Πρωτόκολλα και επικοινωνίες δικτύων
Εργαστήριο 2 Λύσεις

Τμήμα Πληροφορικής και τηλεπικοινωνιών
Πανεπιστήμιο Ιωαννίνων, Άρτα

2023-03-15

Περιεχόμενα

1 ΕΡΩΤΗΜΑ 1

1. Get-WmiObject -Class Cim_NetworkAdapter — Select-Object Name

```
PS C:\WINDOWS\system32> Get-WmiObject -Class Cim_NetworkAdapter | Select-Object Name

Name
----
Microsoft Kernel Debug Network Adapter
Intel(R) I211 Gigabit Network Connection
Hyper-V Virtual Switch Extension Adapter
WAN Miniport (SSTP)
WAN Miniport (IKEv2)
WAN Miniport (L2TP)
WAN Miniport (PPTP)
WAN Miniport (PPPOE)
WAN Miniport (IP)
WAN Miniport (IPv6)
WAN Miniport (Network Monitor)
```

2. Get-NetAdapter -Name *

```
PS C:\WINDOWS\system32> Get-NetAdapter -Name *

Name                      InterfaceDescription                ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                ------- ------       ----------             ---------
Ethernet 3                Intel(R) I211 Gigabit Network Connec...      11 Up         18-C0-4D-0C-84-44       100 Mbps
```

3. getmac

```
PS C:\WINDOWS\system32> getmac

Physical Address    Transport Name
=================== ============================================================
18-C0-4D-0C-84-44   \Device\Tcpip_{71567641-C7D7-458E-A020-12F809DCD98D}
PS C:\WINDOWS\system32>
```

4. Get-WmiObject -Class Win32_NetworkAdapter -Filter "NetConnectionID='Ethernet 3'" — Select-Object Name, Manufacturer

```
PS C:\WINDOWS\system32> Get-WmiObject -Class Win32_NetworkAdapter -Filter "NetConnectionID='Ethernet 3'" | Select-Objec
 Name, Manufacturer

Name                                  Manufacturer
----                                  ------------
Intel(R) I211 Gigabit Network Connection Intel Corporation
```

5. Get-NetAdapterBinding -Name "Ethernet 3" — Select-Object DisplayName, ComponentID

```
PS C:\WINDOWS\system32> Get-NetAdapterBinding -Name "Ethernet 3" | Select-Object DisplayName, ComponentID

DisplayName                                ComponentID
-----------                                -----------
Microsoft Network Adapter Multiplexor Protocol  ms_implat
Link-Layer Topology Discovery Mapper I/O Driver ms_lltdio
Internet Protocol Version 6 (TCP/IPv6)     ms_tcpip6
Internet Protocol Version 4 (TCP/IPv4)     ms_tcpip
Microsoft LLDP Protocol Driver             ms_lldp
Hyper-V Extensible Virtual Switch          vms_pp
Npcap Packet Driver (NPCAP)                INSECURE_NPCAP
Link-Layer Topology Discovery Responder    ms_rspndr
VirtualBox NDIS6 Bridged Networking Driver oracle_VBoxNetLwf
File and Printer Sharing for Microsoft Networks ms_server
Client for Microsoft Networks              ms_msclient
Bridge Driver                              ms_l2bridge
QoS Packet Scheduler                       ms_pacer
```

6. Get-NetAdapter -Name "Ethernet 3" — Select-Object IQR

```
PS C:\WINDOWS\system32> Get-NetAdapterHardwareInfo -Name "Ethernet 3" | Select-Object IRQ

IRQ
---
```

7. Get-NetAdapter -Name "Ethernet 3" — Select-Object DriverFileName, DriverVersion

```
PS C:\WINDOWS\system32> Get-NetAdapter -Name "Ethernet 3" | Select-Object DriverFileName, DriverVersion

DriverFileName DriverVersion
-------------- -------------
e1i68x64.sys   12.19.1.32
```

8. Get-NetAdapter -Name "Ethernet 3" — Select-Object DeviceID, PNPDeviceID

```
PS C:\WINDOWS\system32> Get-NetAdapter -Name "Ethernet 3" | Select-Object DeviceID, PNPDeviceID

DeviceID                             PNPDeviceID
--------                             -----------
{71567641-C7D7-458E-A020-12F809DCD98D} PCI\VEN_8086&DEV_1539&SUBSYS_E0001458&REV_03\18C04DFFFF0C844400
```

Note change Ethernet 3 with your adapter Name

2 ΕΡΩΤΗΜΑ 2

1. arp -a

```
PS C:\WINDOWS\system32> arp -a

Interface: 195.130.74.155 --- 0xb
  Internet Address      Physical Address      Type
  192.168.111.100       00-21-b7-a3-af-1c     dynamic
  195.130.74.129        00-be-75-12-0b-90     dynamic
  195.130.74.153        08-2e-5f-07-74-d2     dynamic
  195.130.74.154        18-c0-4d-de-73-f1     dynamic
  195.130.74.159        ff-ff-ff-ff-ff-ff     static
  195.130.74.190        00-18-19-e9-63-40     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.28.112.1 --- 0x18
  Internet Address      Physical Address      Type
  172.28.127.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

2. ping 195.130.73.235

```
PS C:\WINDOWS\system32> ping 195.130.74.166

Pinging 195.130.74.166 with 32 bytes of data:
Reply from 195.130.74.166: bytes=32 time<1ms TTL=63
Reply from 195.130.74.166: bytes=32 time<1ms TTL=63
Reply from 195.130.74.166: bytes=32 time<1ms TTL=63
Reply from 195.130.74.166: bytes=32 time<1ms TTL=63

Ping statistics for 195.130.74.166:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. ipconfig

```
Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4d45:1efa:f317:369f%12
   IPv4 Address. . . . . . . . . . . : 195.130.74.155
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 195.130.74.190
```

4. Ναι υπάρχουν στο arp table.

```
Interface: 195.130.74.155 --- 0xc
  Internet Address      Physical Address      Type
  195.130.74.129        00-be-75-12-0b-90     dynamic
  195.130.74.154        18-c0-4d-de-73-f1     dynamic
  195.130.74.158        74-86-e2-30-37-85     dynamic
  195.130.74.159        ff-ff-ff-ff-ff-ff     static
  195.130.74.161        00-0c-29-f9-d4-6b     dynamic
  195.130.74.190        00-18-19-e9-63-40     dynamic
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.22            01-00-5e-00-01-16     static
  224.0.1.55            01-00-5e-00-01-37     static
  224.0.1.60            01-00-5e-00-01-3c     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.254.127.63        01-00-5e-7e-7f-3f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.23.144.1 --- 0x18
  Internet Address      Physical Address      Type
  172.23.159.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.22            01-00-5e-00-01-16     static
  224.0.1.55            01-00-5e-00-01-37     static
  224.0.1.60            01-00-5e-00-01-3c     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.254.127.63        01-00-5e-7e-7f-3f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

5. arp -d και ifconfig/ all

```
PS C:\WINDOWS\system32> arp -d
PS C:\WINDOWS\system32> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

6. Υπάρχει ο DNS και η εμφανίζονται στην παρακάτω εικόνα.

```
Interface: 195.130.74.155 --- 0xc
  Internet Address      Physical Address      Type
  195.130.74.190        00-18-19-e9-63-40     dynamic
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.23.144.1 --- 0x18
  Internet Address      Physical Address      Type
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static
```

3 ΕΡΩΤΗΜΑ 3

- Φιλτράρετε τα αποτελέσματα όπως παρουσιάζονται στην Εικόνα 1 και επιλέξτε το πρώτο αποτέλεσμα.

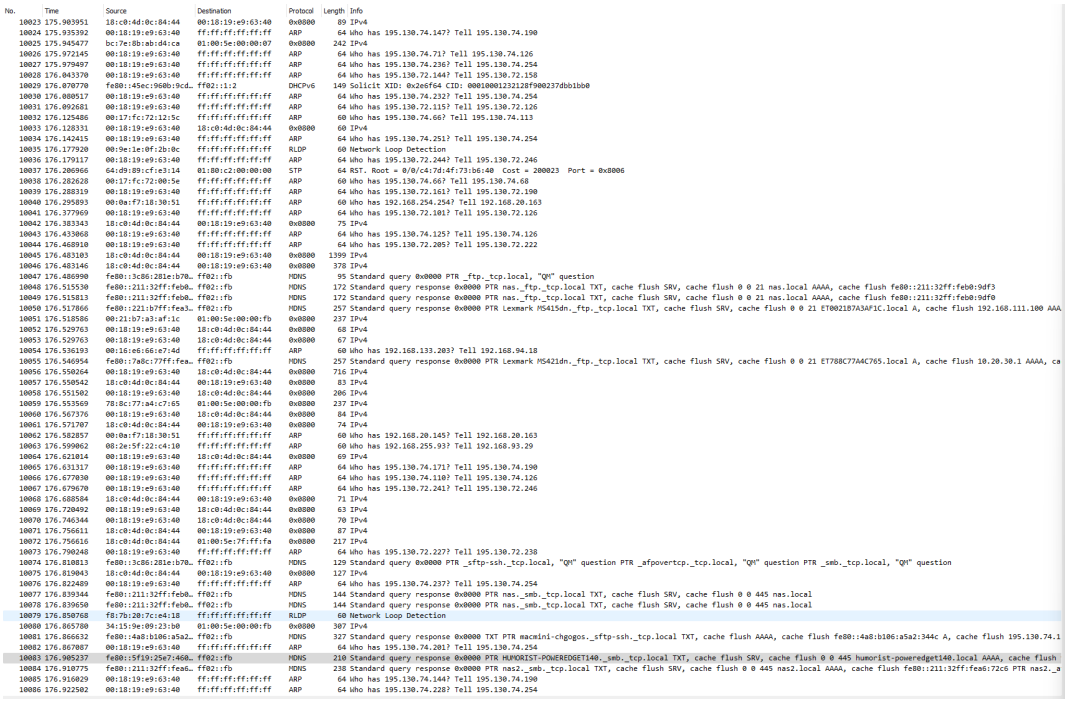

Figure 1: Filter String with Get

- Επιλέξτε την mac adress του source πεδίου όπως παρουσιάζεται στην Εικόνα 2.

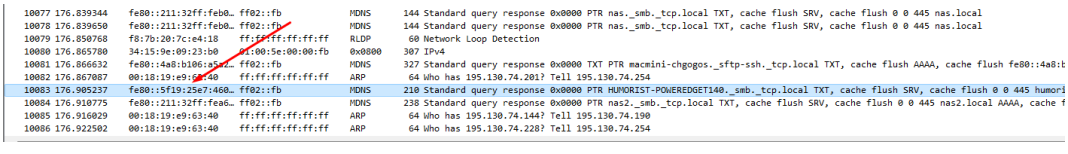

Figure 2: Find Mac Adress

- Στην συνέχεια ελέγχουμε την Mac Adress του Destination Source του πακέτου που επιλέξαμε:

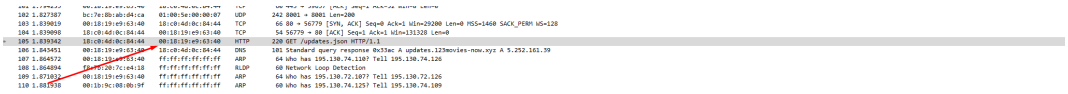

Figure 3: Παράδειγμα εκτέλεσης

Αρχικά η Mac του vm που χρησιμοποιήθηκε στο use case παρουσιάζεται στην εικόνα 4.

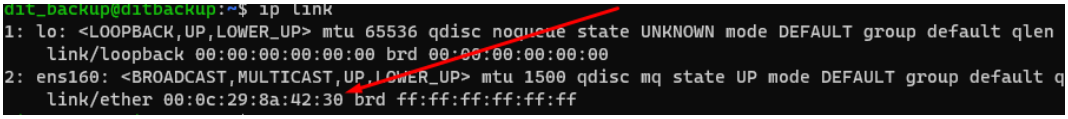

Figure 4: MAC dit backup

Παρατηρώ ότι η mac address του destination source είναι διαφορετική από την mac adress του VM. Η MAC adress αντιστοιχεί στην mac ρούτερ που αναλαμβάνει την δρομολόγηση. Εφόσον τα πακέτα έχουν καταγραφεί σε ένα δίκτυο με μεταγωγείς, μπορείτε να δείτε μόνο τη διεύθυνση MAC της θύρας του switch από το οποίο λαμβάνονται ή προς το οποίοπ αποστέλλονται τα πακέτα.

- Η δεκαεξαδική τιμή του πεδίου Type του πλαισίου Ethernet είναι ένα πεδίο 2 byte που υποδεικνύει τον τύπο του πρωτοκόλλου που χρησιμοποιείται στο ωφέλιμο φορτίο του πλαισίου. Η τιμή αυτού του πεδίου στο παραπάνω πλαίσιο και το πρωτόκολλο που υποδεικνύει εξαρτάται από το συγκεκριμένο πακέτο και παρουσιάζεται στην εικόνα 5 για το πακέτο που έχει επιλεγεί.

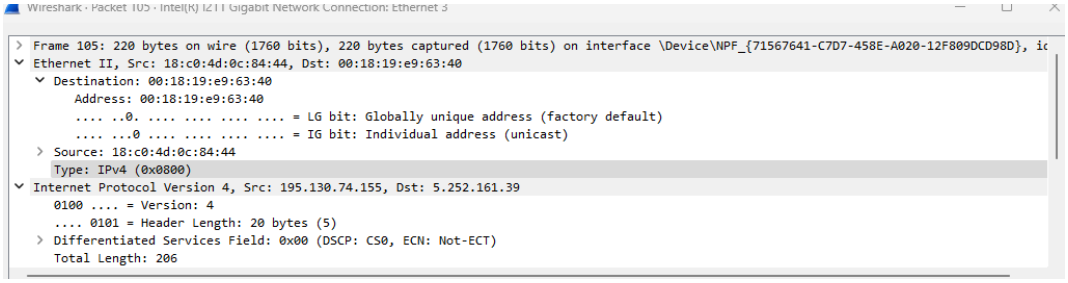

Figure 5: Πεδίο Type επιλεγμένου πακέτου

- Για να μπορέσω στο wireshark πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII "O" της λέξης OK πρέπει να ακολουθήσω τα ακόλουθα βήματα:

  1. Φιλτράρουμε το τα αποτελέσματα αναζήτησης επιλέγοντας **Edit** → **Find Packet** και έχοντας ως επιλεγμένη επιλογή φιλτραρίσματος το string εισάγουμε την λέξη OK όπως φαίνεται στην παρακάτω εικόνα.

Figure 6: Filters applied in search

  2. Επιλέγουμε το πρώτο πακέτο που περιέχει την λέξη OK.

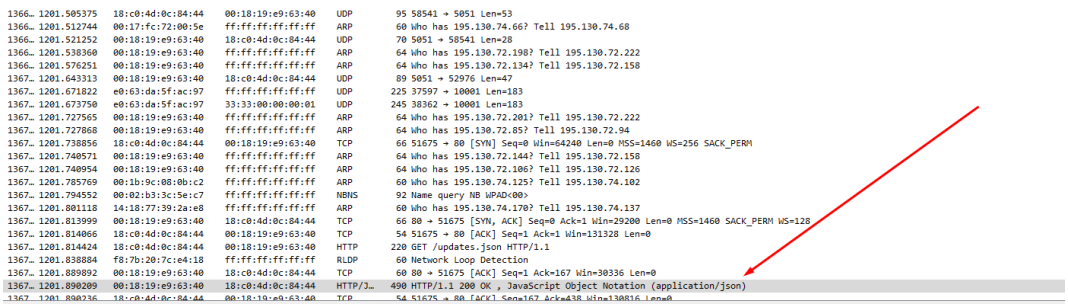

Figure 7: Πακέτο που περιέχει το raw text OK

3. Βρίσκουμε το byte offset που είναι το πρώτο byte του πλαισίου.

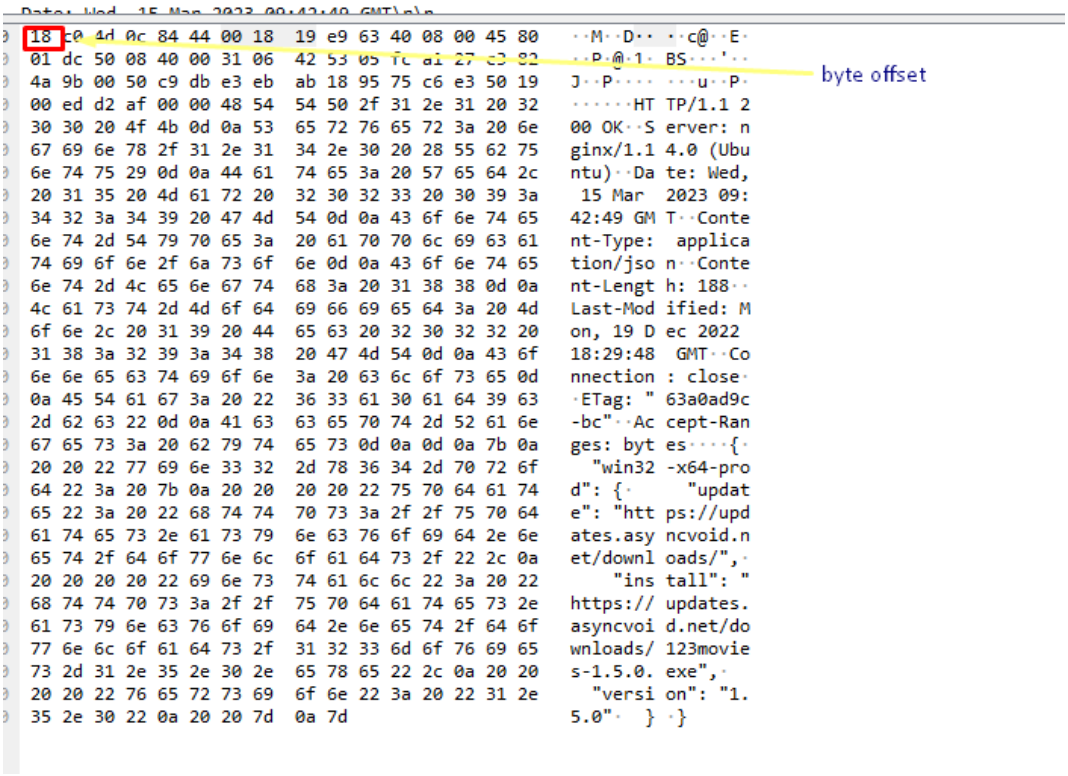

Figure 8: Byte offset

4. Στο παράδειγμα είναι η δεκαεξαδική τιμή 18 που αντιστοιχεί στην δεκαδική τιμή **24**. Τώρα η τελική τιμή θα προκύψει με βάση τον τύπο **Number of bytes = (Byte offset of "O" character) - (Byte offset of first byte) + 1**. Παρατηρώ ότι το O αντιστοιχεί στην δεκαεξαδική τιμή 4f στο παράδειγμα μου(Εικόνα). Άρα προκύπτει **Number of bytes=79-24+1=56**

- Το Μήκος του επιλεγμένου πλαισίου παρουσιάζεται στην εικόνα 9 και για να το υπολογίσεται κλικάρατε το επιλεγμένο πακέτο.

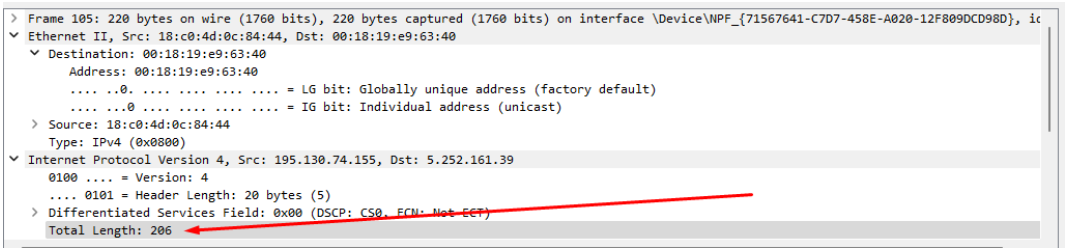

Figure 9: Μήκος επιλεγμένου πλαισίου

- Το Wireshark καταγράφει όλα τα πεδία του πλαισίου Ethernet, συμπεριλαμβανομένων των διευθύνσεων MAC πηγής και προορισμού, του πεδίου type, των δεδομένων ωφέλιμου φορτίου(type field) και του CRC.
- Το CRC συνήθως αφαιρείται από το πλαίσιο Ethernet και απορρίπτεται από τη συσκευή λήψης, οπότε συνήθως δεν καταγράφεται από το Wireshark.