

Πρωτόκολλα και επικοινωνίες δικτύων
Εργαστήριο 2 Λύσεις

Τμήμα Πληροφορικής και τηλεπικοινωνιών
Πανεπιστήμιο Ιωαννίνων, Άρτα

2023-03-15



Περιεχόμενα

1	ΕΡΩΤΗΜΑ 1	2
2	ΕΡΩΤΗΜΑ 2	3
3	ΕΡΩΤΗΜΑ 3	6

1 EPΩTHMA 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-Object 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 EPΩTHMA 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.

No.	Time	Source	Destination	Protocol	Length	Info
10021	175.983951	18:c0:4d:0c:84:44	00:18:19:e9:63:40	ARP	80	IPv4
10024	175.933392	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.147? Tell 195.130.74.190
10025	175.945477	bc:7e:8b:ab:d4:ca	01:00:5e:00:00:07	0x0000	242	IPv4
10026	175.972145	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.71? Tell 195.130.74.126
10027	175.979487	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.230? Tell 195.130.74.254
10028	175.943370	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.144? Tell 195.130.72.150
10029	176.070770	fe80:45ec:960b:9cd...	ff02::1:2	DMCPv6	140	Solicit XID: 0x2e6f6a CID: 00030001232128F90027D0b100
10030	176.000517	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.232? Tell 195.130.74.254
10031	176.092681	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.115? Tell 195.130.72.126
10032	176.125486	00:17:c7:72:12:5c	ff:ff:ff:ff:ff:ff	ARP	60	Who has 195.130.74.66? Tell 195.130.74.123
10033	176.125331	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	80	IPv4
10034	176.142415	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.251? Tell 195.130.74.254
10035	176.177920	00:9e:1e:0f:2b:0c	ff:ff:ff:ff:ff:ff	RDP	60	Network Loop Detection
10036	176.179117	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.244? Tell 195.130.72.246
10037	176.206966	64:d9:89:cfe3:14	01:00:c2:00:00:00	STP	64	RST. Root = 8/0(c4):7d:4f:73:b6:40 Cost = 200023 Port = 0x0006
10038	176.282020	00:17:c7:72:12:5c	ff:ff:ff:ff:ff:ff	ARP	60	Who has 195.130.74.66? Tell 195.130.74.68
10039	176.288319	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.141? Tell 195.130.72.190
10040	176.295893	00:0a:f7:18:13:01	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.254.254? Tell 192.168.20.163
10041	176.377909	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.181? Tell 195.130.72.126
10042	176.383343	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	75	IPv4
10043	176.433868	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.125? Tell 195.130.74.126
10044	176.463918	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.205? Tell 195.130.72.222
10045	176.463383	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	1399	IPv4
10046	176.483146	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	378	IPv4
10047	176.480998	fe80:13d8:202e:107b...	ff02::fb	NDNS	95	Standard query response 0x0000 PTR _ftp_tcp.local, "Q" question
10048	176.515550	fe80:211:32ff:fe0b...	ff02::fb	NDNS	172	Standard query response 0x0000 PTR nas_ftp_tcp.local TXT, cache flush SRV, cache flush 0 0 21 nas.local AAAA, cache flush fe80:211:32ff:fe0b:9d9f
10049	176.515813	fe80:211:32ff:fe0b...	ff02::fb	NDNS	257	Standard query response 0x0000 PTR nas_ftp_tcp.local TXT, cache flush SRV, cache flush 0 0 21 nas.local AAAA, cache flush fe80:211:32ff:fe0b:9d9f
10050	176.517866	fe80:211:32ff:fe0b...	ff02::fb	NDNS	257	Standard query response 0x0000 PTR Lenark H5415dh_ftp_tcp.local TXT, cache flush SRV, cache flush 0 0 21 E70802187A3471C.local A, cache flush 192.168.111.100 AAA
10051	176.518506	00:21:57:a1:af:1c	01:00:5e:00:00:fb	0x0000	237	IPv4
10052	176.529783	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	68	IPv4
10053	176.529783	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	67	IPv4
10054	176.536193	00:16:c6:6b:e7:4d	ff:ff:ff:ff:ff:ff	ARP	64	Who has 192.168.133.203? Tell 192.168.94.18
10055	176.540954	fe80:178c:77ff:fea...	ff02::fb	NDNS	257	Standard query response 0x0000 PTR Lenark H5422dh_ftp_tcp.local TXT, cache flush SRV, cache flush 0 0 21 E708C77AC6785.local A, cache flush 18.20.30.1 AAAA, ca
10056	176.550244	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	716	IPv4
10057	176.550542	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	83	IPv4
10058	176.551582	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	286	IPv4
10059	176.551600	70:8c:77:a1:c1:05	01:00:5e:00:00:fb	0x0000	237	IPv4
10060	176.567376	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	84	IPv4
10061	176.571787	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	74	IPv4
10062	176.582857	00:0a:f7:18:13:01	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.20.145? Tell 192.168.20.163
10063	176.599802	00:2e:5f:22:c4:10	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.255.93? Tell 192.168.93.29
10064	176.621814	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	69	IPv4
10065	176.621317	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.171? Tell 195.130.74.190
10066	176.677930	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.110? Tell 195.130.74.126
10067	176.679670	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.241? Tell 195.130.72.246
10068	176.685584	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	71	IPv4
10069	176.720492	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	63	IPv4
10070	176.746344	00:18:19:e9:63:40	18:c0:4d:0c:84:44	0x0000	70	IPv4
10071	176.756511	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	87	IPv4
10072	176.756516	18:c0:4d:0c:84:44	01:00:5e:7f:ff:fa	0x0000	217	IPv4
10073	176.790248	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.72.227? Tell 195.130.72.238
10074	176.810813	fe80:13d8:202e:107b...	ff02::fb	NDNS	129	Standard query 0x0000 PTR _ftp-ssh_tcp.local, "Q" question PTR _ftp-ssh_tcp.local, "Q" question
10075	176.819043	18:c0:4d:0c:84:44	00:18:19:e9:63:40	0x0000	127	IPv4
10076	176.822489	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.237? Tell 195.130.74.254
10077	176.839344	fe80:211:32ff:fe0b...	ff02::fb	NDNS	144	Standard query response 0x0000 PTR nas_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 nas.local
10078	176.839650	fe80:211:32ff:fe0b...	ff02::fb	NDNS	144	Standard query response 0x0000 PTR nas_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 nas.local
10079	176.850768	fa:7b:28:7c:e4:18	ff:ff:ff:ff:ff:ff	RDP	60	Network Loop Detection
10080	176.865780	34:15:9e:09:23:b0	01:00:5e:00:00:fb	0x0000	307	IPv4
10081	176.866632	fe80:4a8:b106:a5a2...	ff02::fb	NDNS	327	Standard query response 0x0000 TXT PTR macmini-chgogos_ftp-ssh_tcp.local TXT, cache flush AAAA, cache flush fe80:4a8:b106:a5a2:344c A, cache flush 195.130.74.1
10082	176.867087	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.201? Tell 195.130.74.254
10083	176.905237	fe80:1519:25c7:a60b...	ff02::fb	NDNS	210	Standard query response 0x0000 PTR HUMORIST-POWERDEGET140_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 humorist-powerdeget140.local AAAA, cache flush
10084	176.910775	fe80:211:32ff:fe0b...	ff02::fb	NDNS	238	Standard query response 0x0000 PTR nas2_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 nas2.local AAAA, cache flush fe80:211:32ff:fe0b:72c6 PTR nas2_a
10085	176.916029	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.144? Tell 195.130.74.190
10086	176.922502	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.228? Tell 195.130.74.254

Figure 1: Filter String with Get

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

10077	176.839344	fe80:211:32ff:fe0b...	ff02::fb	NDNS	144	Standard query response 0x0000 PTR nas_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 nas.local
10078	176.839650	fe80:211:32ff:fe0b...	ff02::fb	NDNS	144	Standard query response 0x0000 PTR nas_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 nas.local
10079	176.850768	fa:7b:20:7c:e4:18	ff:ff:ff:ff:ff:ff	RDP	60	Network Loop Detection
10080	176.865780	34:15:9e:09:23:b0	01:00:5e:00:00:fb	0x0000	307	IPv4
10081	176.866632	fe80:4a8:b106:a5a2...	ff02::fb	NDNS	327	Standard query response 0x0000 TXT PTR macmini-chgogos_ftp-ssh_tcp.local TXT, cache flush AAAA, cache flush fe80:4a8:b106:a5a2:344c A, cache flush 195.130.74.1
10082	176.867087	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.201? Tell 195.130.74.254
10083	176.905237	fe80:1519:25c7:a60b...	ff02::fb	NDNS	210	Standard query response 0x0000 PTR HUMORIST-POWERDEGET140_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 humorist-powerdeget140.local AAAA, cache flush
10084	176.910775	fe80:211:32ff:fe0b...	ff02::fb	NDNS	238	Standard query response 0x0000 PTR nas2_smb_tcp.local TXT, cache flush SRV, cache flush 0 0 445 nas2.local AAAA, cache flush fe80:211:32ff:fe0b:72c6 PTR nas2_a
10085	176.916029	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.144? Tell 195.130.74.190
10086	176.922502	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64	Who has 195.130.74.228? Tell 195.130.74.254

Figure 2: Find Mac Address

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

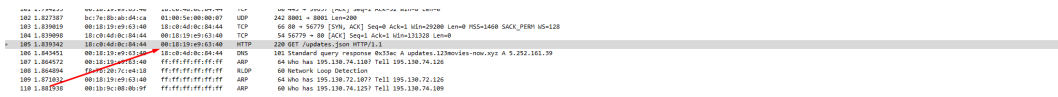


Figure 3: Παράδειγμα εκτέλεσης

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

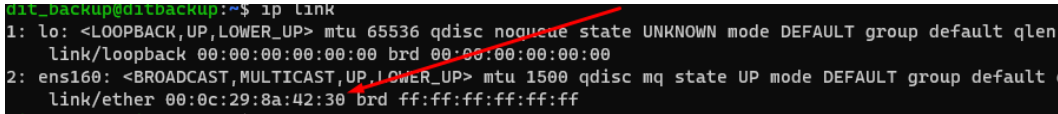


Figure 4: MAC dit backup

Παρατηρώ ότι η mac address του destination source είναι διαφορετική από την mac address του VM. Η MAC address 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 οποίο 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.

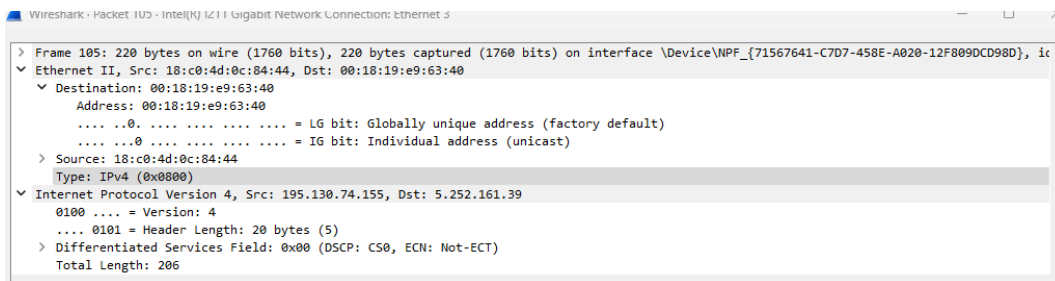


Figure 5: Πεδίο Type επιλεγμένου πακέτου

- 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.

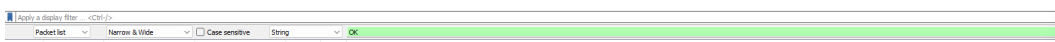


Figure 6: Filters applied in search

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

1366.	1201.505375	18:c0:4d:8c:84:44	00:18:19:e9:63:40	UDP	95 58541 → 5051 Len=53
1366.	1201.512744	00:17:fc:72:00:5e	ff:ff:ff:ff:ff:ff	ARP	60 Who has 195.130.74.66? Tell 195.130.74.68
1366.	1201.521252	00:18:19:e9:63:40	18:c0:4d:8c:84:44	UDP	70 5051 → 58541 Len=28
1366.	1201.538360	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64 Who has 195.130.72.198? Tell 195.130.72.222
1366.	1201.576251	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64 Who has 195.130.72.134? Tell 195.130.72.158
1367.	1201.643113	00:18:19:e9:63:40	18:c0:4d:8c:84:44	UDP	89 5051 → 52976 Len=47
1367.	1201.671822	e0:63:da:5f:ac:97	ff:ff:ff:ff:ff:ff	UDP	225 37597 → 10001 Len=103
1367.	1201.673750	e0:63:da:5f:ac:97	33:33:00:00:00:01	UDP	245 38362 → 10001 Len=103
1367.	1201.727565	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64 Who has 195.130.72.201? Tell 195.130.72.222
1367.	1201.727868	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64 Who has 195.130.72.85? Tell 195.130.72.94
1367.	1201.738856	18:c0:4d:8c:84:44	00:18:19:e9:63:40	TCP	66 51675 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1367.	1201.740571	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64 Who has 195.130.72.144? Tell 195.130.72.158
1367.	1201.740954	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	64 Who has 195.130.72.106? Tell 195.130.72.126
1367.	1201.785769	00:18:19:e9:63:40	ff:ff:ff:ff:ff:ff	ARP	60 Who has 195.130.74.125? Tell 195.130.74.102
1367.	1201.794552	00:02:b3:3c:5e:c7	ff:ff:ff:ff:ff:ff	NBNS	92 Name query NB UPAD<0>
1367.	1201.801110	14:10:77:39:2a:e0	ff:ff:ff:ff:ff:ff	ARP	60 Who has 195.130.74.178? Tell 195.130.74.137
1367.	1201.813999	00:18:19:e9:63:40	18:c0:4d:8c:84:44	TCP	66 80 → 51675 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
1367.	1201.814066	18:c0:4d:8c:84:44	00:18:19:e9:63:40	TCP	54 51675 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1367.	1201.814424	18:c0:4d:8c:84:44	00:18:19:e9:63:40	HTTP	220 GET /updates.json HTTP/1.1
1367.	1201.838884	f8:7b:20:7c:e4:18	ff:ff:ff:ff:ff:ff	RLDP	60 Network Loop Detection
1367.	1201.889892	00:18:19:e9:63:40	18:c0:4d:8c:84:44	TCP	60 80 → 51675 [ACK] Seq=1 Ack=167 Win=30336 Len=0
1367.	1201.898209	00:18:19:e9:63:40	18:c0:4d:8c:84:44	HTTP/1.1	490 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1367.	1201.898236	18:c0:4d:8c:84:44	00:18:19:e9:63:40	TCP	54 51675 → 80 [ACK] Seq=167 Ack=438 Win=130336 Len=0

Figure 7: Πακέτο που περιέχει το raw text OK

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

Date: Wed, 15 Mar 2023 09:42:40 GMT\r\n		
18	00 4d 0c 84 44 00 18 19 e9 63 40 08 00 45 80	..M..D..c@..E..
01	dc 50 08 40 00 31 06 42 53 05 7c a1 27 c3 82	..P.@.1.BS...'
4a	9b 00 50 0c d9 e3 eb ab 18 95 75 c6 e3 50 19	J..P....u..P..
00	ed d2 af 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1 2
30	30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 6e	00 OK..S erver: n
67	69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75	ginx/1.1 4.0 (Ubu
6e	74 75 29 0d 0a 44 61 74 65 3a 20 57 65 64 2c	ntu)..Da te: Wed,
20	31 35 20 4d 61 72 20 32 30 32 33 20 30 39 3a	15 Mar 2023 09:
34	32 3a 3a 39 20 47 4d 54 0d 0a 43 6f 6e 74 65	42:49 GM T..Conte
6e	74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61	nt-Type: applica
74	69 6f 6e 2f 6a 73 6f 6e 0d 0a 43 6f 6e 74 65	tion/jso n..Conte
6e	74 2d 4c 65 6e 67 74 68 3a 20 31 38 38 0d 0a	nt-Lengt h: 188..
4c	61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 4d	Last-Mod ified: M
6f	6e 2c 20 31 39 20 44 65 63 20 32 30 32 32 20	on, 19 D ec 2022
31	38 3a 32 39 3a 34 38 20 47 4d 54 0d 0a 43 6f	18:29:48 GMT..Co
6e	6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d	nnnection : close
0a	45 54 61 67 3a 20 22 36 33 61 30 61 64 39 63	ETag: " 63a0ad9c
2d	62 63 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e	-bc"..Ac cept-Ran
67	65 73 3a 20 62 79 74 65 73 0d 0a 0d 0a 7b 0a	ges: byt es...{.
20	20 22 77 69 6e 33 32 2d 78 36 34 2d 70 72 6f	"win32 -x64-pro
64	22 3a 20 7b 0a 20 20 20 22 75 70 64 61 74	d": {.. "updat
65	22 3a 20 22 68 74 74 70 73 3a 2f 2f 75 70 64	e": "htt ps://upd
61	74 65 73 2e 61 73 79 6e 63 76 6f 69 64 2e 6e	ates.asy ncvoid.n
65	74 2f 64 6f 77 6e 6c 6f 61 64 73 2f 22 2c 0a	et/downl oads/",.
20	20 20 20 22 69 6e 73 74 61 6c 6c 22 3a 20 22	"ins tall": "
68	74 74 70 73 3a 2f 2f 75 70 64 61 74 65 73 2e	https:// updates.
61	73 79 6e 63 76 6f 69 64 2e 6e 65 74 2f 64 6f	asynvoi d.net/do
77	6e 6c 6f 61 64 73 2f 31 32 33 6d 6f 76 69 65	wnloads/ 123movie
73	2d 31 2e 35 2e 30 2e 65 78 65 22 2c 0a 20 20	s-1.5.0. exe",.
20	20 22 76 65 72 73 69 6f 6e 22 3a 20 22 31 2e	"versi on": "1.
35	2e 30 22 0a 20 20 7d 0a 7d	5.0" } }

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 υπολογιστεί κλικάρετε το επιλεγμένο πακέτο.

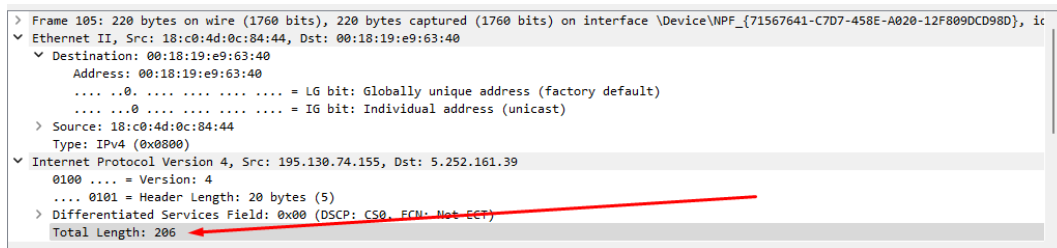


Figure 9: Μήκος επιλεγμένου πλαισίου

- 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.