



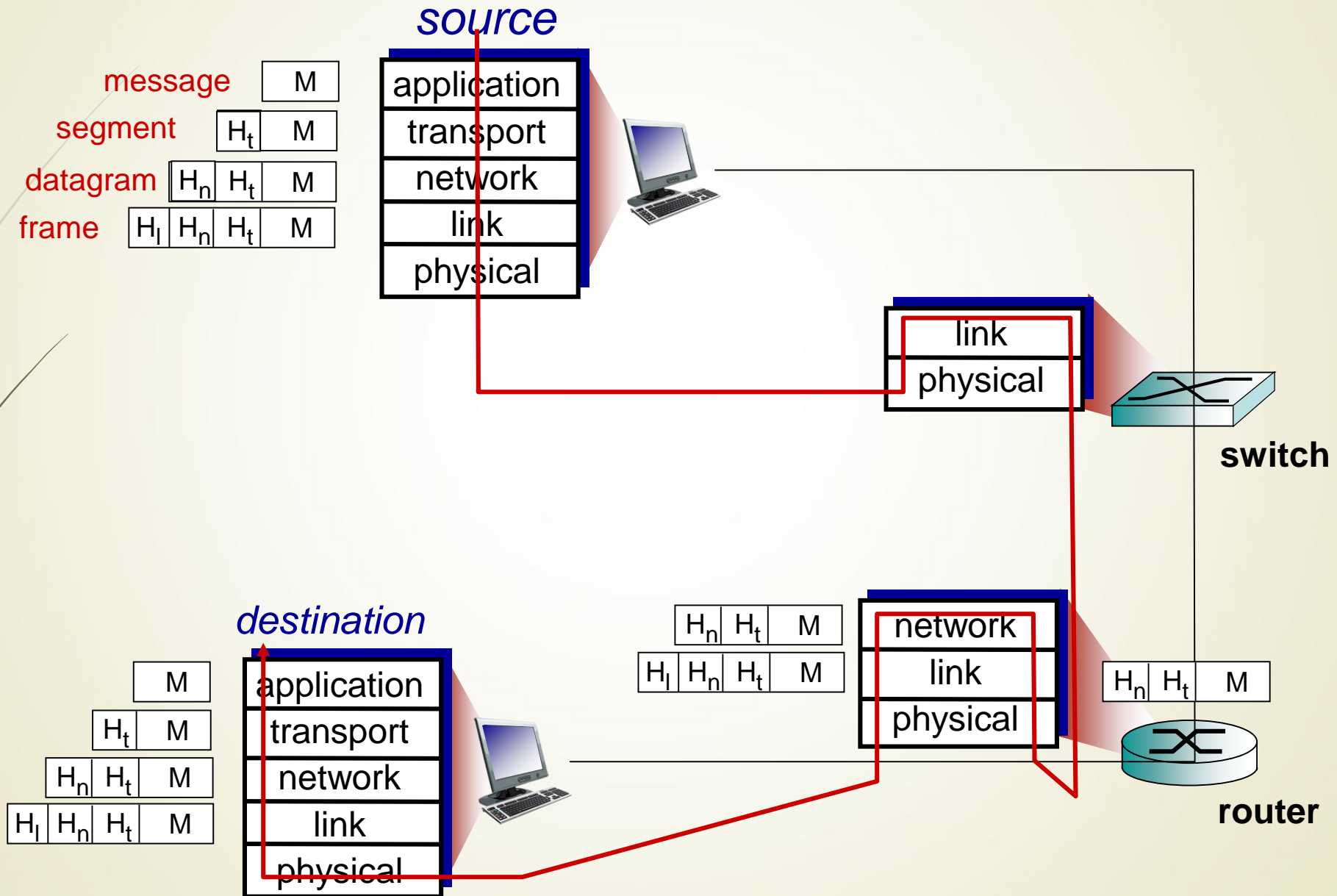
Wireshark基礎實驗



Outline

- 封包的Encapsulation/Decapsulation
- Wireshark 介紹
- Wireshark 下載及安裝過程
- Wireshark 主要視窗功能說明
- Wireshark 可以觀察到那些
- LAB1- 使用 Wireshark 分析packet的內容
- LAB2- 使用 Wireshark ping 學校的首頁

Encapsulation/Decapsulation



Wireshark背景介紹

- ▶ Wireshark (前稱Ethereal) 是一個網路封包分析軟體。網路封包分析軟體的功能是擷取網路封包，並盡可能顯示出最為詳細的網路封包資料，Wireshark能提供下列協助：
 - ▶ 檢測網路問題
 - ▶ 檢查資訊安全相關問題
 - ▶ 為新的通訊協定除錯
 - ▶ 學習網路協定的相關知識
- ▶ Wireshark不是入侵偵測軟體。對於網路上的異常流量行為，Wireshark不會產生警示或是任何提示。然而，仔細分析Wireshark擷取的封包能夠幫助使用者對於網路行為有更清楚的了解。Wireshark不會對網路封包產生內容的修改，它只會反映出目前傳送的封包資訊，Wireshark本身也不會送出封包至網路上。

Wireshark 下載

- ▶ \$sudo apt-get update
\$sudo apt-get install wireshark



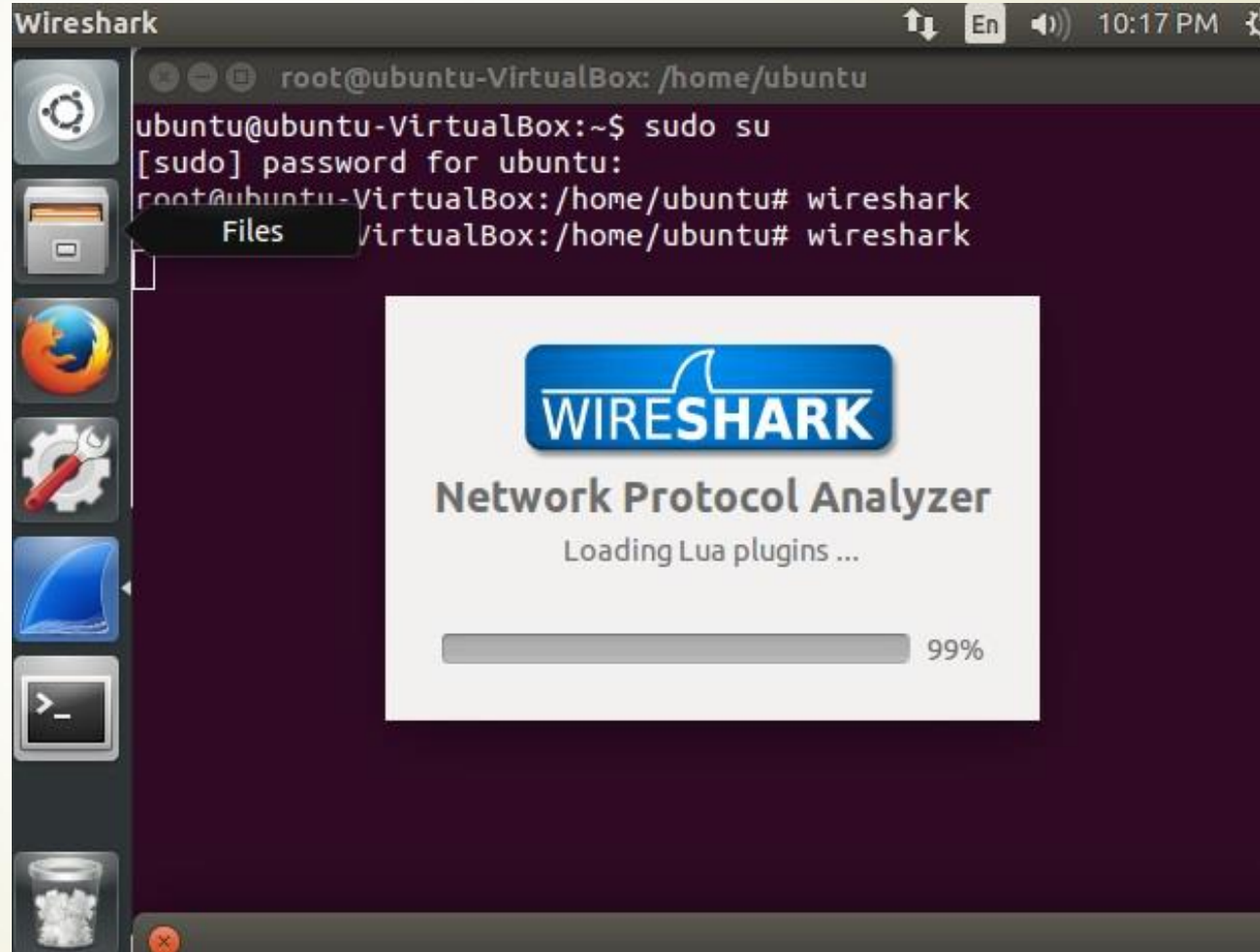
安裝過程

```
root@joe-VirtualBox: /home/joe
joe@joe-VirtualBox:~$ sudo su
[sudo] password for joe:
root@joe-VirtualBox:/home/joe# apt-get update
略過 http://dl.google.com stable InRelease
已有 http://dl.google.com stable Release.gpg
已有 http://dl.google.com stable Release
已有 http://dl.google.com stable/main amd64 Packages
略過 http://dl.google.com stable/main Translation-zh_TW
略過 http://dl.google.com stable/main Translation-zh
略過 http://dl.google.com stable/main Translation-en
略過 http://tw.archive.ubuntu.com trusty InRelease
下載:1 http://tw.archive.ubuntu.com trusty-updates InRelease [65.9 kB]
下載:2 http://tw.archive.ubuntu.com trusty-backports InRelease [65.9 kB]
已有 http://tw.archive.ubuntu.com trusty Release.gpg
略過 http://extras.ubuntu.com trusty InRelease
下載:3 http://tw.archive.ubuntu.com trusty-updates/main Sources [393 kB]
下載:4 http://extras.ubuntu.com trusty Release.gpg [72 B]
下載:5 http://security.ubuntu.com trusty-security InRelease [65.9 kB]
下載:6 http://tw.archive.ubuntu.com trusty-updates/restricted Sources [5,911 B]
已有 http://extras.ubuntu.com trusty Release
下載:7 http://tw.archive.ubuntu.com trusty-updates/universe Sources [175 kB]
下載:8 http://security.ubuntu.com trusty-security/main Sources [126 kB]
下載:9 http://tw.archive.ubuntu.com trusty-updates/multiverse Sources [7,510 B]
已有 http://extras.ubuntu.com trusty/main Sources
升級 0 個，新安裝 0 個，移除 0 個，有 41 個未被升級。
root@joe-VirtualBox:/home/joe#
```

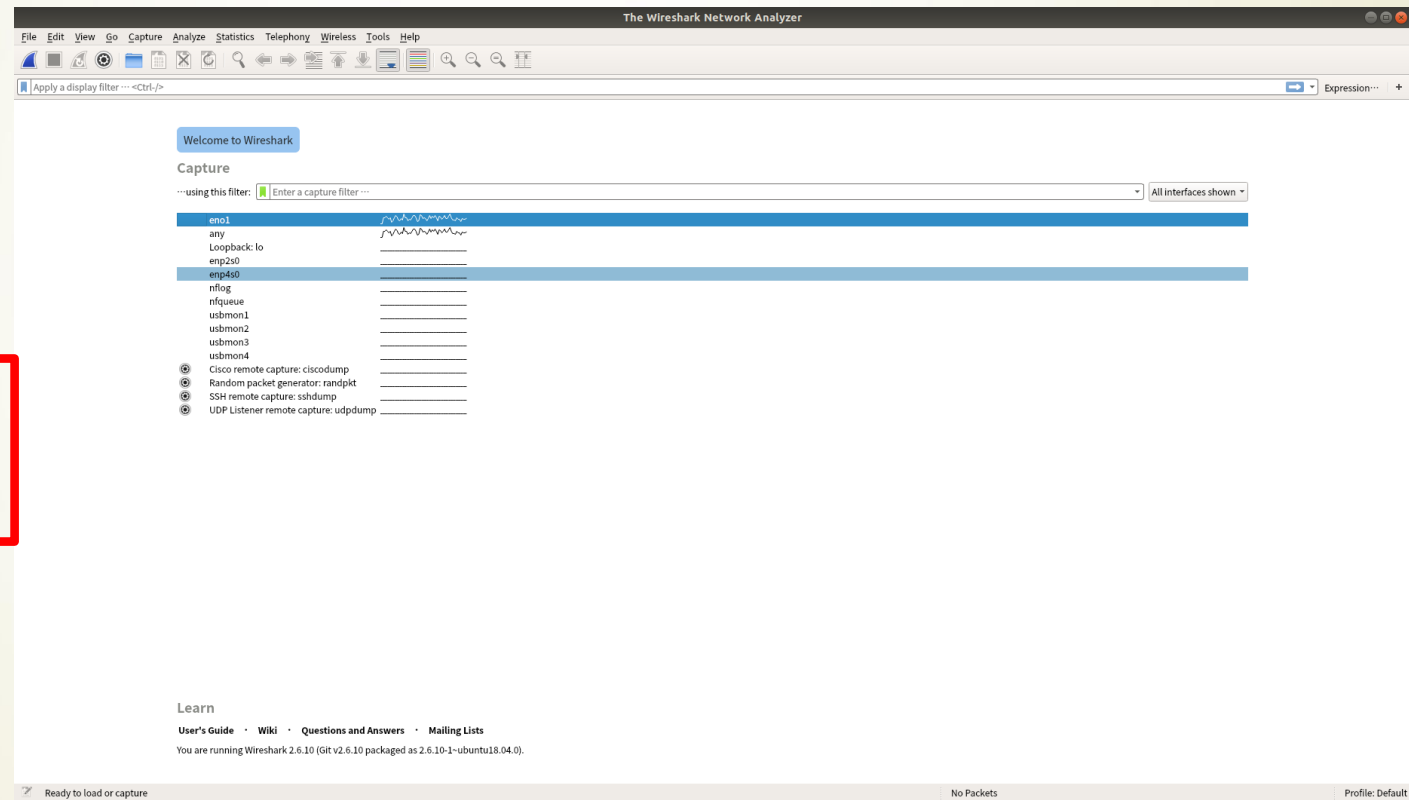
i386 Packages [548 kB]
stricted i386 Packages [13.
erse i386 Packages [154 k
zh_TW
iverse i386 Packages [4,2
zh
translation-en
n
erse Translation-en
ted Translation-en
ie Translation-en
k

開啟wireshark

- ▶ Step1:開啟新的terminal
- ▶ Step2: `$sudo su`，進入root權限
- ▶ Step3:直接打wireshark，並開啟
<or `$sudo wireshark`>



開始畫面



功能表列→

一般工具列→

篩選工具列→

Capturing from eno1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

封包清單窗格→

No.	Time	Source	Destination	Protocol	Length	Info
194	7.974794933	140.123.92.11	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
195	7.985949380	Cisco_af:08:3c	Broadcast	ARP	60	Who has 140.123.92.31? Tell 140.123.92.250
196	8.038246875	140.123.92.69	255.255.255.255	UDP	82	59531 → 1947 Len=40
197	8.050063249	140.123.92.73	239.255.255.250	UDP	694	62577 → 3702 Len=652
198	8.132886831	fe80::8402:c8c2:6d0...	ff02::c	UDP	718	63219 → 3702 Len=656
199	8.251806545	Cisco_af:08:3c	Broadcast	ARP	60	Who has 140.123.92.153? Tell 140.123.92.250
200	8.271470016	Draytek_78:95:69	Broadcast	ARP	60	Who has 140.123.92.60? Tell 140.123.92.41
201	8.292227110	Cisco_af:08:3c	Broadcast	ARP	60	Who has 140.123.92.74? Tell 140.123.92.250
202	8.337138591	Cisco_af:08:3c	Broadcast	ARP	60	Who has 140.123.92.146? Tell 140.123.92.250
203	8.367201542	Dell_b5:ac:79	Broadcast	ARP	60	Who has 192.168.1.1? Tell 169.254.119.79
204	8.395166618	fe80::de4a:3eff:feb...	ff02::1:ff0a:4ce7	ICMPv6	86	Neighbor Solicitation for fe80::cdee:5fd1:680a:4ce7 from dc:4
205	8.488567850	140.123.92.73	140.123.92.255	NBNS	92	Name query NB DESKTOP-A4MNMAT<1c>
206	8.527839031	AsustekC_52:a6:db	Broadcast	ARP	60	Who has 140.123.92.250? Tell 140.123.92.70
207	8.530333136	Giga-Byt_d0:a0:51	Broadcast	ARP	60	Who has 140.123.92.20? Tell 140.123.92.80
208	8.532068390	Cisco_af:08:3c	Broadcast	ARP	60	Who has 140.123.92.3? Tell 140.123.92.250
209	8.555820088	d4:5d:64:c5:0c:72	Broadcast	ARP	60	Who has 140.123.92.150? Tell 140.123.92.129
210	8.591917831	Cisco_af:08:3c	Broadcast	ARP	60	Who has 140.123.92.95? Tell 140.123.92.250
211	8.633507316	fe80::b896:b1cd:a08...	ff02::c	UDP	714	62578 → 3702 Len=652
212	8.659408458	140.123.92.207	239.255.255.250	UDP	698	63218 → 3702 Len=656

封包內容窗格→

(位元組格式)→

狀態列→

eno1: <live capture in progress>

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: Cisco_af:08:3c (8c:60:4f:af:08:3c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▶ Address Resolution Protocol (request)

0000	ff ff ff ff ff ff 8c 60	4f af 08 3c 08 06 00 01	0..<....
0010	08 00 06 04 00 01 8c 60	4f af 08 3c 8c 7b 5c fa	0..<.\.
0020	ff ff ff ff ff ff 8c 7b	5c b8 00 00 00 00 00 00	{ \.....
0030	00 00 00 00 00 00 00 00	00 00 00 00

Wireshark主要視窗功能說明(1/3)

- ▶ 功能表列：執行Wireshark各項功能。
- ▶ 一般功能列：快速啟動功能表列中常用功能。
- ▶ 篩選工具列：在filter欄位中輸入特定語法來過濾封包清單窗格中的封包，語法輸入錯誤時，欄位背景會呈現紅色，這類語法稱為顯示篩選器(display filter)。

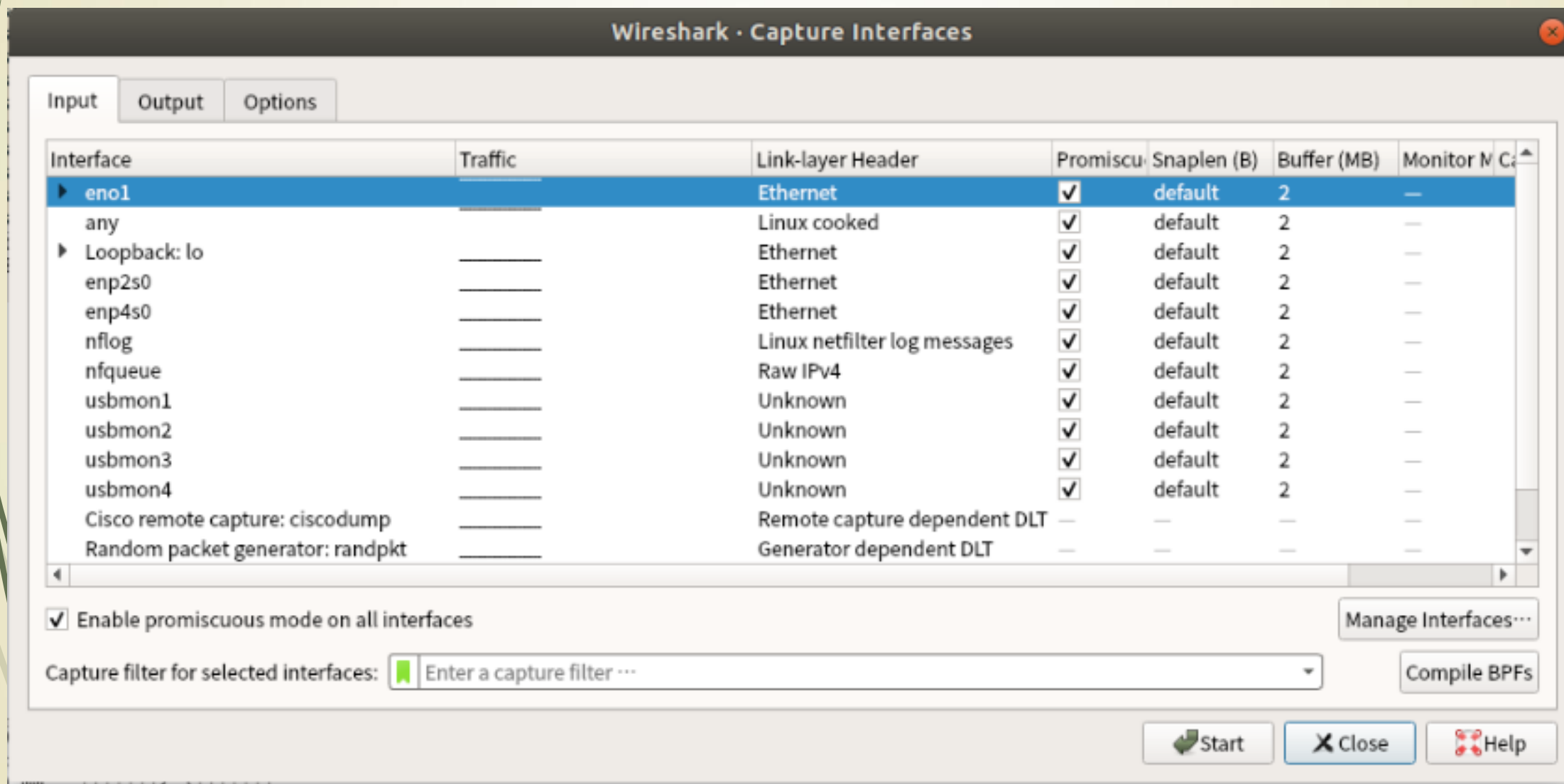
Wireshark主要視窗功能說明(2/3)

- 封包清單窗格(packet list pane)：顯示封包列表，所列出的可能是目前擷取的封包，或是之前存檔的封包清單，預設值會以為第一個欄位(流水號)來排序。
- 封包內容窗格(packet details pane)：會依封包清單窗格所選擇的封包而改變，Wireshark將該封包內容解碼後，以較直覺、較易理解的分層形式顯示出來。

Wireshark主要視窗功能說明(3/3)

- 封包位元組窗格(packet bytes pane)：顯示內容和封包內容窗格相同，但以位元組的格式來呈現，當使用者選取封包內容窗格中的協定欄位時，此處相對應的位元組會自動反白。
- 狀態列：顯示目前程式狀態或其他詳細資訊。

選取想要監聽的網路介面



監聽結果

Wireshark 1.10.6 (v1.10.6 from master-1.10)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression. Clear Apply 儲存

No.	Time	Source	Destination	Protocol	Length	Info
85	16.429214000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
86	16.429444000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=73 Win=65535 Len=0
87	16.667508000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
88	16.667730000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=74 Win=65535 Len=0
89	16.843483000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
90	16.843701000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=75 Win=65535 Len=0
91	17.068123000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
92	17.068375000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=76 Win=65535 Len=0
93	17.195267000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
94	17.195510000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=77 Win=65535 Len=0
95	17.363438000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
96	17.363676000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=78 Win=65535 Len=0
97	17.788195000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
98	17.788417000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6105 Ack=79 Win=65535 Len=0
99	17.796782000	140.112.172.1	10.0.2.15	TELNET	129	Telnet Data ...
100	17.796801000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=79 Ack=6180 Win=41180 Len=0
101	17.797403000	140.112.172.1	10.0.2.15	TELNET	95	Telnet Data ...
102	17.797407000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=79 Ack=6221 Win=41180 Len=0
103	18.309010000	140.112.172.1	10.0.2.15	TELNET	120	Telnet Data ...
104	18.309033000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=79 Ack=6287 Win=41180 Len=0

▶ Frame 85: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0

▶ Ethernet II, Src: CadmusCo_e0:c3:9b (08:00:27:e0:c3:9b), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 140.112.172.1 (140.112.172.1)

▶ Transmission Control Protocol, Src Port: 60130 (60130), Dst Port: telnet (23), Seq: 72, Ack: 6105, Len: 1

▼ Telnet

0000 52 54 00 12 35 02 08 00 27 e0 c3 9b 08 00 45 10 RT..5... '.....E.
0010 00 29 82 2f 40 00 40 06 74 0f 0a 00 02 0f 8c 70 .)./.@. t.....p
0020 ac 01 ea e2 00 17 c3 c0 6f 64 03 33 6d da 50 18 od.3m.P.
0030 a0 dc 44 9c 00 00 69 d i

監聽結果

- ▶ 開始監測之後，畫面會一直動態產生所接收到的封包。你可能會發現很多封包的Source和Destination都不是自己，這是因為我們目前所使用的區域網路大部分為乙太網路，採用廣播為技術基礎，所以在區域網路中我們很容易可以透過Wireshark看到別人的封包，甚至知道別人的隱私內容，本實驗就是要強調明碼的危險性。
- ▶ 明碼傳輸的protocol相當多，telnet、FTP、HTTP等常用協定皆在這個範疇裡面，BBS(Bulletin Board System)就是使用telnet協定運作，透過Wireshark的監聽我們很容易知道別人的帳號密碼。

Capture Options

Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Mon. Mode
<input checked="" type="checkbox"/>	eth0 10.0.2.15 fe80::a00:27ff:fee0:c39b	Ethernet	enabled	default	2	n/a
<input type="checkbox"/>	nflog	Linux netfilter log messages	enabled	default	2	n/a
<input type="checkbox"/>	nfqueue	Raw IPv4	enabled	default	2	n/a
<input type="checkbox"/>	any	Linux cooked	enabled	default	2	n/a

☐ Capture on all interfaces Manage Interfaces

☒ Use promiscuous mode on all interfaces

Capture Filter: Compile selected BPFs

Capture Files

File: Browse...

☐ Use multiple files ☒ Use pcap-ng format

☒ Next file every — +

☐ Next file every — +

☐ Ring buffer with — + files

☐ Stop capture after — + file(s)

Stop Capture Automatically After...

☐ — + packet(s)

☐ — +

☐ — +

Display Options

☒ Update list of packets in real time

☒ Automatically scroll during live capture

☒ Hide capture info dialog

Name Resolution

☒ Resolve MAC addresses

☐ Resolve network-layer names

☒ Resolve transport-layer name

☒ Use external network name resolver

求助(H) Start 關閉(C)



Wireshark有兩種 Filter

- ▶ 擷取中過濾(Filter while capturing)
在擷取封包過程中，已過濾符合條件的封包。
- ▶ 檢視中過濾(Filter packets while viewing)
在擷取完畢後，經由Filter顯示你有興趣的封包，隱藏不感興趣的封包。



Following TCP streams

- ▶ Wireshark針對通訊協定提供了完整的Follow TCP/UDP Stream功能，能夠依序追蹤網路封包所傳送的内容，此種方式可以將有關聯性的網路封包一起呈現，如此在進行網路行為或通訊協定的行為分析時，將更為清楚易讀。

抓取的DNS封包

request

The screenshot shows the Wireshark 1.10.6 interface. The packet list on the left shows several DNS packets. Packet 139 is selected, showing a standard query for clients4.google.com. The packet details pane on the right shows the structure of the DNS query, including the transaction ID (0xb422), flags (0x0100), and the question section. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
139	0.482220000	10.0.2.15	140.123.1.100	DNS	79	Standard query 0xb422 A clients4.google.com
140	0.483422000	140.123.1.100	10.0.2.15	DNS	295	Standard query response 0xb422 CNAME clients4.google.com A 202.169.175.103 A 202.169.175.103
142	0.485659000	10.0.2.15	140.123.1.100	DNS	84	Standard query 0x3871 A translate.googleapis.com
143	0.486609000	140.123.1.100	10.0.2.15	DNS	100	Standard query response 0x3871 A 216.58.200.234
200	0.661474000	10.0.2.15	140.123.1.100	DNS	78	Standard query 0xcd54 A www.googleapis.com
201	0.662599000	140.123.1.100	10.0.2.15	DNS	176	Standard query response 0xcd54 CNAME googleapis.l.google.com A 172.217.24.10 A 172.217.24.10
243	0.699697000	10.0.2.15	140.123.1.100	DNS	79	Standard query 0xbb1e A accounts.google.com
244	0.700787000	140.123.1.100	10.0.2.15	DNS	95	Standard query response 0xbb1e A 172.217.24.13

Frame 139: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: CadmusCo_e0:c3:9b (08:00:27:e0:c3:9b), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 140.123.1.100 (140.123.1.100)
User Datagram Protocol, Src Port: 45727 (45727), Dst Port: domain (53)
Domain Name System (query)
Transaction ID: 0xb422
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries

0000 52 54 00 12 35 02 08 00 27 e0 c3 9b 08 00 45 00 RT...E.....
0010 00 41 5b 2d 40 00 00 11 45 91 0a 00 02 0f 8c 7b .A[-@.@.E.....{
0020 01 64 b2 9f 00 35 00 2d 9a 2c b4 22 01 00 00 01 .d...5-..".....
0030 00 00 00 00 00 00 08 63 6c 69 65 6e 74 73 34 06c llents4.
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 google.com.....

File: "/tmp/wireshark_pcapng_... Packets: 1689 · Displayed: 79 (4.7%) · Dropped: 0 (0.0%) Profile: Default

response

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter: dns

Expression...ClearApply儲存

No.	Time	Source	Destination	Protocol	Length	Info
139	0.482220000	10.0.2.15	140.123.1.100	DNS	79	Standard query 0xb422 A clients4.google.com
140	0.483422000	140.123.1.100	10.0.2.15	DNS	295	Standard query response 0xb422 CNAME clients.l.google.com A 202.169.175.103 A 202.169.175.103
142	0.485659000	10.0.2.15	140.123.1.100	DNS	84	Standard query 0x3871 A translate.googleapis.com
143	0.486609000	140.123.1.100	10.0.2.15	DNS	100	Standard query response 0x3871 A 216.58.200.234
200	0.661474000	10.0.2.15	140.123.1.100	DNS	78	Standard query 0xcd54 A www.googleapis.com
201	0.662599000	140.123.1.100	10.0.2.15	DNS	176	Standard query response 0xcd54 CNAME googleapis.l.google.com A 172.217.24.10 A 216.58.200.234
243	0.699697000	10.0.2.15	140.123.1.100	DNS	79	Standard query 0xbb1e A accounts.google.com
244	0.700787000	140.123.1.100	10.0.2.15	DNS	95	Standard query response 0xbb1e A 172.217.24.13

▶ Frame 140: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on Interface 0

▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_e0:c3:9b (08:00:27:e0:c3:9b)

▶ Internet Protocol Version 4, Src: 140.123.1.100 (140.123.1.100), Dst: 10.0.2.15 (10.0.2.15)

▶ User Datagram Protocol, Src Port: domain (53), Dst Port: 45727 (45727)

▼ Domain Name System (response)

[\[Request In: 139\]](#)

[Time: 0.001202000 seconds]

Transaction ID: 0xb422

▶ Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 13

Authority RRs: 0

Additional RRs: 0

▶ Queries

▶ Answers

0000 08 00 27 e0 c3 9b 52 54 00 12 35 02 08 00 45 00 ...RT..5...E.
0010 01 19 ad d2 00 00 40 11 32 14 8c 7b 01 64 0a 00@.2..{d..
0020 02 0f 00 35 b2 9f 01 05 1a 17 b4 22 81 80 00 01 ...5.... ..
0030 00 0d 00 00 00 00 08 63 6c 69 65 6e 74 73 34 06c llents4.
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 c0 google.c om.....

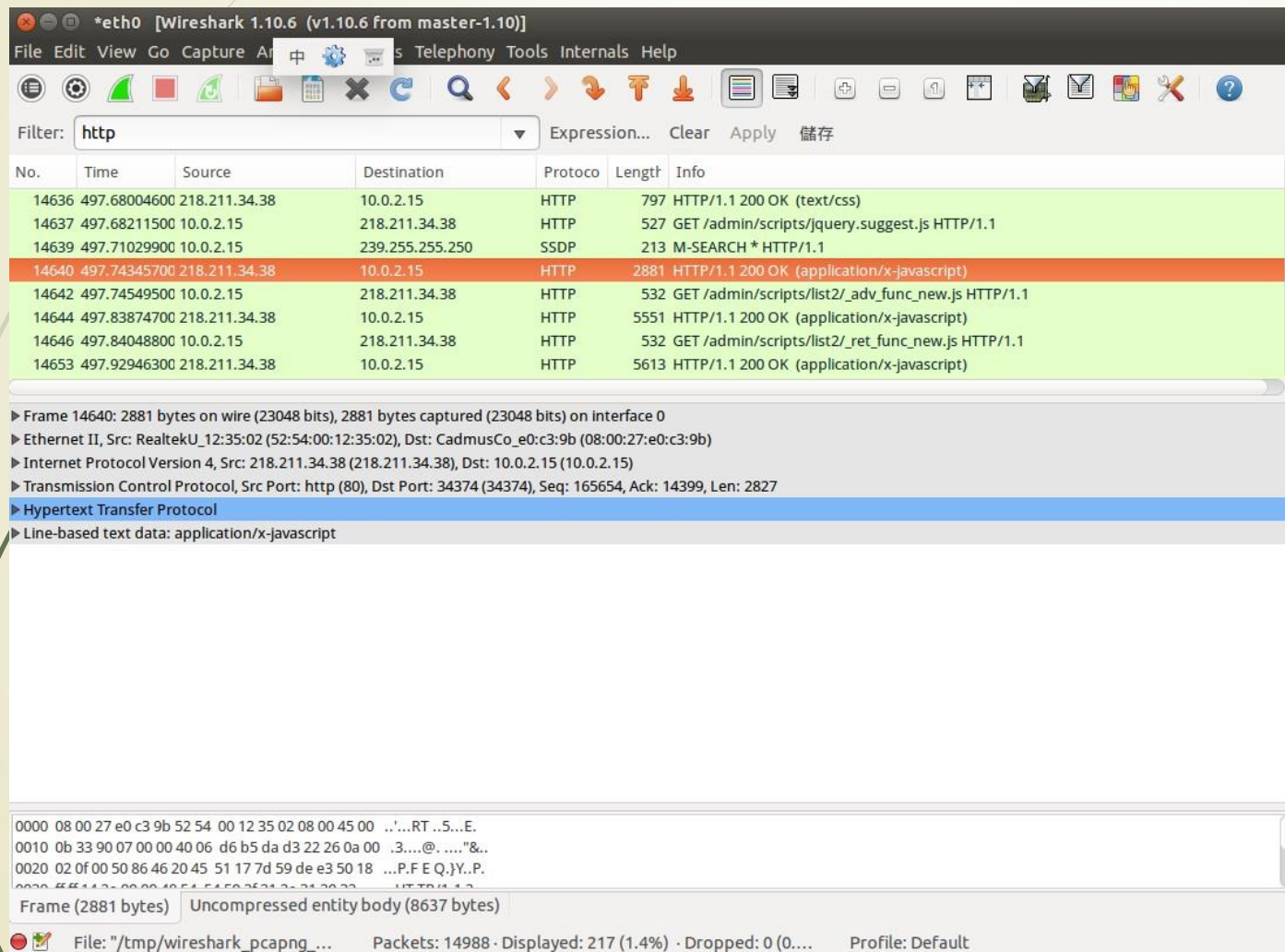
File: "/tmp/wireshark_pcapng_..."

Packets: 1689 · Displayed: 79 (4.7%) · Dropped: 0 (0.0%)

Profile: Default

HTTP

抓取的HTTP封包



Wireshark 1.10.6 (v1.10.6 from master-1.10)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
14636	497.68004600	218.211.34.38	10.0.2.15	HTTP	797	HTTP/1.1 200 OK (text/css)
14637	497.68211500	10.0.2.15	218.211.34.38	HTTP	527	GET /admin/scripts/jquery.suggest.js HTTP/1.1
14639	497.71029900	10.0.2.15	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
14640	497.74345700	218.211.34.38	10.0.2.15	HTTP	2881	HTTP/1.1 200 OK (application/x-javascript)
14642	497.74549500	10.0.2.15	218.211.34.38	HTTP	532	GET /admin/scripts/list2_adv_func_new.js HTTP/1.1
14644	497.83874700	218.211.34.38	10.0.2.15	HTTP	5551	HTTP/1.1 200 OK (application/x-javascript)
14646	497.84048800	10.0.2.15	218.211.34.38	HTTP	532	GET /admin/scripts/list2_ret_func_new.js HTTP/1.1
14653	497.92946300	218.211.34.38	10.0.2.15	HTTP	5613	HTTP/1.1 200 OK (application/x-javascript)

► Frame 14640: 2881 bytes on wire (23048 bits), 2881 bytes captured (23048 bits) on interface 0

► Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_e0:c3:9b (08:00:27:e0:c3:9b)

► Internet Protocol Version 4, Src: 218.211.34.38 (218.211.34.38), Dst: 10.0.2.15 (10.0.2.15)

► Transmission Control Protocol, Src Port: http (80), Dst Port: 34374 (34374), Seq: 165654, Ack: 14399, Len: 2827

► Hypertext Transfer Protocol

► Line-based text data: application/x-javascript

0000 08 00 27 e0 c3 9b 52 54 00 12 35 02 08 00 45 00 ...RT ..5...E.
0010 0b 33 90 07 00 00 40 06 d6 b5 da d3 22 26 0a 00 ...3....@.&..
0020 02 0f 00 50 86 46 20 45 51 17 7d 59 de e3 50 18 ...P.F E Q.JY..P.
0030 ff 1a 2 00 00 40 51 51 50 25 31 2 21 20 22 ...UT 3 1 1 2
Frame (2881 bytes) Uncompressed entity body (8637 bytes)

File: "/tmp/wireshark_pcapng_... Packets: 14988 · Displayed: 217 (1.4%) · Dropped: 0 (0.... Profile: Default

LAB1- 使用 Wireshark 分析packet的內容

- Purpose:

- Use Wireshark to capture an IP packet and analyze the header and payload of this packet.
- Are you able to identify the transport layer protocol and the application layer protocol?
- (觀察不同的protocol找出他們的port number，並說明)
- (也可以對wireshark顯示的資訊作補充)

- Step:

- 1.開啟不同類型的網站，例如:yahoo新聞、facebook、youtube
- 2.觀察protocol的變化，以及所屬的layer

LAB2- 使用 Wireshark 觀察 ping 學校的首頁

- Purpose:

- Use Wireshark to find out how ping is implemented using ICMP、DNS messages. Show the packets captured to verify your answer.
- 需要對request和reply做解釋，另外可以對icmp這個protocol作補充

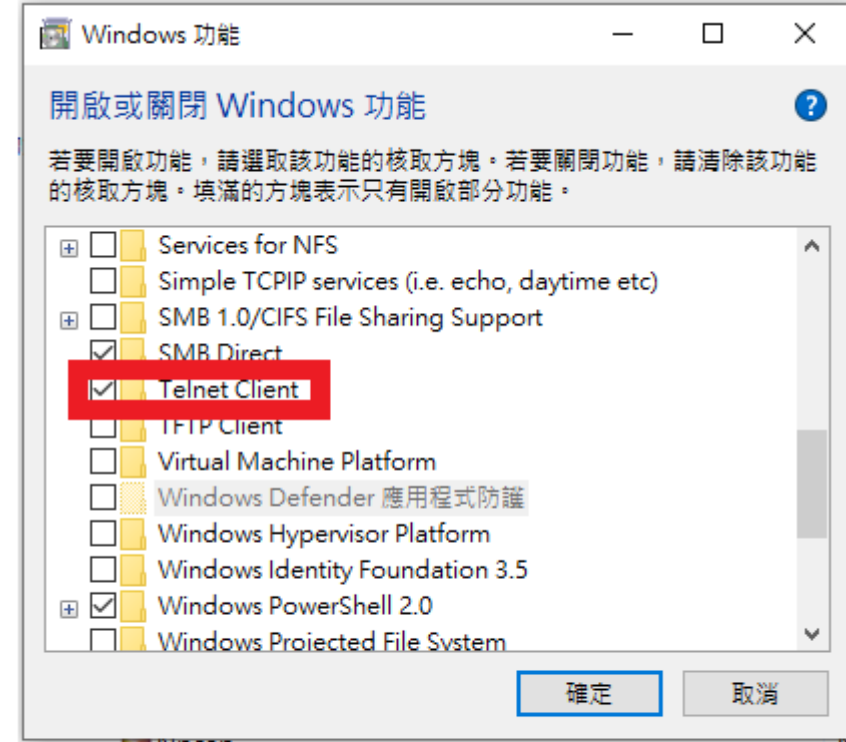
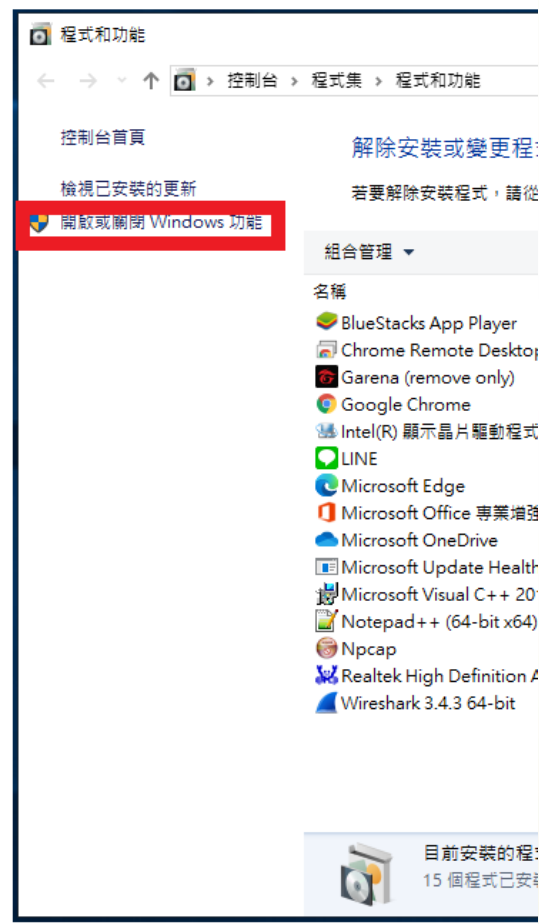
- Step:

- 1.開啟新的terminal
- 2.ping www.ccu.edu.tw
- 3.觀察wireshark運作

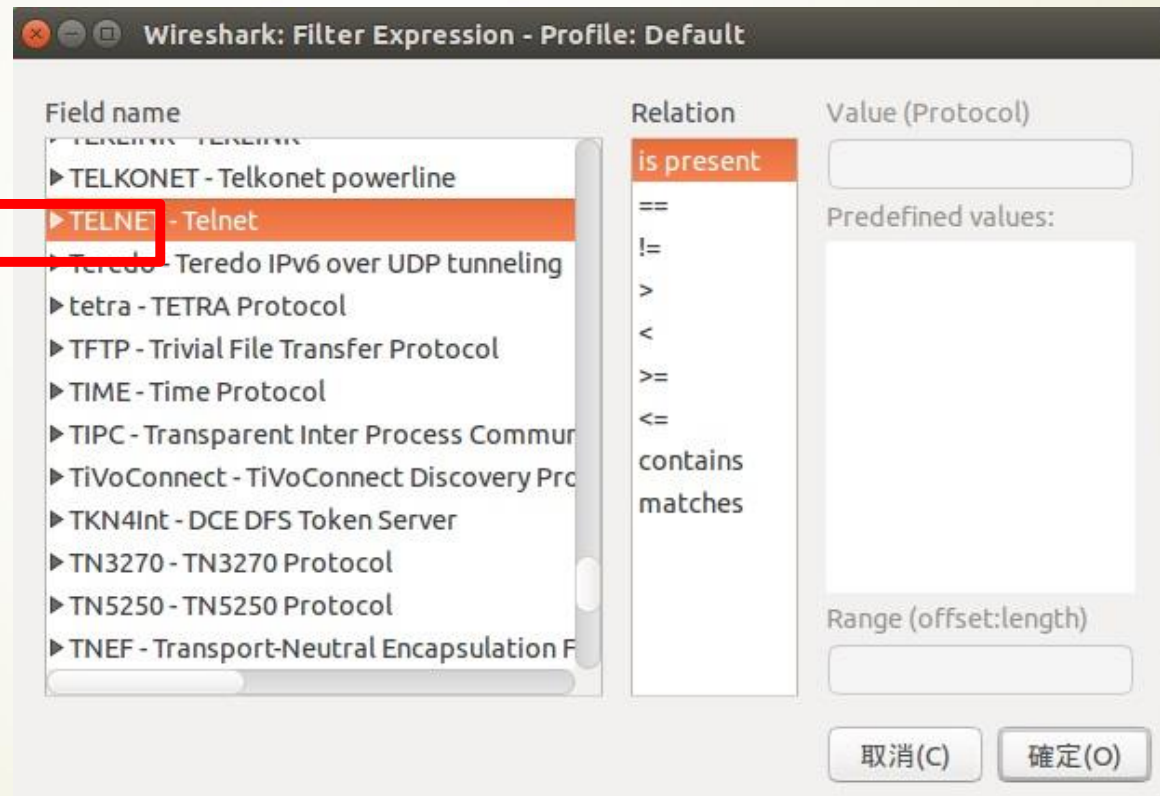
回家作業LAB3- 使用 Wireshark 取得BBS的內容

- ▶ 利用terminal telnet進去PTT，再用wireshark找出你輸入的帳號和密碼(沒有PTT帳號就隨便打一組帳號密碼即可)
- ▶ 另外可以對該怎麼防止帳密外洩作補充，例如:盡量使用https加密協定的網站使用等等。

LAB3提示 – 在windows開啟telnet功能



分析telnet的封包



利用BBS來查看 telnet 運作

```
joe@joe-VirtualBox: ~  
因隻釘A  
所以我么I真...  
g  
區 ]  
by cat91847  
個人設定區 ]  
telnet://ptt.cc 版權所有 <總站·官方> 特別感謝本站最佳主角  
telnet://ptt2.cc 版權也有 <個人·地下> wanedcol  
telnet://ptt3.cc 版權美有 <海外·留學> ...期待您下一次的光臨  
◆ 此次停留時間: 0 小時 0 分 [按任意鍵繼續] Co  
nnection closed by foreign host.  
joe@joe-VirtualBox:~$ luit -encoding big5 telnet ptt.cc
```

*eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply 儲存

No.	Time	Source	Destination	Protocol	Length	Info
14	8.291521000	10.0.2.15	8.8.8.8	ICMP	190	Destination unreachable (Port unreachable)
15	8.293840000	10.0.2.15	140.112.172.1	TELNET	81	Telnet Data ...
16	8.294006000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=1 Ack=28 Win=65535 Len=0
17	8.300036000	140.112.172.1	10.0.2.15	TELNET	2579	Telnet Data ...
18	8.300054000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=28 Ack=2526 Win=34080 Len=0
19	8.300236000	140.112.172.1	10.0.2.15	TELNET	3563	Telnet Data ...
20	8.300243000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=28 Ack=6035 Win=41180 Len=0
21	8.300477000	10.0.2.15	140.112.172.1	TELNET	83	Telnet Data ...
22	8.300596000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6035 Ack=57 Win=65535 Len=0
23	8.308228000	140.112.172.1	10.0.2.15	TELNET	72	Telnet Data ...
24	8.347922000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=57 Ack=6053 Win=41180 Len=0
25	9.328350000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
26	9.328570000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6053 Ack=58 Win=65535 Len=0
27	9.336607000	140.112.172.1	10.0.2.15	TELNET	60	Telnet Data ...
28	9.336628000	10.0.2.15	140.112.172.1	TCP	54	60130 > telnet [ACK] Seq=58 Ack=6054 Win=41180 Len=0
29	9.424254000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
30	9.424476000	140.112.172.1	10.0.2.15	TCP	60	telnet > 60130 [ACK] Seq=6054 Ack=59 Win=65535 Len=0

▼ Frame 17: 2579 bytes on wire (20632 bits), 2579 bytes captured (20632 bits) on interface 0

Interface id: 0

Encapsulation type: Ethernet (1)

Arrival Time: Mar 4, 2017 13:41:47.764690000 CST

[Time shift for this packet: 0.000000000 seconds]

0980 5b 33 33 6d a2 1b 5b 33 30 6d 67 1b 5b 34 33 6d [33m...[30mg.[43m

0990 a2 a9 20 1b 5b 33 33 3b 34 30 6d a2 1b 5b 33 30 ..[33; 40m...[30

09a0 6d ab 1b 5b 33 36 6d a2 aa 20 20 20 20 20 1b 5b m...[36m...[

09b0 33 30 6d a2 1b 5b 34 33 6d a9 a1 1b 5b 31 6d 60 30m...[43 m...[1m`

09c0 1b 5b 3b 33 30 3b 34 33 6d a2 1b 5b 33 36 3b 34 .[;30;43 m...[36;4

09d0 36 6d a8 20 20 20 20 20 20 20 1b 5b 33 37 6d 6m...[37m

09e0 60 20 1b 5b 33 36 3b 34 30 6d a2 a9 1b 5b 31 3b `.[36;40m...[1;

09f0 33 30 6d a3 1b 5b 3b 33 30 3b 34 30 6d a5 1b 5b 30m...[30;40m...[

0a00 33 37 3b 34 33 6d a2 6b 1b 5b 33 33 3b 34 30 6d 37;43m.k.[33;40m

0a10 a2 66 a2 .f.

File: "/tmp/wireshark_pcapng_... Packets: 124 · Displayed: 124 (100.0%) · Dropped: 0 (0.0%) Profile: Default

*eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: telnet Expression... Clear Apply 儲存

No.	Time	Source	Destination	Protocol	Length	Info
81	15.804818000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
83	15.813492000	140.112.172.1	10.0.2.15	TELNET	86	Telnet Data ...
85	16.429214000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
87	16.667508000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
89	16.843483000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
91	17.068123000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
93	17.195267000	10.0.2.15	140.112.172.1	TELNET	55	Telnet Data ...
95	17.363438000	10.0.2.15	140.112.172.1	TELNET		
97	17.788195000	10.0.2.15	140.112.172.1	TELNET		
99	17.796782000	140.112.172.1	10.0.2.15	TELNET		
101	17.797403000	140.112.172.1	10.0.2.15	TELNET		
103	18.309010000	140.112.172.1	10.0.2.15	TELNET		
105	18.323035000	140.112.172.1	10.0.2.15	TELNET		
109	19.091411000	10.0.2.15	140.112.172.1	TELNET		
111	19.100177000	140.112.172.1	10.0.2.15	TELNET		
113	20.442412000	10.0.2.15	140.112.172.1	TELNET		
115	20.452497000	140.112.172.1	10.0.2.15	TELNET		
117	20.570092000	10.0.2.15	140.112.172.1	TELNET		
119	20.579195000	140.112.172.1	10.0.2.15	TELNET		
121	20.579430000	140.112.172.1	10.0.2.15	TELNET		

▶ Frame 93: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0

▶ Ethernet II, Src: CadmusCo_e0:c3:9b (08:00:27:e0:c3:9b), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 140.112.172.1 (140.112.172.1)

▶ Transmission Control Protocol, Src Port: 60130 (60130), Dst Port: telnet (23), Seq: 76, Ack: 10000, Win: 0, Len: 0

▼ Telnet

0000 52 54 00 12 35 02 08 00 27 e0 c3 9b 08 00 45 10 RT..5... '.....E.

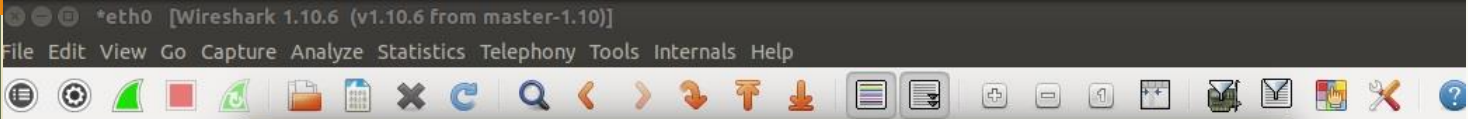
0010 00 29 82 33 40 00 40 06 74 0b 0a 00 02 0f 8c 70 .).3@.@. t.....p

0020 ac 01 ea e2 00 17 c3 c0 6f 68 03 33 6d da 50 18 oh.3m.P.

0030 a0 dc 44 9c 00 00 6e ..D...n

- Mark Packet (toggle)
- Ignore Packet (toggle)
- Set Time Reference (toggle)
- Time Shift...
- Packet Comment...
- Manually Resolve Address
- Apply as Filter ▶
- Prepare a Filter ▶
- Conversation Filter ▶
- Colorize Conversation ▶
- SCTP ▶
- Follow TCP Stream
- Follow UDP Stream
- Follow SSL Stream
- Copy ▶
- Protocol Preferences ▶
- Decode As...
- Print...
- Show Packet in New Window

File: "/tmp/wireshark_pcapng_... Packets: 124 · Displayed: 53 (42.7%) · Dropped: 0 (0.0%) Profile: Default



紅色的部分為我們送出的**DATA**，藍色的部分是我們收到的**DATA**

為了避免被有心人監測到重要資料，有SSH、SSL、HTTPS等加密協定可用就盡量使用，至少別人監聽到的內容是加密過的。



END