Ping 到網路世界

剛進入網路世界探險的各位，除了享受網路無遠弗屆、學無止盡的知識與資訊外，對於網路底層也須了解的我們，也能從中獲得網路原理理論和知識，知識不難找，重要的是如何印證知識理論與實際應用的種種。

而 Ping 大概是所有電腦使用者的一個接觸的網路指令，通常都用來檢查網路的正常性 (雖然時常看到許多人這樣做)，至於足不足夠判斷，我們會在課堂中說明；所以，我們從最簡單的 Ping 來帶各位進入這個網路叢林中。

Ping to Gateway

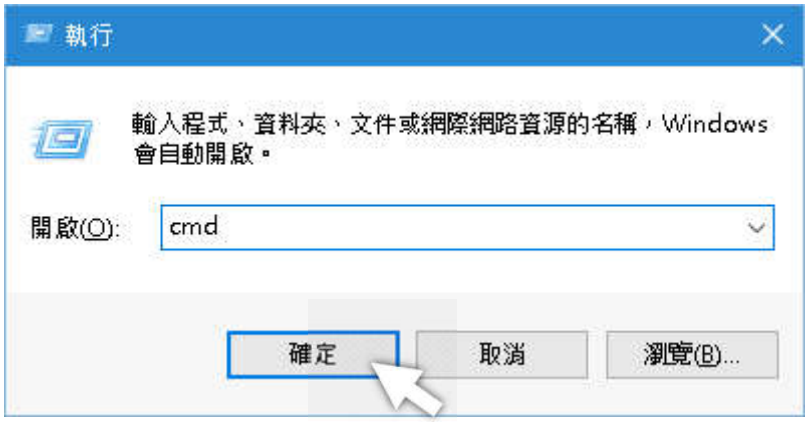
擷取封包的第一步，當然是開啟您的 Wireshark，我們首先來 Ping 我們的 Gateway，藉由 Gateway 回應給我們的封包來觀察回覆資訊與分析網路狀態：

STEP-01：啟動 Wireshark 並擷取封包：

附註：如果您還未熟悉如何啟動 Wireshark，請您回到前面章節回顧如何啟動 Wireshark 並開始擷取封包！

STEP-02：開啟命令提示字元視窗 (以 Windows 10 為例)，以下選其一執行：

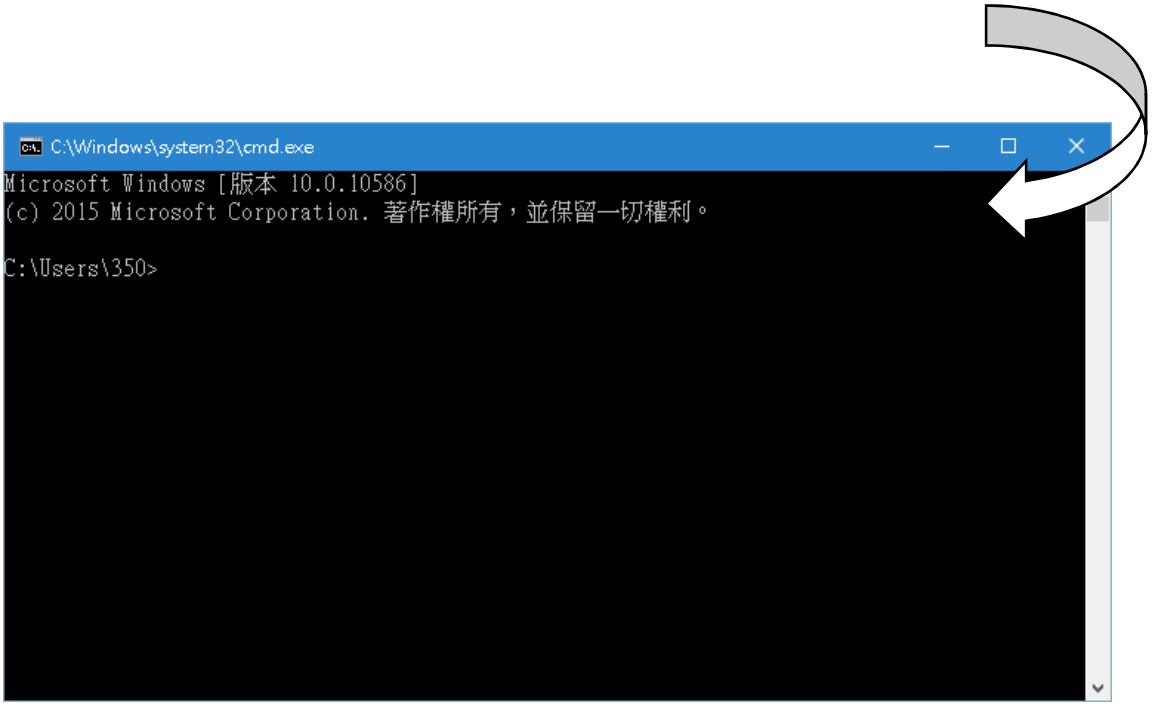
方式一：



「開始」+「R」，輸入「cmd」，按下確定

方式二：

於開始鍵圖示  按下右鍵，選擇「命令提示字元(C)」



STEP-03：於命令提示字元視窗中，輸入指令「ping　192.168.0.1」：

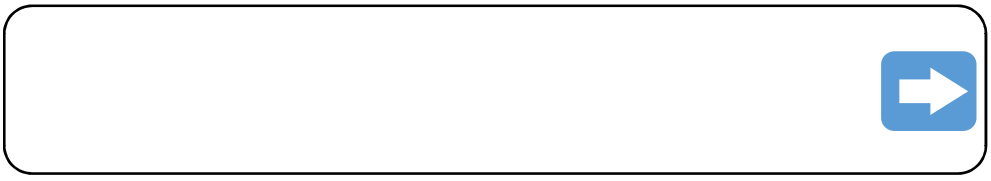
如果您的網路是正常的，您將會在命令提示字元視窗看到如下訊息回應：

```
C:\Users\350>ping 192.168.2.1

Ping 192.168.2.1 (使用 32 位元組的資料):
回覆自 192.168.2.1: 位元組=32 時間<1ms TTL=255
回覆自 192.168.2.1: 位元組=32 時間<1ms TTL=255
回覆自 192.168.2.1: 位元組=32 時間=1ms TTL=255
回覆自 192.168.2.1: 位元組=32 時間<1ms TTL=255

192.168.2.1 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
大約的來回時間 (毫秒):
    最小值 = 0ms, 最大值 = 1ms, 平均 = 0ms

C:\Users\350>
```

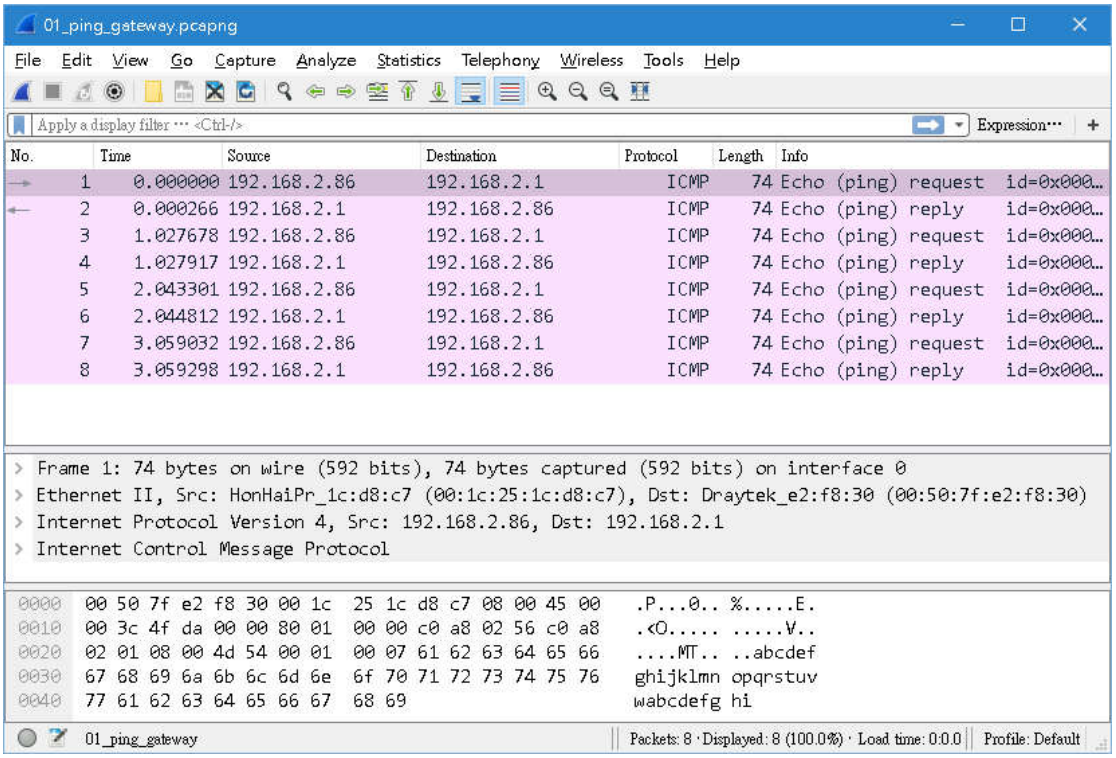
STEP-04：停止 Wireshark 的擷取：

附註：如果您還未熟悉如何停止 Wireshark，請您回到前面章節回顧如何停止 Wireshark 擷取封包！

STEP-05：下達顯示過濾：



您已經可以在 Wireshark 裡看見許多關於 ICMP 的封包資訊 (本範例可以在 \Capture\1-2-Part1_PING\01_ping_gateway.pcapng 取得)：



現在 Windows 的 Ping 為給我們帶來了 Gateway 的回應，且我們也擷取到「真正」網路世界裡面的封包了，現在可以開始來一窺網路的真實世界囉！

不過開始分析之前之前，您應該先知道三個東西，那就是封包每層的表頭 (header)，這是最基本也是分析最重要的部分。