



# DNS& WIRESHARK EXPERIMENT

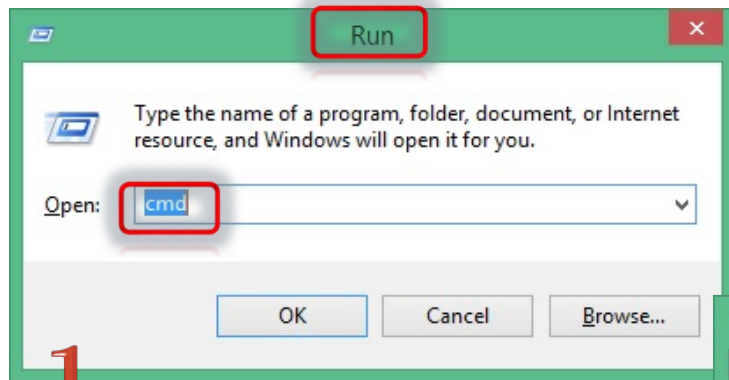
Acknowledgement: Derived for the course by Ibrahim Aljubayri from exercises in Kurose and Ross text (See references provided in the first lecture)

# DNS EXPERIMENT

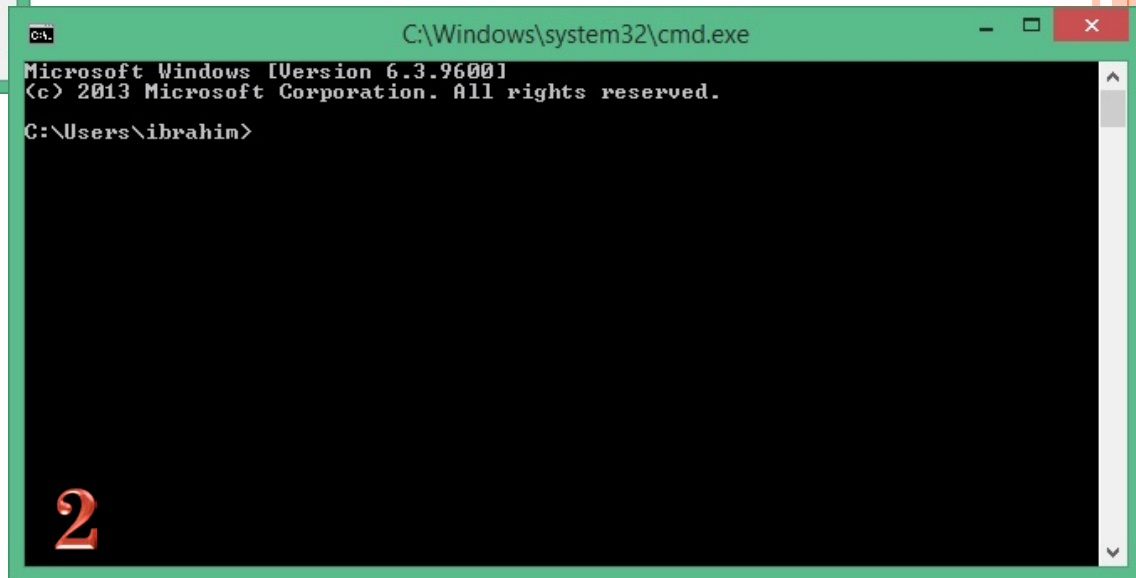
- In this lab, we'll take a closer look at the client side of DNS
- We will start by use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms. To run “nslookup” in Windows, open the Command Prompt and run nslookup on the command line



- We start by opening the Windows Command Prompt application.
- Go to Run → cmd



1



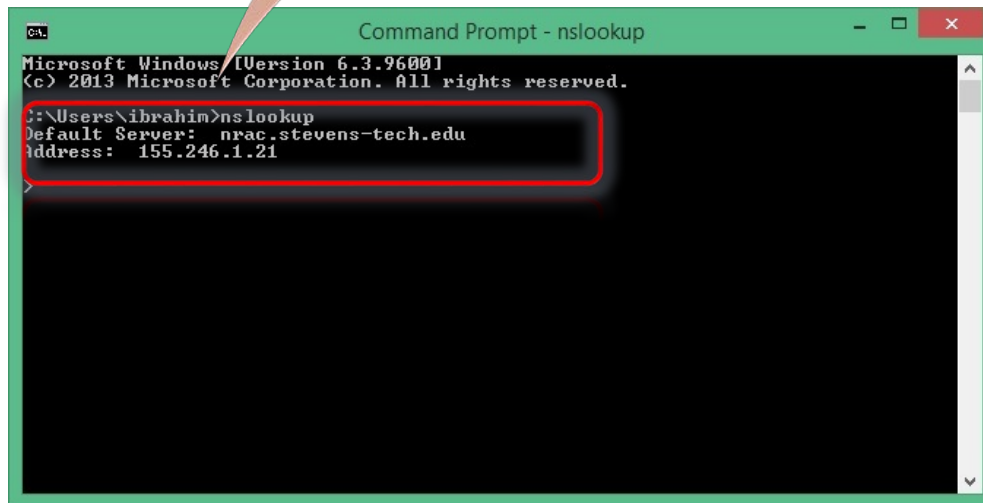
2

# NSLOOKUP

- “nslookup” tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

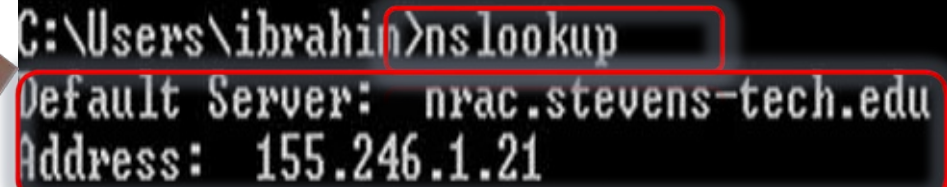


- After we open the cmd window, we type in “nslookup”



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ibrahim>nslookup
Default Server: nrac.stevens-tech.edu
Address: 155.246.1.21
```



```
C:\Users\ibrahim>nslookup
Default Server: nrac.stevens-tech.edu
Address: 155.246.1.21
```

**DNS server details**



- Also we can check actual ip address for a specific website. For example Google. “nslookup www.google.com”



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ibrahim>nslookup www.google.com
Server: nrac.stevens-tech.edu
Address: 155.246.1.21

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:4006:806::1012
          74.125.226.48
          74.125.226.52
          74.125.226.50
          74.125.226.49
          74.125.226.51

C:\Users\ibrahim>
```

Google uses many ip addresses but because of DNS, you only need to know “www.Google.com” to access any of them

# IPCONFIG

- ipconfig is among the most useful little utilities in your host. ipconfig can be used to show your current TCP/IP information, including your DNS server



- Type in “ipconfig /all”

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

Windows IP Configuration

Host Name . . . . . : Mobile780
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : stevens-tech.edu

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 02-00-11-00-CC-CC
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . : stevens-tech.edu
Description . . . . . : Dell Wireless 1510 Wireless-N WLAN Mini-C
ard
Physical Address. . . . . : 02-00-11-00-CC-CC
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4925:ed66:3f95:ee55%4(Preferred)
IPv4 Address. . . . . : 155.246.163.156(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, February 25, 2014 8:13:55 PM
Lease Expires . . . . . : Tuesday, February 25, 2014 10:44:05 PM
Default Gateway . . . . . : 155.246.163.1
DHCP Server . . . . . : 155.246.151.135
DHCPv6 IAID . . . . . : 67118686
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-F7-F5-BB-00-22-19-EB-1A-F9

DNS Servers . . . . . : 155.246.1.21
                        155.246.1.20
Primary WINS Server . . . . . : 155.246.1.109
NetBIOS over Tcpip. . . . . : Enabled
```

DNS details





- Type in “ipconfig /displaydns”

DNS responds about web pages addresses inquiries

```
C:\Users\ibrahim>ipconfig /displaydns

Windows IP Configuration

6to4.ipv6.microsoft.com
-----
Record Name . . . . . : 6to4.ipv6.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 192.88.99.1

Record Name . . . . . : a.gtld-servers.net
Record Type . . . . . : 1
Time To Live . . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 192.5.6.30

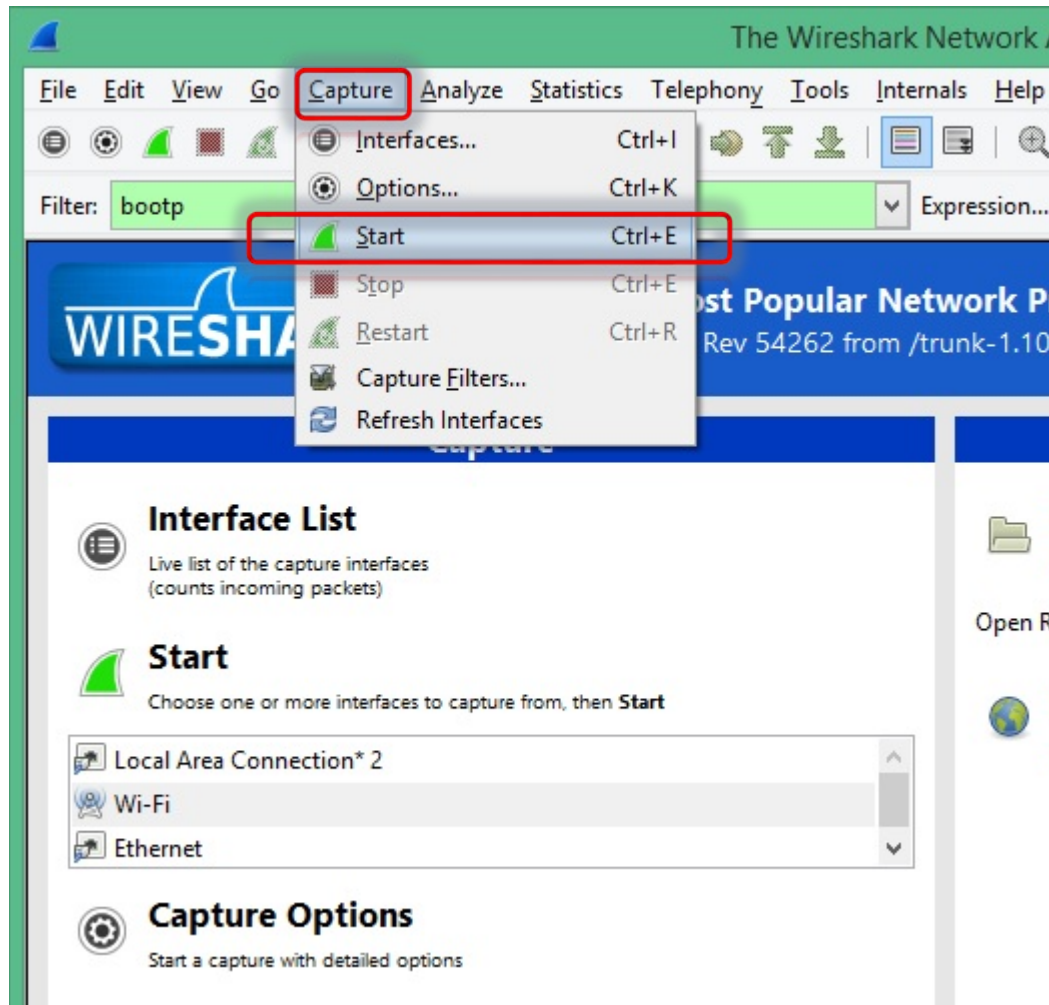
Record Name . . . . . : a.gtld-servers.net
Record Type . . . . . : 28
Time To Live . . . . . : 156
Data Length . . . . . : 16
Section . . . . . : Additional
AAAA Record . . . . . : 2001:503:a83e::2:30
```



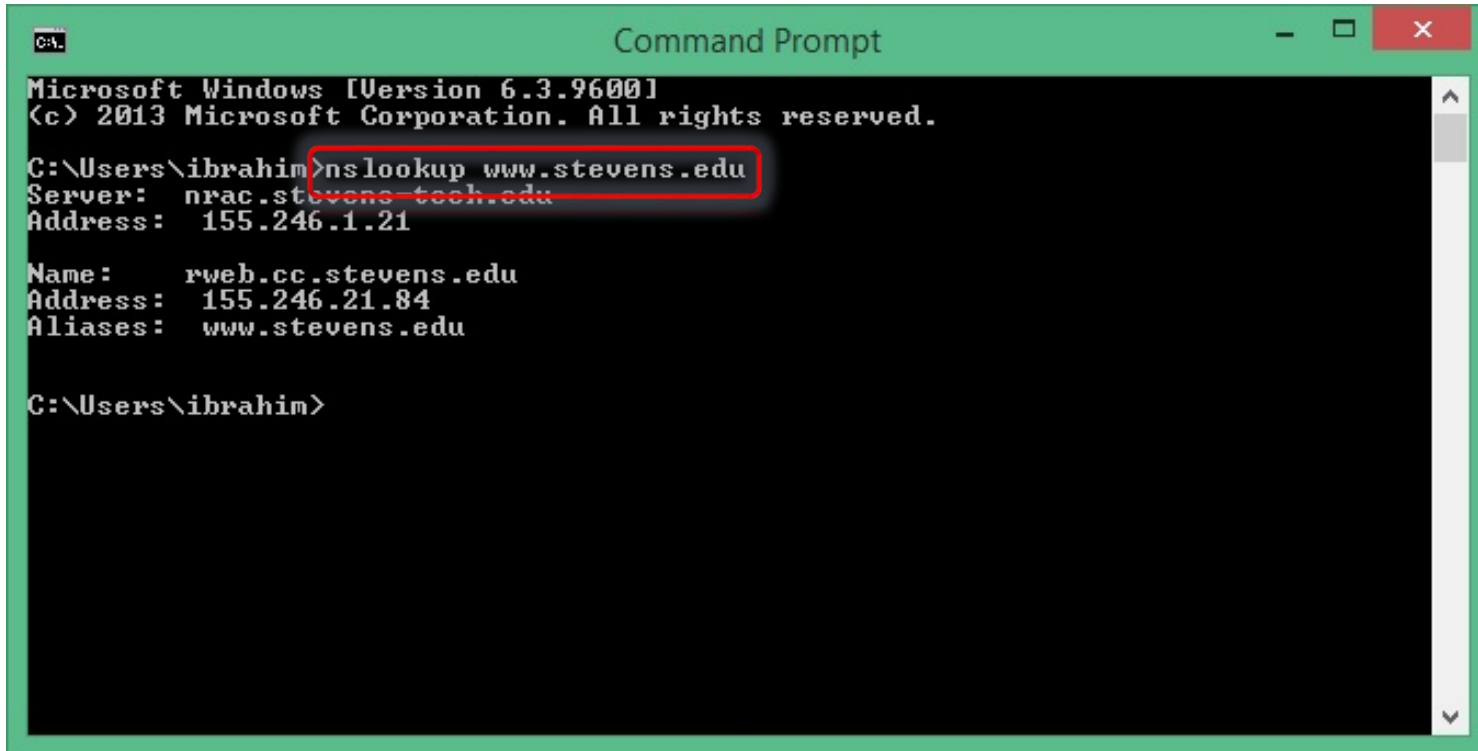
- Now, it's WIRESHARK time



- Now start up the Wireshark packet sniffer, and begin Wireshark packet capture.



- Now go back to the Windows Command Prompt and type “nslookup www.stevens.edu”.

A screenshot of a Windows Command Prompt window. The title bar is green and says "Command Prompt". The window shows the output of the command "nslookup www.stevens.edu". The output is as follows:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ibrahim>nslookup www.stevens.edu
Server:      nrac.stevens-tech.edu
Address:     155.246.1.21

Name:        rweb.cc.stevens.edu
Address:     155.246.21.84
Aliases:     www.stevens.edu

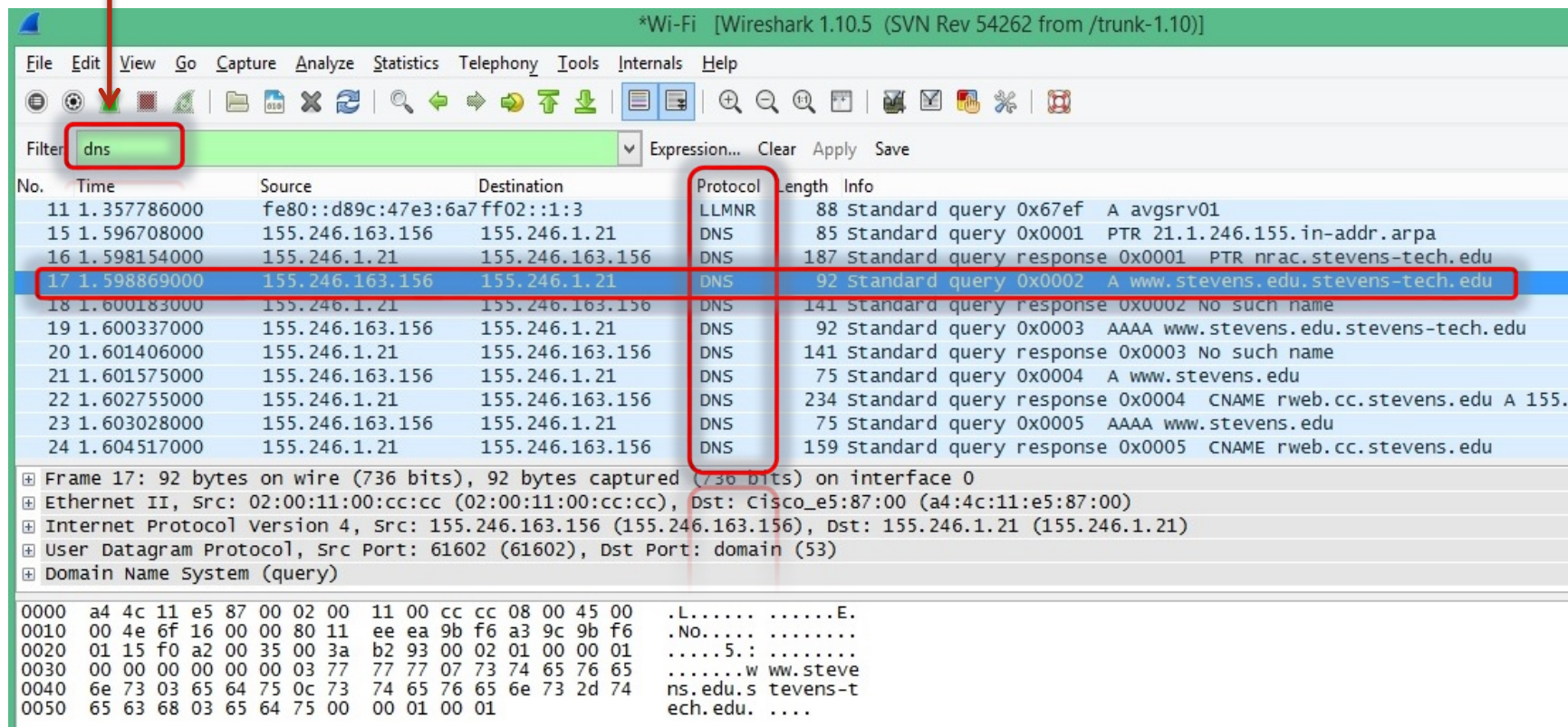
C:\Users\ibrahim>
```

The command "nslookup www.stevens.edu" is highlighted with a red rectangle.

- After that, go back to Wireshark and stop the packet capturing.



- Now let's take a look at the resulting WireShark window.
- **Hint:** We entered “DNS” into the filter field so we only see the DNS packets,



\*Wi-Fi [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter **dns** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
11	1.357786000	fe80::d89c:47e3:6a7ff02::1:3		LLMNR	88	Standard query 0x67ef A avgsrv01
15	1.596708000	155.246.163.156	155.246.1.21	DNS	85	Standard query 0x0001 PTR 21.1.246.155.in-addr.arpa
16	1.598154000	155.246.1.21	155.246.163.156	DNS	187	Standard query response 0x0001 PTR nrac.stevens-tech.edu
17	1.598869000	155.246.163.156	155.246.1.21	DNS	92	Standard query 0x0002 A www.stevens.edu.stevens-tech.edu
18	1.600183000	155.246.1.21	155.246.163.156	DNS	141	Standard query response 0x0002 No such name
19	1.600337000	155.246.163.156	155.246.1.21	DNS	92	Standard query 0x0003 AAAA www.stevens.edu.stevens-tech.edu
20	1.601406000	155.246.1.21	155.246.163.156	DNS	141	Standard query response 0x0003 No such name
21	1.601575000	155.246.163.156	155.246.1.21	DNS	75	Standard query 0x0004 A www.stevens.edu
22	1.602755000	155.246.1.21	155.246.163.156	DNS	234	Standard query response 0x0004 CNAME rweb.cc.stevens.edu A 155.
23	1.603028000	155.246.163.156	155.246.1.21	DNS	75	Standard query 0x0005 AAAA www.stevens.edu
24	1.604517000	155.246.1.21	155.246.163.156	DNS	159	Standard query response 0x0005 CNAME rweb.cc.stevens.edu

Frame 17: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Ethernet II, Src: 02:00:11:00:cc:cc (02:00:11:00:cc:cc), Dst: Cisco\_e5:87:00 (a4:4c:11:e5:87:00)

Internet Protocol Version 4, Src: 155.246.163.156 (155.246.163.156), Dst: 155.246.1.21 (155.246.1.21)

User Datagram Protocol, Src Port: 61602 (61602), Dst Port: domain (53)

Domain Name System (query)

```

0000  a4 4c 11 e5 87 00 02 00 11 00 cc cc 08 00 45 00  .L.....E.
0010  00 4e 6f 16 00 00 80 11 ee ea 9b f6 a3 9c 9b f6  .No.....
0020  01 15 f0 a2 00 35 00 3a b2 93 00 02 01 00 00 01  ....5.: ....
0030  00 00 00 00 00 00 03 77 77 77 07 73 74 65 76 65  ....w ww.steve
0040  6e 73 03 65 64 75 0c 73 74 65 76 65 6e 73 2d 74  ns.edu.s tevens-t
0050  65 63 68 03 65 64 75 00 00 01 00 01             ech.edu. ....

```