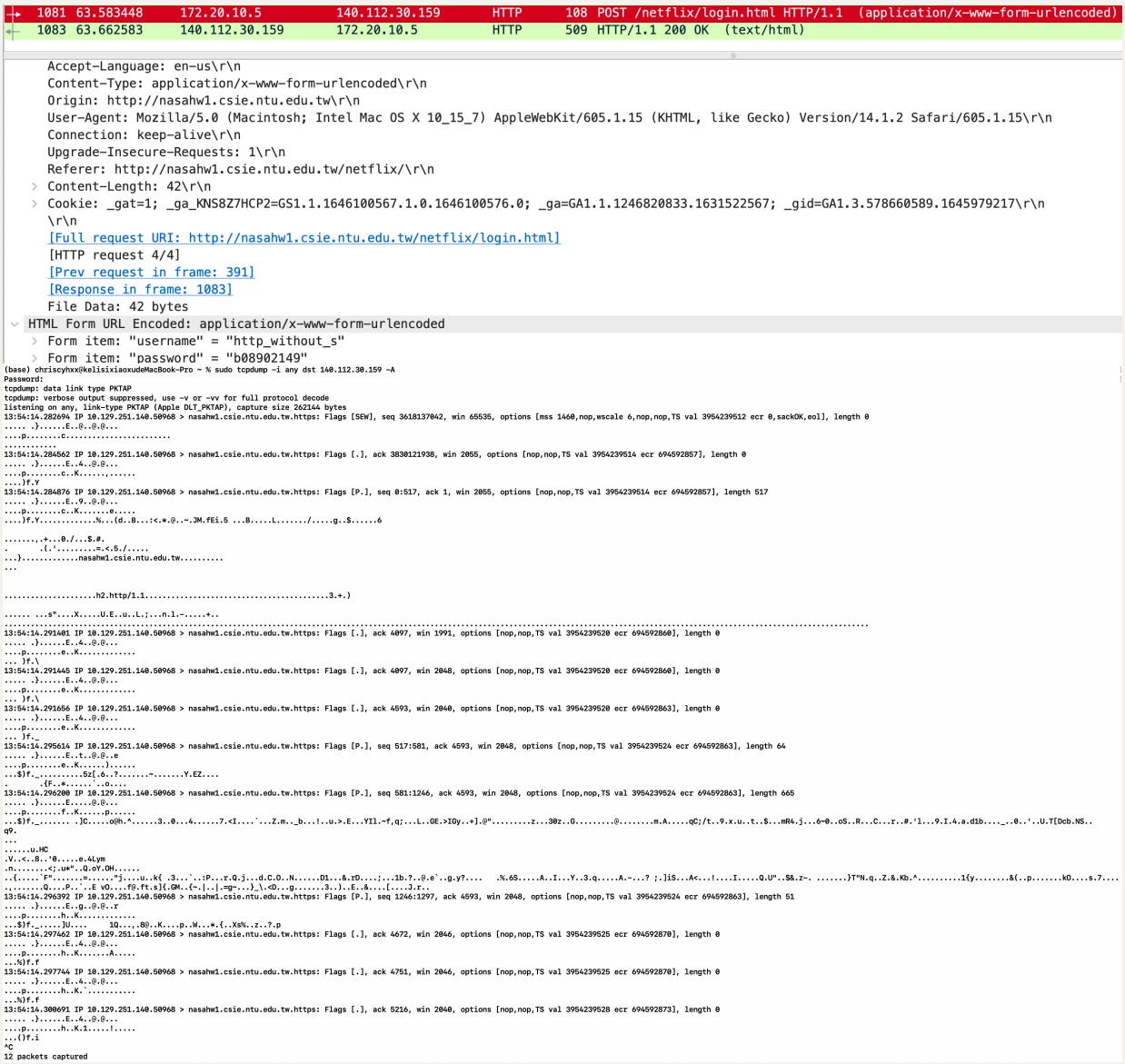
NASA 2022 Homework1

Network Administration

看個影集也會不小心洩漏密碼

1.


2.

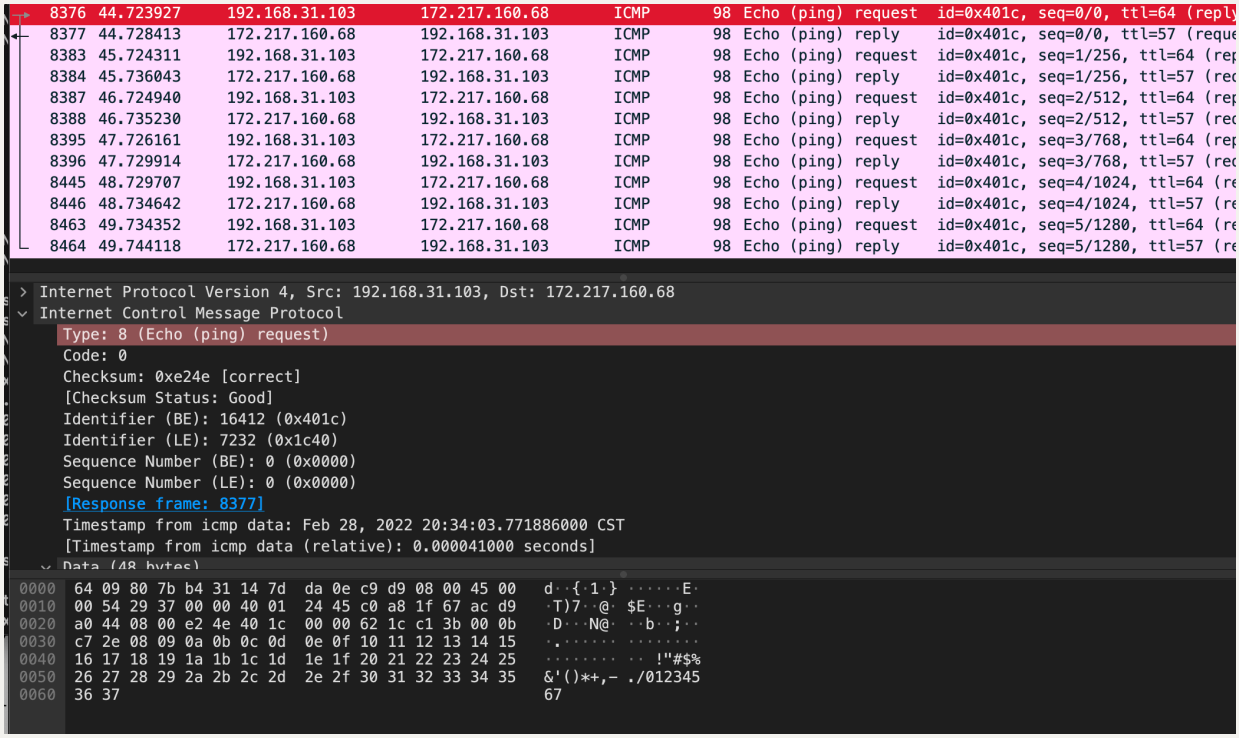
找不到含有帳號密碼的封包，因為HTTPS雖是透過HTTP進行通訊，但會先使用SSL/TLS加密之後才會傳輸。

農場危機

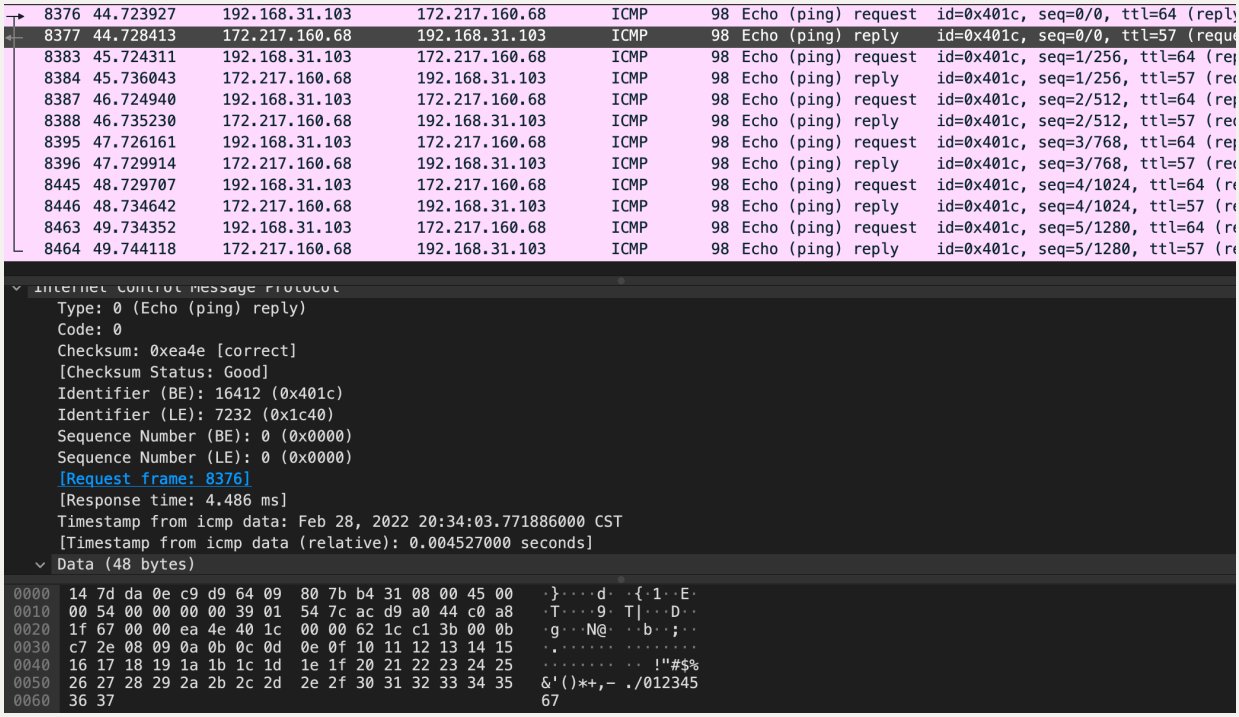
1. 我利用Wireshark將封包過濾，選擇只看HTTP，並將內容下載之後發現有一個QR code，其他都是佩佩豬。
2. 我另外有發現`pig`這個html檔，並且在封包內找到`http://nasahw1.csie.ntu.edu.tw/pig/encode.js`，我將其複製下來，改寫了一下`pig`的內容，使QR code可以透過呼叫`encode.js`內的`converImage()`這個function去修復；得到完整得QR code之後，掃描即得密碼為 **NASA{2022_pig_pig🐷🐽🐷}**。

這麼多網路協定

1. ICMP request:

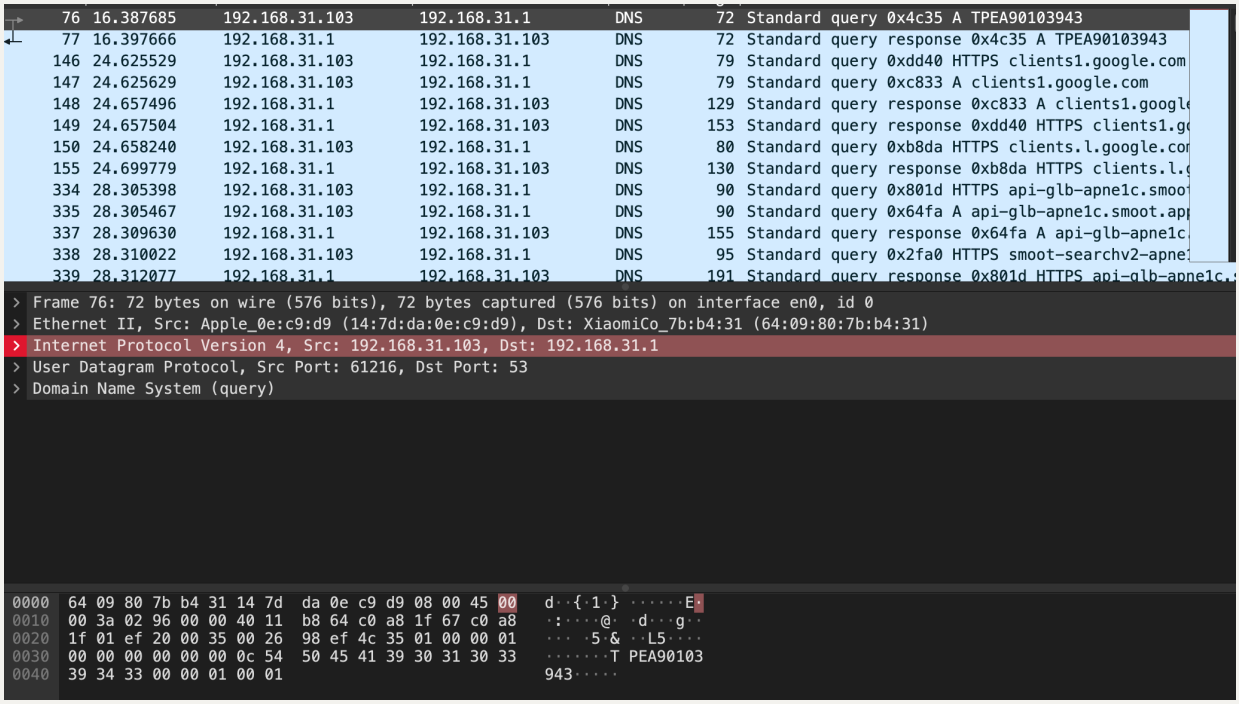


ICMP reply:

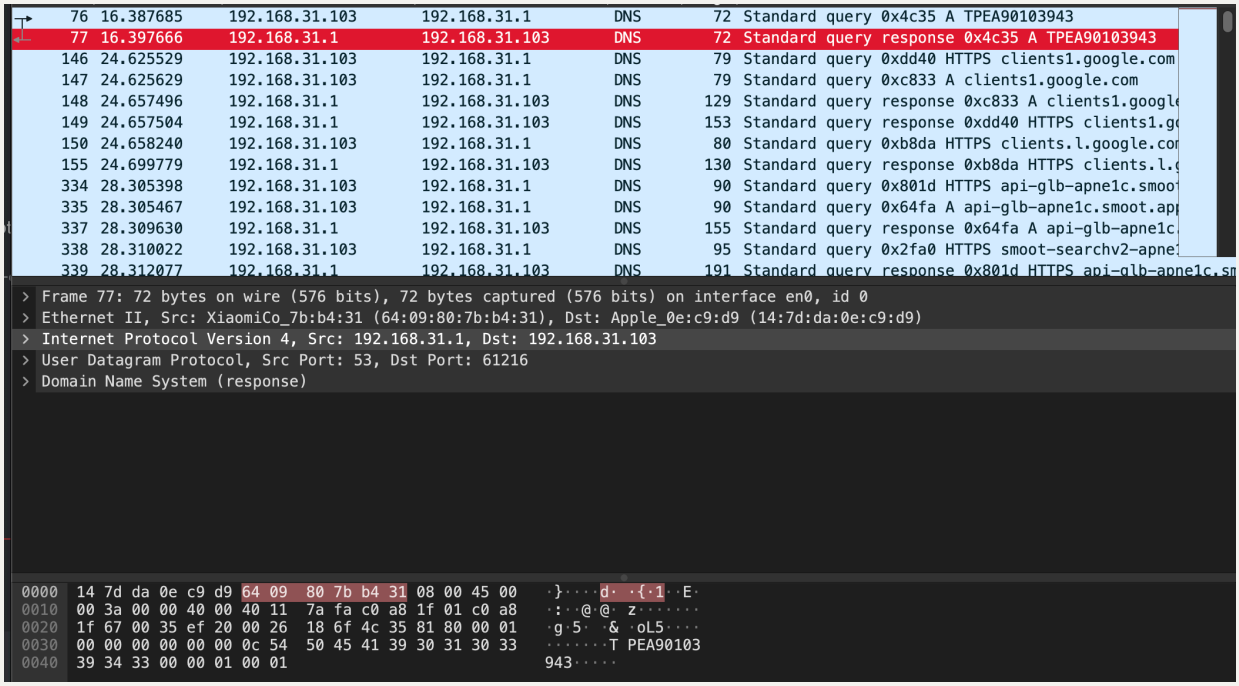


ICMP最主要的目的是用來解析網路封包或是分析路由，大多透過回傳回來的錯誤訊息進行分析，屬於Network layer。

2. DNS query:

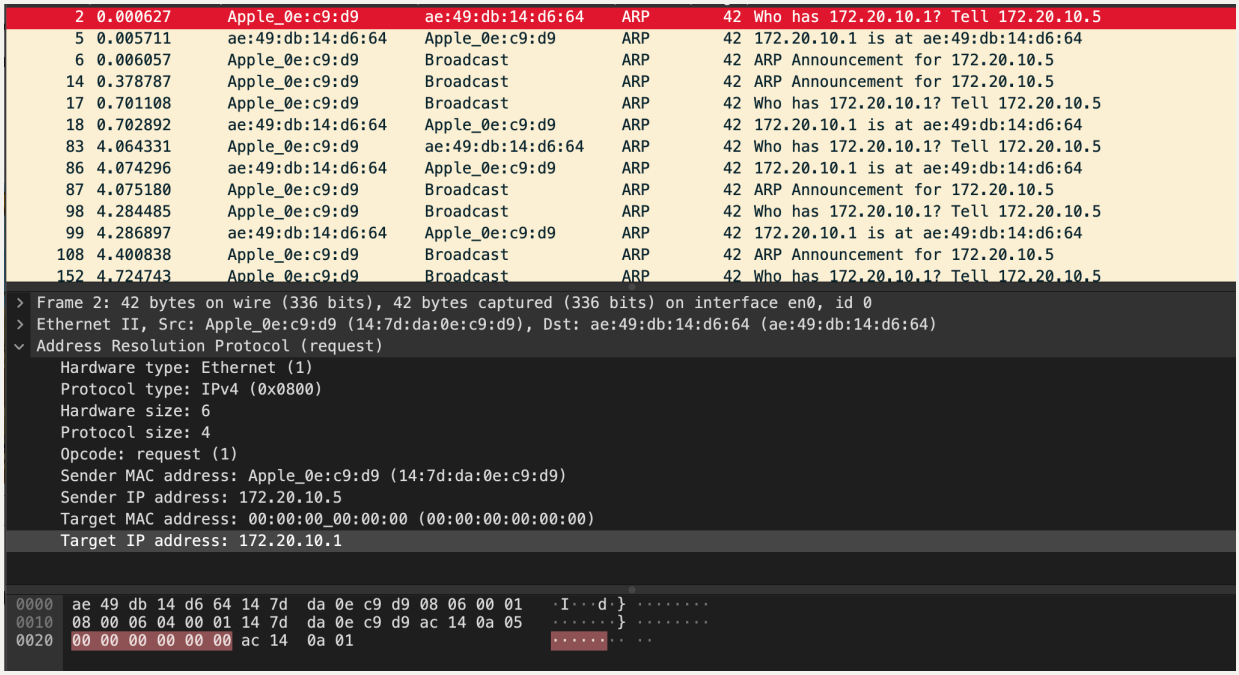


DNS response:

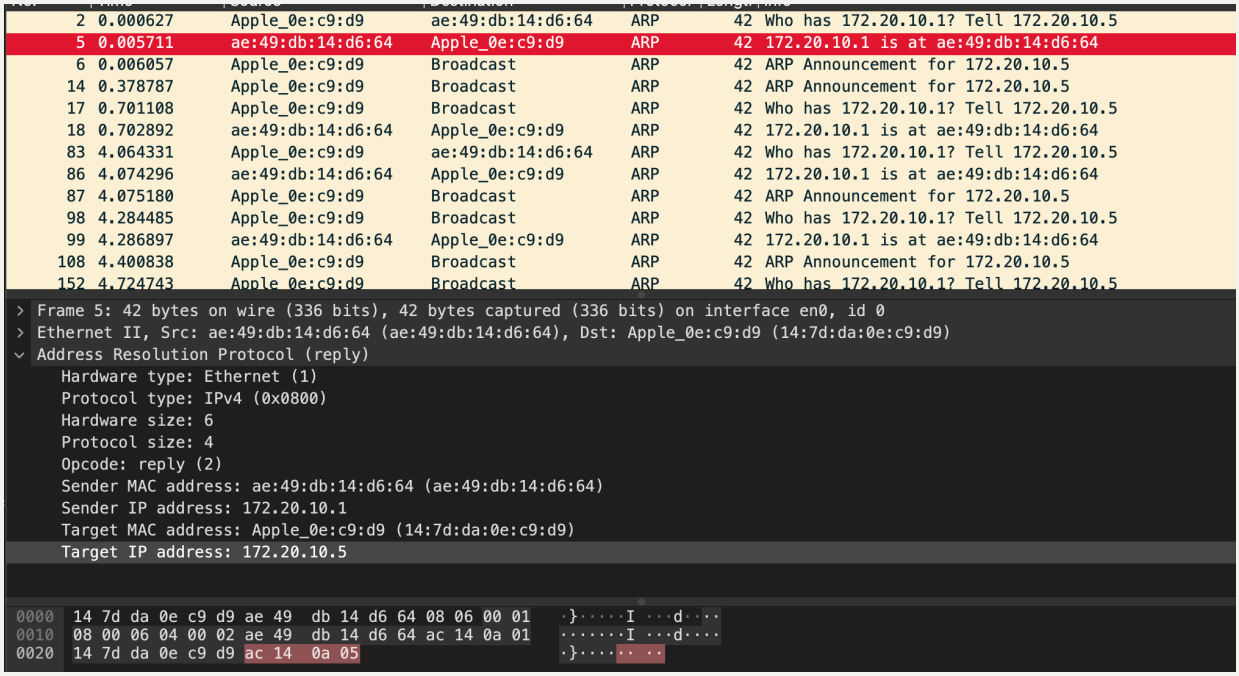


DNS分為client與server，client會向server發query去問一個dmain name的真正IP位址，而server必須response，詢問方法可分recursive與iterative。DNS是屬application layer。

3. ARP request:

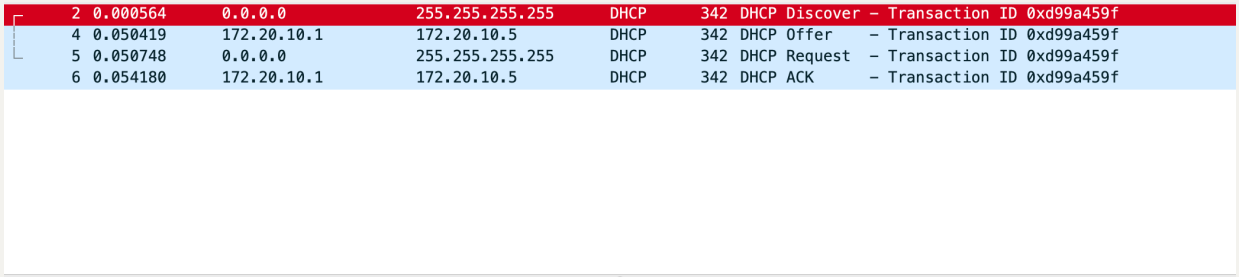


ARP reply:

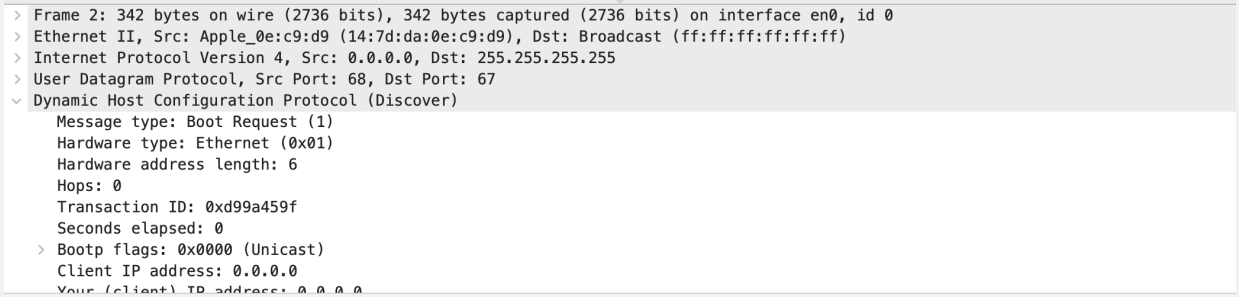


ARP是網址分析協定，以查詢的方式來獲得IP位址和實體位址的對應關係。其屬於Network layer與Link layer。當主機A有一個封包要給主機B，並且已獲得主機B的IP 位址，那主機A會先檢查自己的 ARP 表格中有沒有該 IP 位址相對應的實體位址。如果有的話就將此IP所對應之MAC address填入layer 2的表頭；沒有的話就向網路發出ARP request的廣播封包，查詢主機B的實體位址。

4. DHCP discover:

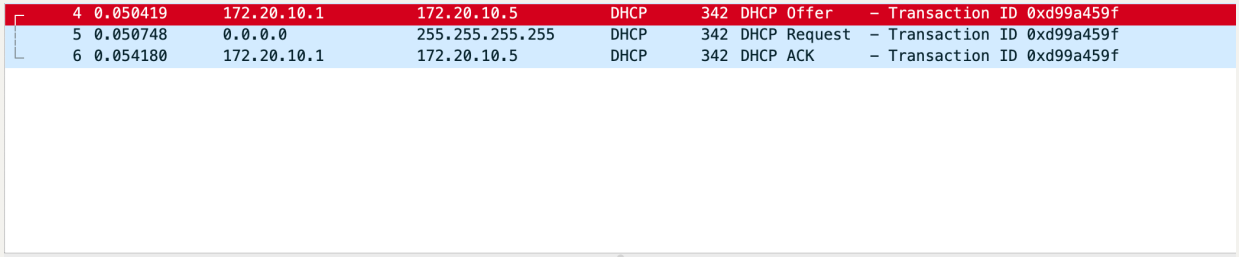


```
    2 0.000564      0.0.0.0           255.255.255.255     DHCP     342 DHCP Discover - Transaction ID 0xd99a459f
    4 0.050419      172.20.10.1       172.20.10.5         DHCP     342 DHCP Offer    - Transaction ID 0xd99a459f
    5 0.050748      0.0.0.0           255.255.255.255     DHCP     342 DHCP Request  - Transaction ID 0xd99a459f
    6 0.054180      172.20.10.1       172.20.10.5         DHCP     342 DHCP ACK      - Transaction ID 0xd99a459f
```

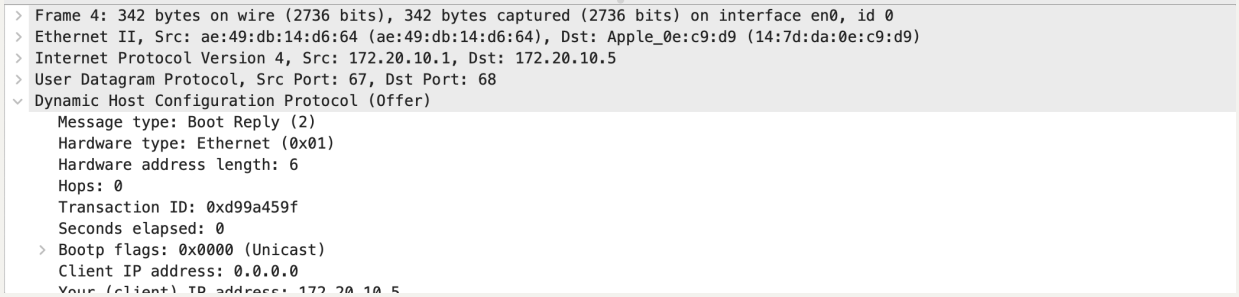


```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: Apple_0e:c9:d9 (14:7d:da:0e:c9:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd99a459f
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
```

DHCP offer:



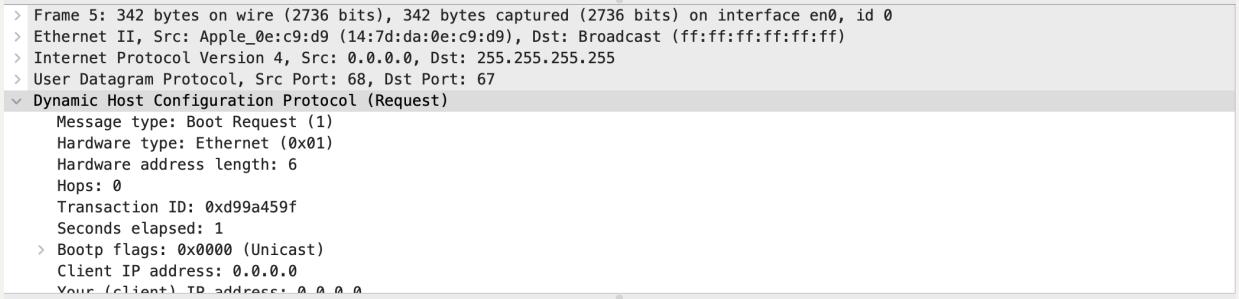
```
    4 0.050419      172.20.10.1       172.20.10.5         DHCP     342 DHCP Offer    - Transaction ID 0xd99a459f
    5 0.050748      0.0.0.0           255.255.255.255     DHCP     342 DHCP Request  - Transaction ID 0xd99a459f
    6 0.054180      172.20.10.1       172.20.10.5         DHCP     342 DHCP ACK      - Transaction ID 0xd99a459f
```



```
> Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: ae:49:db:14:d6:64 (ae:49:db:14:d6:64), Dst: Apple_0e:c9:d9 (14:7d:da:0e:c9:d9)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.5
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd99a459f
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 172.20.10.5
```

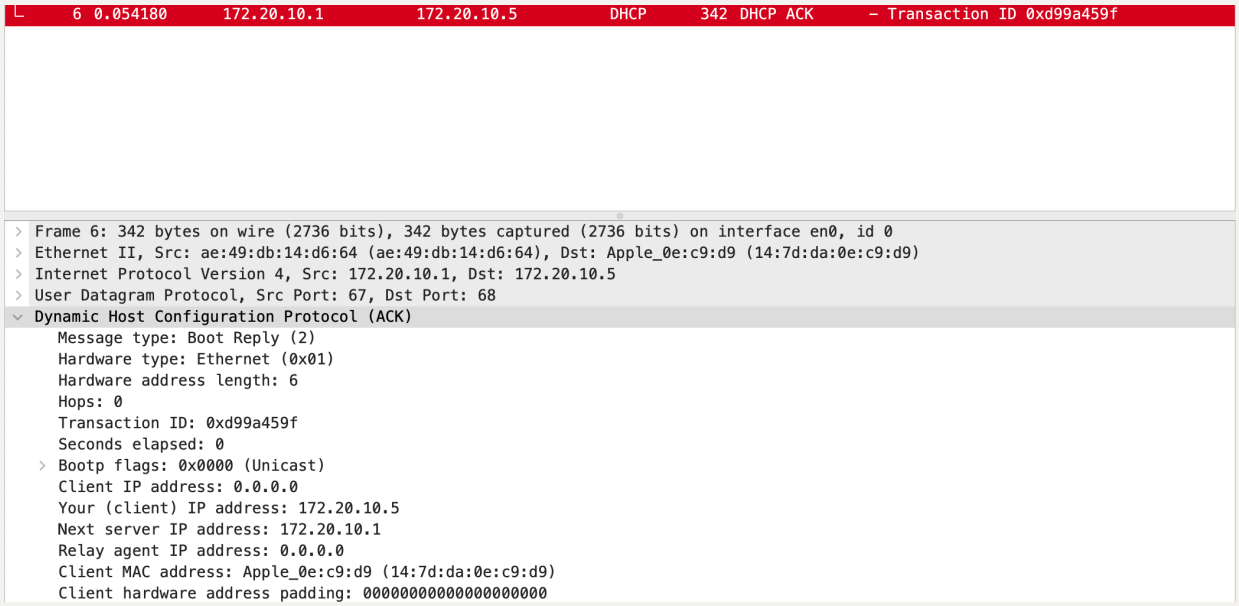
DHCP request:

```
    5 0.050748      0.0.0.0           255.255.255.255     DHCP     342 DHCP Request  - Transaction ID 0xd99a459f
    6 0.054180      172.20.10.1       172.20.10.5         DHCP     342 DHCP ACK      - Transaction ID 0xd99a459f
```



```
> Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: Apple_0e:c9:d9 (14:7d:da:0e:c9:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd99a459f
    Seconds elapsed: 1
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
```

DHCP ACK:



DHCP協定主要是為了節省子網路中IP位址的使用量，可以設定網路中的一台主機做為DHCP server，負責動態的分配IP位址，當網路中有任何電腦需要連線，才會向DHCP server要求一個IP位址，此時DHCP server會在資料庫中找一個未被使用的IP位址給該電腦使用，直到使用結束之後再將此IP位址歸還給DHCP server。DHCP是位於Application layer。

System Administration

Permission

I. Basic

1. **False**，要`ls`一個資料夾，必須對其有`r`的權限。
2. **True**，因為讀一個檔案的基本權限是user對該檔案所在目錄具有`x`權限，且對該檔案本身有`r`權限。
3. **True**，原因同上題，因為對`./dir1`具有`x`權限且對`./dir/dir3`有`r`權限所以可以。
4. **True**，只要對某個目錄具有`x`權限即可進入該目錄。
5. **False**，因為對`dir2`沒有`x`權限。
6. **False**，修改一個檔案至少需要對該檔案所在目錄擁有`x`且對該檔案本身具有`w`的權限。
7. **False**，因為對`fileB`沒有`w`的權限。
8. **True**，如上敘述，對`dir1`有`x`且對`fileC`有`w`的權限，因此可以。
9. **True**，在某目錄新增或刪除檔案，等於是在修改該目錄，因此要對該目錄具有`w`且對其所在目錄具有`x`權限。

10. **False**，對`dir4`沒有`w`所以沒辦法刪除其內部的檔案。

II. ACL

1. 透過`getfacl`可以看到flags為`--t`代表sticky bit有on，所以只有資料夾擁有者或super user或是擁有他們的權限的人可以刪除裡面的檔案。
2. 透過`setfacl -m g:ta:rx b08902149`以及`chmod 0700 b08902149`來將該資料夾改成只有自己與group ta可檢視，另外也要`setfacl -m m:rwx b08902149`防止mask將某些權限擋掉。
3. a. 我使用b09505014當好朋友
   b. 進到`b08902149`，先用`setfacl -m u:b09505014:x .`將b08902149這個資料夾改成讓好友可以進入。接著以`setfacl -m u:b09505014:rwx chatroom`、`setfacl -m g::-- chatroom/`以及`setfacl -m o::-- chatroom/`將`chatroom`設成只有我和好朋友可以新增、刪除檔案以及檢視。另外也要`setfacl -m m:rwx chatroom`才能防止mask將某些權限擋掉。
   c. 接續上一題，用`setfacl -m d:u:b09505014:rwx chatroom`將好友的設定繼承到`chatroom`以下的所有檔案，這樣就可以使之後新增的檔案都可以被雙方編輯。
   d. 透過`setfacl -m u::rx chatroom`將自己設成只可檢視，並透過`setfacl -m m:rx chatroom`來讓好朋友只留下`rx`權限。
4. a. 我透過`setfacl -m g:ta:x wordle`來讓ta可以進入`wordle`，然後用`chmod 0700 game.sh`以及`setfacl -m g:ta:rw game.sh`使得只有ta對`game.sh`有讀寫權限（`chmod`要在`setfacl`之前使用，如果在`setfacl`後才用`chmod`會變成在改ACL的mask）。
   b. 透過`chmod 0400 wordlist.txt`即可。
   c. 如果一個執行檔`setuid`有on，就是讓其他使用者在執行這個執行檔時，effective uid會轉成該執行檔的owner之權限，此時就可以用該owner的權限去執行指令。如果要讓shell script有setuid的效果，就要去對`bin/sh` setuid（假設該sehell script第一行是`#!/bin/sh`），那這樣可能會造成race condition，例如有其他使用者在你所執行的shell script還沒結束前也去使用`/bin/sh`來執行一些操作（且此時也剛好context switch到他），此時他就可以用你的權限去做一些很危險的操作，例如去修改一些只有你有權限的檔案。