SC/CSE 3213 Winter 2013

L8: TCP/IP Overview

Sebastian Magierowski
York University

Outline

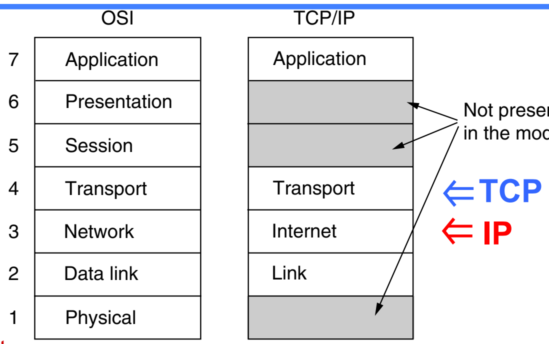
- TCP/IP Reference Model
  - A set of protocols for internetworking
  - The basis of the modern Internet
- IP Datagram Exchange Examples
  - Forwarding over network and data link layers
- Network Analyzer Views
  - A means to view live Internet protocol traffic
- HTTP (maybe)
  - In a bit more detail

Internetworking

- To allow internetworking a set of protocols developed over time
  - The “TCP/IP protocol suite”
    - aka “Internet protocol suite”
- First described in ’74 (Cerf & Kahn)

TCP/IP Arrangement

- Roughly organized into a 4-level model
  - Same idea as OSI
  - But model came after protocols
- Model called…
  - “TCP/IP network architecture”
    - Since it specifies exact services and protocols to be used by each layer
    - Unlike OSI (which is not specific)
  - “TCP/IP reference model” (“TCP/IP model”)
- Named after its two primary protocols

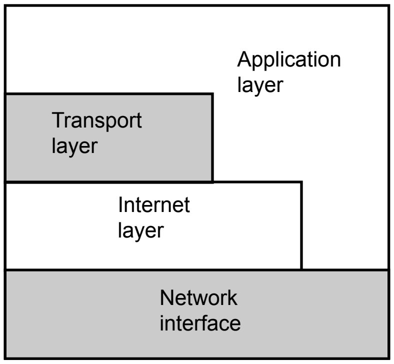


	OSI	TCP/IP
7	Application	Application
6	Presentation	▨
5	Session	▨
4	Transport	Transport ⇐TCP
3	Network	Internet ⇐ IP
2	Data link	Link
1	Physical	▨

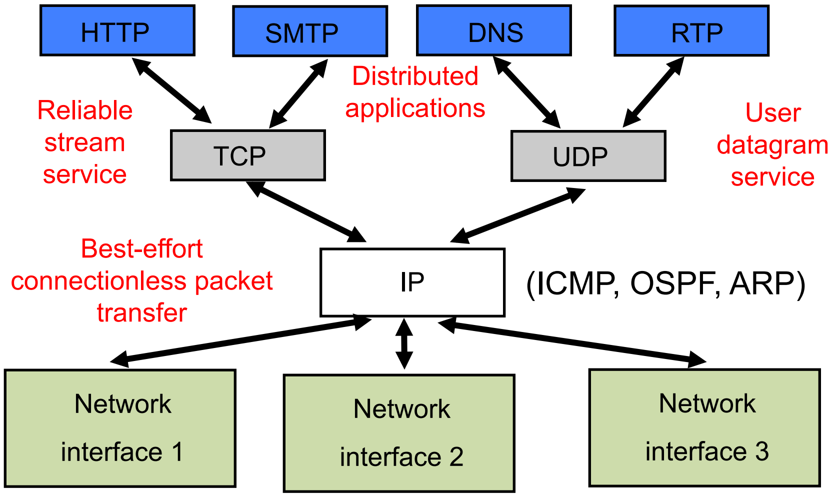
Not present in the model

TCP/IP Model

- 4 layers
  - smaller than OSI
- Model developed “after the fact”
  - Doesn’t partition functions as cleanly as OSI
  - layers don’t have to talk in sequential fashion
  - E.g. direct interaction between application layer and interface possible
- Not a suitable guide for new network designs



TCP/IP Protocol Suite

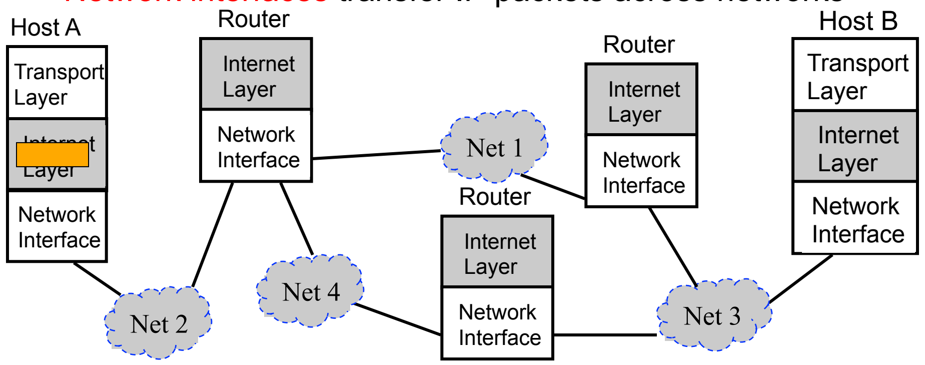


Diverse network technologies

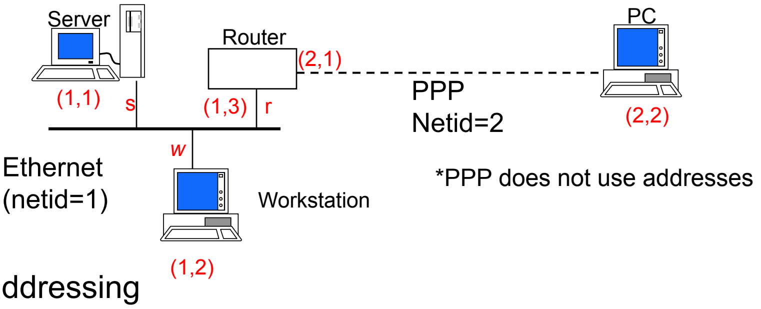
Internet Protocol Approach

- IP packets transfer information across the Internet

  Host A IP → router→ router…→ router→ Host B IP
- IP layer in each router determines next hop (router)
- Network interfaces transfer IP packets across networks



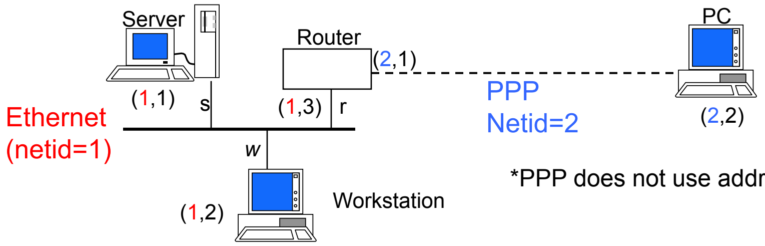
TCP/IP Packet Forwarding Example



*PPP does not use addresses

- IP addressing
  - unique 32-bit logical address
  - 128.34.51.2 = (netid, hostid), simplified in example: e.g. (1,3)
- Physical address
  - unique LAN address
  - e.g. 48-bit Ethernet: 00:90:27:96:68:07, simplified in example: e.g. r

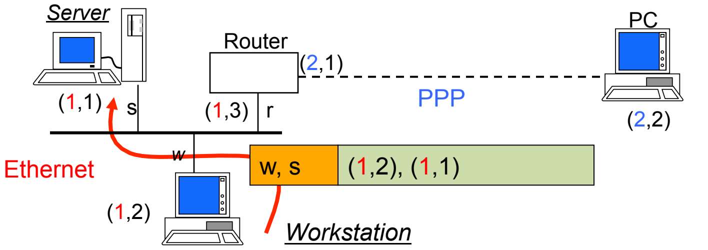
TCP/IP Packet Forwarding Example



*PPP does not use addresses

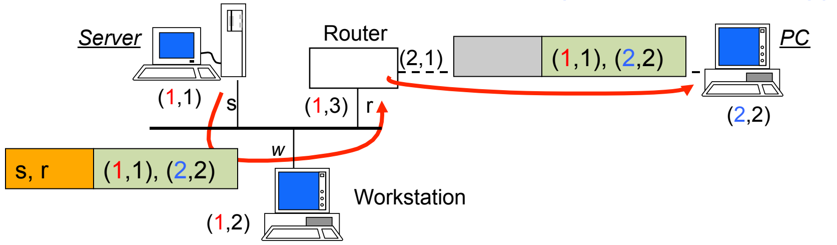
	netid	hostid	Physical address
server	1	1	s
workstation	1	2	w
router	1	3	r
router	2	1	-
PC	2	2	-

IP Packet from Workstation to Server



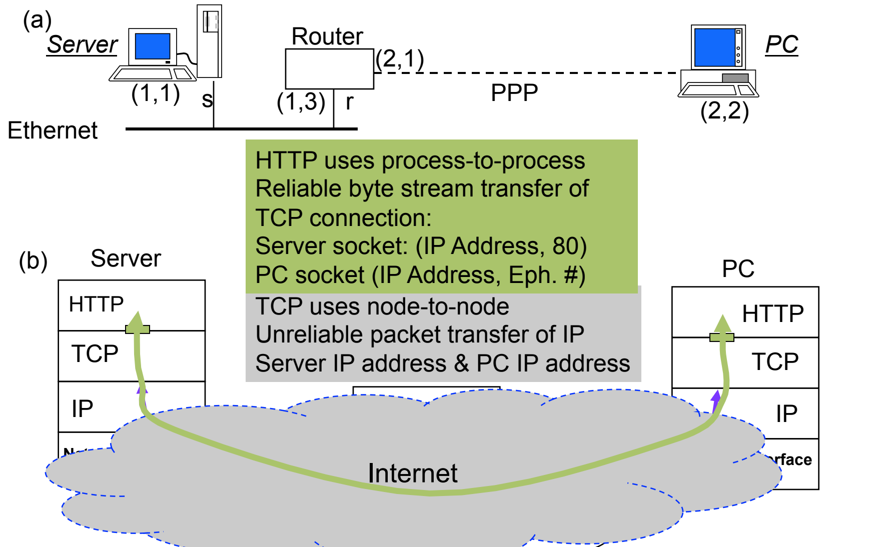
1. IP packet has (1,2) IP address for source and (1,1) IP address for destination
2. IP table at workstation indicates (1,1) connected to same network, so IP packet is encapsulated in Ethernet frame with addresses w and s
3. Ethernet frame is broadcast by workstation NIC and captured by server and router NIC
4. server NIC examines protocol type field and then delivers packet to its IP layer

IP Packet from Server to PC (internetworking)



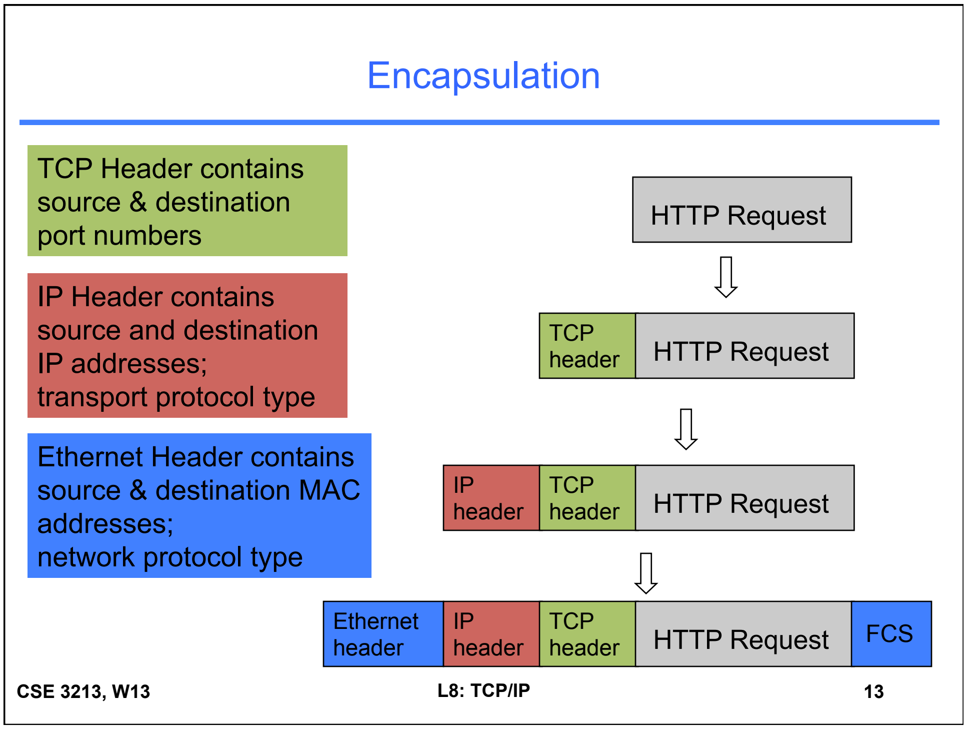
1. IP packet has (1,1) and (2,2) as IP source and destination addresses
2. IP table at server indicates packet should be sent to router, so IP packet is encapsulated in Ethernet frame with addresses s and r
3. Ethernet frame is broadcast by server NIC and captured by router NIC
4. router NIC examines protocol type field and delivers packet to its IP layer
5. IP layer examines IP packet destination address and determines IP packet should be routed to (2,2)
6. Router's table indicates (2,2) is directly connected via PPP link
7. IP packet is encapsulated in PPP frame and delivered to PC
8. PPP at PC examines protocol type field and delivers packet to PC IP layer

What's Happening Above IP?



HTTP uses process-to-process Reliable byte stream transfer of TCP connection:
Server socket: (IP Address, 80)
PC socket (IP Address, Eph. #)

TCP uses node-to-node Unreliable packet transfer of IP
Server IP address & PC IP address

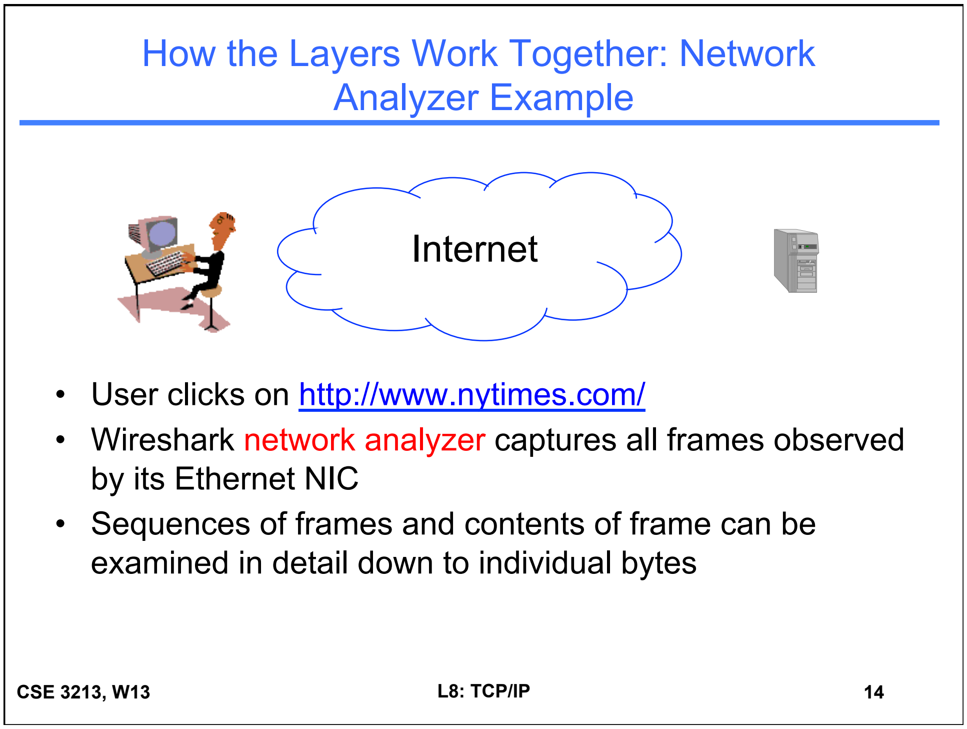


Encapsulation

TCP Header contains source & destination port numbers

IP Header contains source and destination IP addresses; transport protocol type

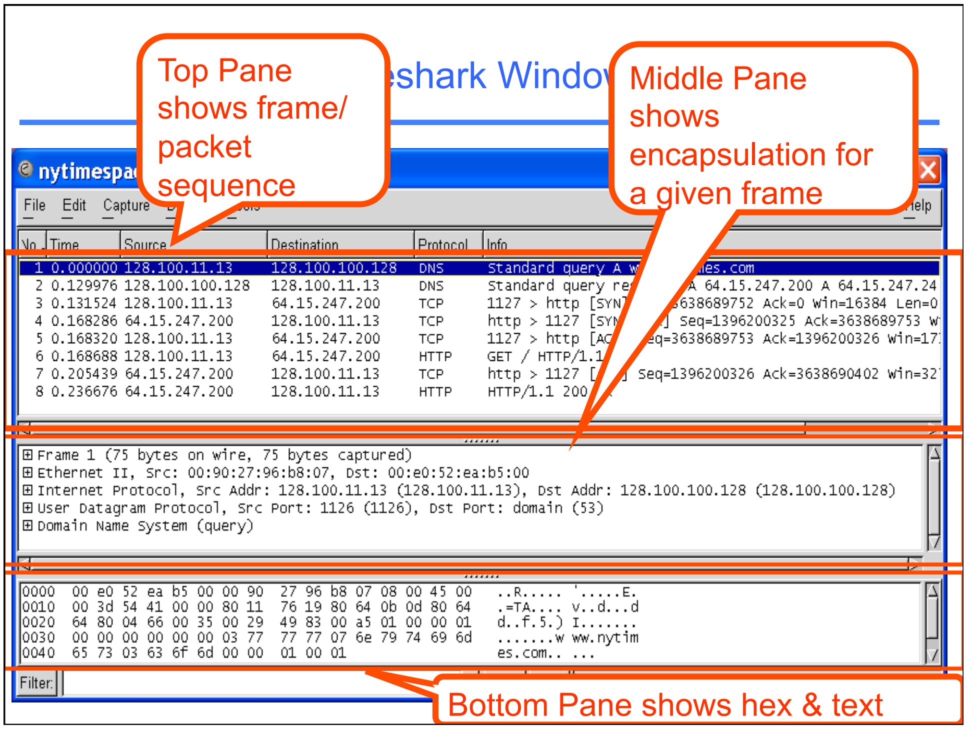
Ethernet Header contains source & destination MAC addresses; network protocol type



How the Layers Work Together: Network Analyzer Example

- User clicks on http://www.nytimes.com/
- Wireshark network analyzer captures all frames observed by its Ethernet NIC
- Sequences of frames and contents of frame can be examined in detail down to individual bytes

eshark Windov



Top Pane shows frame/ packet sequence

Middle Pane shows encapsulation for a given frame

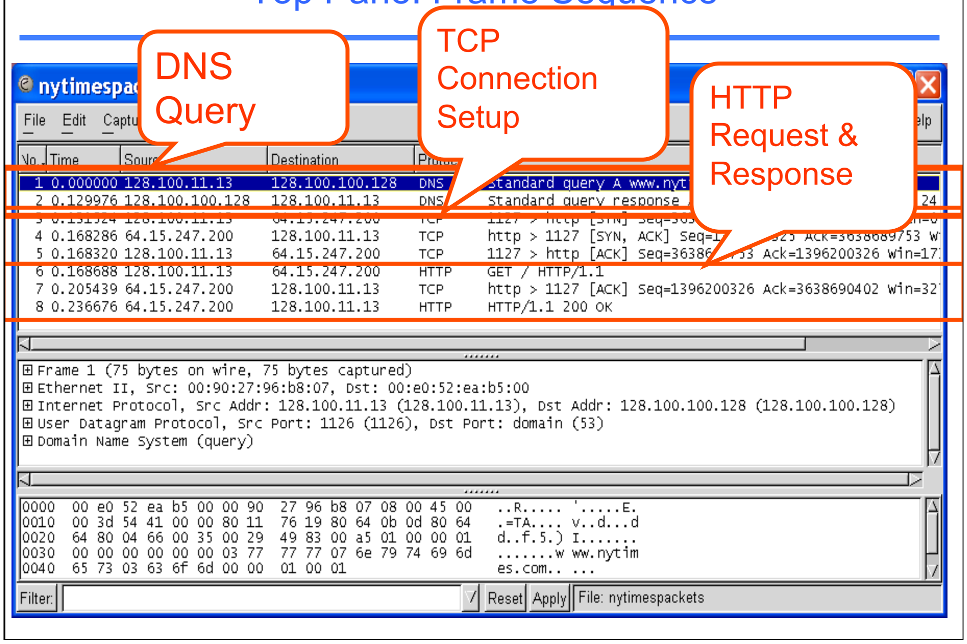
Bottom Pane shows hex & text

```
No. Time     Source          Destination     Protocol Info
  1 0.000000 128.100.11.13   128.100.100.128 DNS      Standard query A w          es.com
  2 0.129976 128.100.100.128 128.100.11.13   DNS      Standard query re         A 64.15.247.200 A 64.15.247.24
  3 0.131524 128.100.11.13   64.15.247.200   TCP      1127 > http [SYN]        638689752 Ack=0 Win=16384 Len=0
  4 0.168286 64.15.247.200   128.100.11.13   TCP      http > 1127 [SYN     ] Seq=1396200325 Ack=3638689753 W
  5 0.168320 128.100.11.13   64.15.247.200   TCP      1127 > http [AC     eq=3638689753 Ack=1396200326 Win=17
  6 0.168688 128.100.11.13   64.15.247.200   HTTP     GET / HTTP/1.1
  7 0.205439 64.15.247.200   128.100.11.13   TCP      http > 1127 [    ] Seq=1396200326 Ack=3638690402 Win=32
  8 0.236676 64.15.247.200   128.100.11.13   HTTP     HTTP/1.1 200
```

```
⊞ Frame 1 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: 00:90:27:96:b8:07, Dst: 00:e0:52:ea:b5:00
⊞ Internet Protocol, Src Addr: 128.100.11.13 (128.100.11.13), Dst Addr: 128.100.100.128 (128.100.100.128)
⊞ User Datagram Protocol, Src Port: 1126 (1126), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000  00 e0 52 ea b5 00 00 90  27 96 b8 07 08 00 45 00   ..R..... '.....E.
0010  00 3d 54 41 00 00 80 11  76 19 80 64 0b 0d 80 64   .=TA.... v..d...d
0020  64 80 04 66 00 35 00 29  49 83 00 a5 01 00 00 01   d..f.5.) I.......
0030  00 00 00 00 00 00 03 77  77 77 07 6e 79 74 69 6d   .......w ww.nytim
0040  65 73 03 63 6f 6d 00 00  01 00 01                  es.com.. ...
```

Top Pane: Frame Sequence



DNS Query

TCP Connection Setup

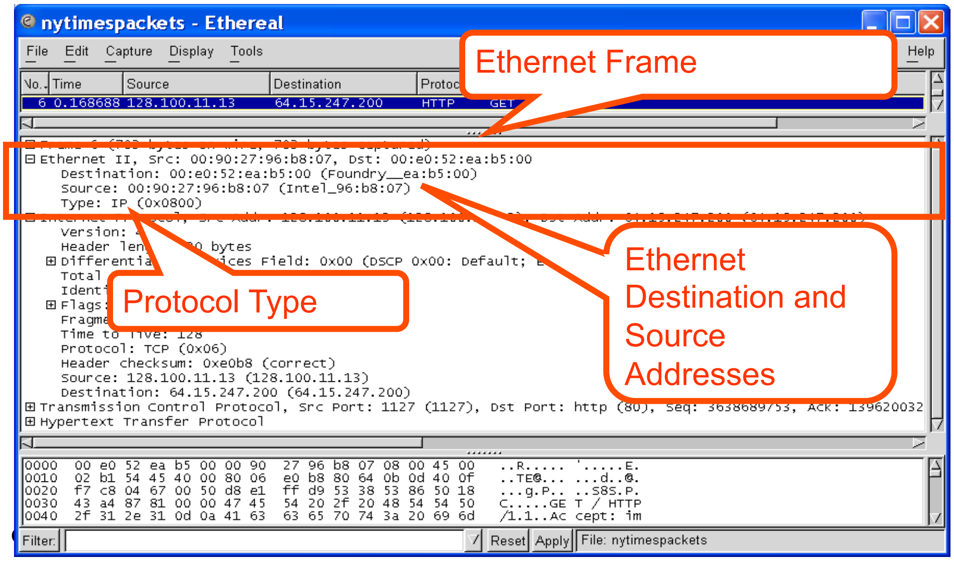
HTTP Request & Response

```
No. Time     Source          Destination     Protoc
  1 0.000000 128.100.11.13   128.100.100.128 DNS      Standard query A www.nyt
  2 0.129976 128.100.100.128 128.100.11.13   DNS      Standard query response                             24
  4 0.168286 64.15.247.200   128.100.11.13   TCP      http > 1127 [SYN, ACK] Seq=1               Ack=3638689753 W
  5 0.168320 128.100.11.13   64.15.247.200   TCP      1127 > http [ACK] Seq=36386    53 Ack=1396200326 Win=17
  6 0.168688 128.100.11.13   64.15.247.200   HTTP     GET / HTTP/1.1
  7 0.205439 64.15.247.200   128.100.11.13   TCP      http > 1127 [ACK] Seq=1396200326 Ack=3638690402 Win=32
  8 0.236676 64.15.247.200   128.100.11.13   HTTP     HTTP/1.1 200 OK
```

```
⊞ Frame 1 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: 00:90:27:96:b8:07, Dst: 00:e0:52:ea:b5:00
⊞ Internet Protocol, Src Addr: 128.100.11.13 (128.100.11.13), Dst Addr: 128.100.100.128 (128.100.100.128)
⊞ User Datagram Protocol, Src Port: 1126 (1126), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000  00 e0 52 ea b5 00 00 90  27 96 b8 07 08 00 45 00   ..R..... '.....E.
0010  00 3d 54 41 00 00 80 11  76 19 80 64 0b 0d 80 64   .=TA.... v..d...d
0020  64 80 04 66 00 35 00 29  49 83 00 a5 01 00 00 01   d..f.5.) I.......
0030  00 00 00 00 00 00 03 77  77 77 07 6e 79 74 69 6d   .......w ww.nytim
0040  65 73 03 63 6f 6d 00 00  01 00 01                  es.com.. ...
```

Middle Pane: Encapsulation


nytimespackets - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protoc
Filter: Reset Apply File: nytimespackets

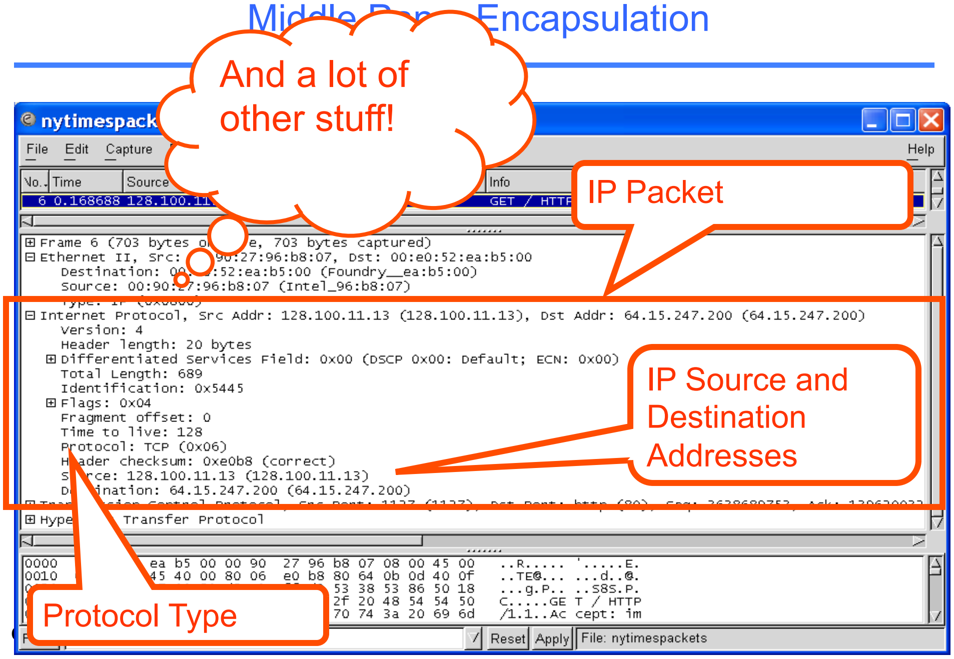
```
6 0.168688 128.100.11.13    64.15.247.200    HTTP    GET

⊟ Ethernet II, Src: 00:90:27:96:b8:07, Dst: 00:e0:52:ea:b5:00
    Destination: 00:e0:52:ea:b5:00 (Foundry__ea:b5:00)
    Source: 00:90:27:96:b8:07 (Intel_96:b8:07)
    Type: IP (0x0800)
    Version:
    Header len      0 bytes
  ⊞ Differentia        ices Field: 0x00 (DSCP 0x00: Default; E
    Total
    Ident
  ⊞ Flags:
    Fragme
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xe0b8 (correct)
    Source: 128.100.11.13 (128.100.11.13)
    Destination: 64.15.247.200 (64.15.247.200)
⊞ Transmission Control Protocol, Src Port: 1127 (1127), Dst Port: http (80), Seq: 3638689753, Ack: 139620032
⊞ Hypertext Transfer Protocol

0000  00 e0 52 ea b5 00 00 90  27 96 b8 07 08 00 45 00   ..R..... '.....E.
0010  02 b1 54 45 40 00 80 06  e0 b8 80 64 0b 0d 40 0f   ..TE@... ...d..@.
0020  f7 c8 04 67 00 50 d8 e1  ff d9 53 38 53 86 50 18   ...g.P.. ..S8S.P.
0030  43 a4 87 81 00 00 47 45  54 20 2f 20 48 54 54 50   C.....GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 69 6d   /1.1..Ac cept: im
```

Ethernet Frame

Protocol Type

Ethernet Destination and Source Addresses

Middle Pane: Encapsulation



```
6 0.168688 128.100.11                         GET / HTTP

⊞ Frame 6 (703 bytes o     e, 703 bytes captured)
⊟ Ethernet II, Src:    90:27:96:b8:07, Dst: 00:e0:52:ea:b5:00
    Destination: 00   :52:ea:b5:00 (Foundry__ea:b5:00)
    Source: 00:90:27:96:b8:07 (Intel_96:b8:07)
⊟ Internet Protocol, Src Addr: 128.100.11.13 (128.100.11.13), Dst Addr: 64.15.247.200 (64.15.247.200)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 689
    Identification: 0x5445
  ⊞ Flags: 0x04
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xe0b8 (correct)
    Source: 128.100.11.13 (128.100.11.13)
    Destination: 64.15.247.200 (64.15.247.200)
⊞ Hype      Transfer Protocol

0000        ea b5 00 00 90  27 96 b8 07 08 00 45 00   ..R..... '.....E.
0010        45 40 00 80 06  e0 b8 80 64 0b 0d 40 0f   ..TE@... ...d..@.
                               53 38 53 86 50 18   ...g.P.. ..S8S.P.
                               2f 20 48 54 54 50   C.....GE T / HTTP
                               70 74 3a 20 69 6d   /1.1..Ac cept: im
```

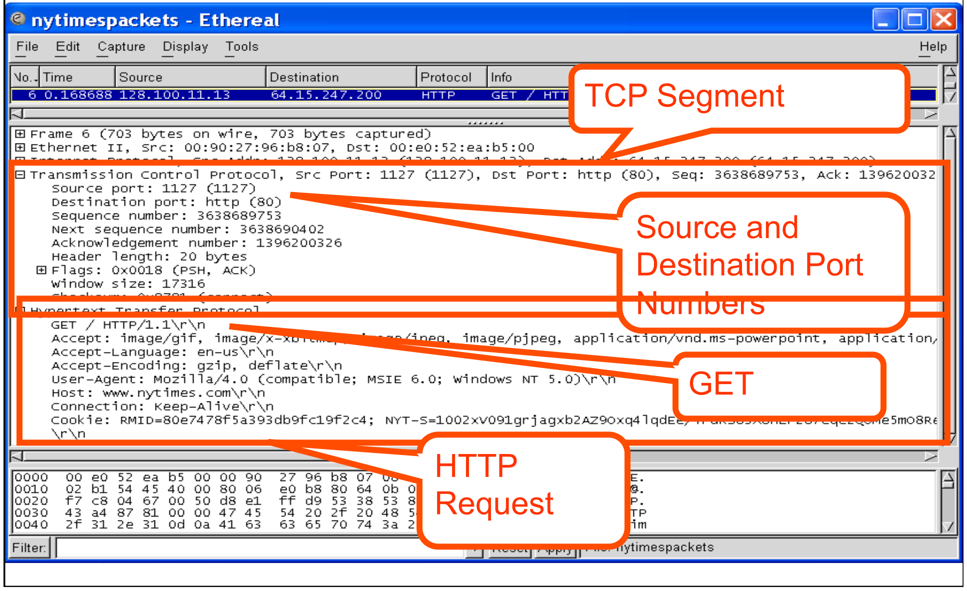
And a lot of other stuff!

IP Packet

IP Source and Destination Addresses

Protocol Type

Middle Pane: Encapsulation


nytimespackets - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
Filter:
Reset Apply
nytimespackets
TCP Segment
Source and Destination Port Numbers
GET
HTTP Request

```
  6 0.168688 128.100.11.13    64.15.247.200    HTTP     GET / HTT
```

```
⊞ Frame 6 (703 bytes on wire, 703 bytes captured)
⊞ Ethernet II, Src: 00:90:27:96:b8:07, Dst: 00:e0:52:ea:b5:00
⊞ Internet Protocol, Src Addr: 128.100.11.13 (128.100.11.13), Dst Addr: 64.15.247.200 (64.15.247.200)
⊟ Transmission Control Protocol, Src Port: 1127 (1127), Dst Port: http (80), Seq: 3638689753, Ack: 139620032
    Source port: 1127 (1127)
    Destination port: http (80)
    Sequence number: 3638689753
    Next sequence number: 3638690402
    Acknowledgement number: 1396200326
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 17316
    Checksum: 0x8781 (correct)
⊟ Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)\r\n
    Host: www.nytimes.com\r\n
    Connection: Keep-Alive\r\n
    Cookie: RMID=80e7478f5a393db9fc19f2c4; NYT-S=1002xV091grjagxb2AZ9Oxq4lqdEE
    \r\n
```

```
0000  00 e0 52 ea b5 00 00 90  27 96 b8 07 08        E.
0010  02 b1 54 45 40 00 80 06  e0 b8 80 64 0b 0     @.
0020  f7 c8 04 67 00 50 d8 e1  ff d9 53 38 53 8     P.
0030  43 a4 87 81 00 00 47 45  54 20 2f 20 48 5     TP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 2     im
```

TCP/IP Summary

- Encapsulation is key to layering
- IP provides for transfer of packets across diverse networks
- TCP and UDP provide universal communications services across the Internet
- Distributed applications that use TCP and UDP can operate over the entire Internet
- Internet names, IP addresses, port numbers, sockets, connections, physical addresses

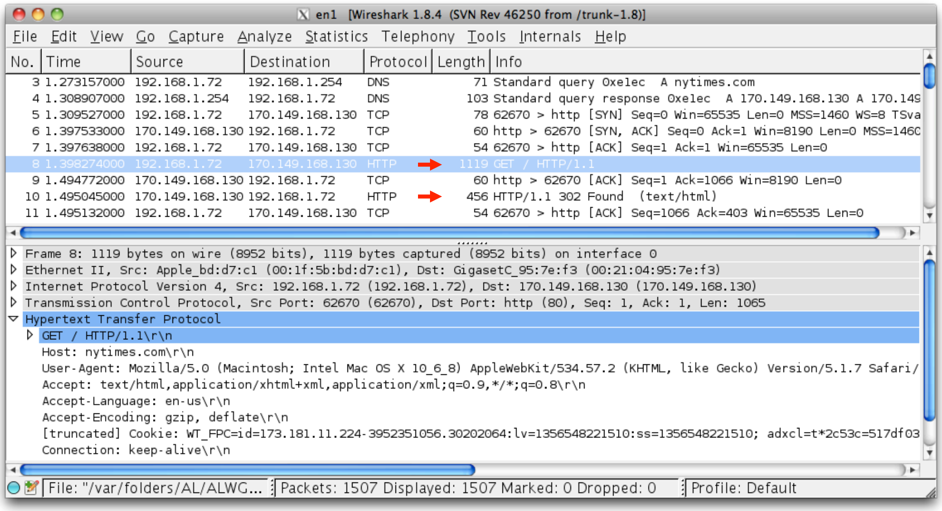
Hypertext Transfer Protocol

- RFC 1945 (HTTP 1.0), RFC 2616 (HTTP 1.1)
- HTTP provides communications between web browsers & web servers
- Web: framework for accessing documents & resources through the Internet
- Hypertext documents: text, graphics, images, hyperlinks
- Documents prepared using Hypertext Markup Language (HTML)

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


en1 [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

```
No. Time        Source          Destination     Protocol Length Info
  3 1.273157000 192.168.1.72    192.168.1.254   DNS          71 Standard query 0xe1ec  A nytimes.com
  4 1.308907000 192.168.1.254   192.168.1.72    DNS         103 Standard query response 0xe1ec  A 170.149.168.130 A 170.149
  5 1.309527000 192.168.1.72    170.149.168.130 TCP          78 62670 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSva
  6 1.397533000 170.149.168.130 192.168.1.72    TCP          60 http > 62670 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=146C
  7 1.397638000 192.168.1.72    170.149.168.130 TCP          54 62670 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  8 1.398274000 192.168.1.72    170.149.168.130 HTTP  →   1119 GET / HTTP/1.1
  9 1.494772000 170.149.168.130 192.168.1.72    TCP          60 http > 62670 [ACK] Seq=1 Ack=1066 Win=8190 Len=0
 10 1.495045000 170.149.168.130 192.168.1.72    HTTP  →    456 HTTP/1.1 302 Found  (text/html)
 11 1.495132000 192.168.1.72    170.149.168.130 TCP          54 62670 > http [ACK] Seq=1066 Ack=403 Win=65535 Len=0

▷ Frame 8: 1119 bytes on wire (8952 bits), 1119 bytes captured (8952 bits) on interface 0
▷ Ethernet II, Src: Apple_bd:d7:c1 (00:1f:5b:bd:d7:c1), Dst: GigasetC_95:7e:f3 (00:21:04:95:7e:f3)
▷ Internet Protocol Version 4, Src: 192.168.1.72 (192.168.1.72), Dst: 170.149.168.130 (170.149.168.130)
▷ Transmission Control Protocol, Src Port: 62670 (62670), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1065
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: nytimes.com\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko) Version/5.1.7 Safari/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    [truncated] Cookie: WT_FPC=id=173.181.11.224-3952351056.30202064:lv=1356548221510:ss=1356548221510; adxcl=t*2c53c=517df03
    Connection: keep-alive\r\n

File: "/var/folders/AL/ALWG...  Packets: 1507 Displayed: 1507 Marked: 0 Dropped: 0  Profile: Default
```

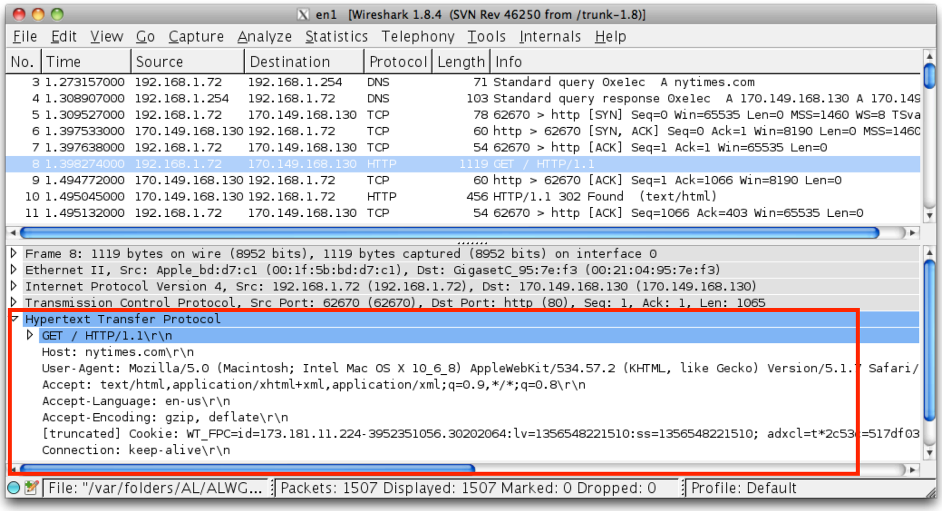
HTTP Message Formats

- HTTP messages written in ASCII text
- Request Message Format
  1. Request Line (Each line ends with carriage return)
     - `Method URL HTTP-Version \r\n`
     - `Method` specifies action to apply to object
     - `URL` specifies object
  2. Header Lines (Each 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
  3. 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 Headers

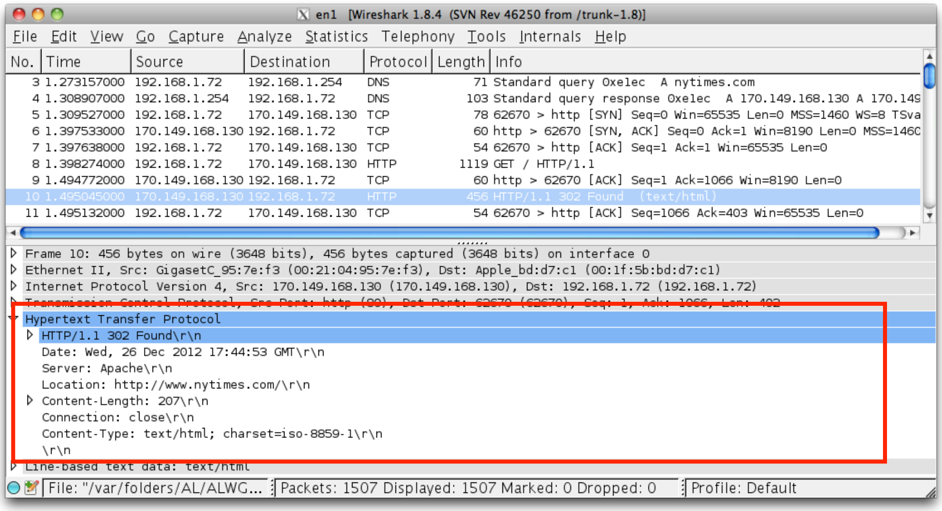

en1 [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

```
No. Time        Source          Destination     Protocol Length Info
  3 1.273157000 192.168.1.72    192.168.1.254   DNS       71 Standard query 0x01ec  A nytimes.com
  4 1.308907000 192.168.1.254   192.168.1.72    DNS      103 Standard query response 0x01ec  A 170.149.168.130 A 170.149
  5 1.309527000 192.168.1.72    170.149.168.130 TCP       78 62670 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSva
  6 1.397533000 170.149.168.130 192.168.1.72    TCP       60 http > 62670 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460
  7 1.397638000 192.168.1.72    170.149.168.130 TCP       54 62670 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  8 1.398274000 192.168.1.72    170.149.168.130 HTTP    1119 GET / HTTP/1.1
  9 1.494772000 170.149.168.130 192.168.1.72    TCP       60 http > 62670 [ACK] Seq=1 Ack=1066 Win=8190 Len=0
 10 1.495045000 170.149.168.130 192.168.1.72    HTTP     456 HTTP/1.1 302 Found  (text/html)
 11 1.495132000 192.168.1.72    170.149.168.130 TCP       54 62670 > http [ACK] Seq=1066 Ack=403 Win=65535 Len=0

▷ Frame 8: 1119 bytes on wire (8952 bits), 1119 bytes captured (8952 bits) on interface 0
▷ Ethernet II, Src: Apple_bd:d7:c1 (00:1f:5b:bd:d7:c1), Dst: GigasetC_95:7e:f3 (00:21:04:95:7e:f3)
▷ Internet Protocol Version 4, Src: 192.168.1.72 (192.168.1.72), Dst: 170.149.168.130 (170.149.168.130)
▷ Transmission Control Protocol, Src Port: 62670 (62670), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1065
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: nytimes.com\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko) Version/5.1.7 Safari/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    [truncated] Cookie: WT_FPC=id=173.181.11.224-3952351056.30202064:lv=1356548221510:ss=1356548221510; adxcl=t*2c53e=517df03
    Connection: keep-alive\r\n

File: "/var/folders/AL/ALWG... Packets: 1507 Displayed: 1507 Marked: 0 Dropped: 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


en1 [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

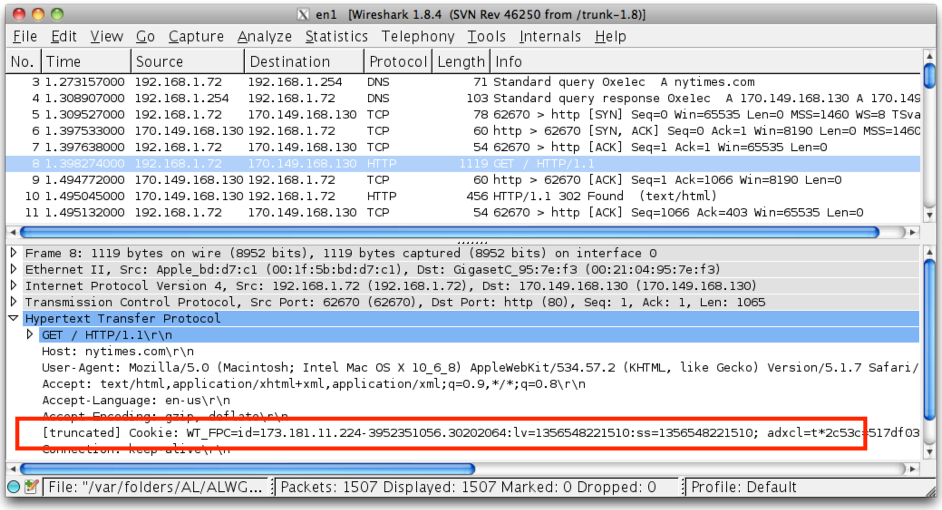
```
No. Time        Source          Destination     Protocol Length Info
  3 1.273157000 192.168.1.72    192.168.1.254   DNS        71 Standard query 0xelec  A nytimes.com
  4 1.308907000 192.168.1.254   192.168.1.72    DNS       103 Standard query response 0xelec  A 170.149.168.130 A 170.149
  5 1.309527000 192.168.1.72    170.149.168.130 TCP        78 62670 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSva
  6 1.397533000 170.149.168.130 192.168.1.72    TCP        60 http > 62670 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460
  7 1.397638000 192.168.1.72    170.149.168.130 TCP        54 62670 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  8 1.398274000 192.168.1.72    170.149.168.130 HTTP     1119 GET / HTTP/1.1
  9 1.494772000 170.149.168.130 192.168.1.72    TCP        60 http > 62670 [ACK] Seq=1 Ack=1066 Win=8190 Len=0
 10 1.495045000 170.149.168.130 192.168.1.72    HTTP      456 HTTP/1.1 302 Found  (text/html)
 11 1.495132000 192.168.1.72    170.149.168.130 TCP        54 62670 > http [ACK] Seq=1066 Ack=403 Win=65535 Len=0

▷ Frame 10: 456 bytes on wire (3648 bits), 456 bytes captured (3648 bits) on interface 0
▷ Ethernet II, Src: GigasetC_95:7e:f3 (00:21:04:95:7e:f3), Dst: Apple_bd:d7:c1 (00:1f:5b:bd:d7:c1)
▷ Internet Protocol Version 4, Src: 170.149.168.130 (170.149.168.130), Dst: 192.168.1.72 (192.168.1.72)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 62670 (62670), Seq: 1, Ack: 1066, Len: 402
▽ Hypertext Transfer Protocol
  ▷ HTTP/1.1 302 Found\r\n
    Date: Wed, 26 Dec 2012 17:44:53 GMT\r\n
    Server: Apache\r\n
    Location: http://www.nytimes.com/\r\n
  ▷ Content-Length: 207\r\n
    Connection: close\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
▷ Line-based text data: text/html
```

File: "/var/folders/AL/ALWG...
Packets: 1507 Displayed: 1507 Marked: 0 Dropped: 0
Profile: Default

Cookies and Web Sessions

- Cookies are data exchanged by clients & servers as header lines
- Since HTTP stateless, cookies can provide context for HTTP interaction
- Set cookie header line in reply message from server + unique ID number for client
- If client accepts cookie, cookie added to client’s cookie file (must include expiration date)
- Henceforth client requests include ID
- Server site can track client interactions, store these in a separate database, and access database to prepare appropriate responses

Cookie Header Line; ID is 24 hex numeral



en1 [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

```
No. Time        Source          Destination     Protocol Length Info
  3 1.273157000 192.168.1.72    192.168.1.254   DNS          71 Standard query 0xe1ec  A nytimes.com
  4 1.308907000 192.168.1.254   192.168.1.72    DNS         103 Standard query response 0xe1ec  A 170.149.168.130 A 170.149
  5 1.309527000 192.168.1.72    170.149.168.130 TCP          78 62670 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSva
  6 1.397533000 170.149.168.130 192.168.1.72    TCP          60 http > 62670 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460
  7 1.397638000 192.168.1.72    170.149.168.130 TCP          54 62670 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  8 1.398274000 192.168.1.72    170.149.168.130 HTTP       1119 GET / HTTP/1.1
  9 1.494772000 170.149.168.130 192.168.1.72    TCP          60 http > 62670 [ACK] Seq=1 Ack=1066 Win=8190 Len=0
 10 1.495045000 170.149.168.130 192.168.1.72    HTTP        456 HTTP/1.1 302 Found  (text/html)
 11 1.495132000 192.168.1.72    170.149.168.130 TCP          54 62670 > http [ACK] Seq=1066 Ack=403 Win=65535 Len=0

▷ Frame 8: 1119 bytes on wire (8952 bits), 1119 bytes captured (8952 bits) on interface 0
▷ Ethernet II, Src: Apple_bd:d7:c1 (00:1f:5b:bd:d7:c1), Dst: GigasetC_95:7e:f3 (00:21:04:95:7e:f3)
▷ Internet Protocol Version 4, Src: 192.168.1.72 (192.168.1.72), Dst: 170.149.168.130 (170.149.168.130)
▷ Transmission Control Protocol, Src Port: 62670 (62670), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1065
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: nytimes.com\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko) Version/5.1.7 Safari/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    [truncated] Cookie: WT_FPC=id=173.181.11.224-3952351056.30202064:lv=1356548221510:ss=1356548221510; adxcl=t*2c53c=517df03
    Connection: keep-alive\r\n

File: "/var/folders/AL/ALWG... Packets: 1507 Displayed: 1507 Marked: 0 Dropped: 0 Profile: Default
```