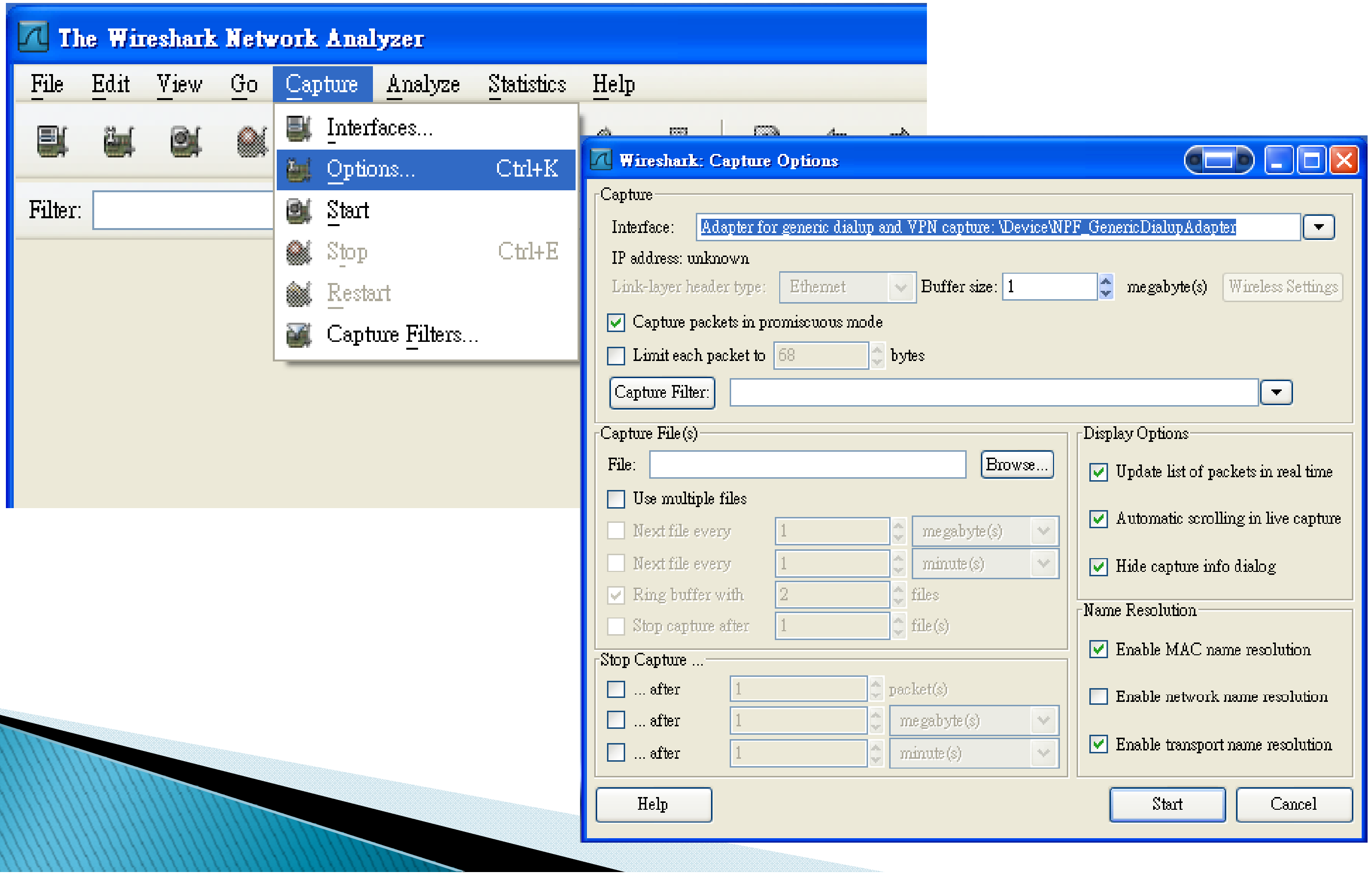
Wireshark(Ethereal)

Wireshark(Ethereal)

- Wireshark is previously known as Ethereal. It switched name in May 2006 due to trademark issues .
- Step 1.
  - **Download and install wireshark** from website(sourceforge)
  - http://www.wireshark.org/download.html
  - Choose "Stable Release 1.0.6"

STEP BY STEP

- Step 2.
  - Start Wireshark, select menu Capture->Options



Wireshark: Capture Options

Capture

Interface: Adapter for generic dialup and VPN capture: \Device\NPF_GenericDialupAdapter

IP address: unknown

Link-layer header type: Ethernet   Buffer size: 1 megabyte(s)   Wireless Settings

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

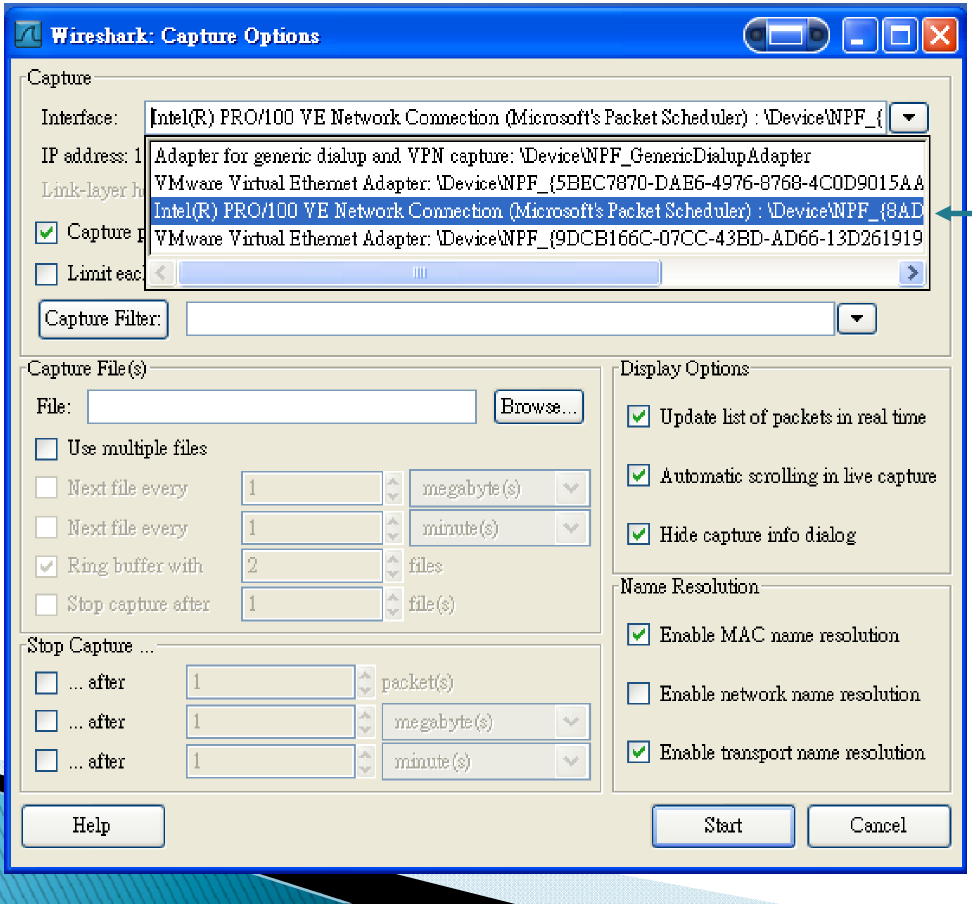
□ Enable network name resolution

☑ Enable transport name resolution

Help   Start   Cancel

STEP BY STEP

- Step 3.
  - Choose your network interface.



Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : \Device\NPF_{

Adapter for generic dialup and VPN capture: \Device\NPF_GenericDialupAdapter
VMware Virtual Ethernet Adapter: \Device\NPF_{5BEC7870-DAE6-4976-8768-4C0D9015AA
Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : \Device\NPF_{8AD
VMware Virtual Ethernet Adapter: \Device\NPF_{9DCB166C-07CC-43BD-AD66-13D261919

IP address: 1

Link-layer h

☑ Capture p

□ Limit eac

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

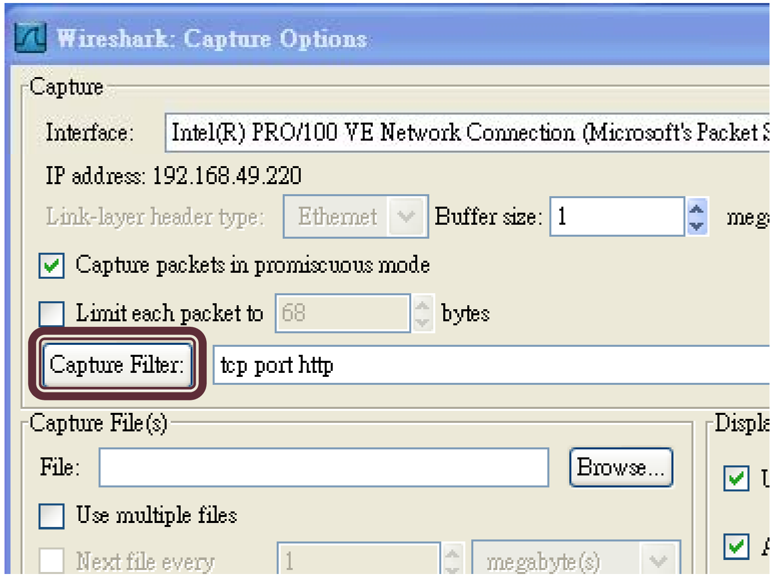
☑ Enable transport name resolution

TA's Interface

Choose your own here

STEP BY STEP

- Step 4.
  - Seletct Capture Filter (more on this later)



Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/100 VE Network Connection (Microsoft's Packet S

IP address: 192.168.49.220

Link-layer header type: Ethernet Buffer size: 1 meg

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter: tcp port http

Capture File(s)

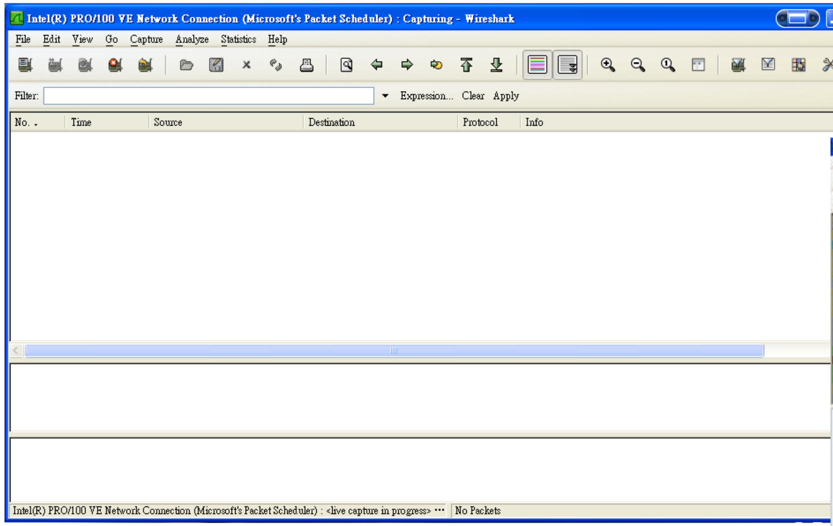
File:

□ Use multiple files

□ Next file every 1 megabyte(s)

STEP BY STEP

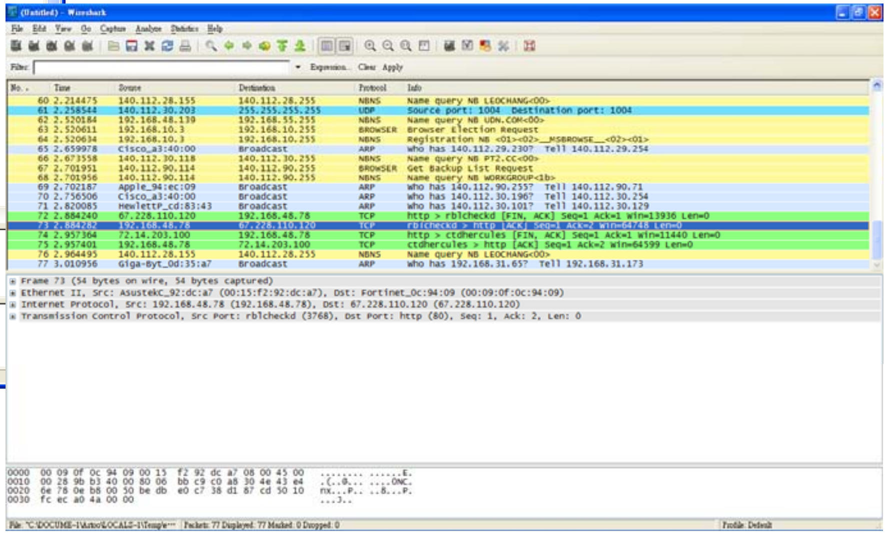
- Step 5.
  - Click start, and use your computer as usual


Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. . Time Source Destination Protocol Info

Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : <live capture in progress> ··· No Packets

Before start capturing

After some network use


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
60	2.214475	140.112.28.155	140.112.28.255	NBNS	Name query NB LEOCHANG<00>
61	2.258544	140.112.30.203	255.255.255.255	UDP	Source port: 1004 Destination port: 1004
62	2.520184	192.168.48.139	192.168.55.255	NBNS	Name query NB UDN.COM<00>
63	2.520611	192.168.10.3	192.168.10.255	BROWSER	Browser Election Request
64	2.520634	192.168.10.3	192.168.10.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
65	2.659978	Cisco_a3:40:00	Broadcast	ARP	Who has 140.112.29.230? Tell 140.112.29.254
66	2.673558	140.112.30.118	140.112.30.255	NBNS	Name query NB PT2.CC<00>
67	2.701951	140.112.90.114	140.112.90.255	BROWSER	Get Backup List Request
68	2.701956	140.112.90.114	140.112.90.255	NBNS	Name query NB WORKGROUP<1b>
69	2.702187	Apple_94:ec:09	Broadcast	ARP	Who has 140.112.90.255? Tell 140.112.90.71
70	2.756506	Cisco_a3:40:00	Broadcast	ARP	Who has 140.112.30.196? Tell 140.112.30.254
71	2.820085	HewlettP_cd:83:43	Broadcast	ARP	Who has 140.112.30.101? Tell 140.112.30.129
72	2.884240	67.228.110.120	192.168.48.78	TCP	http > rblcheckd [FIN, ACK] Seq=1 Ack=1 Win=13936 Len=0
73	2.884282	192.168.48.78	67.228.110.120	TCP	rblcheckd > http [ACK] Seq=1 Ack=2 Win=64748 Len=0
74	2.957364	72.14.203.100	192.168.48.78	TCP	http > ctdhercules [FIN, ACK] Seq=1 Ack=1 Win=11440 Len=0
75	2.957401	192.168.48.78	72.14.203.100	TCP	ctdhercules > http [ACK] Seq=1 Ack=2 Win=64599 Len=0
76	2.964495	140.112.28.155	140.112.28.255	NBNS	Name query NB LEOCHANG<00>
77	3.010956	Giga-Byt_0d:35:a7	Broadcast	ARP	Who has 192.168.31.65? Tell 192.168.31.173

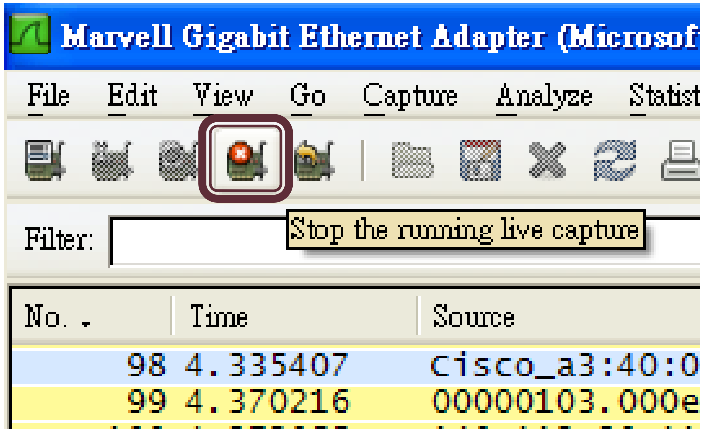
```
⊞ Frame 73 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: AsustekC_92:dc:a7 (00:15:f2:92:dc:a7), Dst: Fortinet_0c:94:09 (00:09:0f:0c:94:09)
⊞ Internet Protocol, Src: 192.168.48.78 (192.168.48.78), Dst: 67.228.110.120 (67.228.110.120)
⊞ Transmission Control Protocol, Src Port: rblcheckd (3768), Dst Port: http (80), Seq: 1, Ack: 2, Len: 0
```

```
0000  00 09 0f 0c 94 09 00 15  f2 92 dc a7 08 00 45 00   ........ ......E.
0010  00 28 9b b3 40 00 80 06  bb c9 c0 a8 30 4e 43 e4   .(..@... ....0NC.
0020  6e 78 0e b8 00 50 be db  e0 c7 38 d1 87 cd 50 10   nx...P.. ..8...P.
0030  fc ec a0 4a 00 00                                  ...J..
```

File: "C:\DOCUME~1\Artoo\LOCALS~1\Temp\e··· | Packets: 77 Displayed: 77 Marked: 0 Dropped: 0 | Profile: Default

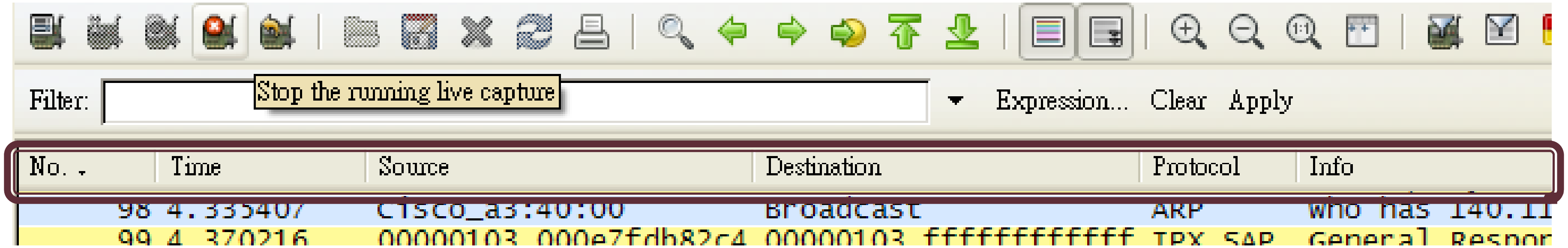
STEP BY STEP

- Step 6.
  - After 5 minutes, click “stop the running live capture”


Marvell Gigabit Ethernet Adapter (Microsof
File
Edit
View
Go
Capture
Analyze
Statist
Stop the running live capture
Filter:

```
No. .   Time        Source
   98   4.335407    Cisco_a3:40:0
   99   4.370216    00000103.000e
```

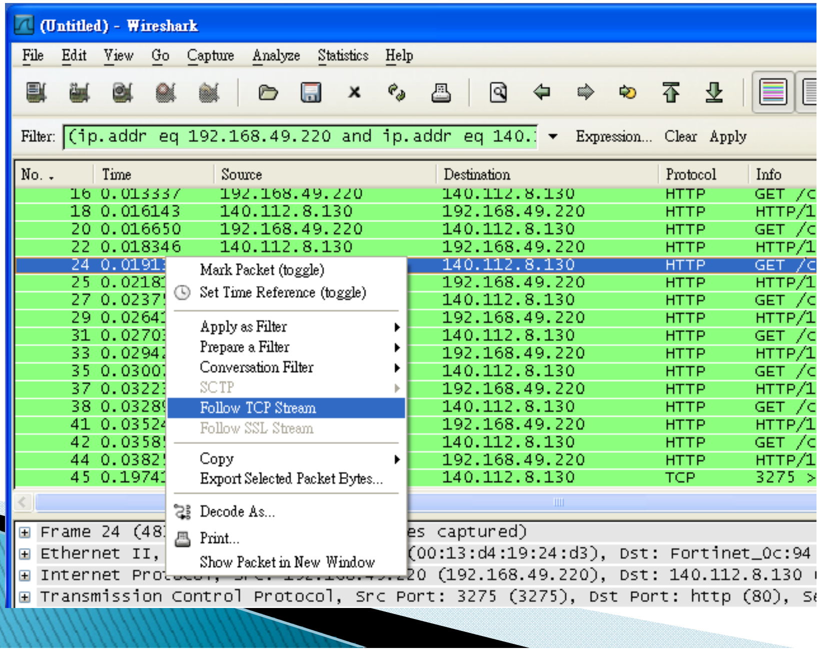
  - Now you’ll have A LOT OF packets, with their time, source and dest. IP, protocol (may be in app., transport, or link layer), etc.



```
No. .   Time        Source                  Destination              Protocol   Info
   98   4.335407    Cisco_a3:40:00          Broadcast                ARP        Who has 140.11
   99   4.370216    00000103.000e7fdb82c4   00000103.ffffffffffff    IPX SAP    General Respon
```

STEP BY STEP

- Step 7.
  - You can type filter string into the ”Filter:” box
    - E.g. “http” can filter out all packets which are not HTTP packet
  - You can right click on a TCP packet, and use “Follow TCP Stream” to trace this TCP stream



Filter: (ip.addr eq 192.168.49.220 and ip.addr eq 140.1

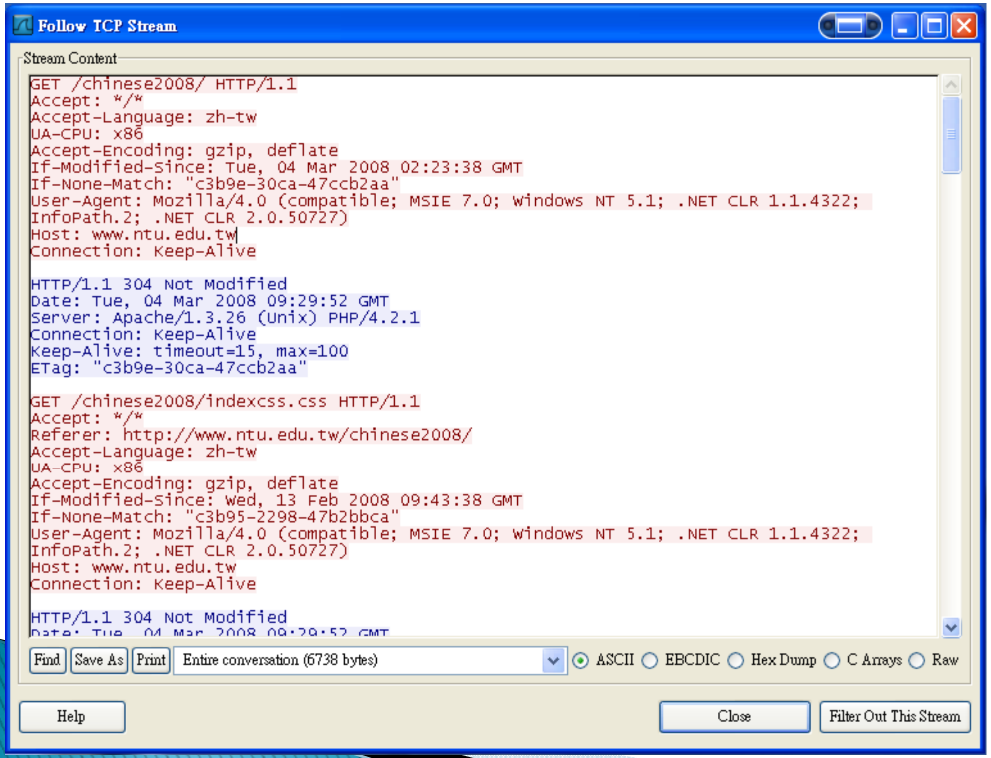
```
No. .   Time      Source            Destination       Protocol  Info
  16 0.013337  192.168.49.220    140.112.8.130     HTTP      GET /c
  18 0.016143  140.112.8.130     192.168.49.220    HTTP      HTTP/1
  20 0.016650  192.168.49.220    140.112.8.130     HTTP      GET /c
  22 0.018346  140.112.8.130     192.168.49.220    HTTP      HTTP/1
  24 0.0191                      140.112.8.130     HTTP      GET /c
  25 0.0218                      192.168.49.220    HTTP      HTTP/1
  27 0.0237                      140.112.8.130     HTTP      GET /c
  29 0.0264                      192.168.49.220    HTTP      HTTP/1
  31 0.0270                      140.112.8.130     HTTP      GET /c
  33 0.0294                      192.168.49.220    HTTP      HTTP/1
  35 0.0300                      140.112.8.130     HTTP      GET /c
  37 0.0322                      192.168.49.220    HTTP      HTTP/1
  38 0.0328                      140.112.8.130     HTTP      GET /c
  41 0.0352                      192.168.49.220    HTTP      HTTP/1
  42 0.0358                      140.112.8.130     HTTP      GET /c
  44 0.0382                      192.168.49.220    HTTP      HTTP/1
  45 0.1974                      140.112.8.130     TCP       3275 >
```

```
⊞ Frame 24 (48                          es captured)
⊞ Ethernet II,                          (00:13:d4:19:24:d3), Dst: Fortinet_0c:94
⊞ Internet Pro                          20 (192.168.49.220), Dst: 140.112.8.130
⊞ Transmission Control Protocol, Src Port: 3275 (3275), Dst Port: http (80), Se
```

“Follow TCP stream” shows packets in sequence and the way that the application layer sees it.

STEP BY STEP

- Step 8.
  - Now you can see detailed information of this TCP stream



```
GET /chinese2008/ HTTP/1.1
Accept: */*
Accept-Language: zh-tw
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 04 Mar 2008 02:23:38 GMT
If-None-Match: "c3b9e-30ca-47ccb2aa"
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322;
InfoPath.2; .NET CLR 2.0.50727)
Host: www.ntu.edu.tw
Connection: Keep-Alive

HTTP/1.1 304 Not Modified
Date: Tue, 04 Mar 2008 09:29:52 GMT
Server: Apache/1.3.26 (Unix) PHP/4.2.1
Connection: Keep-Alive
Keep-Alive: timeout=15, max=100
ETag: "c3b9e-30ca-47ccb2aa"

GET /chinese2008/indexcss.css HTTP/1.1
Accept: */*
Referer: http://www.ntu.edu.tw/chinese2008/
Accept-Language: zh-tw
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 13 Feb 2008 09:43:38 GMT
If-None-Match: "c3b95-2298-47b2bbca"
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322;
InfoPath.2; .NET CLR 2.0.50727)
Host: www.ntu.edu.tw
Connection: Keep-Alive

HTTP/1.1 304 Not Modified
Date: Tue, 04 Mar 2008 09:29:52 GMT
```

Entire conversation (6738 bytes) ● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

The stream content is displayed in the same sequence as it appeared on the network.
Traffic from A to B is marked in red, while traffic from B to A is marked in blue.

Reference/FAQ

- http://www.wireshark.org/
- You may see lots of packet which is marked "incorrect TCP checksum"
  - Here this DOES NOT mean that the packets are corrupted. You can ignore this error, or see following page to know why this happening, and work around it.
  - http://www.wireshark.org/faq.html#q11.1

Reference/FAQ

- 2 types of filters:
  - Capture filter http://wiki.wireshark.org/CaptureFilters
  - Display filter http://wiki.wireshark.org/DisplayFilters