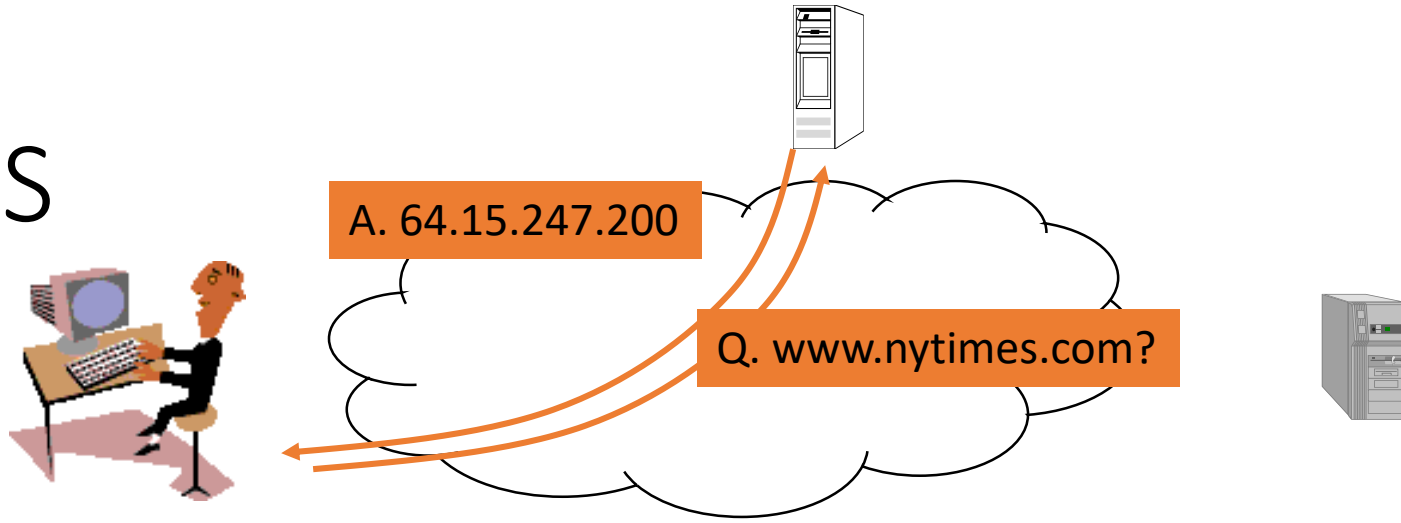


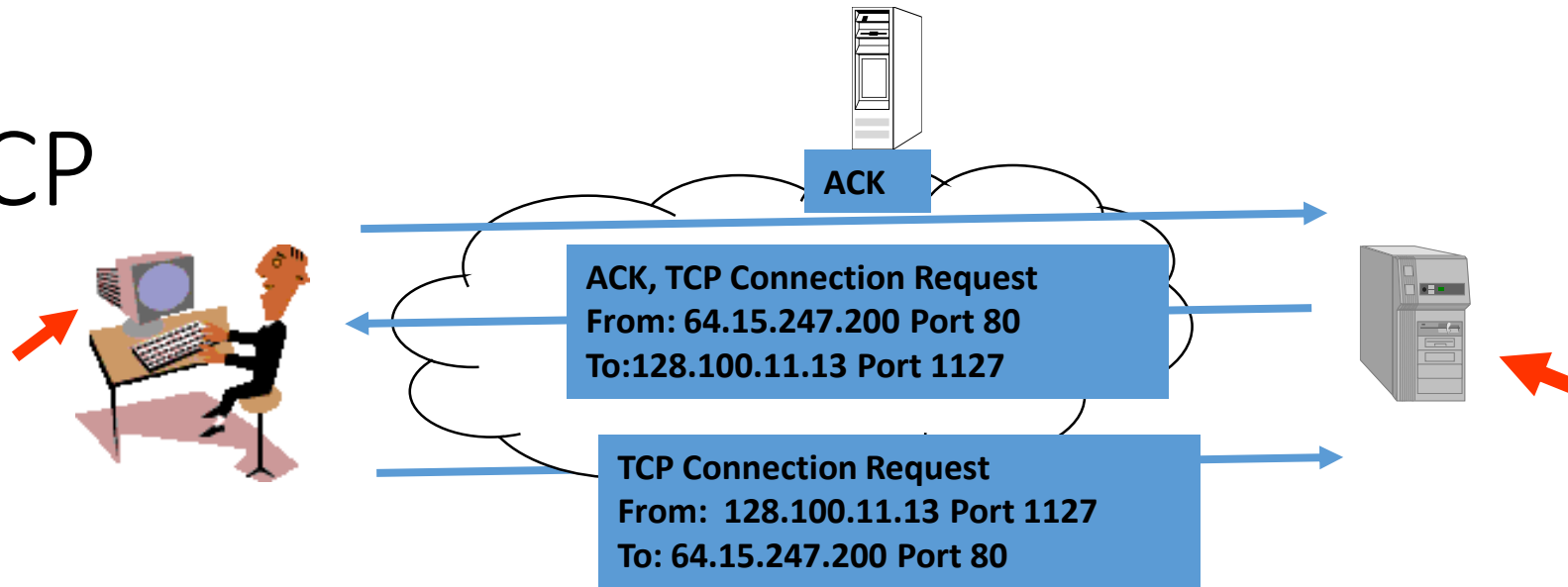
# 實驗二 wireshark

# 1. DNS



- User clicks on <http://www.nytimes.com/>
- URL contains Internet name of machine ([www.nytimes.com](http://www.nytimes.com/)), but not Internet address
- Internet needs Internet address to send information to a machine
- Browser software uses Domain Name System (DNS) protocol to send query for Internet address
- DNS system responds with Internet address

## 2. TCP

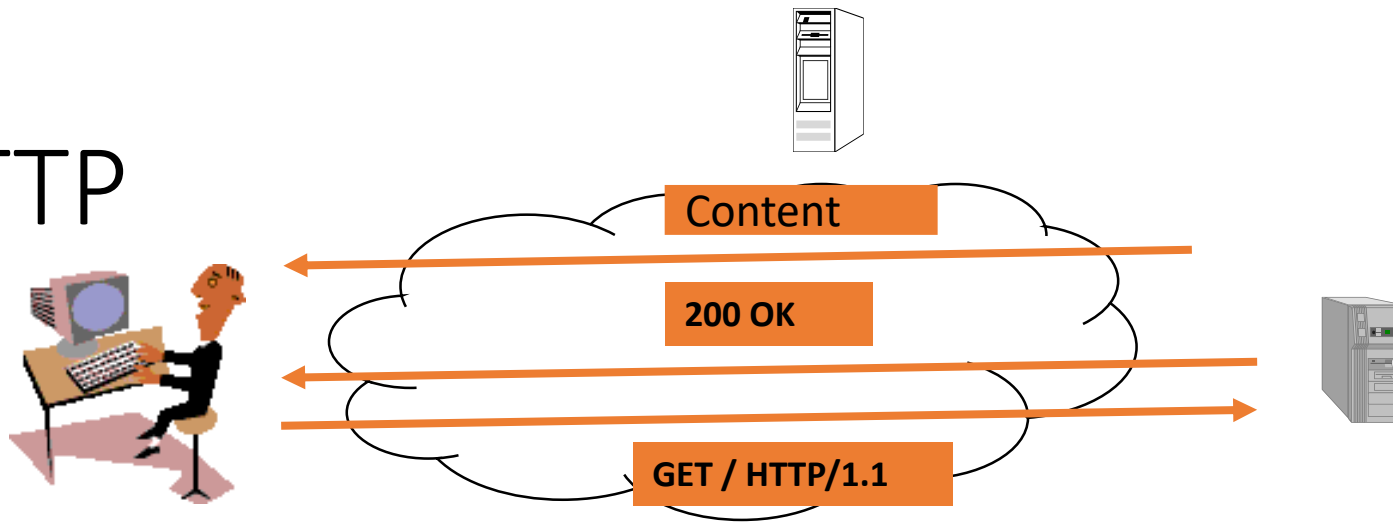


- Browser software uses HyperText Transfer Protocol (HTTP) to send request for document
- HTTP server waits for requests by listening to a well-known port number (80 for HTTP)
- HTTP client sends request messages through an “ephemeral port number,” e.g. 1127
- HTTP needs a Transmission Control Protocol (TCP) connection between the HTTP client and the HTTP server to transfer messages reliably

# Example: TCP

- TCP is a transport layer protocol
- Provides *reliable byte stream service* between two processes in two computers across the Internet
- Sequence numbers keep track of the bytes that have been transmitted and received
- Error detection and retransmission used to recover from transmission errors and losses
- TCP is *connection-oriented*: the sender and receiver must first establish an association and set initial sequence numbers before data is transferred
- Connection ID is specified uniquely by  
(*send port #, send IP address, receive port #, receiver IP address*)

### 3. HTTP

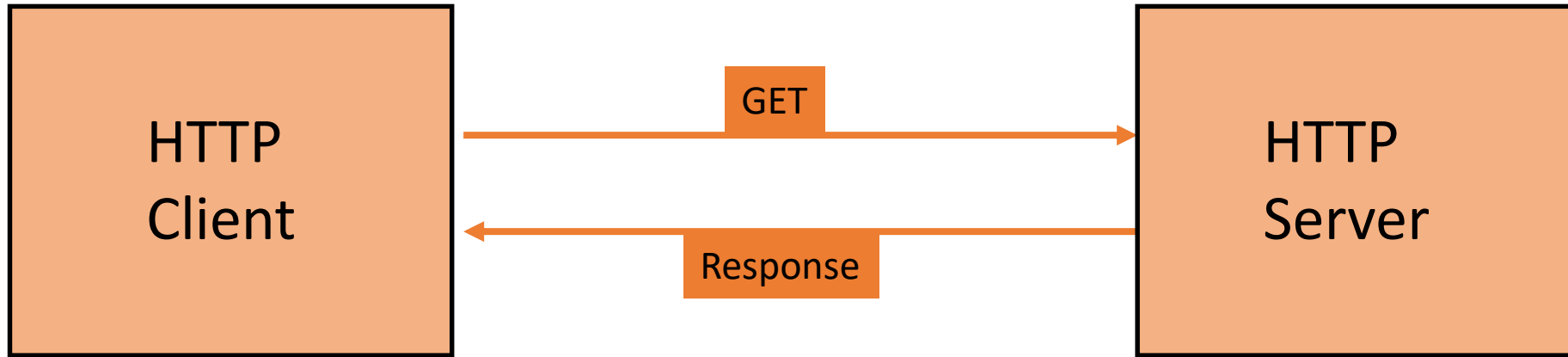


- HTTP client sends its request message: “GET ...”
- HTTP server sends a status response: “200 OK”
- HTTP server sends requested file
- Browser displays document
- Clicking a link sets off a chain of events across the Internet!
- Let’s see how protocols & layers come into play...

# Example: HTTP

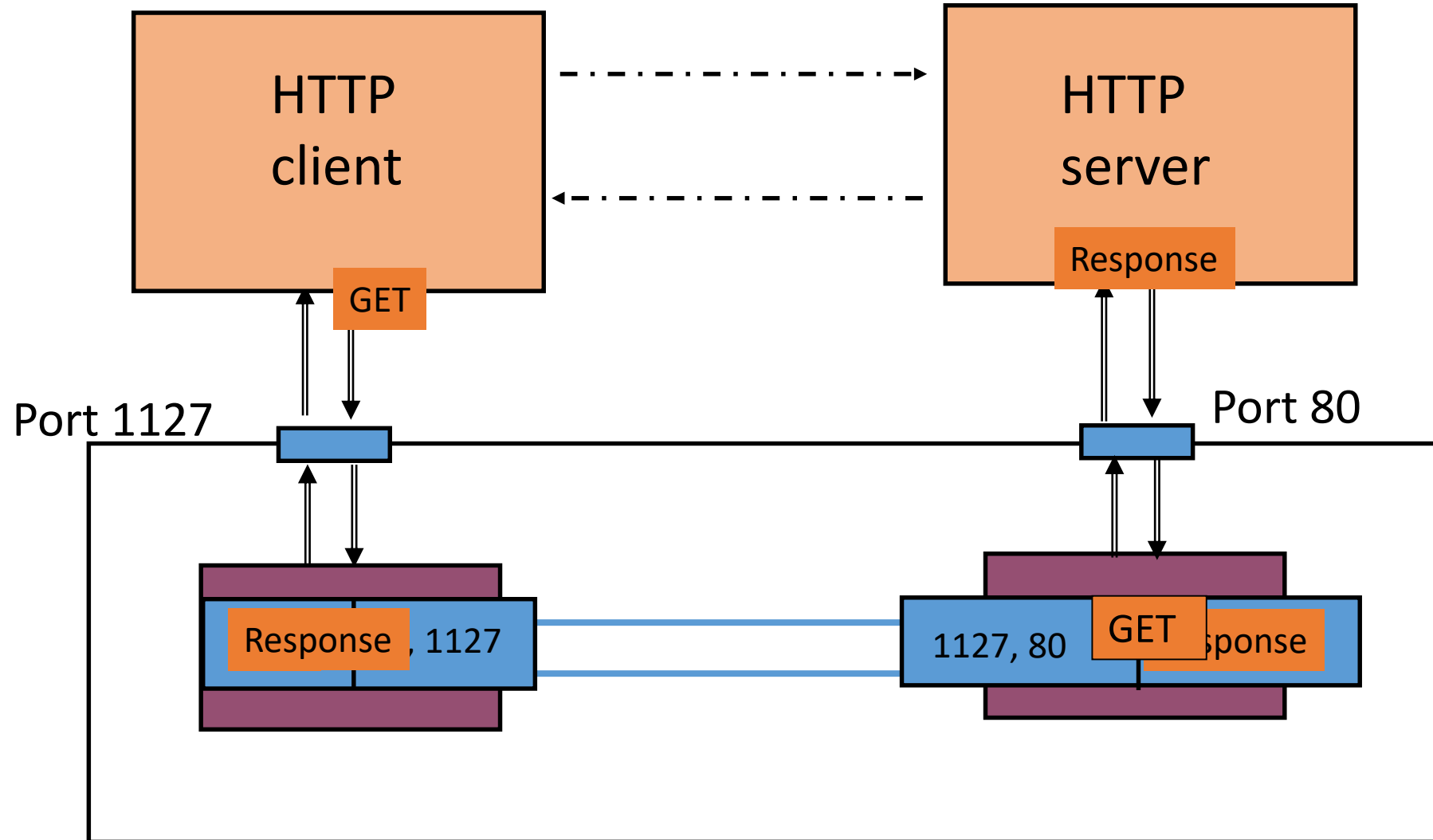
- HTTP is an application layer protocol
- Retrieves documents on behalf of a browser application program
- HTTP specifies fields in request messages and response messages
  - Request types; Response codes
  - Content type, options, cookies, ...
- HTTP specifies actions to be taken upon receipt of certain messages

# HTTP Protocol



- HTTP assumes messages can be exchanged directly between HTTP client and HTTP server
- In fact, HTTP client and server are processes running in two different machines across the Internet
- HTTP uses the reliable stream transfer service provided by TCP

# HTTP uses service of TCP





# HTTP Protocol

- HTTP servers use well-known port 80
- Client request / Server reply
- Stateless: server does not keep any information about client
- HTTP 1.0 new TCP connection per request/reply (non-persistent)
- HTTP 1.1 persistent operation is default

# HTTP Typical Exchange

The image shows a Wireshark packet capture window titled '\*ens33'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter bar set to 'Apply a display filter ... <Ctrl-/>'. The main packet list table shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
284	120.926908706	192.168.126.2	192.168.126.135	DNS	122	Standard query response 0x449c AAAA www.ccu.edu.tw...
285	120.926913856	192.168.126.2	192.168.126.135	DNS	110	Standard query response 0xfc39 A www.ccu.edu.tw CN...
286	120.957139114	140.123.5.5	192.168.126.135	TCP	482	80 → 43792 [PSH, ACK] Seq=1 Ack=435 Win=64240 Len=...
287	120.957161530	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=429 Win=30016 Len=0
288	120.957616821	140.123.5.5	192.168.126.135	TCP	2974	80 → 43792 [PSH, ACK] Seq=429 Ack=435 Win=64240 Le...
289	120.957622478	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=3349 Win=35040 Len=0
290	120.958778417	140.123.5.5	192.168.126.135	TCP	5894	80 → 43792 [PSH, ACK] Seq=3349 Ack=435 Win=64240 L...
291	120.958794456	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=9189 Win=46720 Len=0
292	120.959753066	140.123.5.5	192.168.126.135	TCP	8814	80 → 43792 [PSH, ACK] Seq=9189 Ack=435 Win=64240 L...
293	120.959759975	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=17949 Win=64240 Len=0
294	120.960362750	140.123.5.5	192.168.126.135	TCP	5894	80 → 43792 [PSH, ACK] Seq=17949 Ack=435 Win=64240 ...
295	120.960368491	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=23789 Win=64240 Len=0
296	120.961118545	140.123.5.5	192.168.126.135	TCP	8814	80 → 43792 [PSH, ACK] Seq=23789 Ack=435 Win=64240 ...
297	120.961126198	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=32549 Win=64240 Len=0
298	120.961766503	140.123.5.5	192.168.126.135	HTTP	1689	HTTP/1.1 200 OK (text/html)
299	120.961771416	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=34184 Win=64240 Len=0
300	121.000572639	192.168.126.135	192.168.126.2	DNS	74	Standard query 0xa581 A www.ccu.edu.tw
301	121.000653713	192.168.126.135	192.168.126.2	DNS	74	Standard query 0xb6f6 AAAA www.ccu.edu.tw
302	121.001436086	192.168.126.135	140.123.5.5	HTTP	542	GET /css/template.css HTTP/1.1
303	121.001650872	140.123.5.5	192.168.126.135	TCP	60	80 → 43790 [ACK] Seq=1 Ack=489 Win=64240 Len=0
304	121.002563644	192.168.126.135	192.168.126.2	DNS	79	Standard query 0x8283 A use.fontawesome.com
305	121.002597074	140.123.5.5	192.168.126.135	HTTP	426	HTTP/1.1 304 Not Modified
306	121.002615140	192.168.126.135	140.123.5.5	TCP	54	43790 → 80 [ACK] Seq=489 Ack=373 Win=30016 Len=0
307	121.002750654	192.168.126.135	192.168.126.2	DNS	79	Standard query 0x2cc5 AAAA use.fontawesome.com
308	121.003197551	192.168.126.135	23.111.9.35	TLSv1.2	135	Application Data
309	121.003630381	23.111.9.35	192.168.126.135	TCP	60	443 → 47940 [ACK] Seq=93 Ack=174 Win=64240 Len=0
310	121.003636807	192.168.126.2	192.168.126.135	DNS	110	Standard query response 0xa581 A www.ccu.edu.tw CN...
311	121.004205765	192.168.126.135	192.168.126.2	DNS	75	Standard query 0x8554 A code.jquery.com
312	121.004238211	192.168.126.2	192.168.126.135	DNS	122	Standard query response 0xb6f6 AAAA www.ccu.edu.tw...
313	121.004527715	192.168.126.135	192.168.126.2	DNS	75	Standard query 0x508b AAAA code.jquery.com
314	121.005630576	192.168.126.2	192.168.126.135	DNS	146	Standard query response 0x8283 A use.fontawesome.c...

Below the packet list, the packet details pane shows the structure of packet 280:

- Frame 280: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface 0
- Ethernet II, Src: Vmware\_d0:dd:db (00:0c:29:d0:dd:db), Dst: Vmware\_ef:c8:5b (00:50:56:ef:c8:5b)
- Internet Protocol Version 4, Src: 192.168.126.135, Dst: 140.123.5.5
- Transmission Control Protocol, Src Port: 43792, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data for packet 280:

```
0000 00 50 56 ef c8 5b 00 0c 29 d0 dd db 08 00 45 00  ·PV·····E·
0010 01 da dd a1 40 00 40 06 8a cc c0 a8 7e 87 8c 7b  ····@· ····{
0020 05 05 ab 10 00 50 f1 21 f4 36 0f b8 54 c9 50 18  ····P·! ·6·T·P·
0030 72 10 d2 7c 00 00 47 45 54 20 2f 20 48 54 54 50  ····|··GE T / HTTP
```

The status bar at the bottom indicates: wireshark\_ens33\_20190313024637\_oFU538.pcapng, Packets: 1534 · Displayed: 1534 (100.0%) · Profile: Default

# HTTP Message Formats

- HTTP messages written in ASCII text
- Request Message Format
  - *Request Line (Each line ends with carriage return)*
    - *Method URL HTTP-Version \r\n*
    - Method specifies action to apply to object
    - URL specifies object
  - *Header Lines (Ea. line ends with carriage return)*
    - *Attribute Name: Attribute Value*
    - E.g. type of client, content, identity of requester, ...
    - Last header line has extra carriage return)
  - *Entity Body (Content)*
    - Additional information to server

# HTTP Request Methods

Request method	Meaning
GET	Retrieve information (object) identified by the URL.
HEAD	Retrieve meta-information about the object, but do not transfer the object; Can be used to find out if a document has changed.
POST	Send information to a URL (using the entity body) and retrieve result; used when a user fills out a form in a browser.
PUT	Store information in location named by URL
DELETE	Remove object identified by URL
TRACE	Trace HTTP forwarding through proxies, tunnels, etc.
OPTIONS	Used to determine the capabilities of the server, or characteristics of a named resource.

# HTTP Request Message

The image shows a Wireshark packet capture window titled '\*ens33'. The packet list on the left shows a series of network packets. Packet 302 is selected, which is an HTTP GET request. The packet details pane on the right shows the structure of this request, including the GET method, the request URI, host, user-agent, accept headers, referer, and cookies. The packet bytes pane at the bottom shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
290	120.958778417	140.123.5.5	192.168.126.135	TCP	5894	80 → 43792 [PSH, ACK] Seq=3349 Ack=435 Win=642...
291	120.958794456	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=9189 Win=46720 Le...
292	120.959753066	140.123.5.5	192.168.126.135	TCP	8814	80 → 43792 [PSH, ACK] Seq=9189 Ack=435 Win=642...
293	120.959759975	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=17949 Win=64240 L...
294	120.960362750	140.123.5.5	192.168.126.135	TCP	5894	80 → 43792 [PSH, ACK] Seq=17949 Ack=435 Win=64...
295	120.960368491	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=23789 Win=64240 L...
296	120.961118545	140.123.5.5	192.168.126.135	TCP	8814	80 → 43792 [PSH, ACK] Seq=23789 Ack=435 Win=64...
297	120.961126198	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=32549 Win=64240 L...
298	120.961766503	140.123.5.5	192.168.126.135	HTTP	1689	HTTP/1.1 200 OK (text/html)
299	120.961771416	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=34184 Win=64240 L...
300	121.000572639	192.168.126.135	192.168.126.2	DNS	74	Standard query 0xa581 A www.ccu.edu.tw
301	121.000653713	192.168.126.135	192.168.126.2	DNS	74	Standard query 0xb6f6 AAAA www.ccu.edu.tw
302	121.001436086	192.168.126.135	140.123.5.5	HTTP	542	GET /css/template.css HTTP/1.1
303	121.001650872	140.123.5.5	192.168.126.135	TCP	60	80 → 43790 [ACK] Seq=1 Ack=489 Win=64240 Len=0
304	121.002563644	192.168.126.135	192.168.126.2	DNS	79	Standard query 0x8283 A use.fontawesome.com
305	121.002597074	140.123.5.5	192.168.126.135	HTTP	426	HTTP/1.1 304 Not Modified
306	121.002615140	192.168.126.135	140.123.5.5	TCP	54	43790 → 80 [ACK] Seq=489 Ack=373 Win=30016 Len...
307	121.002750654	192.168.126.135	192.168.126.2	DNS	79	Standard query 0x2cc5 AAAA use.fontawesome.com
308	121.002107551	192.168.126.135	192.168.126.2	TLSv1.2	125	Application Data

Transmission Control Protocol, Src Port: 43790, Dst Port: 80, Seq: 1, Ack: 1, Len: 488

Hypertext Transfer Protocol

- GET /css/template.css HTTP/1.1\r\n
- Host: www.ccu.edu.tw\r\n
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:65.0) Gecko/20100101 Firefox/65.0\r\n
- Accept: text/css,\*/\*;q=0.1\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Referer: http://www.ccu.edu.tw/\r\n
- Connection: keep-alive\r\n
- Cookie: \_ga=GA1.3.1262539727.1552209820; \_gid=GA1.3.1709631136.1552470394\r\n
- If-Modified-Since: Fri, 15 Feb 2019 08:47:03 GMT\r\n
- If-None-Match: "256-2d55-581ead1a7d138"\r\n
- Cache-Control: max-age=0\r\n
- \r\n

[Full request URI: http://www.ccu.edu.tw/css/template.css]  
[HTTP request 1/59]  
[Response in frame: 305]

0000 00 50 56 ef c8 5b 00 0c 29 d0 dd db 08 00 45 00 ..PV..[...].E  
0010 02 10 32 9d 40 00 40 06 35 9b c0 a8 7e 87 8c 7b ...2.@@.5...{  
0020 05 05 ab 0e 00 50 fd 86 1b 32 10 e9 15 2c 50 18 .....P...2...P  
0030 72 10 d2 b2 00 00 47 45 54 20 2f 63 73 73 2f 74 r.....GE T /css/t

wireshark\_ens33\_20190313024637\_ofU538.pcapng Packets: 1567 · Displayed: 1567 (100.0%) · Dropped: 0 (0.0%) Profile: Default

# HTTP Response Message

- Response Message Format
  - *Status Line*
    - *HTTP-Version Status-Code Message*
    - Status Code: 3-digit code indicating result
    - E.g. HTTP/1.0 200 OK
  - *Headers Section*
    - Information about object transferred to client
    - E.g. server type, content length, content type, ...
  - *Content*
    - Object (document)

# HTTP Response Message

The image shows a Wireshark packet capture window titled '\*ens33'. The packet list on the left shows packet 298 selected, which is an HTTP 200 OK response. The packet details pane on the right shows the structure of the HTTP response, including the status line, headers, and body. The status line is 'HTTP/1.1 200 OK (text/html)'. The headers include 'Date: Wed, 13 Mar 2019 09:48:39 GMT', 'Server: Apache/2.2.24 (FreeBSD) PHP/5.4.13 mod\_ssl/2.2.24 OpenSSL/0.9.8y DAV/2', 'X-Powered-By: PHP/5.4.13', 'Vary: User-Agent,Accept-Encoding', 'Content-Encoding: gzip', 'Content-Length: 33755', 'Content-Type: text/html', 'X-Cache: MISS from www.ccu.edu.tw', 'X-Cache-Lookup: MISS from www.ccu.edu.tw:80', 'Via: 1.1 www.ccu.edu.tw (squid/3.4.14-20160509-r13240)', and 'Connection: keep-alive'. The packet bytes pane at the bottom shows the raw data of the response, including the status line and headers.

No.	Time	Source	Destination	Protocol	Length	Info
287	120.957161530	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=429 Win=30016 Len=0
288	120.957616821	140.123.5.5	192.168.126.135	TCP	2974	80 → 43792 [PSH, ACK] Seq=429 Ack=435 Win=64240 Len=0
289	120.957622478	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=3349 Win=35040 Len=0
290	120.958778417	140.123.5.5	192.168.126.135	TCP	5894	80 → 43792 [PSH, ACK] Seq=3349 Ack=435 Win=64240 Len=0
291	120.958794456	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=9189 Win=46720 Len=0
292	120.959753066	140.123.5.5	192.168.126.135	TCP	8814	80 → 43792 [PSH, ACK] Seq=9189 Ack=435 Win=64240 Len=0
293	120.959759975	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=17949 Win=64240 Len=0
294	120.960362750	140.123.5.5	192.168.126.135	TCP	5894	80 → 43792 [PSH, ACK] Seq=17949 Ack=435 Win=64240 Len=0
295	120.960368491	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=23789 Win=64240 Len=0
296	120.961118545	140.123.5.5	192.168.126.135	TCP	8814	80 → 43792 [PSH, ACK] Seq=23789 Ack=435 Win=64240 Len=0
297	120.961126198	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=32549 Win=64240 Len=0
298	120.961766503	140.123.5.5	192.168.126.135	HTTP	1689	HTTP/1.1 200 OK (text/html)
299	120.961771416	192.168.126.135	140.123.5.5	TCP	54	43792 → 80 [ACK] Seq=435 Ack=34184 Win=64240 Len=0
300	121.000572639	192.168.126.135	192.168.126.2	DNS	74	Standard query 0xa581 A www.ccu.edu.tw
301	121.000653713	192.168.126.135	192.168.126.2	DNS	74	Standard query 0xb6f6 AAAA www.ccu.edu.tw
302	121.001436086	192.168.126.135	140.123.5.5	HTTP	542	GET /css/template.css HTTP/1.1
303	121.001650872	140.123.5.5	192.168.126.135	TCP	60	80 → 43790 [ACK] Seq=1 Ack=489 Win=64240 Len=0
304	121.002563644	192.168.126.135	192.168.126.2	DNS	79	Standard query 0x8283 A use.fontawesome.com

Transmission Control Protocol, Src Port: 80, Dst Port: 43792, Seq: 32549, Ack: 435, Len: 1635

[7] Reassembled TCP Segments (34183 bytes): #288(428), #289(2928), #290(3848), #292(8788), #294(3848), #296(8788), #298(1689)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Wed, 13 Mar 2019 09:48:39 GMT\r\n

Server: Apache/2.2.24 (FreeBSD) PHP/5.4.13 mod\_ssl/2.2.24 OpenSSL/0.9.8y DAV/2\r\n

X-Powered-By: PHP/5.4.13\r\n

Vary: User-Agent,Accept-Encoding\r\n

Content-Encoding: gzip\r\n

Content-Length: 33755\r\n

Content-Type: text/html\r\n

X-Cache: MISS from www.ccu.edu.tw\r\n

X-Cache-Lookup: MISS from www.ccu.edu.tw:80\r\n

Via: 1.1 www.ccu.edu.tw (squid/3.4.14-20160509-r13240)\r\n

Connection: keep-alive\r\n

\r\n

[HTTP response 1/7]

[Time since request: 0.038094391 seconds]

0000 00 0c 29 d0 dd db 00 50 56 ef c8 5b 08 00 45 00 ..)....P V...[...E...

0010 06 8b 8c c3 00 00 80 06 d6 f9 8c 7b 05 05 c0 a8 .....{...

0020 7e 87 00 50 ab 10 0f b8 d3 ed f1 21 f5 e8 50 18 ...~P...!...P...

Frame (1689 bytes) Reassembled TCP (34183 bytes) Uncompressed entity body (203440 bytes)

wireshark\_ens33\_20190313024637\_oFU538.pcapng Packets: 1567 · Displayed: 1567 (100.0%) · Dropped: 0 (0.0%) Profile: Default

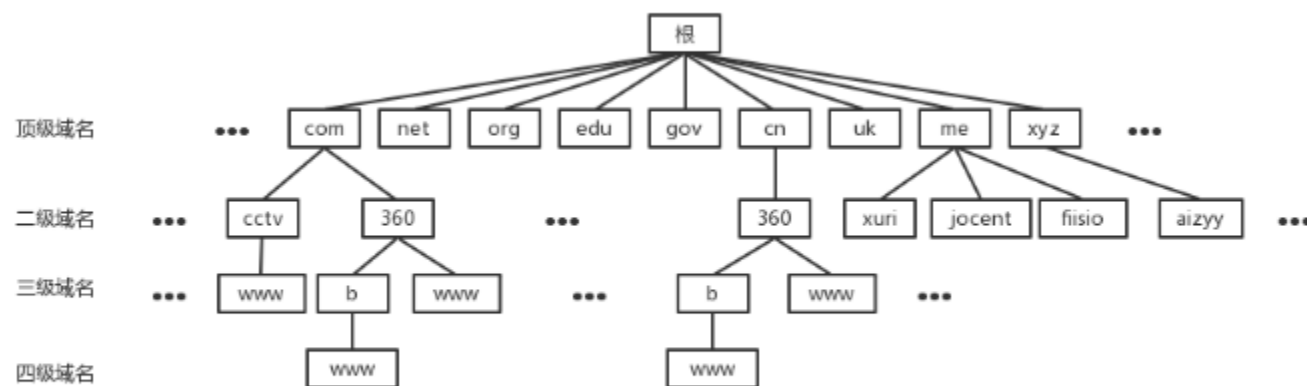
# Example: DNS Protocol

- DNS protocol is an application layer protocol
- DNS is a distributed database that resides in multiple machines in the Internet
- DNS protocol different types's queries
  - iterated query
  - Recursive Queries
  - DNS usually involves short messages and so uses service provided by UDP
- Well-known port 53



# Domain域名結構

比如 www.360.com ，由點來區分成三個域名 www、360、com，其中 com 是頂級域名（TLD，Top Level Domain），360 是二級域名（SLD，Second Level Domain），www 是三級域名



# nslookup介紹

- Nslookup 是用來做DNS測試的工具
- 在terminal 輸入 `$nslookup` (`$sudo nslookup`)
- `>set vc` (學校電腦無法使用，參考用)
- 設定 DNS query over TCP
- `>set novc`
- 設定 DNS query over UDP

lab413@lab413: ~

lab413@lab413:~\$ nslookup

> baidu.com

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

Name: baidu.com

Address: 220.181.57.216

Name: baidu.com

Address: 123.125.115.110

> set novc

> baidu.com

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

Name: baidu.com

Address: 220.181.57.216

Name: baidu.com

Address: 123.125.115.110

> set vc

> baidu.com

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

Name: baidu.com

Address: 220.181.57.216

Name: baidu.com

Address: 123.125.115.110

> set novc

> baidu.com

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

Name: baidu.com

Address: 220.181.57.216

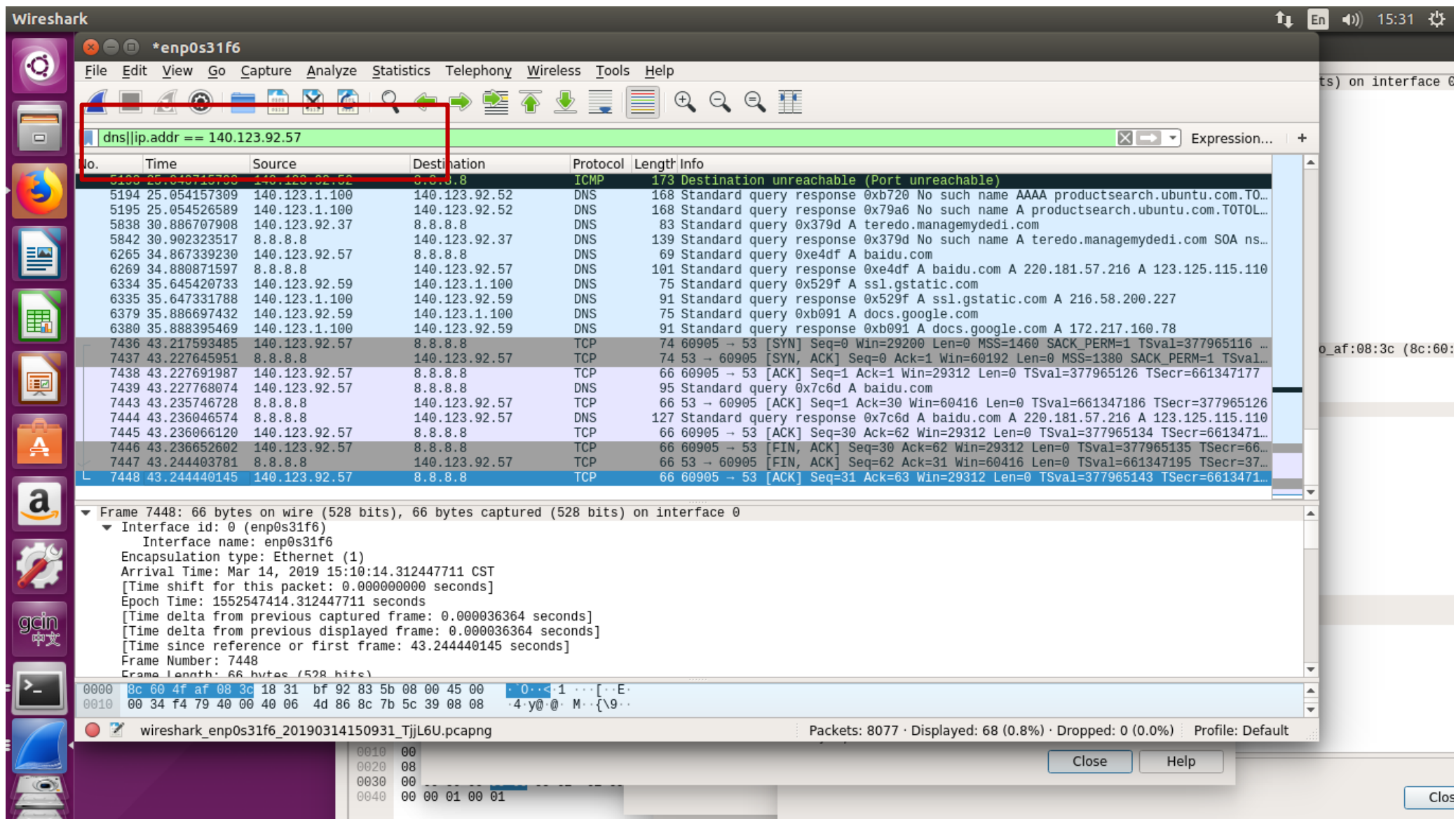
Name: baidu.com

Address: 123.125.115.110

> █

# ifconfig--觀察與修改網路介面的相關參數

```
lab413@lab413: ~  
lab413@lab413:~$ ifconfig  
enp0s31f6 Link encap:Ethernet  HWaddr 18:31:bf:92:83:5b  
        inet addr:140.123.92.57  Bcast:140.123.92.255  Mask:255.255.255.0  
        inet6 addr: fe80::f89:86c5:7eb4:c9f9/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:2150043 errors:0 dropped:92516 overruns:0 frame:0  
        TX packets:71263 errors:119 dropped:0 overruns:0 carrier:119  
        collisions:14819 txqueuelen:1000  
        RX bytes:306690674 (306.6 MB)  TX bytes:7166691 (7.1 MB)  
        Interrupt:16 Memory:df200000-df220000  
  
lo        Link encap:Local Loopback  
        inet addr:127.0.0.1  Mask:255.0.0.0  
        inet6 addr: ::1/128 Scope:Host  
        UP LOOPBACK RUNNING  MTU:65536  Metric:1  
        RX packets:6525 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:6525 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:541443 (541.4 KB)  TX bytes:541443 (541.4 KB)  
  
wlp5s0    Link encap:Ethernet  HWaddr 00:22:b0:5b:a5:d8  
        inet addr:140.123.92.57  Bcast:140.123.92.255  Mask:255.255.255.0  
        inet6 addr: fe80::3956:227b:1e8d:5f6b/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:52778 errors:0 dropped:100 overruns:0 frame:0  
        TX packets:3171 errors:0 dropped:0 overruns:0 carrier:0
```



Wireshark

\*enp0s31f6

File Edit View Go Capture Analyze Statistics Telephony Wireless

dns||ip.addr == 140.123.92.57

No.	Time	Source	Destination	P
5193	25.040715793	140.123.92.52	8.8.8.8	I
5194	25.054157309	140.123.1.100	140.123.92.52	D
5195	25.054526589	140.123.1.100	140.123.92.52	D
5838	30.886707908	140.123.92.37	8.8.8.8	D
5842	30.902323517	8.8.8.8	140.123.92.37	D
6265	34.867339230	140.123.92.57	8.8.8.8	D
6269	34.880871597	8.8.8.8	140.123.92.57	D
6334	35.645420733	140.123.92.59	140.123.1.100	D
6335	35.647331788	140.123.1.100	140.123.92.59	D
6370	35.886607193	140.123.92.59	140.123.1.100	D
6380	35.888395469	140.123.1.100	140.123.92.59	D
7436	43.217593485	140.123.92.57	8.8.8.8	T
7437	43.227645951	8.8.8.8	140.123.92.57	T
7438	43.227691987	140.123.92.57	8.8.8.8	T
7439	43.227768074	140.123.92.57	8.8.8.8	T
7443	43.235746728	8.8.8.8	140.123.92.57	T
7444	43.236046574	8.8.8.8	140.123.92.57	T
7445	43.236066120	140.123.92.57	8.8.8.8	T
7446	43.236652602	140.123.92.57	8.8.8.8	T
7447	43.244403781	8.8.8.8	140.123.92.57	T
7448	43.244440145	140.123.92.57	8.8.8.8	T

Frame 7439: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0 (enp0s31f6)

Interface name: enp0s31f6  
Encapsulation type: Ethernet (1)  
Arrival Time: Mar 14, 2019 15:10:14.295775640 CST  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1552547414.295775640 seconds  
[Time delta from previous captured frame: 0.000076087 seconds]  
[Time delta from previous displayed frame: 0.000076087 seconds]  
[Time since reference or first frame: 43.227768074 seconds]  
Frame Number: 7439  
Frame Length: 95 bytes (760 bits)

0000 8c 60 4f af 08 3c 18 31 bf 92 83 5b 08 00 45 00 .O.<~.1.  
0010 00 51 f4 76 40 00 40 06 4d 6c 8c 7b 5c 39 08 08 .Q.v@.@.M

Wireshark · Packet 7439 · enp0s31f6

Total Length: 81  
Identification: 0xf476 (62582)  
Flags: 0x4000, Don't fragment  
Time to live: 64  
Protocol: TCP (6)  
Header checksum: 0x4d6c [validation disabled]  
[Header checksum status: Unverified]  
Source: 140.123.92.57  
Destination: 8.8.8.8

Transmission Control Protocol, Src Port: 60905, Dst Port: 53, Seq: 1, Ack: 1, Len: 29  
Source Port: 60905  
Destination Port: 53  
[Stream index: 364]  
[TCP Segment Len: 29]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 30 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x018 (PSH, ACK)  
Window size value: 229  
Calculated window size: 29312  
Window size scaling factor: 128  
Checksum: 0xf907 [unverified]  
Checksum Status: Unverified  
Urgent pointer: 0  
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
SEQ/ACK analysis  
[RTT: 0.010098502 seconds]  
[Bytes in flight: 29]  
[Bytes sent since last PSH flag: 29]  
[Timestamps]  
[Time since first frame in this TCP stream: 0.010174589 seconds]  
[Time since previous frame in this TCP stream: 0.000076087 seconds]  
TCP payload (29 bytes)  
[PDU Size: 29]  
Domain Name System (query)  
Length: 27  
Transaction ID: 0x7c6d  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 7444]

Close Help



# UDP/TCP

- UDP的速度會較TCP快一些
- 用UDP的傳輸資料的可靠度較TCP來的低
- 掉了一些封包仍然可以正常運行的，這一類的服務我們就會運用UDP服務來進行。像是DNS服務，我們就是要能夠快速的查詢到網址所對應的IP才行。

# LAB1 TCP、UDP

- 課堂要求

找出**TCP**三向交握和**UDP**的封包。

- 報告

配合封包內容解釋**TCP**三向交握的原理。

(解釋**SYN**、**ACK**..等)

比較**TCP**和**UDP**。



# LAB2 分析HTTP協議

- 課堂要求

打開使用HTTP的網站140.123.5.5

觀察HTTP協議中有哪些內容並截圖。

(找出request、response各一)

- 報告

配合封包內容解釋其中Host、accept、cookie...等。

# LAB3 DNS分析

- 課堂要求

學會使用nslookup

學會用wireshark判斷連線是使用UDP還是TCP

- 報告

解釋為什麼DNS適合用UDP protocol 而不是TCP protocol 。