# 1. Εισαγωγή – Σημαντικά πεδία στα πακέτα δεδομένων

Σημαντικό ρόλο στη διαδικασία της ενθυλάκωσης (encapsulation) παίζουν τα πεδία SAP (Service Access Point). Αυτά αποτελούν ετικέτες αναγνώρισης – στην ουσία είναι ένα πεδίο στην επικεφαλίδα (header) του πακέτου - μέσω των οποίων το κάθε επίπεδο αναγνωρίζει από ποιο πρωτόκολλο του επόμενου επιπέδου θα ζητήσει υπηρεσία. Με άλλα λόγια, σε ποιο πρωτόκολλο του επόμενου επιπέδου θα παραδώσει τα δεδομένα που αποτελούν το φορτίο (payload) του πακέτου που υφίσταται επεξεργασία αυτή τη στιγμή. Μπορούμε, επίσης, να θεωρήσουμε ότι αποτελούν μια εικονική τοποθεσία ή διεπαφή μέσω της οποίας γίνεται η επικοινωνία μεταξύ των επιπέδων. Τα πεδία αυτά ελέγχουν τη διαδικασία πολυπλεξίας ή αποπολύπλεξης των δεδομένων, καθώς αυτά προωθούνται από επίπεδο σε επίπεδο.

Εναλλακτικά, ο όρος μπορεί να ιδωθεί ότι σημαίνει το σημείο τερματισμού της επικοινωνίας μεταξύ ομόλογων επιπέδων. Μερικές φορές χρησιμοποιείται ο γενικός όρος TSAP (Transport Service Access Point), για να σημάνει το συγκεκριμένο σημείο τερματισμού της επικοινωνίας στο επίπεδο μεταφοράς. Το ανάλογο σημείο τερματισμού στο επίπεδο δικτύου ονομάζεται NSAP. Με αυτή την έννοια, οι IP διευθύνσεις αποτελούν παράδειγμα NSAPs [1], [2].

Κάθε πρωτόκολλο δίνει διαφορετικό όνομα στο πεδίο που χρησιμοποιεί, για να σημάνει το πρωτόκολλο του επόμενου επιπέδου προς το οποίο θα παραδώσει τα δεδομένα ενός πακέτου, αφού επεξεργαστεί την επικεφαλίδα του. Στο Ethernet τον ρόλο αυτό παίζει το πεδίο TYPE, στο IP το πεδίο PROTOCOL και στα TCP και UDP το πεδίο PORT NUMBER.

Οι συνηθέστερες τιμές του πεδίου TYPE στο Ethernet παρουσιάζονται στον παρακάτω πίνακα (Πίνακας 4.1). Η διαχείριση των τιμών αρχικά γίνονταν από την XEROX και σταδιακά μεταβιβάστηκε στην IEEE [3][4].

| Τιμή πεδίου | Συντομογραφία πρωτοκόλλου | Περιγραφή |
|---|---|---|
| 0x0800 | IPv4 | DOD Internet Protocol |
| 0x0806 | ARP | Address Resolution Protocol |
| 0x8137 | IPX | Internet Packet Exchange (Novell) |
| 0x86DD | IPv6 | Internet Protocol version 6 |

**Πίνακας 4.1** *Συνηθέστερες τιμές πεδίου TYPE στο Ethernet.*

Οι τιμές του πεδίου PROTOCOL στην επικεφαλίδα του IPv4 ελέγχονται από την IANA (Internet Assigned Numbers Authority) και δημοσιοποιούνται μετά από κάθε επικαιροποίηση [5]. Μερικές από τις συνηθέστερες τιμές του πεδίου παρουσιάζονται στον επόμενο πίνακα (Πίνακας 4.2).

| Δεκαδική τιμή | Συντομογραφία | Περιγραφή | Αναφορά |
|---|---|---|---|
| 1 | ICMP | Internet Control Message | RFC792 |
| 2 | IGMP | Internet Group Management | RFC1112 |
| 6 | TCP | Transmission Control | RFC793 |
| 8 | EGP | Exterior Gateway Protocol | RFC888 |
| 17 | UDP | User Datagram | RFC768 |
| 50 | ESP | Encap Security Payload | RFC4303 |
| 51 | AH | Authentication Header | RFC4302 |
| 58 | ICMPv6 | Internet Control Message Protocol v6 | RFC2460 |

**Πίνακας 4.2** *Συνηθέστερες τιμές του πεδίου PROTOCOL της επικεφαλίδας IPv4.*

Το πεδίο port στην επικεφαλίδα του TCP (και του UDP) περιέχει αριθμούς που δηλώνουν σε ποια (ή από ποια) εφαρμογή του 7ου επιπέδου πρέπει να αποστείλει το 4ο επίπεδο τα δεδομένα που παρέλαβε από το δίκτυο. Οι αριθμοί αυτοί έχουν μέγεθος 16Bit [6]. Οι πρώτοι 1.024 είναι δεσμευμένοι για χρήση από συγκεκριμένες υπηρεσίες και αναφέρονται συχνά ως *well known ports*. Αυτές έχουν οριστεί από οργανισμούς τυποποίησης. Οι εφαρμογές στην πλευρά του πελάτη χρησιμοποιούν τις εφήμερες θύρες (*Ephemeral Ports*) οριζόμενες με τυχαίο τρόπο για κάθε σύνδεση. Τα παραπάνω σύνολα θυρών δεν έχουν τομή και είναι αμοιβαίως αποκλειόμενα. Η περιοχή των εφήμερων θυρών χωρίζεται συνήθως σε δύο υποπεριοχές. Η πρώτη περιλαμβάνει τις θύρες 1024 – 49151. Αυτές, πολλές φορές, προσδιορίζουν λιγότερο χρησιμοποιούμενες TCP/IP εφαρμογές (δεν καθορίζονται από RFCs) στην πλευρά του εξυπηρετητή, π.χ. 27010:Half Life, 6890:BitTorrent, κ.λπ.

Υπεύθυνος για την απόδοση και διαχείριση των αριθμών της πρώτης και δεύτερης κατηγορίας είναι ο οργανισμός IANA [7]. Η δεύτερη περιοχή περιλαμβάνει τους αριθμούς θυρών 49152 – 65535. Αυτοί δεν αντιστοιχίζονται σταθερά σε κάποια εφαρμογή. Χρησιμοποιούνται, για να αναγνωρίσουν την εφαρμογή που λαμβάνει μέρος στην επικοινωνία από την πλευρά του πελάτη. Αποδίδονται τυχαία από τον πόρο - πελάτη και είναι προσωρινοί, δηλαδή ισχύουν μόνο για όσο διαρκεί η σύνδεση. Παρακάτω παρατίθενται μερικοί από τους σημαντικότερους αριθμούς θυρών. Πλήρη κατάλογο θα βρείτε στην [8].

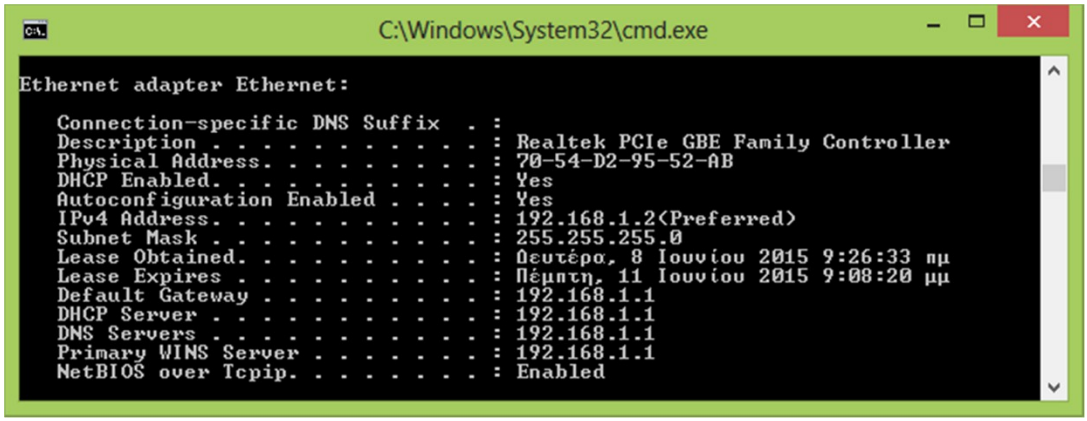
| **Αριθμός θύρας** | **Υπηρεσία** | **Περιγραφή** |
|---|---|---|
| 20 | FTP-data | File Transfer Protocol (data transfer) |
| 21 | FTP-ctrl | File Transfer Protocol (control) |
| 22 | SSH | Secure Shell |
| 23 | Telnet | Telecommunications Networking |
| 25 | SMTP | Simple Mail Transfer Protocol |
| 53 | DNS | Domain Name Server |
| 67 | BOOTPS | Bootstrap Protocol Server / DHCP |
| 68 | BOOTPC | Bootstrap Protocol Client / DHCP |
| 69 | TFTP | Trivial File Transfer Protocol |
| 80 | HTTP | Hypertext Transfer Protocol |
| 110 | POP3 | Post Office Protocol Version 3 |
| 123 | NTP | Network Time Protocol |
| 137 | NETBIOS | Name Service |
| 138 | NETBIOS | Datagram |
| 139 | NETBIOS | Session |
| 143 | IMAP | Interim Mail Access Protocol V2 |
| 161 | SNMP | Simple Network Management Protocol |
| 194 | IRC | Internet Relay Chat Protocol |
| 389 | LDAP | Lightweight Directory Access Protocol |
| 443 | HTTPS | Http Through SSL |
| 5059 | SIP-DS | Session Initiation Protocol Directory Services |
| 5060 | SIP | Session Initiation Protocol |

**Πίνακας 4.3** *Συνηθέστερες τιμές θυρών[8].*

# 2. Διαδικασία Εργαστηρίου – Μέρος Α΄

Στην παρούσα άσκηση θα πρέπει να αναγνωρίσετε, με τη χρήση του αναλυτή πρωτοκόλλων, την επικοινωνία διαφόρων υπολογιστών του εργαστηρίου και συγκεκριμένα: τις κλήσεις ARP, τις κλήσεις DNS, την αρχικοποίηση της TCP σύνδεσης, την επικοινωνία μεταφοράς ενός αρχείου μέσω πρωτοκόλλου FTP και την επικοινωνία δύο υπολογιστών κατά τη μεταφορά ιστοσελίδων (HTTP). Σε κάθε περίπτωση θα πρέπει να αναγνωρίσετε τις διευθύνσεις (τόσο τις IP όσο και τις φυσικές) των υπολογιστών που εμπλέκονται στην επικοινωνία.

Αν η άσκηση διεξάγεται στον χώρο ενός μεγάλου εργαστηρίου, είναι καλό να γνωρίζετε την IP διεύθυνση καθώς και τη φυσική (MAC) διεύθυνση του υπολογιστή σας. Έτσι θα μπορέσετε να εντοπίσετε ευκολότερα τη δική του κίνηση έναντι της κίνησης των υπολοίπων υπολογιστών. Ένας τρόπος για να δείτε τις διευθύνσεις του υπολογιστή σας, είναι μέσω της εντολής *ipconfig /all*. Μεταξύ άλλων, με τη χρήση της εντολής θα μάθετε κι άλλα σημαντικά στοιχεία για το δίκτυο στο οποίο ανήκετε και τις υπηρεσίες του. Στην Εικόνα 4.1 μπορείτε να δείτε εκτός από τις δύο αυτές διευθύνσεις, τις IP διευθύνσεις των εξυπηρετητών DNS και DHCP του τοπικού δικτύου καθώς και την IP διεύθυνση της *προεπιλεγμένης πύλης* (default gateway). Στο συγκεκριμένο παράδειγμα οι διευθύνσεις τυχαίνει να συμπίπτουν, καθώς ανήκουν στην ίδια συσκευή, που είναι το ADSL modem/router που συνδέει μια οικία με το υπόλοιπο δίκτυο. Σε άλλου τύπου δίκτυο (π.χ. οργανισμού, ιδρύματος, κ.α.) οι διευθύνσεις αυτές ενδέχεται (και είναι πιθανότερο) να είναι διαφορετικές.




**Εικόνα 4.1** *Το αποτέλεσμα εκτέλεσης της εντολής ipconfig /all στον υπολογιστή του σπιτιού του συγγραφέα.*

Έστω, λοιπόν, ότι θέλετε να δείτε την ιστοσελίδα του Νεάπολις (www.nup.ac.cy). Ανοίγετε έναν πλοηγό, πληκτρολογείτε το URL, πατάτε Enter και εντός δευτερολέπτων βλέπετε στην οθόνη σας την ιστοσελίδα που ζητήσατε. Για να μπορέσει, όμως, ο πλοηγός να σας δείξει την ιστοσελίδα, προηγήθηκε η επικοινωνία του υπολογιστή σας με διάφορες συσκευές και υπηρεσίες του δικτύου με στόχο τη συλλογή πληροφοριών που χρησιμοποιήθηκαν στην τελική επικοινωνία. Αυτές οι επικοινωνίες γίνονται «διάφανα» προς τον χρήστη αλλά καταγράφονται από το λογισμικό ανάλυσης πρωτοκόλλων που «αφουγκράζεται» την κίνηση στο δίκτυο.

## 2.1 Βήμα 1. Συλλογή δεδομένων

1. Στο υπολογιστή σας φορτώστε τον αναλυτή πρωτοκόλλων Wireshark και επιλέξτε την κάρτα δικτύου που είναι συνδεδεμένη στο δίκτυο που βρίσκεστε.
2. Ανοίξτε έναν πλοηγό και ετοιμαστείτε να του ζητήσετε να συνδεθεί με ένα site, π.χ. το www.nup.ac.cy. Μην εκτελέσετε την εντολή.
3. Ξεκινήστε τη διαδικασία καταγραφής του Wireshark και αμέσως μετά πατήστε το enter στον πλοηγό. Σε λίγο η σελίδα που ζητήσατε θα εμφανιστεί στην οθόνη σας.
4. Όταν τελειώσει η παραπάνω διαδικασία, περιμένετε λίγα λεπτά (2΄-3΄) και μετά κλείστε τον πλοηγό. Μετά από άλλα 2΄ σταματήστε την καταγραφή από τον αναλυτή πρωτοκόλλων. Η αναμονή γίνεται, για να δώσουμε τον χρόνο στις εφαρμογές να ανταλλάξουν όλα τα πιθανά πακέτα που αφορούν στην επικοινωνία.
   Βέβαια με τον τρόπο αυτό μαζεύετε πολύ περισσότερη κίνηση, αλλά θα φιλτράρετε αυτή που αφορά στο μηχάνημά σας σε επόμενο βήμα.
5. Αν εκτελέσατε σωστά τα παραπάνω βήματα (2-4), θα πρέπει να έχετε καταγράψει όλα τα πακέτα που εμπλέκονται στη σύνδεση με τον απομακρυσμένο υπολογιστή.
6. Αναζητήστε τα πακέτα αυτά στα παράθυρα του αναλυτή. Αυτός θα έχει καταγράψει και τα πακέτα των συναδέλφων σας (εφόσον είστε συνδεδεμένοι σε hub). Πώς θα ξεχωρίσετε την επικοινωνία του δικού σας υπολογιστή;
7. Ελέγξτε τις δυνατότητες του Wireshark στο φιλτράρισμα συγκεκριμένων πακέτων. Δείτε το αρχείο βοήθειας του προγράμματος.

## 2.2 Βήμα 2. Αναγνώριση συγκεκριμένων πακέτων και υπηρεσιών

### 2.2.1 ARP – Address Resolution Protocol

Η πρώτη ενέργεια που χρειάζεται να κάνει ο υπολογιστής σας είναι να εντοπίσει τη φυσική διεύθυνση της *προεπιλεγμένης πύλης*, γιατί όλη η επικοινωνία του με τον έξω κόσμο θα γίνει μέσω αυτής και καθώς βρίσκεται σε ένα δίκτυο Ethernet θα πρέπει να σχηματίσει *πλαίσια* (frames) που θα απευθύνονται προς αυτήν.

Ο υπολογιστής σας γνωρίζει ήδη (βλ. Εικόνα 4.1) την IP διεύθυνση της *προεπιλεγμένης πύλης* (default gateway). Αυτή είναι μια γνώση που απέκτησε με τη ρύθμιση των παραμέτρων της κάρτας δικτύου και είναι μια πληροφορία την οποία είτε τη θέσατε χειροκίνητα, αφού συμβουλευτήκατε τον διαχειριστή του δικτύου

σας είτε ο υπολογιστής σας την έλαβε δυναμικά μέσω του πρωτοκόλλου DHCP (Dynamic Host Configuration Protocol) [9].

Μια δικτυακή συσκευή Α, που είναι συνδεδεμένη σε ένα τμήμα Ethernet (Ethernet segment) και γνωρίζει ήδη την IP διεύθυνση μιας άλλης συσκευής, έστω Β, στο ίδιο τμήμα του δικτύου, μπορεί να ανακαλύψει τη φυσική διεύθυνση της δεύτερης συσκευής με χρήση του πρωτοκόλλου ARP (Address Resolution Protocol) [10]. Σύμφωνα με το πρωτόκολλο, η συσκευή Α ελέγχει την προσωρινή ARP μνήμη της (ARP cache), για να δει αν έχει ήδη τη διεύθυνση. Αν δεν την έχει, στέλνει ένα πλαίσιο ευρυεκπομπής (broadcast) το οποίο απευθύνεται σε όλους (στη διεύθυνση FF:FF:FF:FF:FF:FF) και ζητά από τη συσκευή με την IP διεύθυνση της Β να απαντήσει. Αν η Β βρίσκεται στο ίδιο Ethernet segment και ακούει, απαντά με ένα πλαίσιο Ethernet που έχει διεύθυνση προορισμού τη φυσική (MAC) διεύθυνση του Α και διεύθυνση αποστολέα τη φυσική (MAC) διεύθυνση του Β. Το σύστημα πρέπει να κρατήσει την πληροφορία αυτή στον ARP πίνακά του, ώστε να τη χρησιμοποιεί απευθείας στο μέλλον. Η καταχωρισμένη πληροφορία διαγράφεται μετά από κάποιο χρονικό διάστημα.

### 2.2.2 Ανάλυση ονόματος περιοχής (DNS)

Το επόμενο βήμα, προτού εμφανιστεί η ιστοσελίδα που ζητήσατε, είναι να βρει ο υπολογιστής σας την IP διεύθυνση του εξυπηρετητή ο οποίος φιλοξενεί το site που θέλετε να επισκεφτείτε. Στον φυλλομετρητή γράψατε το URL (Uniform Resource Locator) του στόχου σας - για την ακρίβεια γράψατε το όνομα της περιοχής, ήτοι www.teicm.gr, και ο φυλομετρητής συμπλήρωσε αυτόματα και το πρωτόκολλο της εφαρμογής που θα αναλάβει να σας παρουσιάσει το περιεχόμενο της ιστοσελίδας, ήτοι http://www.teicm.gr. Όμως, οι μηχανές στο Διαδίκτυο βρίσκουν η μία την άλλη με χρήση των IP διευθύνσεών τους. Έτσι, ο υπολογιστής σας πρέπει τώρα να ζητήσει τη βοήθεια μιας άλλης υπηρεσίας, η οποία αναλαμβάνει να μεταφράσει τα ονόματα των μηχανών (τα οποία θυμούνται εύκολα οι άνθρωποι) σε ακολουθίες από 32bit που αποτελούν τις IP διευθύνσεις τους (τις οποίες χρειάζονται οι μηχανές). Η υπηρεσία αυτή είναι το Σύστημα Ονομάτων Περιοχών (Domain Name System – DNS) [11], [12], [13]. Η μορφή των πακέτων θα πρέπει να μοιάζει με αυτά που παρουσιάζονται στις Εικόνες 4.4 και 4.5

**Ερώτηση 1**: Βρείτε τα πακέτα που αφορούν στην ανάλυση του ονόματος περιοχής που αναζητήσατε. Μελετήστε τα πακέτα και δείτε την πληροφορία που παρέχουν. Συγκρίνετέ τα με τη μορφή της DNS επικεφαλίδας. Βρείτε τα εξής στοιχεία για κάθε πακέτο: (α) ποιος είναι ο αποστολέας, (β) ποιος είναι ο παραλήπτης, (γ) ποιο είναι το μέγεθος του πακέτου, (δ) ποια πρωτόκολλα εμπλέκονται στην επικοινωνία, (ε) ποιες θύρες εμπλέκονται στην επικοινωνία, (στ) πώς υποβάλλεται το ερώτημα, (ζ) πώς επιστρέφεται η απάντηση;

```
Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: 00:1f:29:17:cc:42 (00:1f:29:17:cc:42), Dst: Pegatron_95:52:ab (70:54:d2:95:52:ab)
    Destination: Pegatron_95:52:ab (70:54:d2:95:52:ab)
        Address: Pegatron_95:52:ab (70:54:d2:95:52:ab)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 00:1f:29:17:cc:42 (00:1f:29:17:cc:42)
        Address: 00:1f:29:17:cc:42 (00:1f:29:17:cc:42)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:1f:29:17:cc:42 (00:1f:29:17:cc:42)
    Sender IP address: 192.168.1.1 (192.168.1.1)
    Target MAC address: Pegatron_95:52:ab (70:54:d2:95:52:ab)
    Target IP address: 192.168.1.2 (192.168.1.2)

0000  70 54 d2 95 52 ab 00 1f 29 17 cc 42 08 06 00 01   pT..R...)..B....
0010  08 00 06 04 00 02 00 1f 29 17 cc 42 c0 a8 01 42   ........)..B....
0020  70 54 d2 95 52 ab c0 a8 01 02 00 00 00 00 00 00   pT..R...........
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

**Εικόνα 4.3** *Η ενδεικτική πληροφορία μιας απάντησης ARP (reply).*

```
No.     Time           Source                Destination           Protocol Length Info
    206 28.124151000   192.168.1.2           192.168.1.1           DNS      72     Standard query 0x3d62  A www.teicm.gr

Frame 206: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)
User Datagram Protocol, Src Port: 55042 (55042), Dst Port: 53 (53)
Domain Name System (query)
    [Response In: 210]
    Transaction ID: 0x3d62
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.teicm.gr: type A, class IN
            Name: www.teicm.gr
            [Name Length: 12]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  00 3a 6f 0b 00 00 80 11 00 00 c0 a8 01 02 c0 a8   .:o.............
0020  01 01 d7 02 00 35 00 26 83 8b 3d 62 01 00 00 01   .....5.&..=b....
0030  00 00 00 00 00 00 03 77 77 77 05 74 65 69 63 6d   .......www.teicm
0040  02 67 72 00 00 01 00 01                           .gr.....
```

**Εικόνα 4.4** *Ενδεικτικό ερώτημα ανάλυσης ονόματος περιοχής (DNS query).*

### 2.2.3 Διαδικασία κλήσης και αποδοχής επικοινωνίας – Η χειραψία τριών σημείων

Τώρα που ο υπολογιστής μας ξέρει την IP διεύθυνση του web server, μπορεί να αποστείλει πακέτα απευθείας σε αυτόν. Το πρωτόκολλο HTTP (Hyper Text Transfer Protocol), το οποίο είναι υπεύθυνο για τη μεταφορά και παρουσίαση ιστοσελίδων, είναι ένα πρωτόκολλο επιπέδου εφαρμογής που λειτουργεί πάνω από το πρωτόκολλο TCP (που βρίσκεται στο επίπεδο μεταφοράς). Το πρωτόκολλο TCP είναι εκ κατασκευής *συνδεσμοστραφές* (connection-oriented). Αυτό σημαίνει ότι η αρχικοποίηση και ο τερματισμός της επικοινωνίας πρέπει να

δηλωθούν ρητά – όπως π.χ. συμβαίνει με τις κλήσεις τηλεφωνίας. Έτσι, το TCP πρέπει πρώτα να εξασφαλίσει ότι ο εξυπηρετητής λειτουργεί και αποδέχεται τη σύνδεση. Η διαδικασία αρχικοποίησης της σύνδεσης που το εξασφαλίζει αυτό, είναι γνωστή ως *χειραψία τριών σημείων* (three way handshake). Στη διάρκειά της ο πελάτης και ο εξυπηρετητής ανταλλάσσουν τρία πακέτα συγχρονισμού και επιβεβαίωσης, που θεωρούνται αρκετά για την επίτευξη της συμφωνίας [1], [2]. Τα πακέτα αυτά ονοματίζονται από τις *σημαίες* (flags) που είναι ενεργοποιημένες στην επικεφαλίδα του TCP. Ο πελάτης στέλνει ένα πακέτο SYN ζητώντας συγχρονισμό, ο εξυπηρετητής, εφόσον αποδέχεται, αποκρίνεται με ένα πακέτο SYN-ACK και η διαδικασία ολοκληρώνεται με ένα πακέτο επιβεβαίωσης ACK από την πλευρά του πελάτη ότι έλαβε το δεύτερο [6]. Μετά το τρίτο πακέτο ξεκινά αυτή καθαυτή η επικοινωνία και συνήθως το αμέσως επόμενο πακέτο είναι από τον πελάτη προς τον εξυπηρετητή και περιλαμβάνει το αίτημα που υποβάλλει.

**Ερώτηση 2**. Εντοπίστε τα τρία πακέτα που υλοποιούν τη χειραψία τριών σημείων μεταξύ του υπολογιστή σας και του εξυπηρετητή που φιλοξενεί την ιστοσελίδα που ζητήσατε. Καταγράψτε τα πακέτα και μελετήστε τη δομή τους. Πώς καταλαβαίνετε ότι το τρίτο πακέτο επιβεβαίωσης αποτελεί επιβεβαίωση λήψης του δεύτερου και δεν αφορά σε άλλη επικοινωνία; Βρείτε τα εξής στοιχεία για κάθε πακέτο: (α) ποιος είναι ο αποστολέας, (β) ποιος είναι ο παραλήπτης, (γ) ποιο είναι το μέγεθος του πακέτου, (δ) ποια πρωτόκολλα εμπλέκονται στην επικοινωνία, (ε) ποιες θύρες εμπλέκονται στην επικοινωνία;

```
No.     Time           Source                Destination           Protocol Length Info
    210 28.139006000   192.168.1.1           192.168.1.2           DNS      88     Standard query response 0x3d62  A 195.130.67.5

Frame 210: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
Ethernet II, Src: Zte_91:42:a8 (cc:1a:fa:91:42:a8), Dst: Pegatron_95:52:ab (70:54:d2:95:52:ab)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 55042 (55042)
Domain Name System (response)
    [Request In: 206]
    [Time: 0.014855000 seconds]
    Transaction ID: 0x3d62
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.teicm.gr: type A, class IN
            Name: www.teicm.gr
            [Name Length: 12]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers

0000  70 54 d2 95 52 ab cc 1a fa 91 42 a8 08 00 45 00   pT..R.....B...E.
0010  00 4a 00 00 40 00 40 11 b7 4f c0 a8 01 01 c0 a8   .J..@.@..O......
0020  01 02 00 35 d7 02 00 36 57 4e 3d 62 81 80 00 01   ...5...6WN=b....
0030  00 01 00 00 00 00 03 77 77 77 05 74 65 69 63 6d   .......www.teicm
0040  02 67 72 00 00 01 00 01 c0 0c 00 01 00 01 00 00   .gr.............
0050  0a 86 00 04 c3 82 43 05                           ......C.
```

**Εικόνα 4.5** *Ενδεικτική απάντηση ανάλυσης ονόματος περιοχής από τον τοπικό name server (DNS response).*

Τα τρία πακέτα της χειραψίας τριών σημείων θα πρέπει να μοιάζουν με εκείνα που ενδεικτικά παρουσιάζονται στις Εικόνες 4.6, 4.7 και 4.8.

### 2.2.4 Μεταφορά δεδομένων (με χρήση του πρωτοκόλλου HTTP)

Εφόσον, λοιπόν, οι δύο μηχανές αποδέχθηκαν την έναρξη της μεταξύ τους επικοινωνίας, μπαίνουμε στη φάση ανταλλαγής δεδομένων. Εδώ, η μηχανή *πελάτης* (client) θα ζητήσει – χρησιμοποιώντας τις διαδικασίες που προβλέπονται από το *πρωτόκολλο εφαρμογής* – τα δεδομένα που θέλει ο χρήστης της μηχανής και η μηχανή *εξυπηρετητής* (server) θα τα αποστείλει. Στην περίπτωσή μας το πρωτόκολλο εφαρμογής είναι το HTTP, οπότε περιμένουμε να δούμε την αίτηση για αποστολή των αρχείων μιας ιστοσελίδας και την αποστολή τους από τον εξυπηρετητή.

Η μέθοδος με την οποία ο πελάτης αιτείται έναν πόρο από τον εξυπηρετητή, είναι η GET και ο εξυπηρετητής αποκρίνεται ανάλογα με το τι καλείται να παραδώσει. Στην αρχή της απάντησής του αναφέρει, συνήθως, κάποιον *κωδικό κατάστασης* (Status-Code) που είναι το κωδικοποιημένο αποτέλεσμα της

προσπάθειάς του να κατανοήσει και να ικανοποιήσει το αίτημα του πελάτη. Η κωδικοποίηση γίνεται με ένα σύστημα τριών αριθμών. Επίσης, συνοδεύεται κι από μια *φράση επεξήγησης* (Reason-Frame). Ο τριψήφιος κωδικός απευθύνεται στη μηχανή, ενώ η φράση επεξήγησης στον άνθρωπο που πιθανόν κάθεται πίσω από τη μηχανή. Το πρώτο ψηφίο της κατάστασης ορίζει την κλάση της απάντησης. Υπάρχουν πέντε κλάσεις που φαίνονται στον Πίνακα 4.4 [15].

```
No.     Time           Source                Destination           Protocol Length
      3 2.002736000    192.168.1.2           195.130.67.5          TCP      66

                                Info 33962→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 195.130.67.5 (195.130.67.5)
Transmission Control Protocol, Src Port: 33962 (33962), Dst Port: 80 (80), Seq: 0, Len: 0

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  00 34 29 1d 40 00 80 06 00 00 c0 a8 01 02 c3 82   .4).@...........
0020  43 05 84 aa 00 50 bc 24 45 0e 00 00 00 00 80 02   C....P.$E.......
0030  20 00 c8 58 00 00 02 04 05 b4 01 03 03 08 01 01    ..X............
0040  04 02                                             ..
```

**Εικόνα 4.6** *Το πακέτο SYN από τον πελάτη προς τον εξυπηρετητή.*

```
No.     Time           Source                Destination           Protocol Length
      4 2.026114000    195.130.67.5          192.168.1.2           TCP      66
                        Info
                        80→33962 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1

Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Zte_91:42:a8 (cc:1a:fa:91:42:a8), Dst: Pegatron_95:52:ab (70:54:d2:95:52:ab)
Internet Protocol Version 4, Src: 195.130.67.5 (195.130.67.5), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 33962 (33962), Seq: 0, Ack: 1, Len: 0

0000  70 54 d2 95 52 ab cc 1a fa 91 42 a8 08 00 45 3c   pT..R.....B...E<
0010  00 34 48 9d 40 00 79 06 f0 b8 c3 82 43 05 c0 a8   .4H.@.y.....C...
0020  01 02 00 50 84 aa 23 32 fb 6a bc 24 45 0f 80 12   ...P..#2.j.$E...
0030  20 00 e2 52 00 00 02 04 05 64 01 03 03 08 01 01    ..R.....d......
0040  04 02                                             ..
```

**Εικόνα 4.7** *Το πακέτο SYN-ACK από τον εξυπηρετητή προς τον πελάτη.*

```
No.     Time           Source                Destination           Protocol Length
      5 2.026252000    192.168.1.2           195.130.67.5          TCP      54
                        Info
                        33962→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0

Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 195.130.67.5 (195.130.67.5)
Transmission Control Protocol, Src Port: 33962 (33962), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  00 28 29 1e 40 00 80 06 00 00 c0 a8 01 02 c3 82   .().@...........
```

**Εικόνα 4.8** *Το τελικό πακέτο ACK της χειραψίας από τον πελάτη προς τον εξυπηρετητή.*

Επομένως, το πρώτο πακέτο από τον πελάτη προς τον εξυπηρετητή θα είναι ένα πακέτο που θα περιέχει τη μέθοδο GET (Εικόνα 4.9). Η εικόνα 4.9 δεν παρουσιάζει ολόκληρη την πληροφορία του πακέτου για λόγους οικονομίας χώρου. Όπως φαίνεται, το πακέτο έχει μέγεθος 348 bytes. Είναι, όμως, προφανής η χρήση του πρωτοκόλλου HTTP, η χρήση της μεθόδου GET, οι θύρες που χρησιμοποιούν οι συσκευές, κ.α. Τα πακέτα που θα ακολουθήσουν θα είναι μια διαδοχή πακέτων που περιέχουν τα περιεχόμενα της ιστοσελίδας και πακέτων επιβεβαίωσης που ενημερώνουν για την ορθή λήψη της πληροφορίας. Ενδεικτική αλληλουχία φαίνεται στις Εικόνες 4.10 – 4.12.

| Κωδικός κατάστασης | Φράση επεξήγησης |
|---|---|
| 1xx | Ενημερωτικό – Η αίτηση παραλήφθηκε, συνεχίζω τη διαδικασία |
| 2xx | Επιτυχία – Η ενέργεια παραλήφθηκε, κατανοήθηκε και έγινε αποδεκτή με επιτυχία |
| 3xx | Ανακατεύθυνση – Απαιτούνται περαιτέρω ενέργειες για την ολοκλήρωση του αιτήματος |
| 4xx | Σφάλμα Πελάτη - Η αίτηση περιέχει κακή διατύπωση ή δεν μπορεί να εξυπηρετηθεί |
| 5xx | Σφάλμα Εξυπηρετητή - Ο εξυπηρετητής απέτυχε να ολοκληρώσει μια έγκυρη αίτηση |

**Πίνακας 4.4** *Οι πέντε κλάσεις κωδικών κατάστασης.*

**Ερώτηση 3**. Εντοπίστε και παρουσιάστε τα πρώτα πακέτα ανταλλαγής δεδομένων που συλλέξατε για τον δικό σας υπολογιστή. Μελετήστε τα πεδία του κάθε πακέτου. Πώς αναγνωρίζετε προς ποια κατεύθυνση κινείται το κάθε πακέτο; Πώς αναγνωρίζετε το πακέτο επιβεβαίωσης (acknowledgment) για κάθε πακέτο που βρίσκετε; Βρείτε τα εξής στοιχεία για κάθε πακέτο: (α) Ποιος είναι ο αποστολέας, (β) ποιος είναι ο παραλήπτης, (γ) ποιο είναι το μέγεθος του πακέτου, (δ) ποια πρωτόκολλα εμπλέκονται στην επικοινωνία, (ε) ποιες θύρες εμπλέκονται στην επικοινωνία, (στ) τι τύπου είναι κάθε πακέτο (ενεργοποιημένα flags).

**Ερώτηση 4.** Έχει κάθε πακέτο δεδομένων το δικό του πακέτο επιβεβαίωσης; Μπορείτε να εντοπίσετε κάποια διαφορετική περίπτωση; Πως μπορείτε να αποδείξετε ότι ένα πακέτο ACK επιβεβαιώνει περισσότερα από ένα πακέτα;

(*Βοήθεια: Το πακέτο της εικόνας 4.12 είναι ένα πακέτο ACK που επιβεβαιώνει δύο πακέτα μαζί. Αν παρατηρήσετε τον αριθμό του κάθε πακέτου, όπως τα λαμβάνει και τα αριθμεί το Wireshark (πεδίο No.), θα δείτε ότι το πακέτο της εικόνας 4.11 έχει τον αριθμό 8 και εκείνο της εικόνας 4.12 τον αριθμό 10. Ανάμεσά τους υπήρχε ένα πακέτο που δεν απεικονίζεται εδώ και για το οποίο σας δίνουμε την πληροφορία ότι μετέφερε ακόμη 1380 bytes δεδομένων από τον εξυπηρετητή προς τον πελάτη.*)

```
No.     Time           Source                Destination           Protocol Length Info
      6 2.027001000    192.168.1.2           195.130.67.5          HTTP     348    GET / HTTP/1.1

Frame 6: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 195.130.67.5 (195.130.67.5)
Transmission Control Protocol, Src Port: 33962 (33962), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 294
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Host: www.teicm.gr\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-GB,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  01 4e 29 1f 40 00 80 06 00 00 c0 a8 01 02 c3 82   .N).@...........
0020  43 05 84 aa 00 50 bc 24 45 0f 23 32 fb 6b 50 18   C....P.$E.#2.kP.
0030  01 02 c9 72 00 00 47 45 54 20 2f 20 48 54 54 50   ...r..GET / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e   /1.1..Host: www.
0050  74 65 69 63 6d 2e 67 72 0d 0a 55 73 65 72 2d 41   teicm.gr..User-A
0060  67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e   gent: Mozilla/5.
```

**Εικόνα 4.9** *Παράδειγμα πακέτου HTTP που χρησιμοποιεί τη μέθοδο GET, για να αιτηθεί τα δεδομένα μιας ιστοσελίδας.*

```
No.     Time           Source                Destination           Protocol Length Info
      7 2.254049000    195.130.67.5          192.168.1.2           TCP      60     80→33962 [ACK] Seq=1 Ack=295 Win=66048 Len=0

Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Zte_91:42:a8 (cc:1a:fa:91:42:a8), Dst: Pegatron_95:52:ab (70:54:d2:95:52:ab)
Internet Protocol Version 4, Src: 195.130.67.5 (195.130.67.5), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 33962 (33962), Seq: 1, Ack: 295, Len: 0

0000  70 54 d2 95 52 ab cc 1a fa 91 42 a8 08 00 45 3c   pT..R.....B...E<
0010  00 28 48 9f 40 00 79 06 f0 c2 c3 82 43 05 c0 a8   .(H.@.y.....C...
0020  01 02 00 50 84 aa 23 32 fb 6b bc 24 46 35 50 10   ...P..#2.k.$F5P.
0030  01 02 40 ae 00 00 00 00 00 00 00 00               ..@.........
```

**Εικόνα 4.10** *Το πακέτο επιβεβαίωσης για το προηγούμενο πακέτο GET.*

```
No.     Time           Source                Destination           Protocol Length Info
      8 3.260901000    195.130.67.5          192.168.1.2           TCP      1434   [TCP segment of a reassembled PDU]

Frame 8: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
Ethernet II, Src: Zte_91:42:a8 (cc:1a:fa:91:42:a8), Dst: Pegatron_95:52:ab (70:54:d2:95:52:ab)
Internet Protocol Version 4, Src: 195.130.67.5 (195.130.67.5), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 33962 (33962), Seq: 1, Ack: 295, Len: 1380

0000  70 54 d2 95 52 ab cc 1a fa 91 42 a8 08 00 45 3c   pT..R.....B...E<
0010  05 8c 48 bc 40 00 79 06 eb 41 c3 82 43 05 c0 a8   ..H.@.y..A..C...
0020  01 02 00 50 84 aa 23 32 fb 6b bc 24 46 35 50 10   ...P..#2.k.$F5P.
0030  01 02 6a b9 00 00 48 54 54 50 2f 31 2e 31 20 32   ..j...HTTP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 43 6f 6e   00 OK..Cache-Con
0050  74 72 6f 6c 3a 20 6e 6f 2d 73 74 6f 72 65 2c 20   trol: no-store,
0060  6e 6f 2d 63 61 63 68 65 2c 20 6d 75 73 74 2d 72   no-cache, must-r
```

**Εικόνα 4.11** *Το πρώτο TCP πακέτο (segment) με την απάντηση 200 OK και τα πρώτα δεδομένα.*

```
No.     Time           Source                Destination           Protocol Length Info
     10 3.262430000    192.168.1.2           195.130.67.5          TCP      54     33962→80 [ACK] Seq=295 Ack=2761 Win=66048 Len=0

Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 195.130.67.5 (195.130.67.5)
Transmission Control Protocol, Src Port: 33962 (33962), Dst Port: 80 (80), Seq: 295, Ack: 2761, Len: 0

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  00 28 29 20 40 00 80 06 00 00 c0 a8 01 02 c3 82   .() @...........
0020  43 05 84 aa 00 50 bc 24 46 35 23 33 06 33 50 10   C....P.$F5#3.3P.
0030  01 02 c8 4c 00 00                                 ...L..
```

**Εικόνα 4.12** *Ένα πακέτο επιβεβαίωσης.*

**Ερώτηση 5**. Επιλέξτε ένα από τα πακέτα της επικοινωνίας που βρήκατε και μετά επιλέξτε το εργαλείο Analyze ->Follow TCP Stream του Wireshark. Εδώ θα δείτε όλη την πληροφορία συγκεντρωμένη, με έμφαση στις επικεφαλίδες HTTP των πακέτων. Μελετήστε και καταγράψτε τις.

### 2.2.5 Ο τερματισμός της επικοινωνίας

Είδαμε ότι επειδή το TCP είναι ένα συνδεσμοστραφές (connection-oriented) πρωτόκολλο θα πρέπει η έναρξη της επικοινωνίας να δηλώνεται ρητά. Για τον ίδιο λόγο, ρητά πρέπει να δηλώνεται και ο τερματισμός της επικοινωνίας. Όταν, λοιπόν, ο πελάτης ολοκληρώσει τη δουλειά που ήθελε να κάνει και προτίθεται να κλείσει, πρέπει να ανακοινώσει ρητά προς τον συνομιλητή του το γεγονός αυτό. Η διαδικασία περιλαμβάνει την ανταλλαγή πακέτων με ενεργοποιημένη τη σημαία (flag) FIN. Για τις λεπτομέρειες της διαδικασίας– η οποία περιλαμβάνει και μερικά ενδιαφέροντα στοιχεία χρονισμού και συγχρονισμού απομακρυσμένων συστημάτων
– ο αναγνώστης παραπέμπεται στο σχετικό RFC [6] ή σε οποιοδήποτε βιβλίο τεχνολογίας δικτύων, όπως τα [1] και [2].

Η τυπική διαδικασία τερματισμού περιλαμβάνει την ανταλλαγή τεσσάρων πακέτων FIN από τον πελάτη – ACK από τον εξυπηρετητή – FIN από τον εξυπηρετητή – τελικό ACK από τον πελάτη. Στη διαδικασία υπάρχουν μερικές παραλλαγές, με κυριότερη την περίπτωση Half-Close, όπου οι δύο συσκευές δηλώνουν σχεδόν ταυτόχρονα η μια προς την άλλη τον τερματισμό της επικοινωνίας.

**Ερώτηση 6**. Εντοπίστε τα πακέτα τερματισμού κάποιας από τις ενεργές συνδέσεις του υπολογιστή σας, μελετήστε τη μορφή τους και περιγράψτε τη διαδικασία. Βρείτε τα εξής στοιχεία για κάθε πακέτο: (α) ποιος είναι ο αποστολέας, (β) ποιος είναι ο παραλήπτης, (γ) ποιο είναι το μέγεθος του πακέτου, (δ) ποια πρωτόκολλα εμπλέκονται στην επικοινωνία, (ε) ποιες θύρες εμπλέκονται στην επικοινωνία, (στ) τι τύπου είναι κάθε πακέτο (ποια είναι τα ενεργοποιημένα flags).

*(Βοήθεια: Το τελικό FIN και το τελικό ACK συμβαίνουν μετά από κάποιο χρονικό διάστημα. Πρέπει να αφήσετε το Wireshark να καταγράφει αρκετή ώρα μετά τη λήψη της ιστοσελίδας και το κλείσιμο του browser, ώστε να καταγραφούν όλα).*

Ενδεικτικά πακέτα τερματισμού μιας TCP σύνδεσης φαίνονται στις εικόνες 4.13 – 4.15.

```
No.     Time           Source                Destination           Protocol Length Info
   2996 121.030627000  192.168.1.2           78.46.39.16           TCP      54     33980→80 [FIN, ACK] Seq=352 Ack=2026 Win=66560 Len=0

Frame 2996: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 78.46.39.16 (78.46.39.16)
Transmission Control Protocol, Src Port: 33980 (33980), Dst Port: 80 (80), Seq: 352, Ack: 2026, Len: 0
    Source Port: 33980 (33980)
    Destination Port: 80 (80)
    [Stream index: 19]
    [TCP Segment Len: 0]
    Sequence number: 352    (relative sequence number)
    Acknowledgment number: 2026    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 0001 = Flags: 0x011 (FIN, ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0x3703 [validation disabled]
    Urgent pointer: 0

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  00 28 2f ff 40 00 80 06 00 00 c0 a8 01 02 4e 2e   .(/.@.........N.
0020  27 10 84 bc 00 50 d6 fa 51 3f 46 3a bf f8 50 11   '....P..Q?F:..P.
0030  01 04 37 03 00 00                                 ..7...
```

**Εικόνα 4.13** *Διαδικασία τερματισμού TCP σύνδεσης. Ο πελάτης στέλνει πακέτο FIN.*

```
No.     Time           Source                Destination           Protocol Length Info
   3005 121.176119000  78.46.39.16           192.168.1.2           TCP      60     80→33980 [FIN, ACK] Seq=2026 Ack=353 Win=66560 Len=0

Frame 3005: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Zte_91:42:a8 (cc:1a:fa:91:42:a8), Dst: Pegatron_95:52:ab (70:54:d2:95:52:ab)
Internet Protocol Version 4, Src: 78.46.39.16 (78.46.39.16), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 33980 (33980), Seq: 2026, Ack: 353, Len: 0
    Source Port: 80 (80)
    Destination Port: 33980 (33980)
    [Stream index: 19]
    [TCP Segment Len: 0]
    Sequence number: 2026    (relative sequence number)
    Acknowledgment number: 353    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 0001 = Flags: 0x011 (FIN, ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0xc46c [validation disabled]
    Urgent pointer: 0
    [SEQ/ACK analysis]

0000  70 54 d2 95 52 ab cc 1a fa 91 42 a8 08 00 45 38   pT..R.....B...E8
0010  00 28 11 df 40 00 73 06 be d0 4e 2e 27 10 c0 a8   .(..@.s...N.'...
0020  01 02 00 50 84 bc 46 3a bf f8 d6 fa 51 40 50 11   ...P..F:....Q@P.
0030  01 04 c4 6c 00 00 00 00 00 00 00 00               ...l........
```

**Εικόνα 4.14** *Ο εξυπηρετητής στέλνει πακέτο FIN και ταυτόχρονα επιβεβαιώνει με ACK το FIN που έλαβε.*

```
No.     Time           Source                Destination           Protocol Length Info
   3006 121.176248000  192.168.1.2           78.46.39.16           TCP      54     33980→80 [ACK] Seq=353 Ack=2027 Win=66560 Len=0

Frame 3006: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Pegatron_95:52:ab (70:54:d2:95:52:ab), Dst: Zte_91:42:a8 (cc:1a:fa:91:42:a8)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 78.46.39.16 (78.46.39.16)
Transmission Control Protocol, Src Port: 33980 (33980), Dst Port: 80 (80), Seq: 353, Ack: 2027, Len: 0
    Source Port: 33980 (33980)
    Destination Port: 80 (80)
    [Stream index: 19]
    [TCP Segment Len: 0]
    Sequence number: 353    (relative sequence number)
    Acknowledgment number: 2027    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 0000 = Flags: 0x010 (ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0x3703 [validation disabled]
    Urgent pointer: 0
    [SEQ/ACK analysis]

0000  cc 1a fa 91 42 a8 70 54 d2 95 52 ab 08 00 45 00   ....B.pT..R...E.
0010  00 28 30 05 40 00 80 06 00 00 c0 a8 01 02 4e 2e   .(0.@.........N.
0020  27 10 84 bc 00 50 d6 fa 51 40 46 3a bf f9 50 10   '....P..Q@F:..P.
0030  01 04 37 03 00 00                                 ..7...
```

**Εικόνα 4.15** *Ο πελάτης επιβεβαιώνει με ACK το πακέτο FIN του εξυπηρετητή*