CS 716: Introduction to communication networks

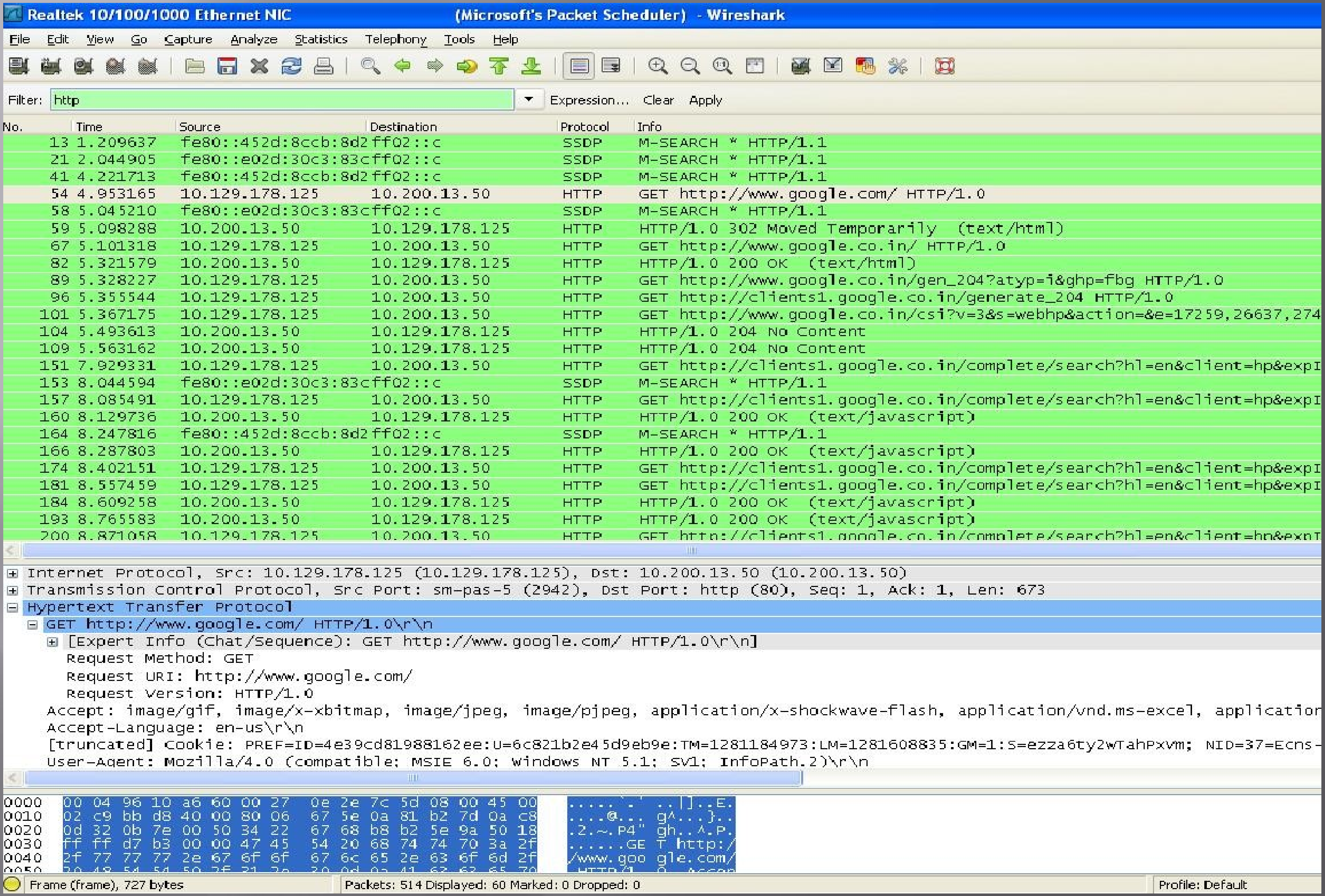
- 17th class; 30th Sept 2011

Instructor: Sridhar Iyer

Demo by: Swati Patil

IIT Bombay

Recap: HTTP Packet Sniffing using Wireshark


Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: http

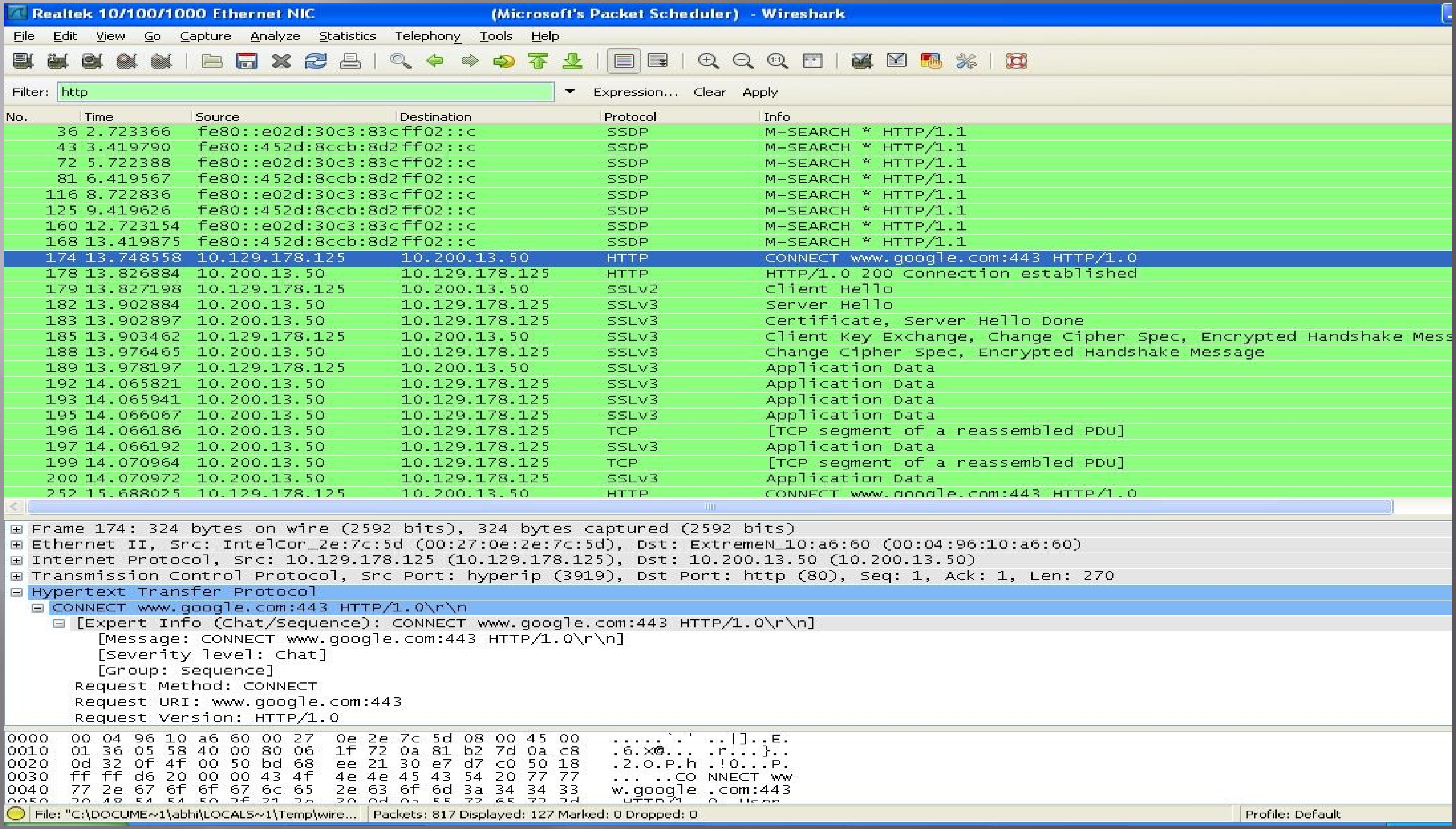
```
No.   Time     Source                   Destination      Protocol Info
   13 1.209637 fe80::452d:8ccb:8d2 ff02::c          SSDP     M-SEARCH * HTTP/1.1
   21 2.044905 fe80::e02d:30c3:83c ff02::c          SSDP     M-SEARCH * HTTP/1.1
   41 4.221713 fe80::452d:8ccb:8d2 ff02::c          SSDP     M-SEARCH * HTTP/1.1
   54 4.953165 10.129.178.125      10.200.13.50     HTTP     GET http://www.google.com/ HTTP/1.0
   58 5.045210 fe80::e02d:30c3:83c ff02::c          SSDP     M-SEARCH * HTTP/1.1
   59 5.098288 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 302 Moved Temporarily  (text/html)
   67 5.101318 10.129.178.125      10.200.13.50     HTTP     GET http://www.google.co.in/ HTTP/1.0
   82 5.321579 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 200 OK  (text/html)
   89 5.328227 10.129.178.125      10.200.13.50     HTTP     GET http://www.google.co.in/gen_204?atyp=i&ghp=fbg HTTP/1.0
   96 5.355544 10.129.178.125      10.200.13.50     HTTP     GET http://clients1.google.co.in/generate_204 HTTP/1.0
  101 5.367175 10.129.178.125      10.200.13.50     HTTP     GET http://www.google.co.in/csi?v=3&s=webhp&action=&e=17259,26637,274
  104 5.493613 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 204 No Content
  109 5.563162 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 204 No Content
  151 7.929331 10.129.178.125      10.200.13.50     HTTP     GET http://clients1.google.co.in/complete/search?hl=en&client=hp&expI
  153 8.044594 fe80::e02d:30c3:83c ff02::c          SSDP     M-SEARCH * HTTP/1.1
  157 8.085491 10.129.178.125      10.200.13.50     HTTP     GET http://clients1.google.co.in/complete/search?hl=en&client=hp&expI
  160 8.129736 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 200 OK  (text/javascript)
  164 8.247816 fe80::452d:8ccb:8d2 ff02::c          SSDP     M-SEARCH * HTTP/1.1
  166 8.287803 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 200 OK  (text/javascript)
  174 8.402151 10.129.178.125      10.200.13.50     HTTP     GET http://clients1.google.co.in/complete/search?hl=en&client=hp&expI
  181 8.557459 10.129.178.125      10.200.13.50     HTTP     GET http://clients1.google.co.in/complete/search?hl=en&client=hp&expI
  184 8.609258 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 200 OK  (text/javascript)
  193 8.765583 10.200.13.50        10.129.178.125   HTTP     HTTP/1.0 200 OK  (text/javascript)
  200 8.871058 10.129.178.125      10.200.13.50     HTTP     GET http://clients1.google.co.in/complete/search?hl=en&client=hp&expI
```

```
⊞ Internet Protocol, Src: 10.129.178.125 (10.129.178.125), Dst: 10.200.13.50 (10.200.13.50)
⊞ Transmission Control Protocol, Src Port: sm-pas-5 (2942), Dst Port: http (80), Seq: 1, Ack: 1, Len: 673
⊟ Hypertext Transfer Protocol
  ⊟ GET http://www.google.com/ HTTP/1.0\r\n
    ⊞ [Expert Info (Chat/Sequence): GET http://www.google.com/ HTTP/1.0\r\n]
      Request Method: GET
      Request URI: http://www.google.com/
      Request Version: HTTP/1.0
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application
    Accept-Language: en-us\r\n
    [truncated] Cookie: PREF=ID=4e39cd81988162ee:U=6c821b2e45d9eb9e:TM=1281184973:LM=1281608835:GM=1:S=ezza6ty2wTahPxVm; NID=37=Ecns-
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)\r\n
```

```
0000  00 04 96 10 a6 60 00 27  0e 2e 7c 5d 08 00 45 00   .....`.'  ..|]..E.
0010  02 c9 bb d8 40 00 80 06  67 5e 0a 81 b2 7d 0a c8   ....@...  g^...}..
0020  0d 32 0b 7e 00 50 34 22  67 68 b8 b2 5e 9a 50 18   .2.~.P4"  gh..^.P.
0030  ff ff d7 b3 00 00 47 45  54 20 68 74 74 70 3a 2f   ......GE  T http:/
0040  2f 77 77 77 2e 67 6f 6f  67 6c 65 2e 63 6f 6d 2f   /www.goo  gle.com/
```

Frame (frame), 727 bytes | Packets: 514 Displayed: 60 Marked: 0 Dropped: 0 | Profile: Default

Recap: HTTPS Packet Sniffing using Wireshark



Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: http

```
No.    Time       Source                   Destination      Protocol  Info
    36 2.723366   fe80::e02d:30c3:83cff02::c                 SSDP      M-SEARCH * HTTP/1.1
    43 3.419790   fe80::452d:8ccb:8d2ff02::c                 SSDP      M-SEARCH * HTTP/1.1
    72 5.722388   fe80::e02d:30c3:83cff02::c                 SSDP      M-SEARCH * HTTP/1.1
    81 6.419567   fe80::452d:8ccb:8d2ff02::c                 SSDP      M-SEARCH * HTTP/1.1
   116 8.722836   fe80::e02d:30c3:83cff02::c                 SSDP      M-SEARCH * HTTP/1.1
   125 9.419626   fe80::452d:8ccb:8d2ff02::c                 SSDP      M-SEARCH * HTTP/1.1
   160 12.723154  fe80::e02d:30c3:83cff02::c                 SSDP      M-SEARCH * HTTP/1.1
   168 13.419875  fe80::452d:8ccb:8d2ff02::c                 SSDP      M-SEARCH * HTTP/1.1
   174 13.748558  10.129.178.125           10.200.13.50     HTTP      CONNECT www.google.com:443 HTTP/1.0
   178 13.826884  10.200.13.50             10.129.178.125   HTTP      HTTP/1.0 200 Connection established
   179 13.827198  10.129.178.125           10.200.13.50     SSLv2     Client Hello
   182 13.902884  10.200.13.50             10.129.178.125   SSLv3     Server Hello
   183 13.902897  10.200.13.50             10.129.178.125   SSLv3     Certificate, Server Hello Done
   185 13.903462  10.129.178.125           10.200.13.50     SSLv3     Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
   188 13.976465  10.200.13.50             10.129.178.125   SSLv3     Change Cipher Spec, Encrypted Handshake Message
   189 13.978197  10.129.178.125           10.200.13.50     SSLv3     Application Data
   192 14.065821  10.200.13.50             10.129.178.125   SSLv3     Application Data
   193 14.065941  10.200.13.50             10.129.178.125   SSLv3     Application Data
   195 14.066067  10.200.13.50             10.129.178.125   SSLv3     Application Data
   196 14.066186  10.200.13.50             10.129.178.125   TCP       [TCP segment of a reassembled PDU]
   197 14.066192  10.200.13.50             10.129.178.125   SSLv3     Application Data
   199 14.070964  10.200.13.50             10.129.178.125   TCP       [TCP segment of a reassembled PDU]
   200 14.070972  10.200.13.50             10.129.178.125   SSLv3     Application Data
   252 15.688025  10.129.178.125           10.200.13.50     HTTP      CONNECT www.google.com:443 HTTP/1.0
```

```
⊞ Frame 174: 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits)
⊞ Ethernet II, Src: IntelCor_2e:7c:5d (00:27:0e:2e:7c:5d), Dst: ExtremeN_10:a6:60 (00:04:96:10:a6:60)
⊞ Internet Protocol, Src: 10.129.178.125 (10.129.178.125), Dst: 10.200.13.50 (10.200.13.50)
⊞ Transmission Control Protocol, Src Port: hyperip (3919), Dst Port: http (80), Seq: 1, Ack: 1, Len: 270
⊟ Hypertext Transfer Protocol
  ⊟ CONNECT www.google.com:443 HTTP/1.0\r\n
    ⊟ [Expert Info (Chat/Sequence): CONNECT www.google.com:443 HTTP/1.0\r\n]
        [Message: CONNECT www.google.com:443 HTTP/1.0\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: CONNECT
      Request URI: www.google.com:443
      Request Version: HTTP/1.0
```

```
0000   00 04 96 10 a6 60 00 27  0e 2e 7c 5d 08 00 45 00   .....`.' ..|]..E.
0010   01 36 05 58 40 00 80 06  1f 72 0a 81 b2 7d 0a c8   .6.X@... .r...}..
0020   0d 32 0f 4f 00 50 bd 68  ee 21 30 e7 d7 c0 50 18   .2.O.P.h .!0...P.
0030   ff ff d6 20 00 00 43 4f  4e 4e 45 43 54 20 77 77   ... ..CO NNECT ww
0040   77 2e 67 6f 6f 67 6c 65  2e 63 6f 6d 3a 34 34 33   w.google .com:443
```

File: "C:\DOCUME~1\abhi\LOCALS~1\Temp\wire... Packets: 817 Displayed: 127 Marked: 0 Dropped: 0 Profile: Default

Components of HTTPS

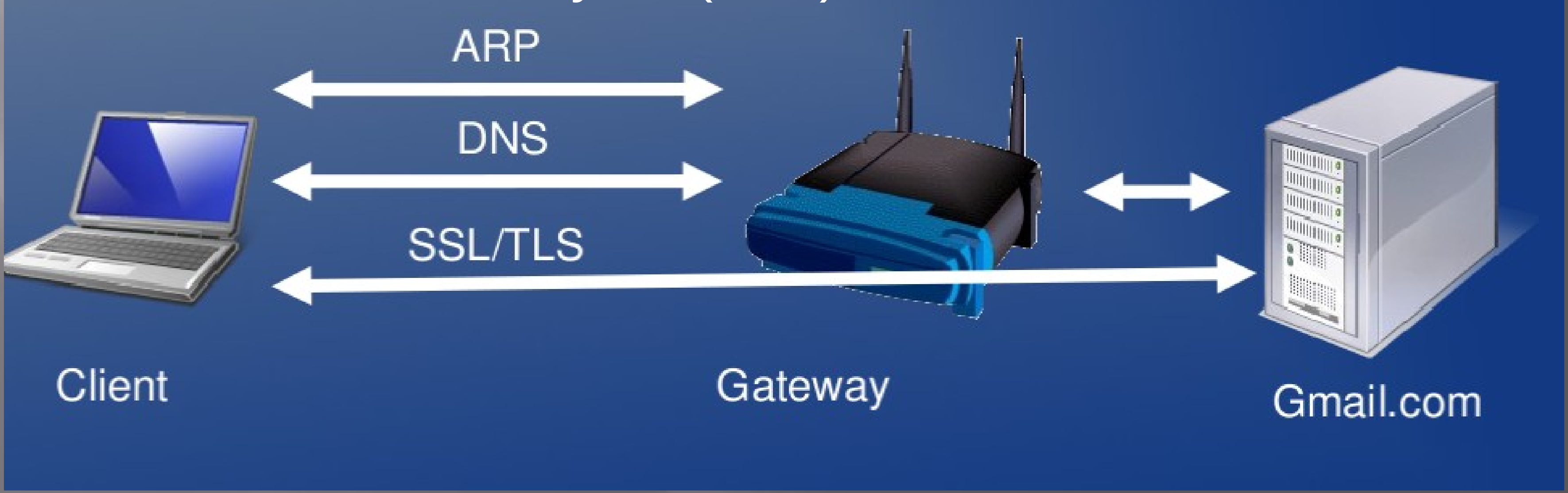
When you use a secure session (HTTPS), these protocols

work together:

Address Resolution Protocol (ARP)

Domain Name System (DNS)

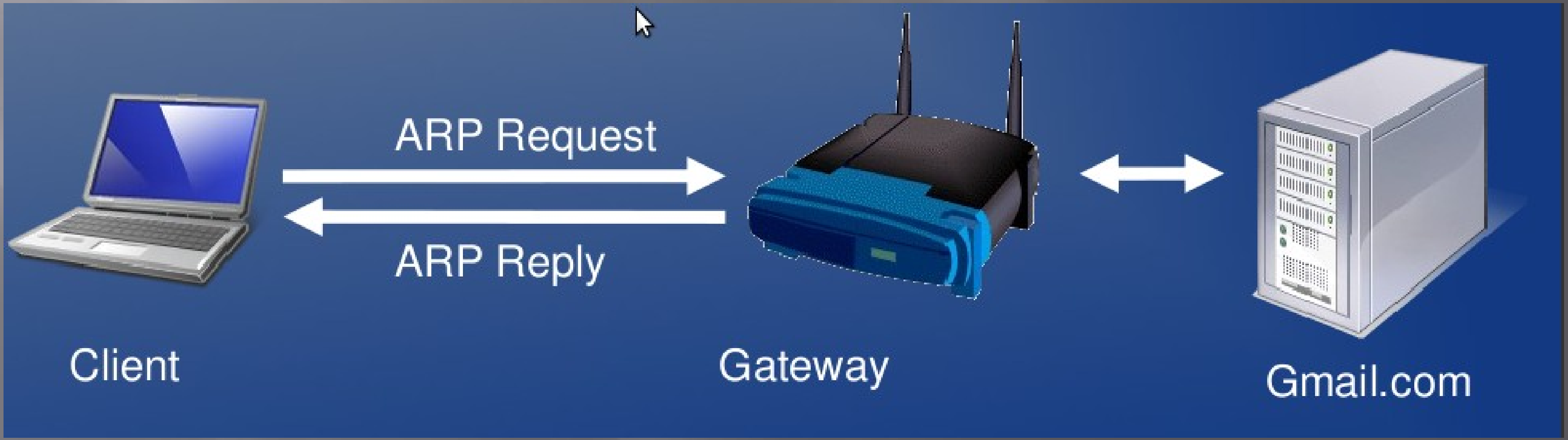
Secure Sockets Layers (SSL)



ARP Request and Reply

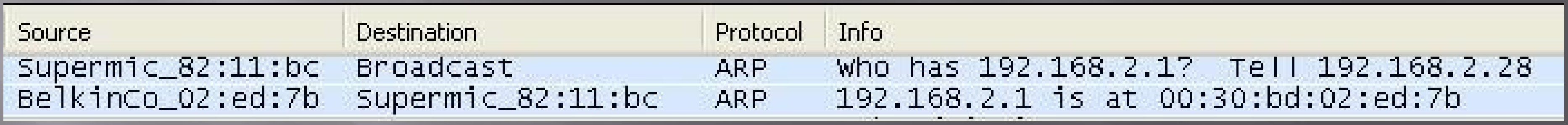
- Client wants to find Gateway
- ARP Request: Who has 192.168.2.1?
- ARP Reply:

MAC: 00-30-bd-02-ed-7b has 192.168.2.1



Demonstration
Sniffing ARP with Wireshark

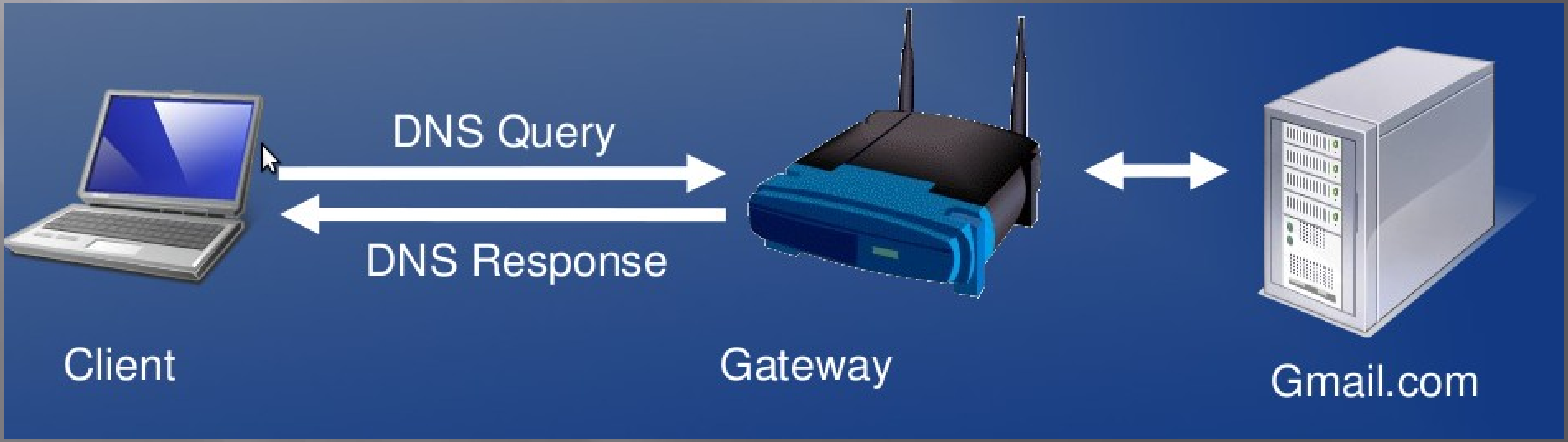
- Start Wireshark capturing packets
- Clear the ARP cache
- arp –d *
- Ping the default gateway



```
Source             Destination        Protocol  Info
Supermic_82:11:bc  Broadcast          ARP       Who has 192.168.2.1?  Tell 192.168.2.28
BelkinCo_02:ed:7b  Supermic_82:11:bc  ARP       192.168.2.1 is at 00:30:bd:02:ed:7b
```

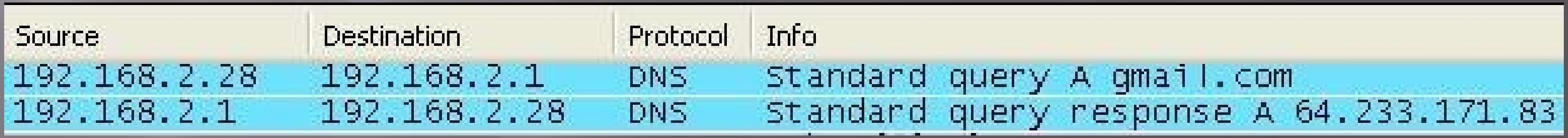
DNS Query and Response

- Client wants to find Gmail.com
- DNS Query: Where is Gmail.com?
- DNS Response3:
- Gmail.com is at 64.233.171.8



Demonstration
Sniffing DNS with Wireshark

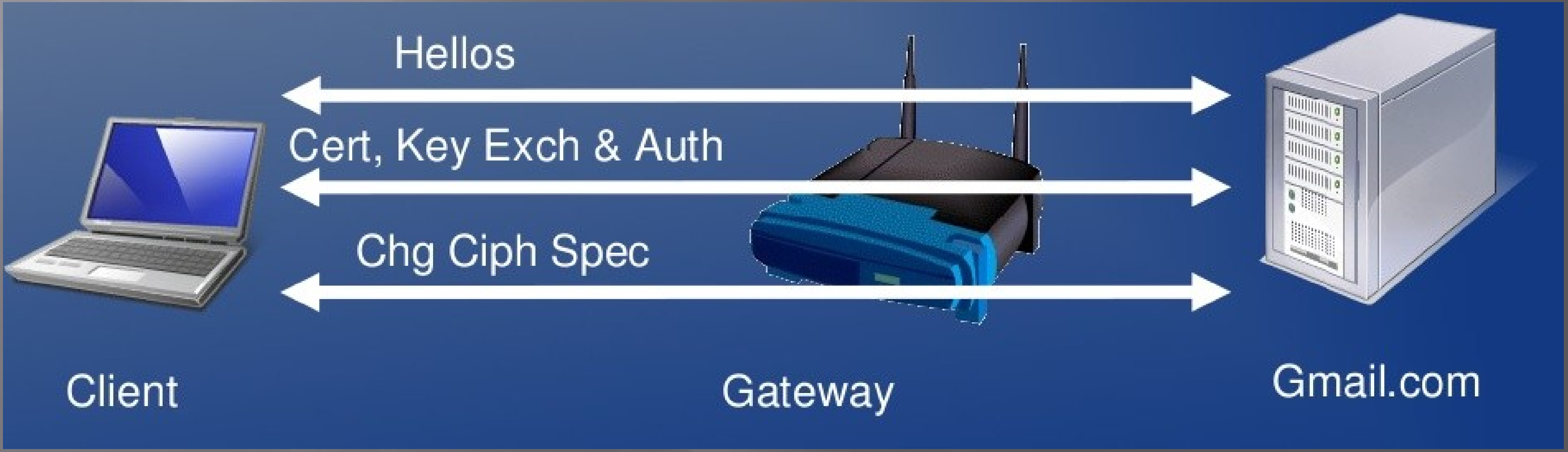
- Start Wireshark capturing packets
- Clear the DNS cache
- ipconfig /flushdns
- Ping Gmail.com



Source	Destination	Protocol	Info
192.168.2.28	192.168.2.1	DNS	Standard query A gmail.com
192.168.2.1	192.168.2.28	DNS	Standard query response A 64.233.171.83

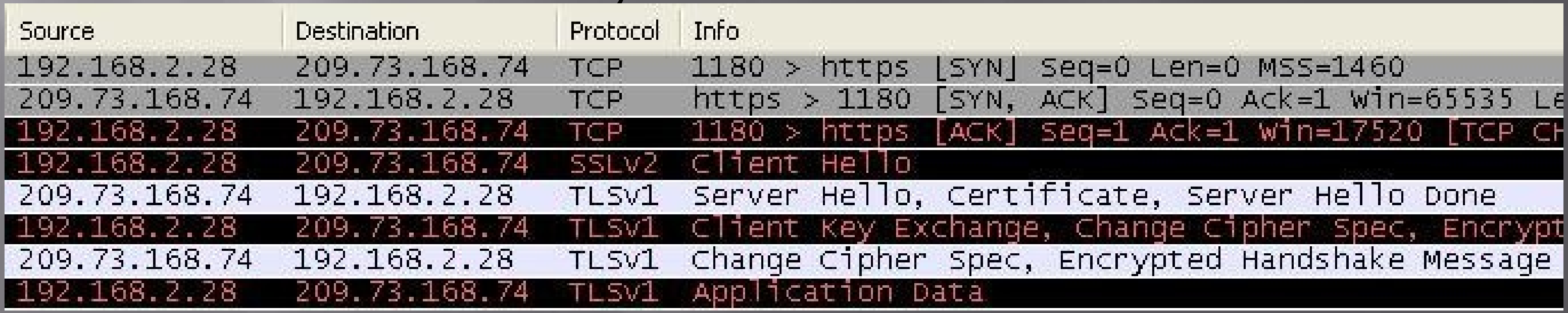
SSL Handshake

- SSL handshake has three stages:
- Hellos
- Certificate, Key Exchange, and Authentication
- "Change cipher spec" – handshake finished
- The Gateway just forwards all this traffic to the Web server



Demonstration Sniffing SSL Handshake with Wireshark

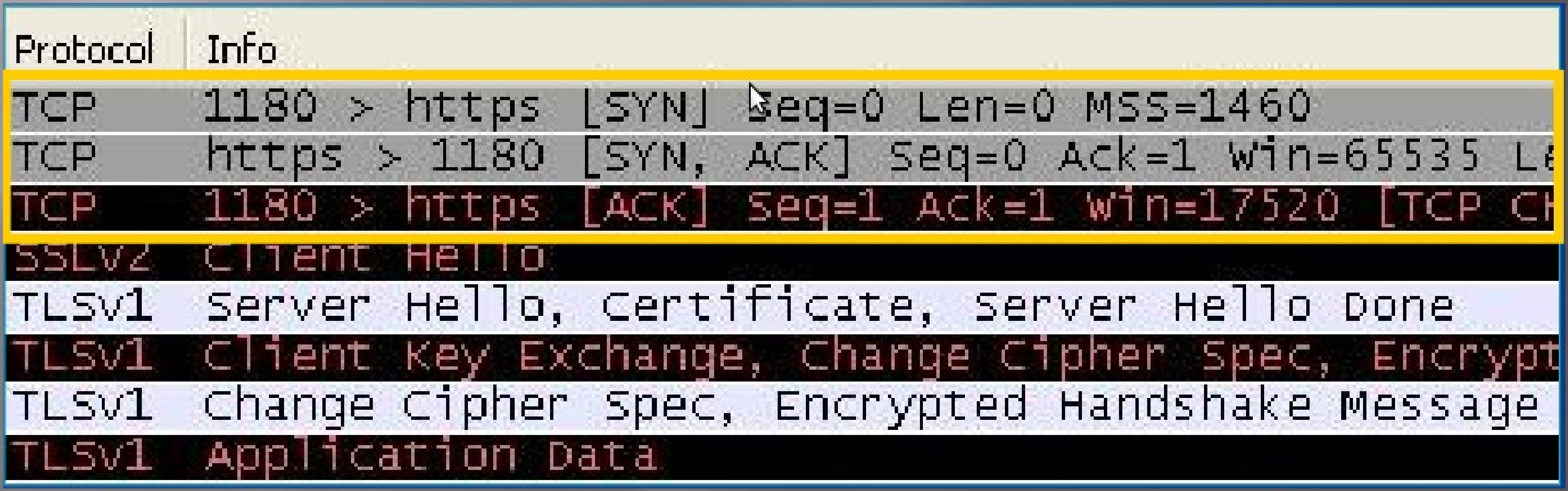
- Start Wireshark capturing packets
- Open a browser and go to yahoo.com
- Click the My Mail button



Source	Destination	Protocol	Info
192.168.2.28	209.73.168.74	TCP	1180 > https [SYN] Seq=0 Len=0 MSS=1460
209.73.168.74	192.168.2.28	TCP	https > 1180 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
192.168.2.28	209.73.168.74	TCP	1180 > https [ACK] Seq=1 Ack=1 Win=17520 [TCP CH
192.168.2.28	209.73.168.74	SSLv2	Client Hello
209.73.168.74	192.168.2.28	TLSv1	Server Hello, Certificate, Server Hello Done
192.168.2.28	209.73.168.74	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypt
209.73.168.74	192.168.2.28	TLSv1	Change Cipher Spec, Encrypted Handshake Message
192.168.2.28	209.73.168.74	TLSv1	Application Data

Open a Socket to Port 443

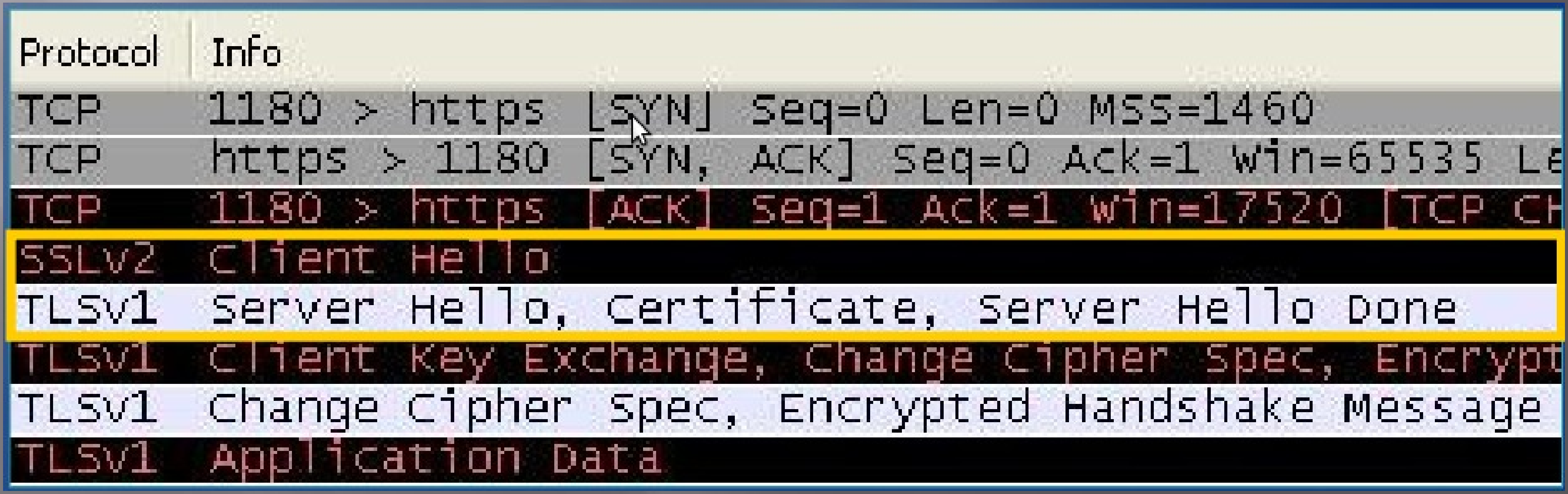
- This is the usual SYN, SYN/ACK, SYN TCP handshake
- Port 443 is used for HTTPS



```
Protocol  Info
TCP       1180 > https [SYN] Seq=0 Len=0 MSS=1460
TCP       https > 1180 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
TCP       1180 > https [ACK] Seq=1 Ack=1 Win=17520 [TCP C
SSLv2     Client Hello
TLSv1     Server Hello, Certificate, Server Hello Done
TLSv1     Client Key Exchange, Change Cipher Spec, Encrypt
TLSv1     Change Cipher Spec, Encrypted Handshake Message
TLSv1     Application Data
```

Hellos

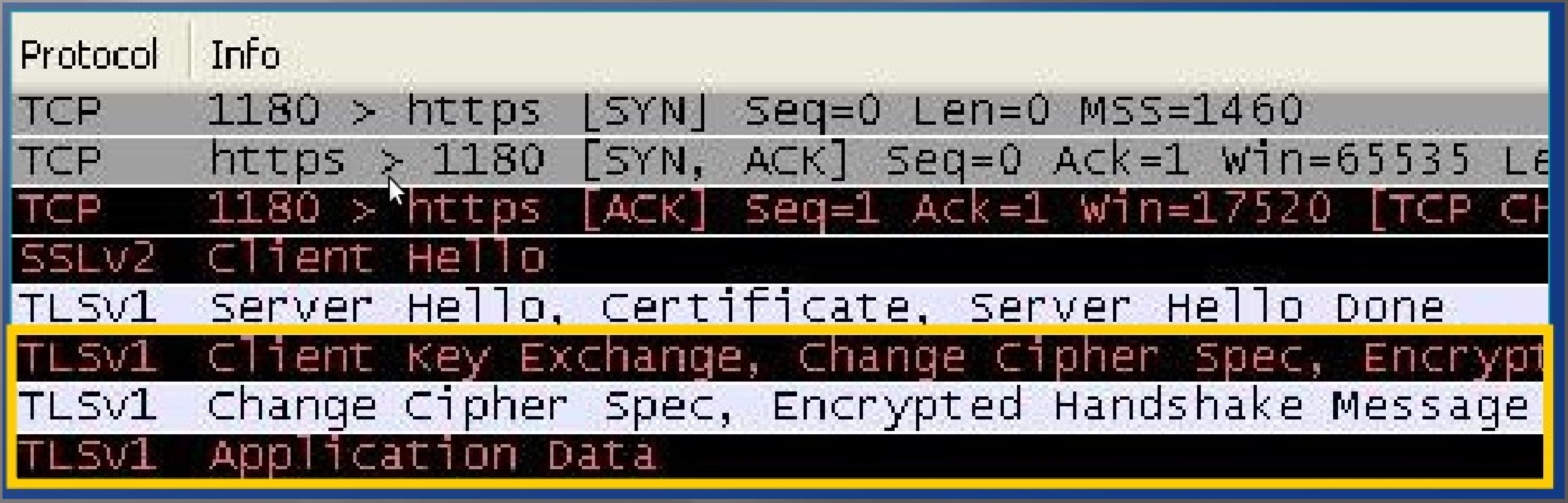
- Client Hello
- Server sends Hello
- This exchange is used to agree on aprotocol version and encryption method



```
Protocol  Info
TCP       1180 > https [SYN] Seq=0 Len=0 MSS=1460
TCP       https > 1180 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
TCP       1180 > https [ACK] Seq=1 Ack=1 Win=17520 [TCP CH
SSLv2     Client Hello
TLSv1     Server Hello, Certificate, Server Hello Done
TLSv1     Client Key Exchange, Change Cipher Spec, Encrypt
TLSv1     Change Cipher Spec, Encrypted Handshake Message
TLSv1     Application Data
```

Change Cipher Spec

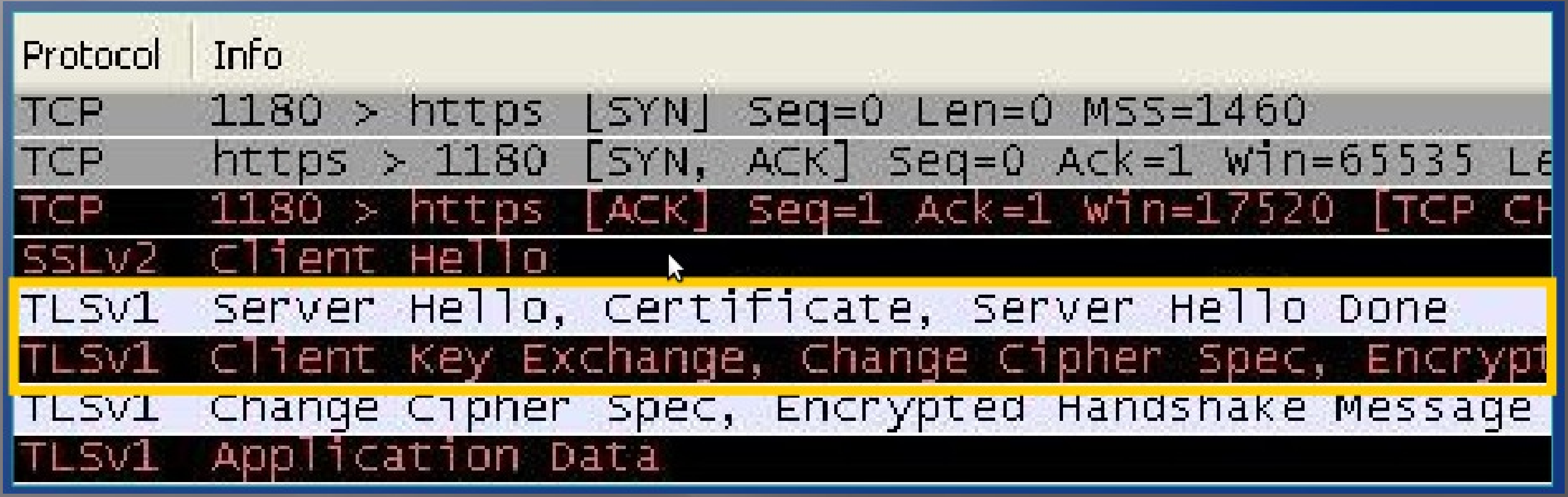
- Server sends "Change Cipher Spec"
- Client sends "Change Cipher Spec"
- SSL Handshake is done, now client can send encrypted Application Data



```
Protocol  Info
TCP       1180 > https [SYN] Seq=0 Len=0 MSS=1460
TCP       https > 1180 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
TCP       1180 > https [ACK] Seq=1 Ack=1 Win=17520 [TCP CH
SSLv2     Client Hello
TLSv1     Server Hello, Certificate, Server Hello Done
TLSv1     Client Key Exchange, Change Cipher Spec, Encrypt
TLSv1     Change Cipher Spec, Encrypted Handshake Message
TLSv1     Application Data
```

Certificate, Key Exchange, and Authentication

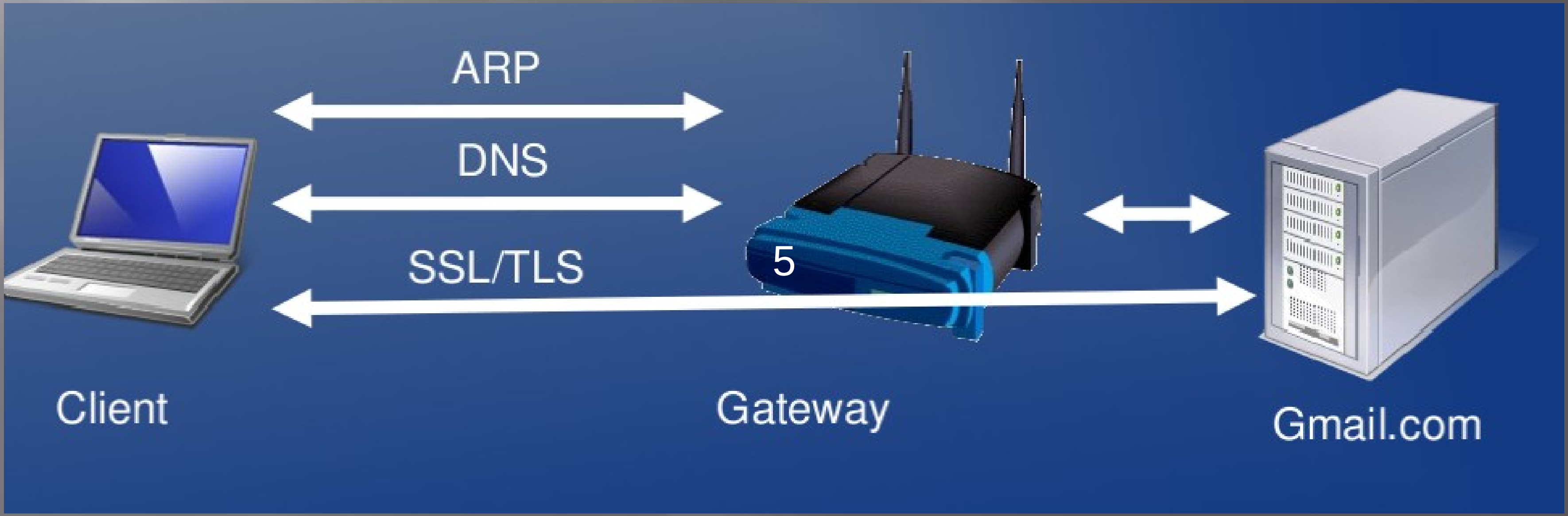
- Server sends Certificate
- Client sends Public Key
- Client Authenticates Certificate with Certificate Authority (not visible)



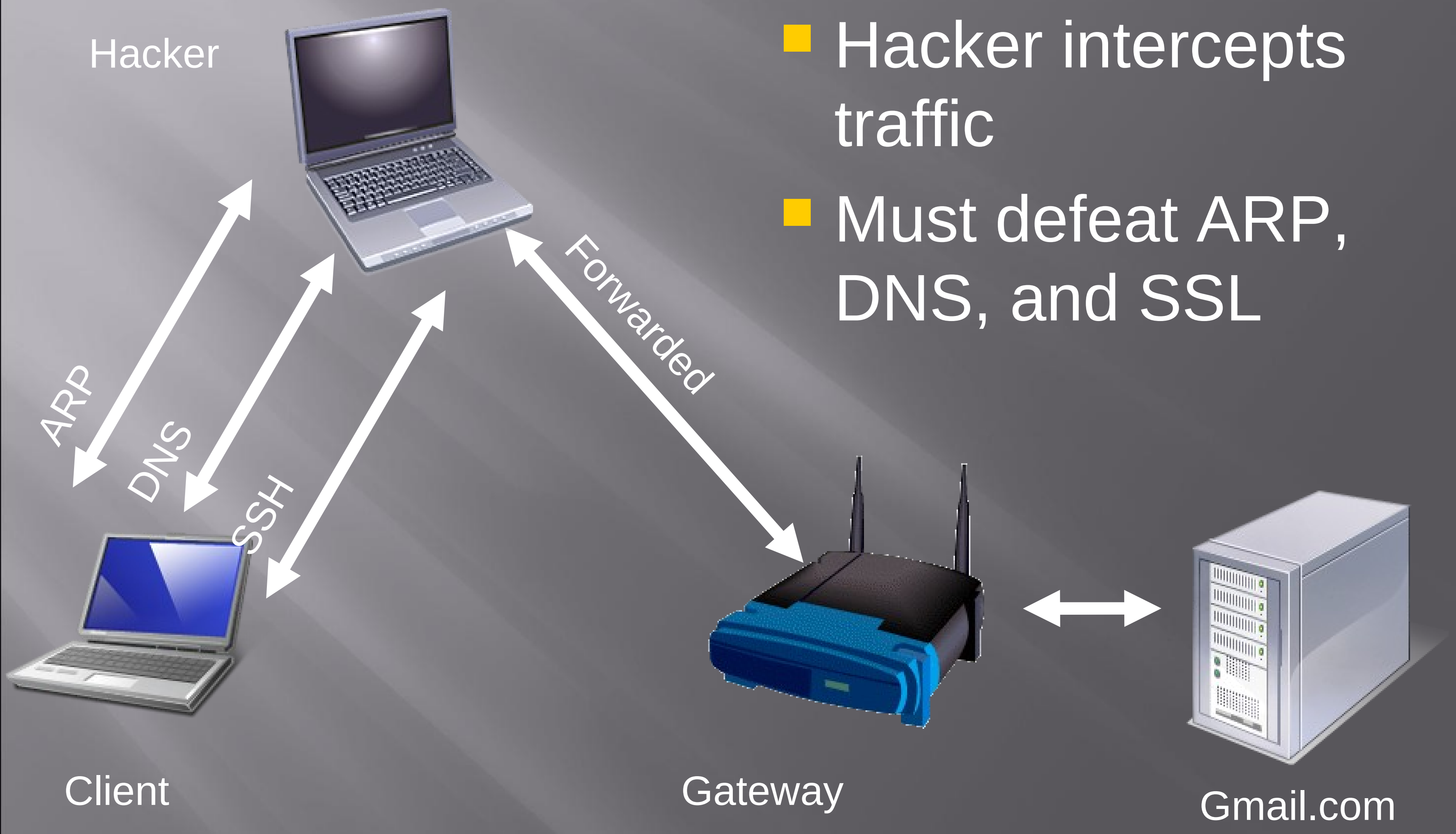
Protocol	Info
TCP	1180 > https [SYN] Seq=0 Len=0 MSS=1460
TCP	https > 1180 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
TCP	1180 > https [ACK] Seq=1 Ack=1 Win=17520 [TCP CH
SSLv2	Client Hello
TLSv1	Server Hello, Certificate, Server Hello Done
TLSv1	Client Key Exchange, Change Cipher Spec, Encrypt
TLSv1	Change Cipher Spec, Encrypted Handshake Message
TLSv1	Application Data

Summary of HTTPS Process

- SSL handshake has three stages:
- Hellos
- Certificate, Key Exchange, and Authentication
- "Change cipher spec" – handshake finished



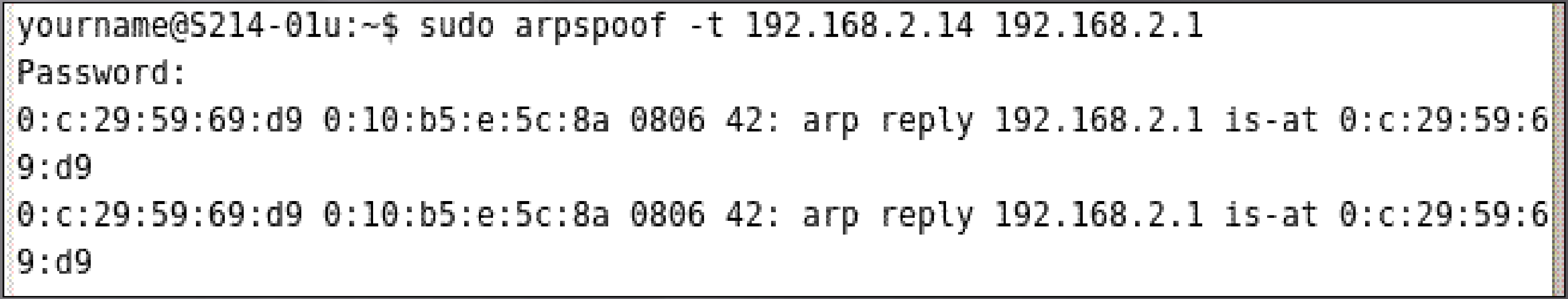
Man-in-the-Middle Attack



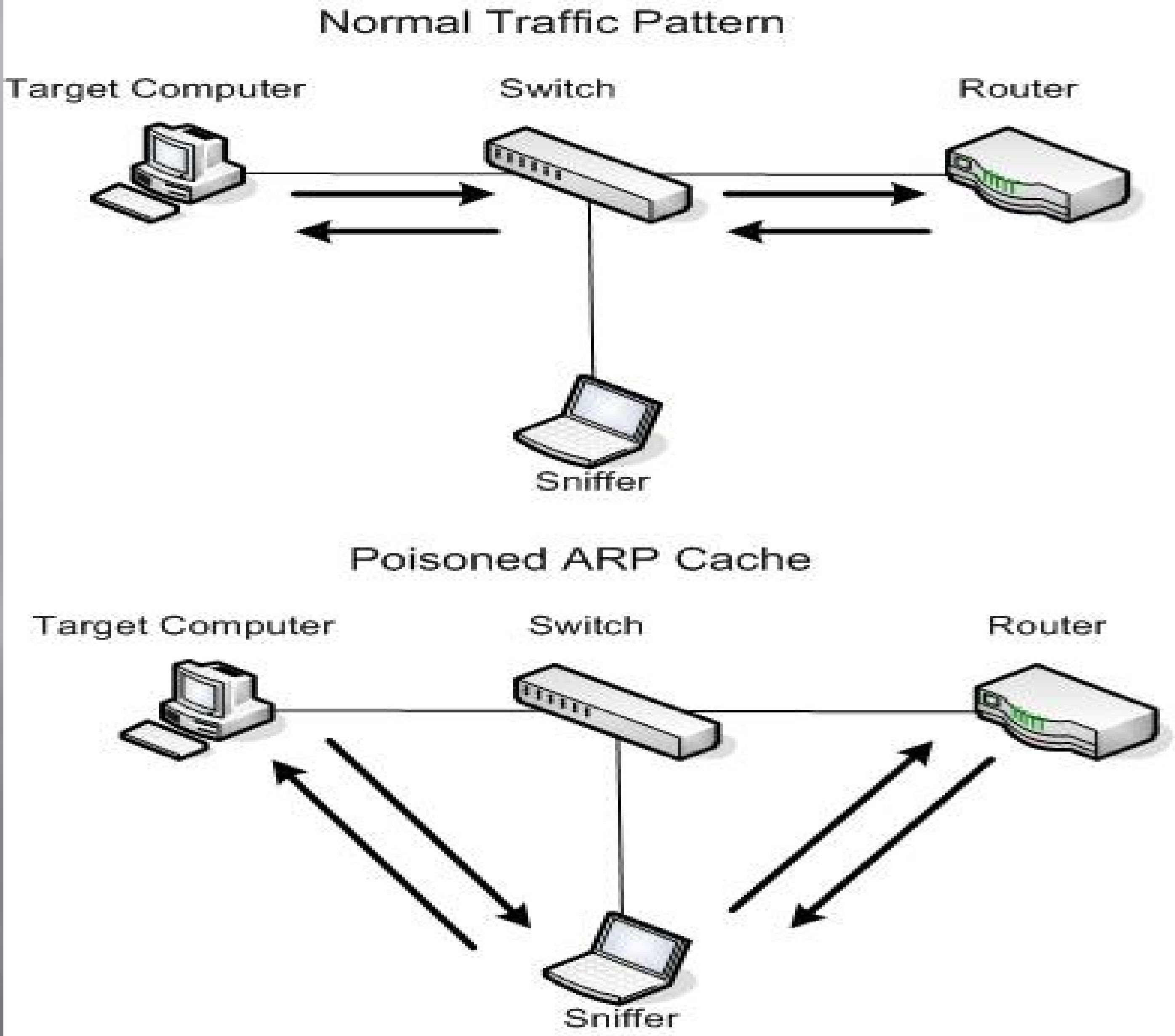
- Hacker intercepts traffic
- Must defeat ARP, DNS, and SSL

ARP Cache Poisoning

ARP cache poisoning, also known as ARP spoofing.
It is the process of falsifying the source Media Access Control (MAC) addresses of packets being sent on an Ethernet network.
It is a MAC layer attack that can only be carried out when an attacker is connected to the same local network as the target machines.



```
yourname@S214-01u:~$ sudo arpspoof -t 192.168.2.14 192.168.2.1
Password:
0:c:29:59:69:d9 0:10:b5:e:5c:8a 0806 42: arp reply 192.168.2.1 is-at 0:c:29:59:6
9:d9
0:c:29:59:69:d9 0:10:b5:e:5c:8a 0806 42: arp reply 192.168.2.1 is-at 0:c:29:59:6
9:d9
```

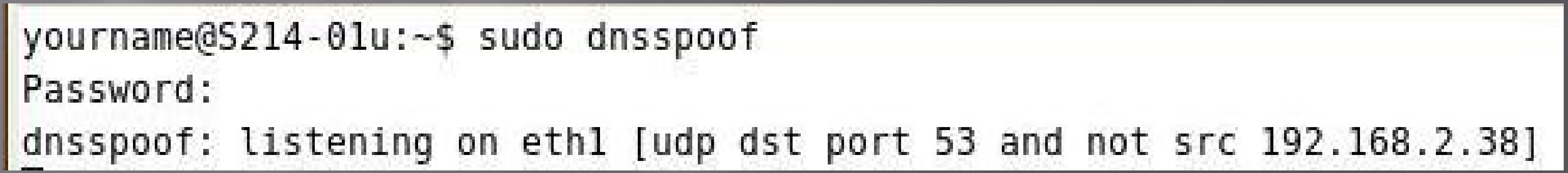


Normal Traffic Pattern

Poisoned ARP Cache

DNS SPOOFING

The mechanism of DNS spoofing is based on the fact of presenting false or fake DNS information to the victim in a response to their DNS request and as a result forcing them to visit a site which is not the real one.



```
yourname@S214-01u:~$ sudo dnsspoof
Password:
dnsspoof: listening on eth1 [udp dst port 53 and not src 192.168.2.38]
```