


Εργαστηριακή Άσκηση 1

Δικτύωση στα Microsoft Windows

Wireshark: Αναλυτής Πρωτοκόλλων

Σκοπός της πρώτης σειράς ασκήσεων είναι, κατ' αρχήν, η εξοικείωση με τις βασικές δικτυακές δυνατότητες της οικογένειας λειτουργικών συστημάτων Microsoft Windows. Στις συγκεκριμένες ασκήσεις, το λειτουργικό σύστημα που θα χρησιμοποιηθεί είναι τα Windows XP. Επιπλέον, θα έχετε μια πρώτη επαφή με το Wireshark, ένα εργαλείο ανάλυσης πρωτοκόλλων σε γραφικό περιβάλλον.

Για την ανεύρεση των στοιχείων που ζητούνται στη συνέχεια, μπορείτε να χρησιμοποιήσετε είτε εντολές του λειτουργικού συστήματος ή πληροφορίες μέσω του γραφικού περιβάλλοντος. Πληροφορίες σχετικά με τη δικτύωση του υπολογιστή μπορούν να αντληθούν από το γραφικό περιβάλλον. Αν αφήσετε τον δρομέα ακίνητο για λίγο πάνω από το εικονίδιο  των δύο συνδεδεμένων υπολογιστών στο δεξί μέρος της μπάρας εργασίας (tray), εμφανίζεται ο τίτλος της τοπικής σύνδεσης, συνήθως, Local Area Connection. Σε περίπτωση που ο υπολογιστής διαθέτει περισσότερες από μια κάρτες τοπικού δικτύου, υπάρχει ανάλογος αριθμός τέτοιων εικονιδίων, καθένα από τα οποία δίνει πρόσβαση στις ρυθμίσεις της αντίστοιχης κάρτας. Με διπλό κλικ στο εικονίδιο και επιλέγοντας το πλήκτρο *Properties* (εάν εμφανισθεί παράθυρο με ενημερωτικό μήνυμα απαντήστε θετικά) θα βρείτε περισσότερες πληροφορίες για το υλικό της κάρτας και τα πρωτόκολλα επικοινωνίας.

Για να εισέλθετε στο σταθμό εργασίας του ΕΠΥ, χρησιμοποιείτε **το όνομα χρήστη και συνθηματικό για πρόσβαση στις ηλεκτρονικές υπηρεσίες του Ιδρύματος** (που σας έχει δοθεί από το ΚΗΥ). Μετά από επιτυχή ταυτοποίησή σας από τον εξυπηρετητή LDAP, θα αποκτήσετε πρόσβαση στον τοπικό υπολογιστή με όνομα χρήστη labuser. Εάν στην οθόνη δεν εμφανίζεται σχετικό παράθυρο διαλόγου για την εισαγωγή στο σύστημα, πιάστε ταυτόχρονα τα πλήκτρα *Alt+Ctrl+Del*.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα παραδοθεί στο τέλος του εργαστηρίου στον επιβλέποντα.

Άσκηση 1

Βασικά χαρακτηριστικά των καρτών δικτύωσης

Η κάρτα δικτύου συνδέει τον υπολογιστή σας στο τοπικό δίκτυο του εργαστηρίου και επιτρέπει την επικοινωνία με άλλους υπολογιστές. Για τον σκοπό αυτό παράγει και λαμβάνει μηνύματα που τα αποκαλούμε πλαίσια (frames). Της μετάδοσης του πλαισίου προηγείται μια σειρά εναλλασσόμενων bit 1 και 0 που καταλήγει σε δύο συνεχόμενα bit 1. Η σειρά αυτή αποκαλείται *Preamble* (*Προοίμιο*) και επιτρέπει τον συγχρονισμό του δέκτη με τον αποστολέα σηματοδοτώντας ταυτόχρονα την αρχή του πλαισίου. Τα πλαίσια ακολουθούν το πρότυπο Ethernet II ή το IEEE 802.3. Ξεκινούν με την *επικεφαλίδα* (*header*) και ακολουθούν τα *Δεδομένα* (*Data*), δηλαδή, η προς μετάδοση πληροφορία. Το πλαίσιο τελειώνει με το πεδίο *CRC* (*Άθροισμα Ελέγχου*) μήκους 4 byte που ακολουθείται από ένα υποχρεωτικό κενό (*interframe gap*) μήκους 12 byte. Η επικεφαλίδα περιλαμβάνει μια σειρά πεδίων ως εξής. Δύο *διευθύνσεις* 6 byte, μία για τον προορισμό και μία για την πηγή. Το πεδίο *Type* (*Τύπος*) ή το πεδίο *Length* (*Μήκος*), ανάλογα με το κατά πόσο πρόκειται για πλαίσιο Ethernet II ή IEEE 802.3, αντίστοιχα. Ο *Τύπος* δείχνει το πρωτόκολλο του ανώτερου στρώματος, συνήθως, το πρωτόκολλο IP. Το *Μήκος* δηλώνει πόσα byte βρίσκονται στο πεδίο δεδομένων, από ένα ελάχιστο 0 μέχρι ένα μέγιστο 1.500 byte. Ο δέκτης εξετάζει το πεδίο ελέγχου και αν ανιχνευθεί σφάλμα το πλαίσιο απορρίπτεται. Ένα έγκυρο πλαίσιο έχει μήκος τουλάχιστον 64 byte, από τη διεύθυνση προορισμού μέχρι το άθροισμα ελέγχου. Εάν το τμήμα δεδομένων ενός πλαισίου είναι μικρότερο από

46 byte, τα δεδομένα παραγεμίζεται (pad) μέχρι το ελάχιστο μέγεθος. Στο επόμενο σχήμα φαίνεται παραστατικά ένα πλαίσιο Ethernet II με το προοίμιό του.

Προοίμιο (8 byte)	Διεύθυνση παραλήπτη (6 byte)	Διεύθυνση αποστολέα (6 byte)	Τύπος (2 byte)	Δεδομένα (46 -1500 byte)	CRC (4 byte)
----------------------	------------------------------------	------------------------------------	-------------------	-----------------------------	-----------------

0x800	Πακέτο IP (46 -1500 byte)
-------	------------------------------

0x806	Πακέτο ARP (28 byte)	PAD (18 byte)
-------	-------------------------	------------------

Κάθε κάρτα δικτύου διαθέτει μια φυσική διεύθυνση, αυτήν του υποστρώματος MAC. Έχει μήκος 48 bit και η δομή της ορίζεται στο πρότυπο IEEE 802.3. Το πρώτο bit της διεύθυνσης που μεταδίδεται, ορίζει το κατά πόσο πρόκειται για Ομαδική (τιμή 1) ή Ατομική (τιμή 0) διεύθυνση. Όταν ένα πλαίσιο στέλνεται σε ομαδική διεύθυνση, το λαμβάνουν όλες οι κάρτες δικτύου της ομάδας. Αυτή η αποστολή ονομάζεται πολλαπλή διανομή (multicast). Το πλαίσιο που περιέχει μόνο 1 στο πεδίο προορισμού (δηλαδή “11...1”) υποδηλώνει εκπομπή (broadcast) και λαμβάνεται από όλες τις κάρτες του τοπικού δικτύου.

Το δεύτερο σε σειρά μετάδοσης bit διαχωρίζει τις τοπικές (τιμή 1) από τις παγκόσμιες (τιμή 0) διευθύνσεις. Οι τοπικές διευθύνσεις εκχωρούνται από τον διαχειριστή του τοπικού δικτύου και δεν έχουν σημασία έξω από το τοπικό δίκτυο. Οι μοναδικές (παγκόσμιες) διευθύνσεις εκχωρούνται από το IEEE ως εξής: τα επόμενα 22 bit της διεύθυνσης προσδιορίζουν τον κατασκευαστή της κάρτας και τα τελευταία 24 bit είναι ο αύξων αριθμός της κάρτας. Έτσι εξασφαλίζεται ότι δεν υπάρχουν δυο υπολογιστές οπουδήποτε στον κόσμο με την ίδια παγκόσμια διεύθυνση.

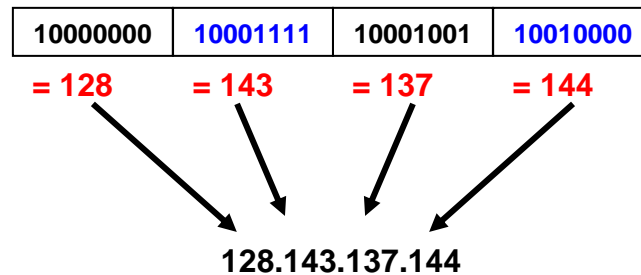
Χρησιμοποιώντας το γραφικό περιβάλλον της κάρτας δικτύωσης του υπολογιστή σας, βρείτε και καταγράψτε:

- 1.1 Την ονομασία της κάρτας δικτύωσης (network adapter)
- 1.2 Την ταχύτητα σύνδεσης.
- 1.3 Τη διεύθυνση υπο-στρώματος MAC σε δεκαεξαδική μορφή. [Υπόδειξη: θα χρειαστεί να αφήσετε το δρομέα του ποντικιού ακίνητο πάνω από το πεδίο του ονόματος της κάρτας.]
- 1.4 Τον κατασκευαστή της κάρτας δικτύωσης.
- 1.5 Τα συνδεδεμένα με αυτήν πρωτόκολλα δικτύωσης.
- 1.6 Τη διακοπή (interrupt – IRQ) που χρησιμοποιεί.
- 1.7 Την έκδοση του οδηγού (driver) της κάρτας και το όνομα του σχετικού αρχείου.
- 1.8 Τη θέση της στο PCI bus του υπολογιστή.

Άσκηση 2

Πρωτόκολλο επικοινωνίας TCP/IP

Κάθε δικτυακή διεπαφή (network interface) ενός host διαθέτει τη δική της διεύθυνση IP, η οποία είναι λογική (όχι φυσική, όπως της κάρτας δικτύου). Οι δρομολογητές έχουν πολλαπλές διεπαφές και κάθε μία διαθέτει τη δική της διεύθυνση IP. Η τρέχουσα έκδοση του IP είναι η 4 και οι αντίστοιχες διευθύνσεις λέγονται IPv4. Αυτές έχουν μήκος 4 byte και γράφονται στο λεγόμενο δεκαδικό συμβολισμό με υποδιαστολή (dotted decimal notation). Κάθε byte είναι δεκαδικός αριθμός στην περιοχή [0..255]. Π.χ.,



Οι διευθύνσεις IP έχουν δομή ιεραρχίας δύο επιπέδων:

1. αριθμός δικτύου
2. αριθμός host

Οι διευθύνσεις IP διακρίνονται από τα αρχικά bit της διεύθυνσης σε κατηγορίες (classes):

- 0 → class A (πρώτο byte < 128, αριθμός δικτύου το πρώτο byte και αριθμός host τρία byte)
- 10 → class B (πρώτο byte στην περιοχή 128-191, αριθμός δικτύου τα δύο πρώτα byte και αριθμός host δύο byte)
- 110 → class C (πρώτο byte στην περιοχή 192-223, αριθμός δικτύου τα τρία πρώτα byte και αριθμός host ένα byte)
- 1110 → class D (διευθύνσεις πολλαπλής διανομής με πρώτο byte στην περιοχή 224-239)
- 11110 → class E (δεσμευμένες για μελλοντική χρήση διευθύνσεις με πρώτο byte στην περιοχή 240-247)

Με τη βοήθεια της μάσκας υποδικτύου (subnet mask), ο αριθμός δικτύου της διεύθυνσης IP μπορούσε να επεκταθεί ώστε να προκύπτουν υποδίκτυα. Για παράδειγμα, η διεύθυνση 147.102.40.1 είναι κατηγορίας B, με αριθμό δικτύου 147.102 και αριθμό host 40.1. Για μάσκα υποδικτύου 255.255.255.0, τα τρία πρώτα byte της διεύθυνσης IP ορίζουν τη διεύθυνση υποδικτύου, που δηλώνεται ως 147.102.40.0 (λογικό AND της μάσκας και της διεύθυνσης IP εκφρασμένες σε bit). Το εναπομένον byte είναι ο αριθμός host. Σήμερα η παραπάνω διάκριση έχει αντικατασταθεί από το αταξικό σύστημα (Classless InterDomain Routing – CIDR). Αντί της μάσκας χρησιμοποιείται το πρόθεμα (prefix) δικτύου, δηλούμενο ως το σύμβολο "/" ακολουθούμενο από ακέραιο αριθμό. Το πρόθεμα ορίζει το μήκος σε bit του μέρους της διεύθυνσης IP που αντιστοιχεί σε δίκτυο. Έτσι, η διεύθυνση 147.102.40.1/24 υποδηλώνει host με αριθμό 1 και (υπο)δίκτυο μήκους 24 bit που στο αταξικό σύστημα δηλώνεται ως 147.102.40.0/24.

Για τη λειτουργία της στοίβας πρωτοκόλλων TCP/IP κάθε υπολογιστής υποχρεούται να διαθέτει μία τουλάχιστον διεύθυνση IP για κάθε διεπαφή που διαθέτει, ανεξαρτήτως του τύπου της (Ethernet, LAN, WAN, virtual κτλ), αρκεί να είναι μοναδική στο τοπικό δίκτυο όπου ανήκει. Τη διεύθυνση αυτή μπορεί να θέτει στατικά ο ίδιος ο υπολογιστής (αφού σιγουρευτεί ότι δεν τη χρησιμοποιεί ήδη κάποιος άλλος στο τοπικό δίκτυο), μετά από αντίστοιχο προγραμματισμό από το χρήστη ή μπορεί να την «ενοικιάζει» δυναμικά από ένα ειδικό εξυπηρετητή. Ο τελευταίος τρόπος παρουσιάζει προφανές και σημαντικό διαχειριστικό πλεονέκτημα σε ένα δίκτυο, ιδίως αν σ' αυτό μετέχουν πολλοί υπολογιστές. Ένας τέτοιος εξυπηρετητής (και αντίστοιχο πρωτόκολλο) είναι το DHCP (Dynamic Host Configuration Protocol), δουλειά του οποίου είναι να «μισθώνει» διευθύνσεις IP σε κάρτες δικτύου, καταγράφοντάς τες παράλληλα σε ειδικό πίνακα έτσι ώστε να μη δοθεί ποτέ μία IP σε περισσότερες της μιας κάρτας δικτύου. Το DHCP μπορεί να αναθέσει και άλλα πράγματα εκτός από διεύθυνση IP, όπως μάσκα υποδικτύου, προκαθορισμένη πύλη, εξυπηρετητές DNS, κ.ά.

Στη συνέχεια θα αντλήσετε διάφορα στοιχεία σχετικά με τις παραμέτρους δικτύωσης του υπολογιστή σας μέσω εντολών φλοιού. Χρήσιμες τέτοιες εντολές φλοιού είναι οι `hostname`, `getmac`, `ipconfig`, `net`, `netstat` και `route`. Για την εκτέλεσή τους ανοίξτε ένα παράθυρο εντολών (command prompt), πηγαίνατε στο *Start* → *Run...*, και αφού γράψετε την εντολή `cmd`, πιάστε το πλήκτρο *Enter*. Για να βρείτε πληροφορίες σχετικά με αυτές γράψτε την εντολή ακολουθούμενη από `/?` ή `-?` και πιάστε το πλήκτρο *Enter*. Εάν το κείμενο δεν χωρά στην οθόνη

προσθέστε το `| more` είτε μετακινήσετε τη δεξιά μπάρα (ή χρησιμοποιήστε τον τροχό του ποντικιού) για να εμφανισθεί το μέρος του παραθύρου που δεν είναι ορατό.

Για περισσότερες πληροφορίες σχετικά με όλα τα εργαλεία που υπάρχουν για TCP/IP στα Windows, πηγαίνετε στο *Start* → *Help and Support* και στο πλαίσιο *Search* πληκτρολογήστε *TCP/IP utilities*. Ειδικά για την *net* θα χρειασθεί να αναζητήσετε το *net services commands*. Αφού μελετήσετε το *help* για τις εντολές *hostname*, *ipconfig*, *route*, *netstat* και *net*, δίνοντας έμφαση στις επιλογές *view* και *config* της τελευταίας, να απαντήσετε στα ακόλουθα ερωτήματα και να καταγράψετε μαζί με την απάντηση **την ακριβή σύνταξη της εντολής** που χρησιμοποιήθηκε:

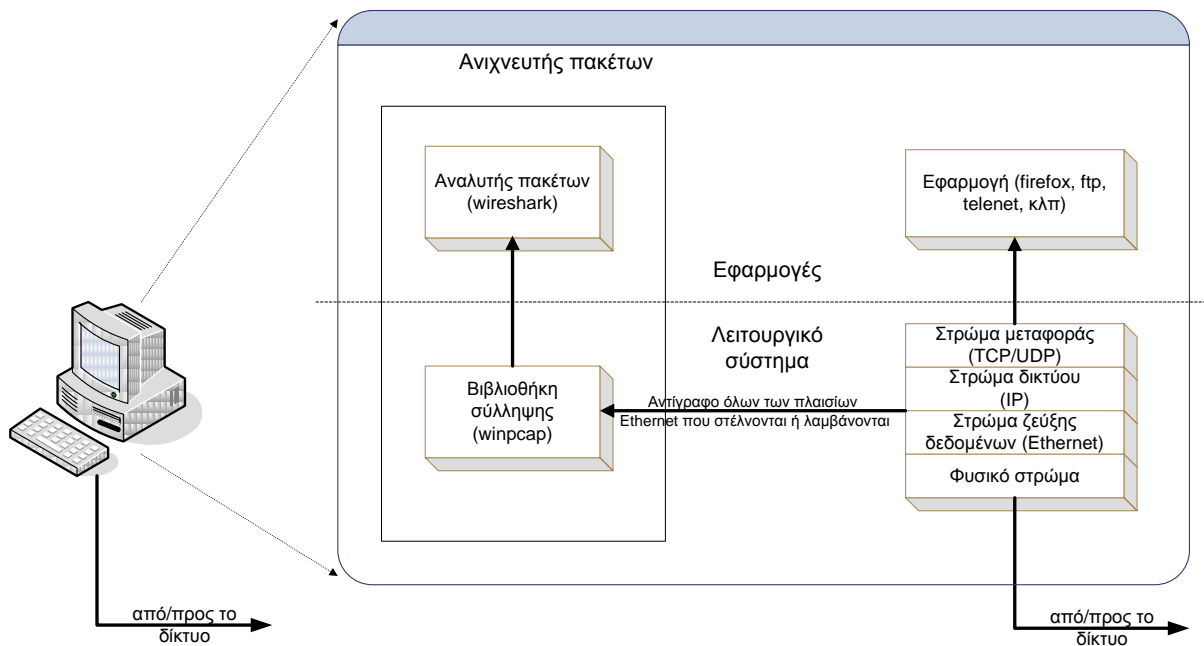
- 2.1 Το όνομα του υπολογιστή σας. *[Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]*
- 2.2 Την περιοχή (Workstation domain) που ανήκει ο υπολογιστής σας.
- 2.3 Τη διεύθυνση υπο-στρώματος MAC. *[Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]*
- 2.4 Τη διεύθυνση IP του υπολογιστή σας. *[Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]*
- 2.5 Την κατηγορία (class) που ανήκει η διεύθυνση IP του υπολογιστή σας.
- 2.6 Τη μάσκα του υποδικτύου. Με βάση τη μάσκα αυτή (και χωρίς την εκτέλεση επιπλέον εντολών):
 - i. Να υπολογίσετε τον αριθμό των bit που χρησιμοποιούνται για το τμήμα του δικτύου της διεύθυνσης IP του υπολογιστή σας.
 - ii. Να καταγράψετε τη διεύθυνση του υποδικτύου.
- 2.7 Τη διεύθυνση IP της προκαθορισμένης πύλης (default gateway).
- 2.8 Τη διεύθυνση IP του εξυπηρετητή DHCP και τη διάρκεια της περιόδου απονομής (lease).
- 2.9 Τον αριθμό των:
 - i. πακέτων IP
 - ii. πλαισίων μονο-εκπομπής (unicast)
 - iii. πλαισίων εκπομπής (broadcast)
 - iv. byte

που έστειλε και έλαβε η κάρτα δικτύου του υπολογιστή σας. *[Υποδ. Πρέπει να εκτελεστούν δύο διαφορετικές εντολές]*
- 2.10 Τον συνολικό αριθμό των ανοικτών συνδέσεων TCP που έχει ο σταθμός εργασίας σας καθώς και το πλήθος των εγκατεστημένων συνδέσεων TCP με άλλους υπολογιστές..
- 2.11 Υπάρχουν δύο διαφορετικές εντολές προκειμένου να δείτε τον πίνακα δρομολόγησης (routing table) του υπολογιστή. Να καταγραφεί η ακριβής σύνταξη και στις δύο περιπτώσεις.
- 2.12 Καταγράψτε την ακριβή σύνταξη μιας ακόμη εντολής (πέραν αυτής που χρησιμοποιήσατε στο προηγούμενο ερώτημα 2.3) με τη βοήθεια της οποίας μπορείτε να βρείτε τη διεύθυνση υποστρώματος MAC της κάρτας δικτύου.

Άσκηση 3

Αναλυτής Πρωτοκόλλων Wireshark

Η άσκηση αυτή αποτελεί εισαγωγή στη χρήση του αναλυτή πρωτοκόλλων Wireshark, του οποίου οι βασικές λειτουργίες είναι οι εξής: α) καταγραφή – σύλληψη (capture) και β) ανάλυση της δικτυακής κίνησης του υπολογιστή. Το πρόγραμμα Wireshark¹ είναι ένας ανιχνευτής πακέτων² (packet sniffer) που διατίθεται ως ανοικτό λογισμικό (www.wireshark.org) για πληθώρα λειτουργικών συστημάτων. Η βασική του λειτουργία έγκειται στη σύλληψη των μηνυμάτων που στέλνονται ή λαμβάνονται από τον υπολογιστή σας. Τα περιεχόμενα των διαφόρων πεδίων των μηνυμάτων εμφανίζονται στην οθόνη αποκωδικοποιημένα. Ο ρόλος ενός ανιχνευτή πακέτων είναι παθητικός, με την έννοια ότι απλά παρατηρεί τα μηνύματα που στέλνονται και λαμβάνονται από την κάρτα δικτύωσης, χωρίς ο ίδιος να παράγει δικτυακή κίνηση. Πιο συγκεκριμένα, ο ανιχνευτής πακέτων παίρνει ένα αντίγραφο όλων των πλαισίων που στέλνονται/λαμβάνονται προς/από τις διάφορες εφαρμογές και πρωτόκολλα του υπολογιστή όπου εκτελείται. Στο σχήμα που ακολουθεί, φαίνεται η δομή ενός ανιχνευτή πακέτων.



Στο παραπάνω σχήμα βλέπουμε τη στοιβή πρωτοκόλλων TCP/IP, καθώς επίσης, και διάφορες συνηθισμένες δικτυακές εφαρμογές που εκτελούνται σε ένα υπολογιστή, όπως ένας πλοηγός ιστού ή πελάτης FTP. Ο ανιχνευτής πακέτων, που παριστάνεται με το διαγραμμισμένο πλαίσιο στο σχήμα, είναι μια προσθήκη στο λογισμικό του συστήματος όπου εκτελείται και αποτελείται από δύο τμήματα: α) τη βιβλιοθήκη σύλληψης πακέτων και β) τον αναλυτή πακέτων.

Η βιβλιοθήκη σύλληψης πακέτων λαμβάνει ένα αντίγραφο κάθε πλαισίου που στέλνεται ή λαμβάνεται από την κάρτα δικτύωσης. Τα πλαίσια αυτά ανήκουν στο επίπεδο ζεύξης δεδομένων του προτύπου OSI και περιέχουν ενθυλακωμένα τα διάφορα μηνύματα που ανταλλάσσονται μεταξύ των πρωτοκόλλων ανώτερων στρωμάτων. Το παραπάνω σχήμα αφορά την περίπτωση του Ethernet όπου το φυσικό επίπεδο μετάδοσης των πλαισίων είναι το καλώδιο Ethernet. Το δεύτερο τμήμα του ανιχνευτή πακέτων, δηλαδή, ο αναλυτής πακέτων, εμφανίζει τα περιεχόμενα όλων των πεδίων που περιέχονται σε ένα μήνυμα. Για τον σκοπό αυτό, πρέπει να γνωρίζει τη δομή των μηνυμάτων όλων των πρωτοκόλλων. Για παράδειγμα, στην περίπτωση ενός μηνύματος HTTP, απαιτείται, κατ' αρ-

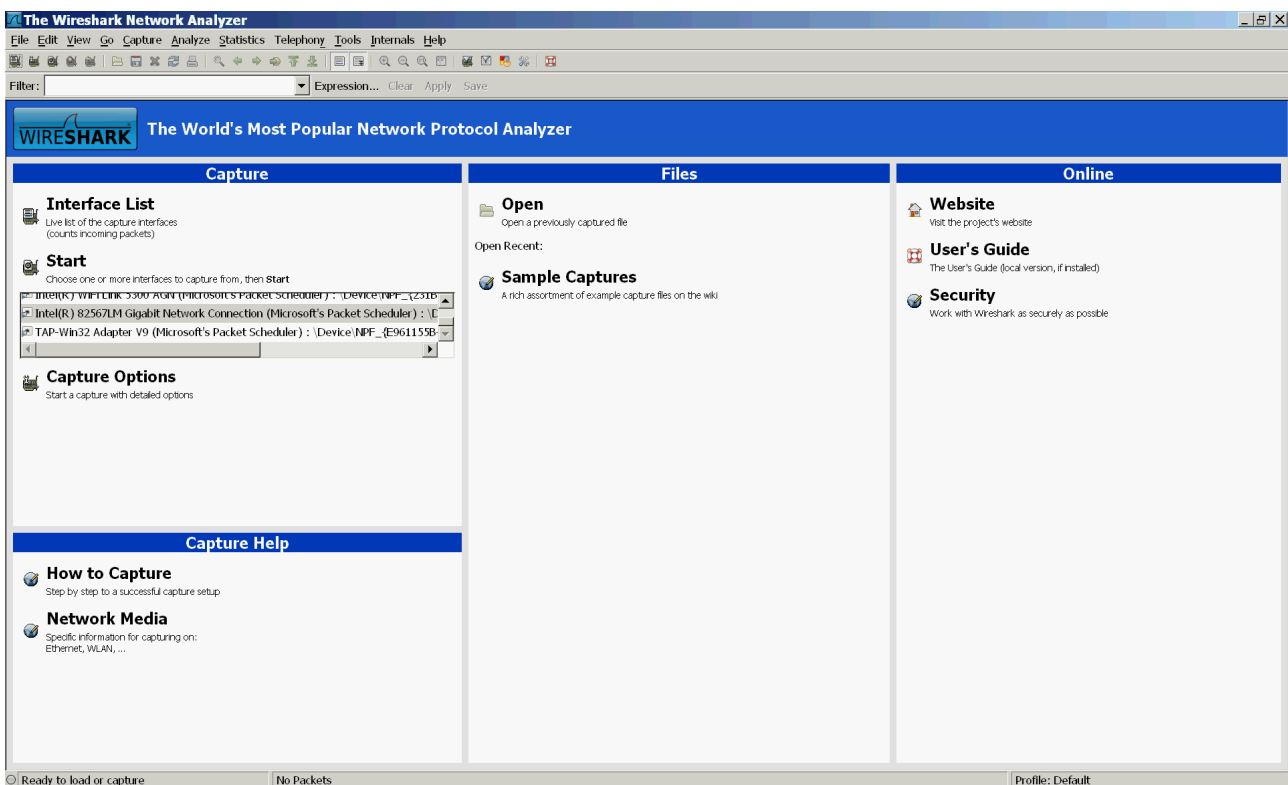
¹ Το Wireshark είναι μετονομασία του γνωστού Ethereal[®] (www.ethereal.org), λόγω διαμάχης για το σήμα κατατεθέν (trademark). Το Ethereal εξακολουθεί να διατίθεται ως ανοικτό λογισμικό, αν και από ότι φαίνεται η ανάπτυξη έχει σταματήσει τον Μάιο 2006.

² Οι όροι «πλαίσιο» (frame) και «πακέτο» (packet), δεν είναι ταυτόσημοι και χρησιμοποιούνται λανθασμένα συχνά ο ένας αντί του άλλου.

χίν, γνώση της δομής των πλαισίων Ethernet, ώστε ο αναλυτής πρωτοκόλλων να είναι σε θέση να αναγνωρίσει το πακέτο IP που έχει ενθυλακωθεί στο πλαίσιο Ethernet. Επιπλέον, δεδομένης της δομής ενός πακέτου IP, μπορεί να αναλυθεί το τεμάχιο (segment) TCP που εμπεριέχεται μέσα στο IP. Ομοίως, η δομή του τεμαχίου TCP επιτρέπει την αποκωδικοποίηση του μηνύματος HTTP, ενώ περαιτέρω ανάλυση οδηγεί στο συγκεκριμένο τύπο του μηνύματος HTTP, δηλαδή GET, POST κ.ά.

Στο ΕΠΥ θα βρείτε το πρόγραμμα Wireshark εγκατεστημένο. Μπορείτε όμως για εξάσκηση να το εγκαταστήσετε και στον προσωπικό σας υπολογιστή κατεβάζοντας, ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείτε, το αντίστοιχο αρχείο από την ιστοσελίδα <http://www.wireshark.org/download.html>. Για να λειτουργήσει το Wireshark απαιτείται η ύπαρξη της βιβλιοθήκης σύλληψης πακέτων libpcap. Για τα συστήματα Windows η βιβλιοθήκη ονομάζεται WinPcap και εγκαθίσταται μαζί με το πρόγραμμα. Εναλλακτικά, μπορείτε να την κατεβάσετε από την ιστοσελίδα <http://www.winpcap.org/>. Περισσότερες πληροφορίες σχετικά με τον αναλυτή πρωτοκόλλων Wireshark μπορείτε να βρείτε στη σελίδα <http://www.wireshark.org/docs/> όπου υπάρχουν σύνδεσμοι για το εγχειρίδιο χρήσης σε διάφορες μορφές ([html](#), [pdf](#), κλπ) καθώς και στην <http://www.wireshark.org/faq.html> σε περίπτωση που συναντήσετε δυσκολίες.

Όταν ξεκινήσετε το Wireshark θα εμφανισθεί το ένα γραφικό περιβάλλον όπως το ακόλουθο.



Στο άνω μέρος υπάρχει το μενού των διαθέσιμων εντολών για την έναρξη διάφορων λειτουργιών, η κύρια εργαλειοθήκη (main toolbar) με συντομεύσεις για τις πιο συχνά χρησιμοποιούμενες εντολές του μενού καθώς και η εργαλειοθήκη φίλτρων³. Το κάτω μέρος έχει τη μορφή ιστοσελίδας και περιέχει χρήσιμους συνδέσμους καθώς και γρήγορη πρόσβαση στις βασικές εντολές του μενού που σχετίζονται με την καταγραφή πλαισίων.

Μπορείτε να ξεκινήσετε μια καταγραφή κάνοντας κλικ στο Capture Options της προαναφερθείσης οθόνης που είναι μια συντόμευση για τη διαδρομή *Capture* → *Options...* από το μενού επιλογών. Στο παράθυρο που θα εμφανισθεί πρέπει να επιλέξετε την ή τις διεπαφές που επιθυμείτε και η κα-

³ Για κάθε λειτουργία ο χρήστης μπορεί να ορίσει κατάλληλα φίλτρα καταγραφής/ανάλυσης τα οποία περιορίζουν την κίνηση που καταγράφεται/αναλύεται σύμφωνα με τα κριτήριά του. Σύμφωνα με την ορολογία του Wireshark διακρίνουμε τα *capture* και τα *display filters*, αντίστοιχα, τα οποία θα δείτε στις επόμενες σειρές ασκήσεων. Η εργαλειοθήκη φίλτρων επιτρέπει την άμεση αλλαγή των φίλτρων ανάλυσης.

ταγραφή θα ξεκινήσει πατώντας το *Start*. Αμέσως θα εμφανισθεί το κύριο γραφικό περιβάλλον του Wireshark όπως φαίνεται στο σχήμα που ακολουθεί.

The screenshot displays the Wireshark interface with the following sections:

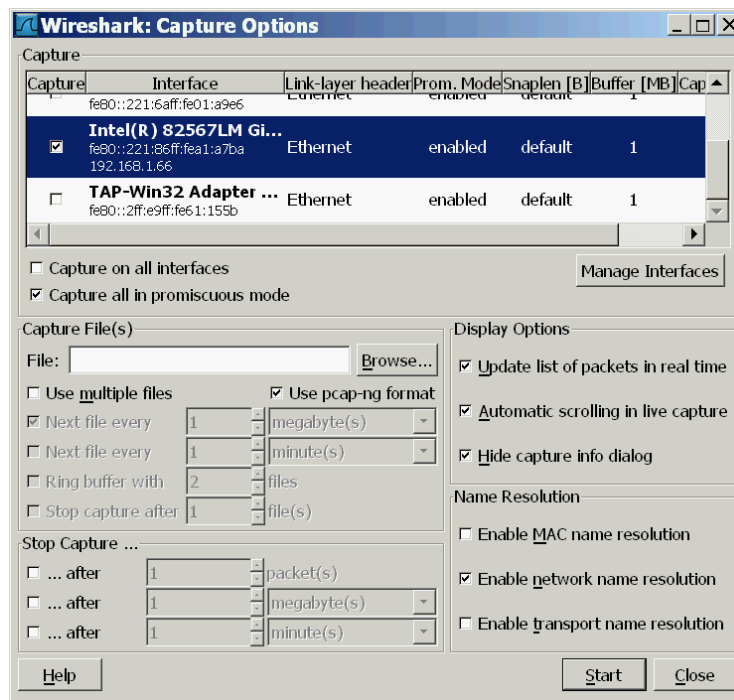
- Display filter:** A text box containing the filter 'http'.
- Packet list:** A table of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. Packet 39 is highlighted.
- Packet details:** A tree view showing the structure of the selected packet (39), including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.
- Packet bytes:** A hex dump and ASCII representation of the selected packet's data.

Μπορούμε να διακρίνουμε τέσσερα βασικά μέρη:

- Το πεδίο όπου μπορεί να οριστεί το **φίλτρο ανάλυσης (display filter)**. Κάνοντας κλικ στο *Apply* εφαρμόζετε το φίλτρο ανάλυσης και στο επόμενο παράθυρο εμφανίζονται τα πλαίσια σας ενδιαφέρουν ενώ αποκρύπτονται τα υπόλοιπα.
- Το παράθυρο με τη **λίστα καταγεγραμμένων πακέτων (packet list)** όπου εμφανίζονται περιληπτικές πληροφορίες για το καθένα. Αυτές περιλαμβάνουν τον αύξοντα αριθμό πλαισίου κατά την καταγραφή, το χρόνο καταγραφής, τη διεύθυνση αποστολέα (*source*) και παραλήπτη (*destination*), το πρωτόκολλο, καθώς και σύντομες πληροφορίες σχετικές με αυτό. Κάνοντας κλικ σε κάποιο πακέτο ελέγχετε το τι θα εμφανισθεί στα επόμενα δύο παράθυρα.
- Το παράθυρο με τις **λεπτομέρειες επικεφαλίδας (packet details)** όπου εμφανίζονται περισσότερες πληροφορίες σχετικά με την ενθυλάκωση των πρωτοκόλλων στο επιλεγμένο πακέτο από τη λίστα των καταγεγραμμένων πακέτων. Στο παράθυρο εμφανίζονται, ένα ανά γραμμή, όλα τα πρωτόκολλα που περιλαμβάνει το πλαίσιο με τη σειρά ενθυλάκωσής τους. Οι πληροφορίες για τα περιεχόμενα των επικεφαλίδων κάθε πρωτοκόλλου μπορούν να αντληθούν πατώντας το αντίστοιχο '+'. .
- Το παράθυρο με τα **περιεχόμενα (packet bytes)** του επιλεγμένου πλαισίου σε δεκαεξαδική μορφή και μορφή ASCII. Τα δεδομένα που αντιστοιχούν στο επιλεγμένο πεδίο του παραθύρου με τις λεπτομέρειες επικεφαλίδας εμφανίζονται σε σκούρο φόντο (*highlighted*).

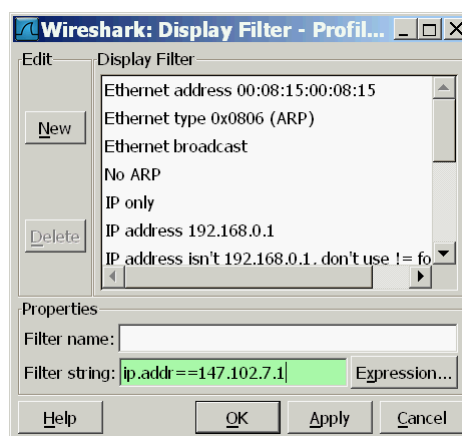
Τέλος στη γραμμή κατάστασης βλέπετε την τρέχουσα κατάσταση του προγράμματος και των καταγραφόμενων δεδομένων.

Ως εισαγωγικό παράδειγμα θα παρατηρήσετε την κίνηση που παράγεται από την επίσκεψη μιας ιστοσελίδας. Ανοίξτε πρώτα τον Internet Explorer και μετά ξεκινήσετε το Wireshark. Οι διάφορες επιλογές που αφορούν τη λειτουργία της καταγραφής ρυθμίζονται ακολουθώντας από το μενού επιλογών τη διαδρομή *Capture* → *Options*.... Στο παράθυρο που εμφανίζεται βεβαιωθείτε ότι έχετε επιλέξει τη διεπαφή της κάρτας δικτύου του υπολογιστή σας (ερώτημα 1.1) και επιπλέον ότι η επιλογή *Enable network name resolution* είναι ενεργοποιημένη.



Πατώντας το *Start* αρχίζει η καταγραφή. Τα πακέτα που συλλαμβάνονται εμφανίζονται σε πραγματικό χρόνο υπό τη μορφή κυλιόμενης λίστας στο παράθυρο με τη λίστα καταγεγραμμένων πακέτων. Μπορείτε να σταματήσετε την καταγραφή ακολουθώντας από το μενού επιλογών τη διαδρομή *Capture* → *Stop...* ή πληκτρολογώντας *Ctrl+E*.

Επισκεφτείτε με τον Internet Explorer την ιστοσελίδα <http://www.telecom.ntua.gr/> και μόλις φορτωθεί πλήρως σταματήστε την καταγραφή. Στο κύριο παράθυρο του Wireshark, όπου φαίνεται η καταγεγραμμένη δικτυακή κίνηση, μπορεί ενδεχομένως να παρατηρήσετε κίνηση που δε σχετίζεται με την επίσκεψη της ιστοσελίδας. Η ζητούμενη κίνηση μπορεί να απομονωθεί με την εφαρμογή φίλτρου παρατήρησης ως εξής: πηγαίνετε στο *Analyze* → *Display Filters...* και πατήστε το πλήκτρο *Expression*. Από το πεδίο *Field name* βρείτε⁴ την επιλογή *IPv4*, πατήστε το +, διαλέξτε στη λίστα που θα εμφανισθεί την επιλογή *ip.addr*, επιλέξτε από το πεδίο *Relation* το *==*, πληκτρολογήστε στο πεδίο *Value* (*IPv4 address*) *147.102.7.1* και τέλος πατήστε *OK*. Το φίλτρο ενεργοποιείται με το πάτημα του *Apply*.



Εναλλακτικά, θα μπορούσατε να γράψετε απευθείας την έκφραση *ip.addr==147.102.7.1* στο πεδίο *Field string*. Εάν η σύνταξη της έκφρασης είναι σωστή το πεδίο θα χρωματισθεί πράσινο, όπως στο σχήμα, αλλιώς θα είναι ροζ. Κλείνοντας το παράθυρο διαλόγου με *OK* θα διαπιστώσετε ότι η κίνηση είναι ενδεχομένως περιορισμένη σε σχέση με την παρατήρηση χωρίς φίλτρο. Στη λίσ-

⁴ Αρκεί να πληκτρολογήσετε τους χαρακτήρες *i,p,v,4*.

τα των καταγεγραμμένων πακέτων, και κάτω από την επικεφαλίδα Protocol, εμφανίζεται το εκάστοτε πρωτόκολλο υψηλότερου στρώματος που περιέχει το πλαίσιο. Εντοπίστε το πρώτο μήνυμα HTTP GET που έστειλε ο υπολογιστής σας για να κατεβάσει τη σελίδα και την αντίστοιχη απόκριση HTTP του εξυπηρετητή. Με βάση τα στοιχεία της καταγραφής σας απαντήστε τις επόμενες ερωτήσεις.

- 3.1 Ποια είναι η διεύθυνση IP του `www.telecom.ntua.gr`;
- 3.2 Ποια είναι η διεύθυνση IP του υπολογιστή σας;
- 3.3 Ποια είναι η διεύθυνση MAC του υπολογιστή σας σε δεκαεξαδική μορφή;
- 3.4 Ποιος είναι ο κατασκευαστής της κάρτας δικτύου;

Κάνοντας κλικ στην επικεφαλίδα Protocol του παράθυρου με τη λίστα καταγεγραμμένων πακέτων, τα πλαίσια θα ταξινομηθούν ανά είδος πρωτοκόλλου. Παρατηρείστε ότι η αύξουσα (ή φθίνουσα) σειρά ταξινόμησης υποδηλώνεται με ένα μικρό βέλος προς τα πάνω ή κάτω. Επιλέξτε ένα από τα πλαίσια που καταγράψατε.

- 3.5 Να καταγράψετε τα πρωτόκολλα που παρατηρείτε ότι χρησιμοποιούνται για την επικοινωνία με την ιστοσελίδα.

Ταξινομείστε και πάλι τα πλαίσια με αύξουσα αριθμητική σειρά. Κατόπιν τοποθετήστε τον δρομέα στο πρώτο πλαίσιο που περιέχει τεμάχιο TCP, πιέστε το δεξί πλήκτρο του ποντικιού και επιλέξτε το Follow TCP Stream. Στην οθόνη που θα εμφανισθεί βλέπετε το περιεχόμενο της συγκεκριμένης ροής TCP, δηλαδή, την ανταλλαγή μηνυμάτων HTTP μεταξύ του πλοηγού και του εξυπηρετητή ιστού. Τα μηνύματα (εντολές) του πλοηγού ιστού εμφανίζονται σε ροζ φόντο, ενώ τα μηνύματα (αποκρίσεις) του εξυπηρετητή ιστού εμφανίζονται σε γαλάζιο φόντο, όπως στο ακόλουθο παράδειγμα:

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Accept-Language: el
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.mit.edu
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Fri, 05 Nov 2004 08:25:08 GMT
Server: MIT Web Server Apache/1.3.26 Mark/1.4 (Unix) mod_ssl/2.8.9
OpenSSL/0.9.6g
Last-Modified: Fri, 05 Nov 2004 04:59:29 GMT
ETag: "71d07dc-40a9-418b08b1"
Accept-Ranges: bytes
Content-Length: 16553
Keep-Alive: timeout=15, max=400
Connection: Keep-Alive
Content-Type: text/html
```

- 3.6 Με βάση τα αποτελέσματα της προηγούμενης καταγραφής βρείτε:
 - i. τον τύπο του εξυπηρετητή ιστού που φιλοξενεί τη σελίδα που επισκεφθήκατε,
 - ii. τον τίτλο και το αντίστοιχο HTML tag της σελίδας που επισκεφθήκατε,
 - iii. σε ποιο σημείο του παραθύρου του browser εμφανίζεται αυτός ο τίτλος;
- 3.7 Ποια είναι η σύνταξη του φίλτρου που εμφανίζεται τώρα στο παράθυρο του φίλτρου ανάλυσης;
- 3.8 Με εφαρμογή κατάλληλου φίλτρου εμφανίστε τώρα μόνο τα μηνύματα HTTP. Ποια είναι η σύνταξή του;

3.9 Θέλετε τώρα να δείτε μόνο τα μηνύματα HTTP που έστειλε ο υπολογιστής σας. Ποια είναι η σύνταξή του; [Υποδ. Θα πρέπει να σχηματίσετε μια έκφραση με τον λογικό τελεστή *KAI* (*and* ή *&&*), όπως στο ερώτημα 3.7, που να επιλέγει πακέτα IP με διεύθυνση πηγής αυτήν του υπολογιστή σας τα οποία να περιέχουν μηνύματα HTTP].

Όνοματεπώνυμο:		Όνομα PC:	
Ομάδα:		Ημερομηνία:	
Διεύθυνση IP: . . .		Διεύθυνση MAC: - - - - -	

Εργαστηριακή Άσκηση 1

Δικτύωση στα Microsoft Windows

Wireshark: Αναλυτής Πρωτοκόλλων

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

- 1.1
- 1.2
- 1.3
- 1.4
- 1.5
- 1.6
- 1.7
- 1.8

Άσκηση 2

- 2.1
-
- 2.2
-
- 2.3
-
- 2.4
-
- 2.5
-
- 2.6
-
- 2.7
-
- 2.8
-

2.9

.....

.....

.....

2.10

.....

.....

2.11

.....

2.12

.....

Άσκηση 3

3.1

.....

3.2

.....

3.3

.....

3.4

.....

3.5

.....

.....

.....

3.6

.....

.....

.....

3.7

.....

3.8

.....

3.9

.....