WiresharkLab\_DNS

建議:把比例放到150%圖才會清楚

組別:A10

組長:資管二甲 B0444132 張仁樵(做最多事)

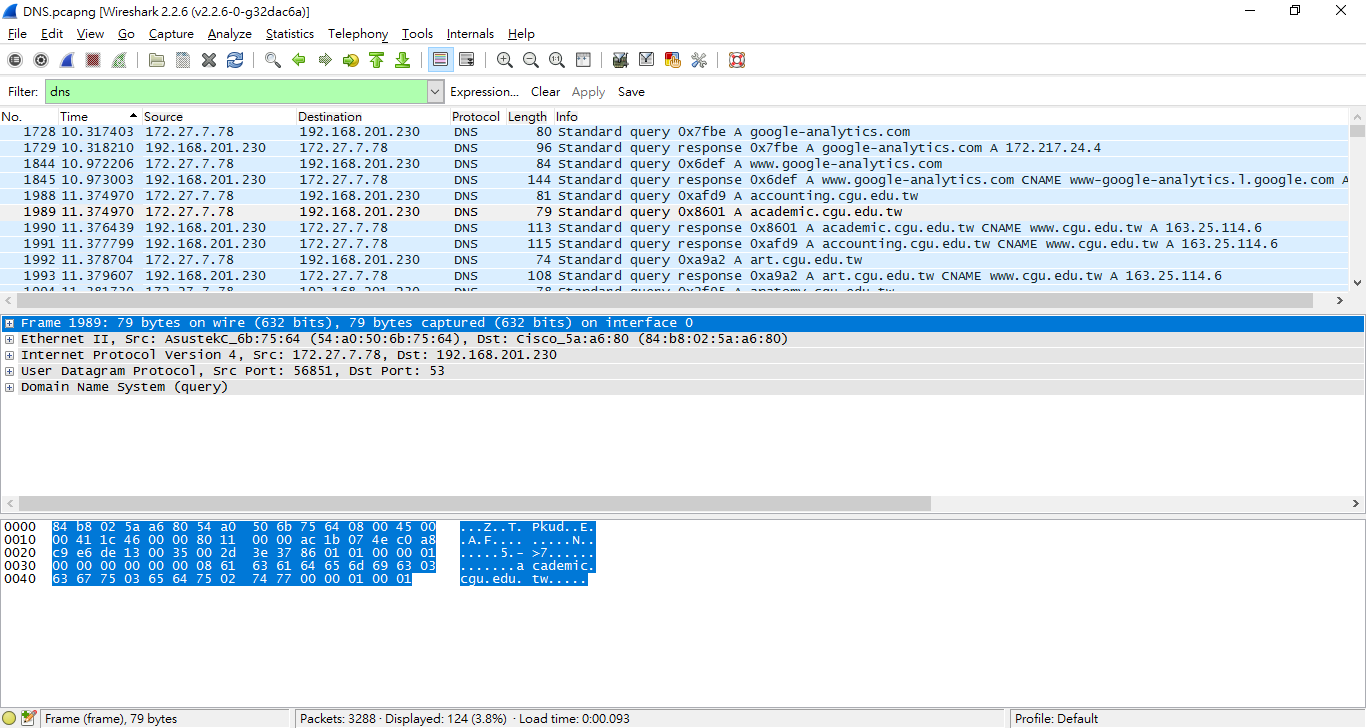
組員:資管二甲 B0444101 李積舜

組員:資管二甲 B0444138 潘楚華

組員:資管二甲 B0444146 林子由



->進入長庚大學首頁



->選取DNS，在這邊我們選教務處的DNS

accounting.cgu.edu.tw-->會計室

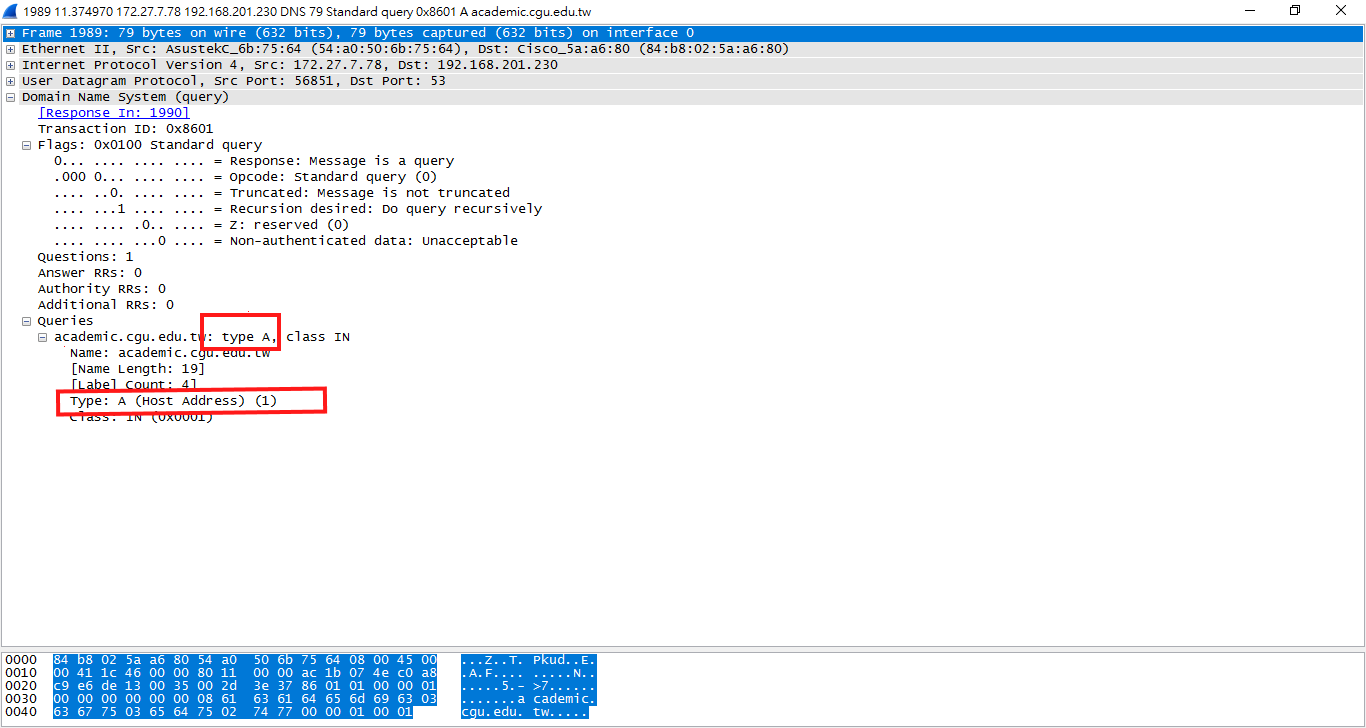
academic.cgu.edu.tw-->教務處

art.cgu.edu.tw-->藝文委員會

im.cgu.edu.tw-->資管系

nurse.cgu.edu.tw-->護理系

一、Type=A



1.封包為本機(Source : 172.27.7.78)向DNS伺服器(Destination :192.168.201.230)發出詢問，其中Src Port 為56851 ﹔Dst Port 為 53

2.用來識別其詢問所得到回應的識別碼，此處為0x8601

3. 表示問題內訊息數目，此處為1

表示答案內訊息數目，此處為0

表示管轄內訊息數目，此處為0

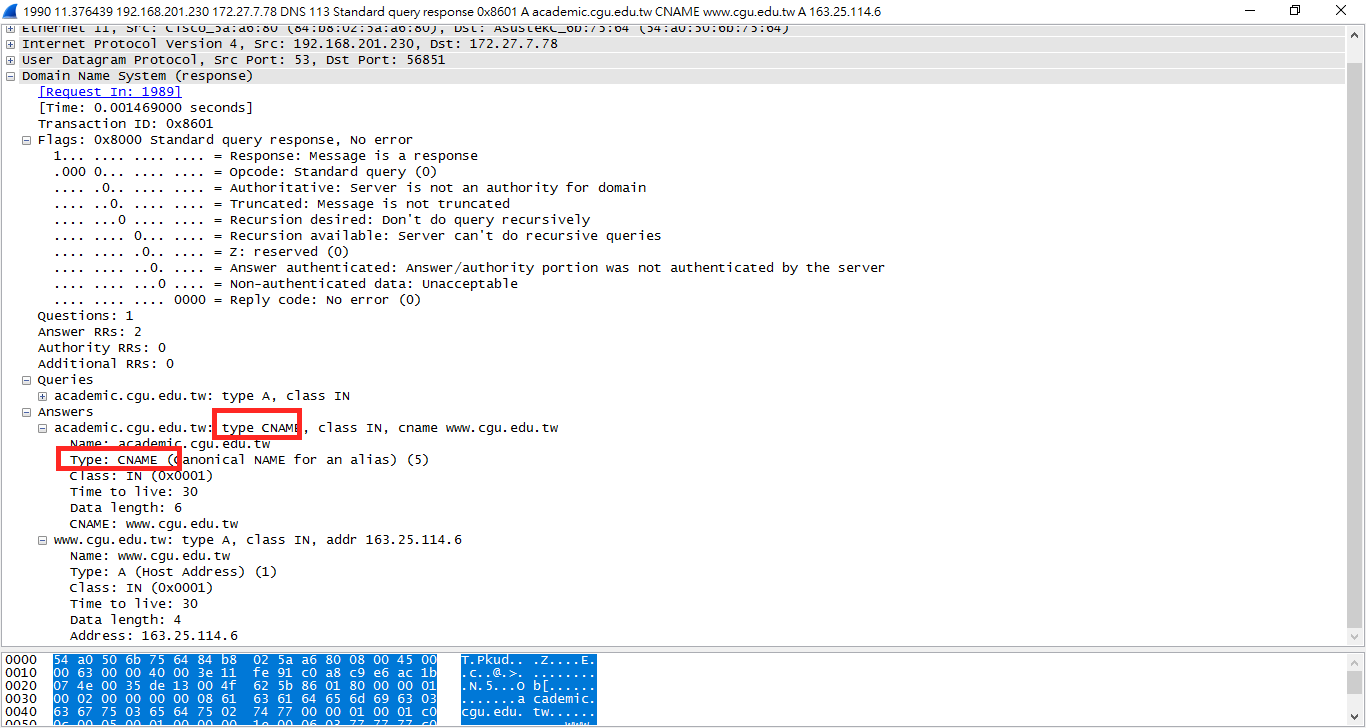
表示額外內訊息數目，此處為0

4.Type=A，Name為主機名稱，Value為主機名稱的IP位址。

(在此為academic.cgu.edu.tw,163.25.114.6,A,62)(62為TTL，用cmd得知)

5.一筆Type A 的紀錄提供了標準的主機名稱與IP位址的對應資訊。

二、Type=CNAME



1.封包為DNS伺服器(Source : 192.168.201.130)向本機(Destination :172.27.7.78)發出詢問，其中Src Port 為53 ﹔Dst Port 為 56851

2.用來識別其詢問所得到回應的識別碼，此處為0x8601

3. 表示問題內訊息數目，此處為1

表示答案內訊息數目，此處為2

表示管轄內訊息數目，此處為0

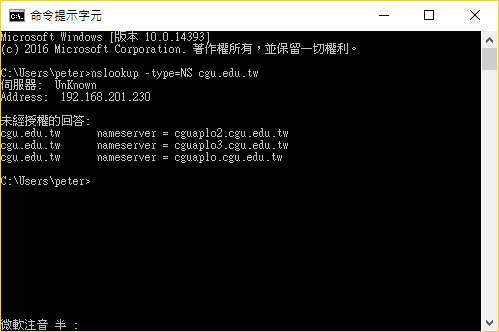
表示額外內訊息數目，此處為0

4.Type=CNAME，Name為主機別名，Value為正規主機名稱。

(在此為academic.cgu.edu.tw,www.cgu.edu.tw,CHANE)

5.這類紀錄可以提供某個主機名稱的正規名稱給發出查詢的主機。

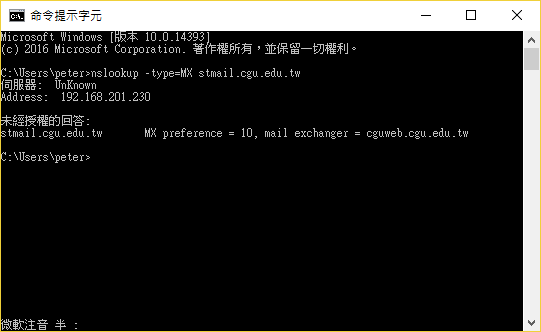
三、Type=NS



1.本部電腦預設的DNS伺服器查詢cgu.edu.tw , 結果有三台Server。

2.這類紀錄是用來在查詢鏈中進一步繞送DNS查詢。

四、Type=MX



1.MX紀錄讓郵件伺服器的主機名稱可以使用簡單的別名，藉由使用MX紀錄，公司就可以使用相同的別名來代表其郵件伺服器和其他伺服器(例如網頁伺服器)。要取得郵件伺服器的正規名稱，DNS用戶端會查詢MX紀錄；要取得其他伺服器的正規名稱，DNS用戶端會查詢CHANE紀錄。

2.(stmail.cgu.edu.tw,cguweb.cgu.edu.tw,MX)

五、心得

DNS，一項將域名和IP位址相互對映的一個分散式資料庫，使我們能夠更方便的存取網際網路。他就像編譯器一樣，編譯器將我們寫出的程式語言轉化為電腦能讀懂得語言，我們若呼叫域名，DNS幫我們將網址轉化為IP位址供電腦辨認。而我們在這次實驗中，選取不同的域名(網址)可以取得不同處室、不同系的資料，而又透過不同的Type去辨認資料。透過wireshark，我們能將以往用命令提示字元取得IP位址的步驟用更具體、完整的方式呈現，也更加了解其運作的內容。