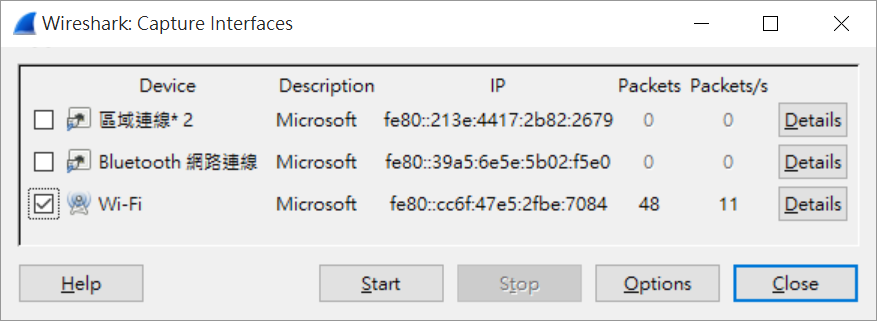
資訊網路概論 實作 1 (W2)

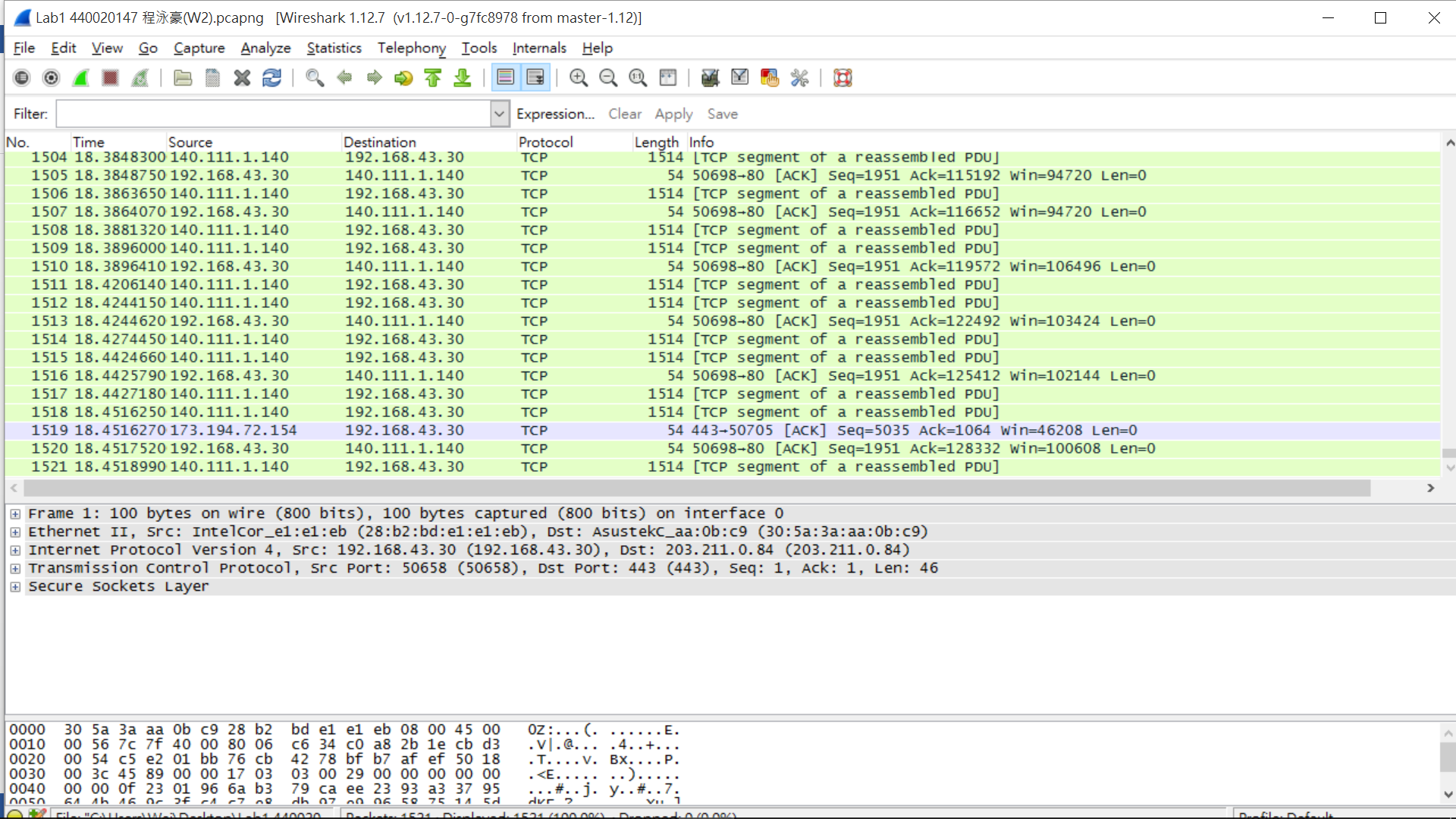
使用 Wireshark 擷取及分析封包

1. 顯示電腦的網路卡



二、 擷取封包

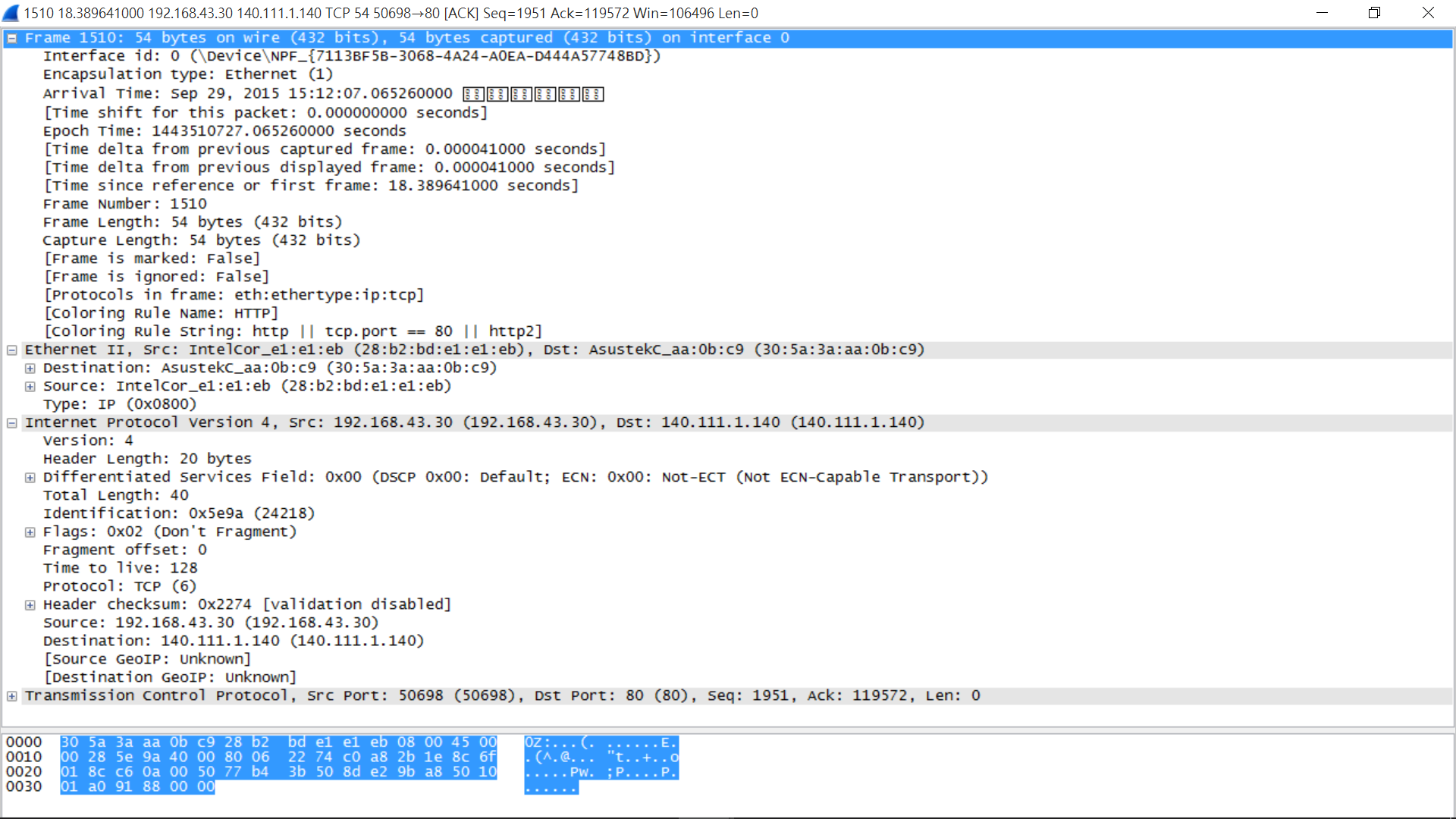




1. 封包分析 (參考課本 2-6 , 2-7 節，p.2-17~2-26)

過濾下列 3 種通訊協定，分別使用「封包詳細資訊」分析封包，顯示網路模 型的每一層封裝後表頭檔內容(「封包詳細資訊」畫面)，並對封包大小、來源 IP 及 MAC 位址、目的 IP 及 MAC 位址、協定等資訊進行分析。

1. 過濾 TCP 封包，從中選取一個封包進行分析



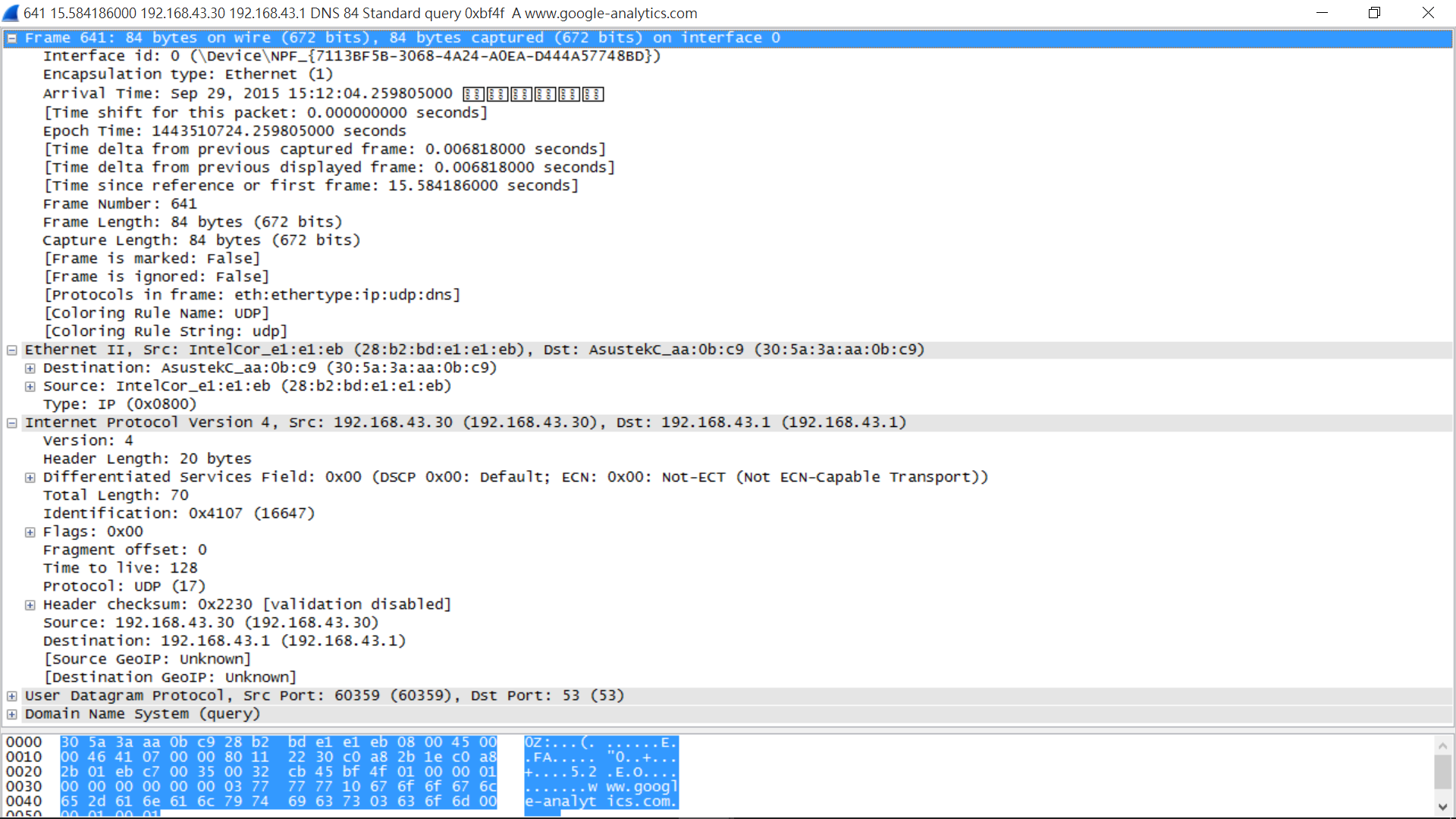
封包大小：54 bytes

來源 IP：192.168.43.30 來源 MAC 位址：28:b2:bd:e1:e1:ed

目的 IP：140.111.1.140 目的 MAC 位址：30:5a:3a:aa:0b:c9

協定：TCP

1. 過濾 DNS 封包，從中選取一個封包進行分析，DNS 封包的傳輸層是使用 TCP 還是 UDP?



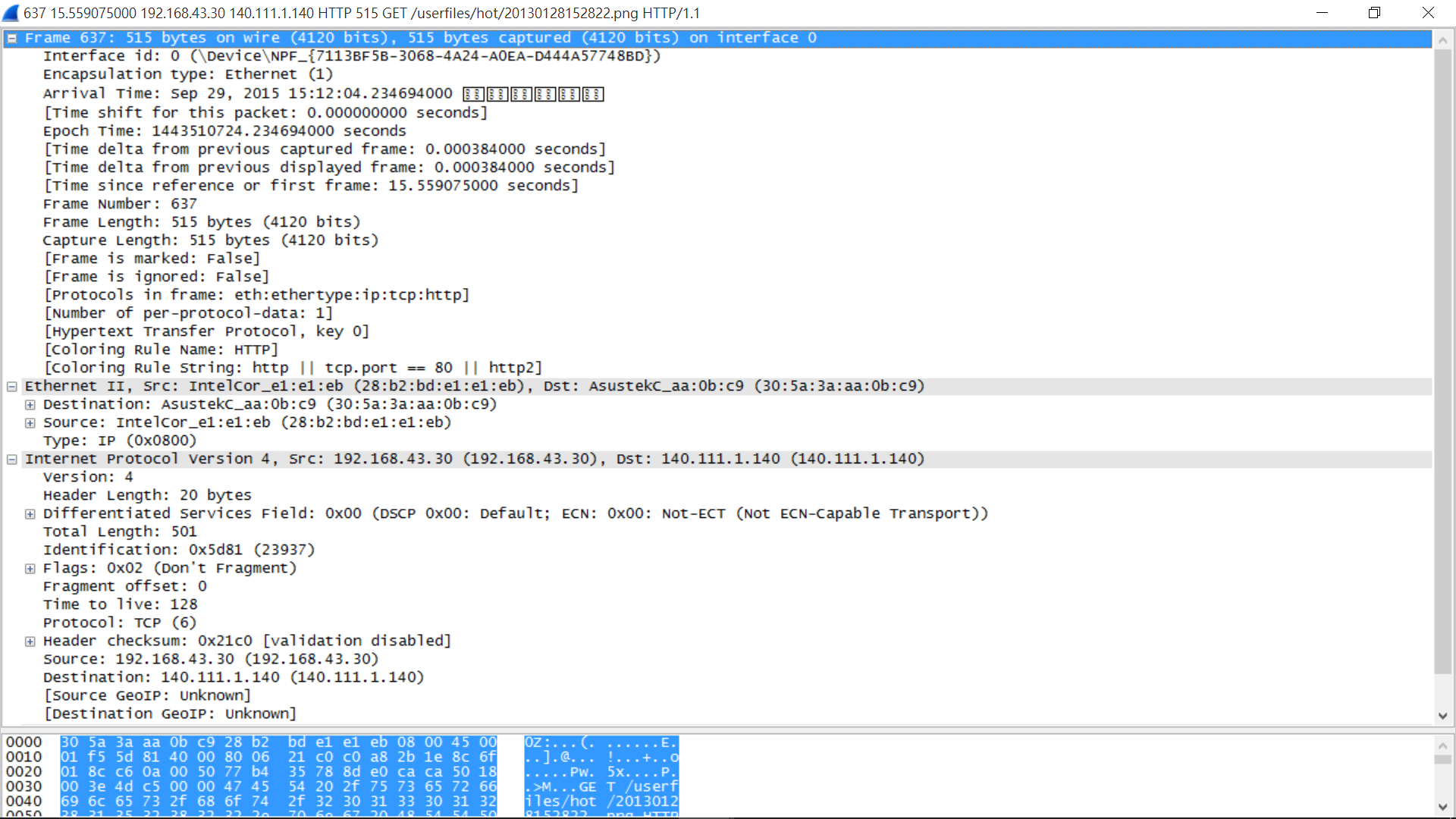
封包大小：84 bytes

來源 IP：192.168.43.30 來源 MAC 位址：28:b1:bd:e1:e1:eb

目的 IP：192.168.43.1 目的 MAC 位址：30:5a:3a:aa:0b:c9

協定：DNS

1. 過濾 HTTP 封包，從中選取一個封包進行分析，HTTP 封包的傳輸層是使 用 TCP 還是 UDP?



封包大小：511 bytes

來源 IP：192.168.43.30 來源 MAC 位址：28:b2:bd:e1:e1:eb

目的 IP：140.111.1.140 目的 MAC 位址：30:5a:3a:aa:0b:c9

協定：HTTP

四、 儲存擷取封包結果

滑鼠點選「File > Save」，即可將擷取封包的結果儲存成檔案名稱為「Lab1 學號-姓名(W2).pcapng」，並與報告 Word 檔案(名稱為「Lab1 學號-姓名 (W2).docx」傳至 iLMS 教學平台。