 2013071001  
refresh = 16384 (4 hours 33 mins 4 secs)  
retry = 2048 (34 mins 8 secs)  
expire = 1048576 (12 days 3 hours 16 mins 16 secs)  
default TTL = 3960 (1 hour 6 mins)  
  
C:\Windows\system32>nslookup dns1.iitb.ac.in 4.2  
伺服器: dns.hinet.net  
Address: 168.95.192.1  
  
未經授權的回答:  
名稱: dns1.iitb.ac.in  
Address: 103.21.125.129
```

5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?

Ans:(1) 61 (2) UDP

```

61 2.906326 192.168.15.10 168.95.192.1 DNS 77 Standard query 0x0336 A gaia.cs.umass.edu
> Frame 61: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF{...}
> Ethernet II, Src: ASUSTekC_b1:04:0a (f0:2f:74:b1:04:0a), Dst: DrayTek_1b:34:ec (00:1d:aa:1b:34:ec)
> Internet Protocol Version 4, Src: 192.168.15.10, Dst: 168.95.192.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 63
  Identification: 0x8d55 (36181)
> 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: 192.168.15.10
  Destination Address: 168.95.192.1
> User Datagram Protocol, Src Port: 60019, Dst Port: 53 7.1
> Domain Name System (query)

```

6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

Ans:(1)77 (2) UDP

```

77 3.171681 168.95.192.1 192.168.15.10 DNS 93 Standard query response 0x0336 A gaia.cs.umass.edu
> Frame 77: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF{...}
> Ethernet II, Src: DrayTek_1b:34:ec (00:1d:aa:1b:34:ec), Dst: ASUSTekC_b1:04:0a (f0:2f:74:b1:04:0a)
> Internet Protocol Version 4, Src: 168.95.192.1, Dst: 192.168.15.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 79
  Identification: 0xa184 (41348)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 57
  Protocol: UDP (17)
  Header Checksum: 0xa806 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 168.95.192.1
  Destination Address: 192.168.15.10 7.2
> User Datagram Protocol, Src Port: 53, Dst Port: 60019
> Domain Name System (response)

```

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

Ans: Both 53

8. To what IP address is the DNS query message sent? Ans: 168.95.192.1

```

61 2.906326 192.168.15.10 168.95.192.1 DNS 77 Standard query 0x0336 A gaia.cs.umass.edu

```

9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

Ans:(1) 1 (2) 0

```
> Frame 61: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\
> Ethernet II, Src: ASUSTekC_b1:04:0a (f0:2f:74:b1:04:0a), Dst: DrayTek_1b:34:ec (00:1d:aa:
> Internet Protocol Version 4, Src: 192.168.15.10, Dst: 168.95.192.1
> User Datagram Protocol, Src Port: 60019, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x0336
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0 No answer
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > gaia.cs.umass.edu: type A, class IN
  [Response In: 77]
```

10. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

Ans:(1) 1 (2) 1

```
> Frame 77: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\
> Ethernet II, Src: DrayTek_1b:34:ec (00:1d:aa:1b:34:ec), Dst: ASUSTekC_b1:04:0a (f0:2f:74:
> Internet Protocol Version 4, Src: 168.95.192.1, Dst: 192.168.15.10
> User Datagram Protocol, Src Port: 53, Dst Port: 60019
v Domain Name System (response)
  Transaction ID: 0x0336
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > gaia.cs.umass.edu: type A, class IN
v Answers
  > gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
  [Request In: 61]
  [Time: 0.265355000 seconds]
```

11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/?

73	3.095274	192.168.15.10	128.119.245.12	HTTP	542 GET /kurose_ross/ HTTP/1.1
----	----------	---------------	----------------	------	--------------------------------

What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address?

61	2.906326	192.168.15.10	168.95.192.1	DNS	77 Standard query 0x0336 A gaia.cs.umass.edu
----	----------	---------------	--------------	-----	--

What is the packet number in the trace of the received DNS response?

77	3.171681	168.95.192.1	192.168.15.10	DNS	93	Standard query response 0x0336 A gaia.cs.umass.edu A 128.119.245.12
----	----------	--------------	---------------	-----	----	---

What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg?

279	3.848503	192.168.15.10	128.119.245.12	HTTP	526	GET /kurose_ross/header_graphic_book_8E_3.jpg
-----	----------	---------------	----------------	------	-----	---

What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address?

61	2.906326	192.168.15.10	168.95.192.1	DNS	77	Standard query 0x0336 A gaia.cs.umass.edu
----	----------	---------------	--------------	-----	----	---

Discuss how DNS caching affects the answer to this last question.

Ans: (1)73 (2)61 (3)77 (4)279 (5)61 (6)Since the domain has been resolved, the following requests to this domain don't need to solve again.

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

Ans: Both 53

```
> Frame 9: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on  
> Ethernet II, Src: ASUSTekC_b1:04:0a (f0:2f:74:b1:04:0a), Dst: DrayTek  
> Internet Protocol Version 4, Src: 192.168.15.10, Dst: 168.95.192.1  
v User Datagram Protocol, Src Port: 62962, Dst Port: 53
```

Source Port: 62962

Destination Port: 53

```
> Frame 10: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on  
> Ethernet II, Src: DrayTek_1b:34:ec (00:1d:aa:1b:34:ec), Dst: ASUSTek  
> Internet Protocol Version 4, Src: 168.95.192.1, Dst: 192.168.15.10  
v User Datagram Protocol, Src Port: 53, Dst Port: 62962
```

Source Port: 53

Destination Port: 62962

13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans: (1)168.95.192.1(2)YES

9	0.226816	192.168.15.10	168.95.192.1	DNS	76	Standard query 0x0002 A www.cs.umass.edu
---	----------	---------------	--------------	-----	----	--

```
C:\Users\chiul>nslookup www.cs.umass.edu
伺服器: dns.hinet.net
Address: 168.95.192.1

未經授權的回答:
名稱: www.cs.umass.edu
Address: 128.119.240.84
```


14. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans:(1)A (2) NO

```
> Frame 9: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\
> Ethernet II, Src: ASUSTekC_b1:04:0a (f0:2f:74:b1:04:0a), Dst: DrayTek_1b:34:ec (00:1d:a
> Internet Protocol Version 4, Src: 192.168.15.10, Dst: 168.95.192.1
  User Datagram Protocol, Src Port: 62962, Dst Port: 53
    Source Port: 62962
    Destination Port: 53
    Length: 42
    Checksum: 0x384f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
  UDP payload (34 bytes)
  Domain Name System (query)
    Transaction ID: 0x0002
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    > www.cs.umass.edu: type A, class IN
    [Response In: 10]
```

15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?

Ans:(1) 1 (2) 1

```
> Frame 10: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\
> Ethernet II, Src: DrayTek_1b:34:ec (00:1d:aa:1b:34:ec), Dst: ASUSTekC_b1:04:0a (f0:2f:74:
> Internet Protocol Version 4, Src: 168.95.192.1, Dst: 192.168.15.10
  User Datagram Protocol, Src Port: 53, Dst Port: 62962
  Domain Name System (response)
    Transaction ID: 0x0002
    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    > www.cs.umass.edu: type A, class IN
  > Answers
    > www.cs.umass.edu: type A, class IN, addr 128.119.240.84
    [Request In: 9]
    [Time: 0.251151000 seconds]
```

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans: (1)168.95.192.1(2)YES

3	0.002762	192.168.15.10	168.95.192.1	DNS	69	Standard query 0x0002 NS umass.edu
---	----------	---------------	--------------	-----	----	------------------------------------

```
C:\Users\chiul>nslookup -type=NS umass.edu
服务器: dns.hinet.net
Address: 168.95.192.1
```

17. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?

Ans: (1) 1 (2) NO

```
> Frame 3: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\N
> Ethernet II, Src: ASUSTekC_b1:04:0a (f0:2f:74:b1:04:0a), Dst: DrayTek_1b:34:ec (00:1d:aa:
> Internet Protocol Version 4, Src: 192.168.15.10, Dst: 168.95.192.1
> User Datagram Protocol, Src Port: 63392, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0 No answer
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > umass.edu: type NS, class IN
      [Response In: 4]
```

18. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource

Ans: (1) 3 (2) umass.edu domain's nameserver (3) 0

```
> Frame 4: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device
> Ethernet II, Src: DrayTek_1b:34:ec (00:1d:aa:1b:34:ec), Dst: ASUSTekC_b1:04:0a (f0:2f:74:
> Internet Protocol Version 4, Src: 168.95.192.1, Dst: 192.168.15.10
> User Datagram Protocol, Src Port: 53, Dst Port: 63392
v Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3 3 answers
    Authority RRs: 0
    Additional RRs: 0 No additional resources
  v Queries
    > umass.edu: type NS, class IN
  v Answers
    > umass.edu: type NS, class IN, ns ns1.umass.edu
    > umass.edu: type NS, class IN, ns ns3.umass.edu
    > umass.edu: type NS, class IN, ns ns2.umass.edu umass.edu domain's nameserver
      [Request In: 3]
  [Time: 0.225268000 seconds]
```