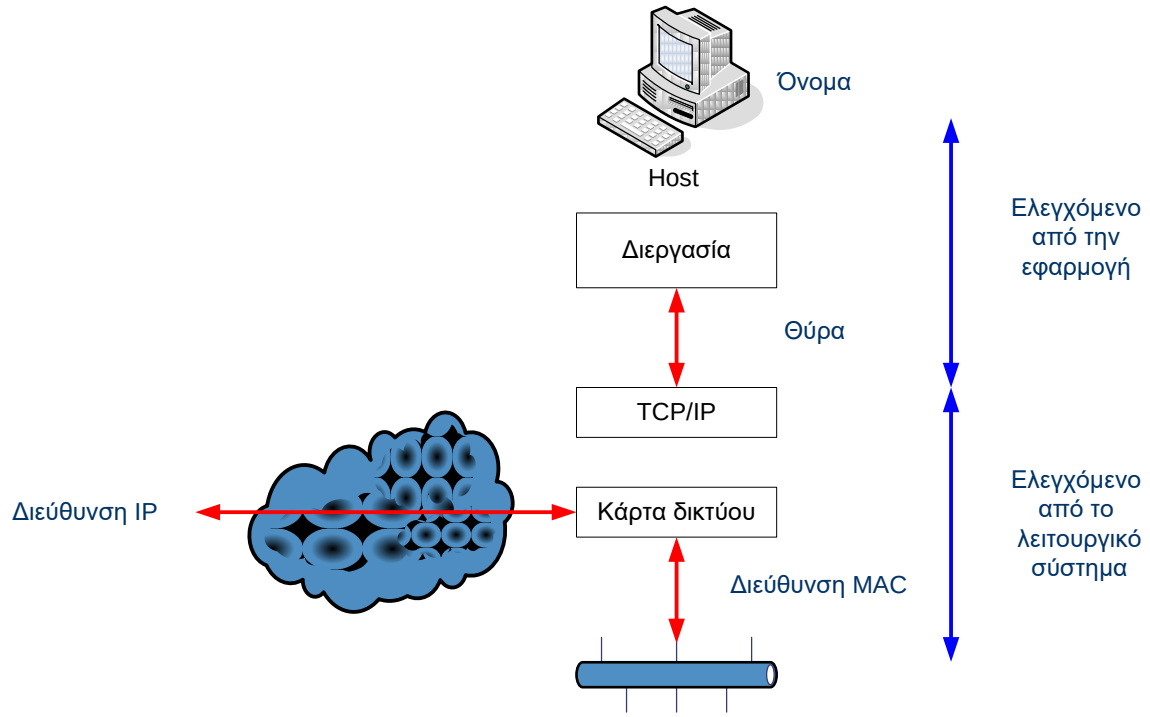
Εργαστηριακή Άσκηση 1
Αναλυτής Πρωτοκόλλων Wireshark

Σκοπός της πρώτης σειράς ασκήσεων είναι η εξοικείωση με το Wireshark, ένα εργαλείο ανάλυσης πρωτοκόλλων σε γραφικό περιβάλλον. Ταυτόχρονα, θα έχετε μια πρώτη επαφή με το θέμα της διευθυνσιοδότησης και ονοματοδότησης στο διαδίκτυο.

Στα δίκτυα υπολογιστών, για να είναι εφικτή οποιαδήποτε επικοινωνία μεταξύ δύο οντοτήτων, πρέπει προηγουμένως να έχουν προσδιορισθεί τρία θεμελιώδη χαρακτηριστικά τους: το όνομα (δηλαδή, ποιος επικοινωνεί), η διεύθυνση (πού βρίσκεται) και η διαδρομή (πώς φτάνουμε εκεί). Οποιοδήποτε από τα προηγούμενα χαρακτηριστικά μπορεί να θεωρηθεί ως ένα είδος ταυτότητας (identifier). Ανάλογα με τι ακριβώς υποδηλώνει η ταυτότητα, χρησιμοποιούνται ειδικότερες λέξεις, όπως, Όνομα (name), Διεύθυνση (Address), Διαδρομή (Route). Στην περίπτωση ενός κόμβου (host) συνδεδεμένου στο διαδίκτυο, π.χ. του προσωπικού σας υπολογιστή, όπου για την επικοινωνία χρησιμοποιείται η στοίβα πρωτοκόλλων TCP/IP, οι οντότητες που χρήζουν ταυτοτήτων είναι: η ίδια η συσκευή (όνομα), οι διεργασίες (θύρα TCP ή UDP), οι διεπαφές (διεύθυνση IP) και οι κάρτες δικτύου (διεύθυνση Medium Access Control – MAC).

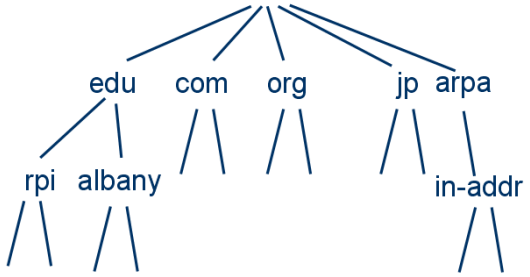


Σχήμα 1: Ονόματα, διευθύνσεις και θύρες στο διαδίκτυο

Το Σχήμα 1 δείχνει τη μεταξύ τους σχέση, αλλά κρύβει την πολυπλοκότητα της ανάθεσης και διαχείρισής τους. Στο διαδίκτυο υπάρχουν μηχανισμοί και αντίστοιχα πρωτόκολλα για τη μετάφραση του ονόματος ενός κόμβου στη διεύθυνση IP αυτού, την απόδοση διεύθυνσης IP σε μια διεπαφή και τελικά τη μετάφραση της διεύθυνσης IP σε διεύθυνση MAC. Για τις παραπάνω λειτουργίες χρησιμοποιούνται εξυπηρετητές του συστήματος ονομασίας περιοχών DNS (Domain Name System), εξυπηρετητές δυναμικής διάρθρωσης κόμβων DHCP (Dynamic Host Configuration Protocol) καθώς και το Πρωτόκολλο Επίλυσης Διευθύνσεων ARP (Address Resolution Protocol), αντίστοιχα.

Ονόματα

Το διαδίκτυο είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές **περιοχές** (domains) υψηλού επιπέδου, οι οποίες χωρίζονται με τη σειρά τους σε άλλες υποπεριοχές (subdomains) με πολλούς hosts (υπολογιστές ή κόμβους) η καθεμία. Η ιεραρχία των περιοχών μπορεί να παρασταθεί με ένα δέντρο (Σχήμα 2). Το όνομα κάθε host αποτελείται από μια ακολουθία *ετικετών* (labels) που χωρίζονται με τελείες (π.χ. www.mit.edu). Κάθε ετικέτα μπορεί να έχει μέχρι 63 χαρακτήρες, ενώ το όνομα του host συνολικά, μπορεί να έχει το πολύ 255 χαρακτήρες. Μια περιοχή είναι ένα υποδέντρο του παγκόσμιου δέντρου ονομάτων και ως εκ τούτου, το όνομα περιοχής (domain name) για ένα host είναι η ακολουθία των ετικετών που οδηγούν από το host (φύλλο στο δέντρο ονομάτων) στην κορυφή του παγκόσμιου δέντρου ονομάτων.

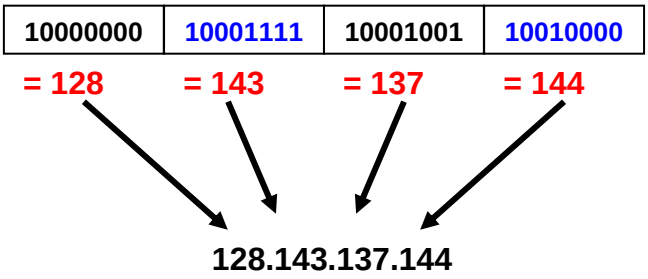


Σχήμα 2: Ιεραρχία DNS

Διευθύνσεις IP

Το διαδίκτυο βασίζεται στη χρήση της στοίβας πρωτοκόλλων TCP/IP, οπότε οι διευθύνσεις είναι αυτές που ορίζει το πρωτόκολλο IP. Κάθε κόμβος του υποχρεούται να διαθέτει μία διεύθυνση IP για κάθε δικτυακή διεπαφή (network interface) που διαθέτει, ανεξαρτήτως του τύπου της (Ethernet, LAN, WAN, virtual κτλ), αρκεί να είναι μοναδική στο τοπικό δίκτυο όπου ανήκει. Οι υπολογιστές τυπικά έχουν μία διεπαφή, ενώ οι δρομολογητές έχουν πολλαπλές διεπαφές και κάθε μία διαθέτει τη δική της διεύθυνση IP. Η διεύθυνση IP περιέχει πληροφορία που χρησιμοποιείται για τη δρομολόγηση.

Η αρχική έκδοση του πρωτοκόλλου IP (Internet Protocol) είναι το IPv4 (IP version 4) και οι αντίστοιχες διευθύνσεις IPv4 έχουν μήκος 4 byte. Γράφονται με τον λεγόμενο δεκαδικό συμβολισμό και τελείες (dotted decimal notation). Κάθε byte είναι δεκαδικός αριθμός στην περιοχή [0,1,…,255]. Π.χ.,



Στη νεώτερη έκδοση IPv6 (IP version 6) του πρωτοκόλλου IP η διεύθυνση έχει μήκος 16 byte, τέσσερις φορές περισσότερο από αυτό του IPv4. Δεδομένου του μεγάλου μήκος των διευθύνσεων, η αναπαράστασή τους γίνεται με χρήση δεκαεξαδικών συμβόλων, τα οποία ομαδοποιούνται σε 8 ομάδες των 4 συμβόλων. Για να βελτιωθεί η αναγνωσιμότητα, οι ομάδες χωρίζονται με “:”. Επιτρέπονται συντομεύσεις, όπως η παράλειψη των αρχικών μηδενικών και η σύντμηση του “:0000:…:0000:” σε “::”. Για παράδειγμα οι ακόλουθες αναπαριστούν όλες την ίδια διεύθυνση IPv6:

2001:0db8:0000:0000:0000:0000:1428:57ab
2001:db8:0:0:0:0:1428:57ab
2001:db8::1428:57ab

Οι διευθύνσεις IP (IPv4 και IPv6) έχουν δομή ιεραρχίας δύο επιπέδων: (αριθμός δικτύου, αριθμός host). Στο παρελθόν οι διευθύνσεις IPv4 διακρίνονταν από τα *αρχικά bit* της διεύθυνσης σε κατηγορίες (classes) από τις οποίες προέκυπτε αυτόματα ο αριθμός δικτύου και ο αριθμός host, ως εξής:

- 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)

Για παράδειγμα, το ΕΜΠ διαθέτει ένα μπλοκ διευθύνσεων IPv4 μεγέθους 65K που ξεκινούν με 147.102. Αυτό όμως αντιστοιχεί ένα μεγάλο δίκτυο IPv4 και για διαχειριστικούς λόγους πρέπει να χωρισθεί σε υπο-δίκτυα. Στο IP τα υπο-δίκτυα χρησιμοποιούν μια ομάδα συνεχόμενων διευθύνσεων που το μέγεθός της είναι δύναμη του 2. Αυτό γίνεται με τη βοήθεια της μάσκας υποδικτύου (subnet mask), που δηλώνει το μέρος της διεύθυνσης IP που αντιστοιχεί στο υπο-δίκτυο. Για παράδειγμα, η διεύθυνση 147.102.40.1 είναι κατηγορίας B, με αριθμό δικτύου 147.102 και αριθμό host 40.1. Με μάσκα υποδικτύου 255.255.255.0, τα τρία πρώτα byte αυτής της διεύθυνσης IPv4 είναι διεύθυνση υπο-δικτύου, που δηλώνεται ως 147.102.40.0 (το λογικό AND της μάσκας και της διεύθυνσης IPv4 εκφρασμένες σε bit). Το εναπομένον byte, ο αριθμός 1, είναι ο αριθμός host.

Ο χωρισμός των διευθύνσεων σε κατηγορίες επιτρέπει την ύπαρξη λίγων μεγάλων δικτύων IPv4 (126 δίκτυα class A και 16K δίκτυα class B). Με την ανάπτυξη του διαδικτύου δεν ήταν δυνατόν να οι ικανοποιηθούν οι ανάγκες αριθμοδότητησης νέων δικτύων. Σήμερα, η διάκριση σε ταξικές διευθύνσεις έχει καταργηθεί και αντικατασταθεί από το αταξικό σύστημα CIDR (Classless InterDomain Routing). Αντί της μάσκας χρησιμοποιείται το μήκος προθέματος (prefix length) δικτύου, δηλούμενο ως /xx, όπου xx ακέραιος αριθμός από 0 έως 32. Το xx ορίζει το μήκος σε bit του μέρους της διεύθυνσης IP που αντιστοιχεί σε δίκτυο, δηλαδή, το πρόθεμα (prefix) δικτύου. Έτσι, η διεύθυνση 147.102.40.1/24 υποδηλώνει host με αριθμό 1 και πρόθεμα (υπο-δίκτυο) μήκους 24 bit, που στο αταξικό σύστημα δηλώνεται ως 147.102.40.0/24. Αντίστοιχα, κατά την αναγραφή μιας διεύθυνσης IPv6 υποδεικνύουμε το πρόθεμα δικτύου με τον συμβολισμό CIDR. Για παράδειγμα, μια διεπαφή με IPv6 διεύθυνση 2001:db8:a::123 που συνδέεται στο υποδίκτυο 2001:db8:a::/64 γράφεται ως 2001:db8:a::123/64.

Οι διευθύνσεις μπορούν να τεθούν στατικά από τον ίδιο τον κόμβο (αφού σιγουρευτεί ότι δεν τη χρησιμοποιεί ήδη κάποιος άλλος στο τοπικό δίκτυο), μετά από αντίστοιχο προγραμματισμό από το χρήστη ή μπορεί να «ενοικιάζεται» δυναμικά από εξυπηρετητή DHCP. Ο τελευταίος τρόπος παρουσιάζει προφανές και σημαντικό διαχειριστικό πλεονέκτημα σε ένα δίκτυο, ιδίως αν σ' αυτό μετέχουν πολλοί υπολογιστές. Ο εξυπηρετητής DHCP «μισθώνει» διευθύνσεις IP σε κάρτες δικτύου, καταγράφοντάς τες παράλληλα σε ειδικό πίνακα έτσι ώστε να μη δοθεί ποτέ μία διεύθυνση 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.

Για να είναι εύκολος ο εντοπισμός των διευθύνσεων, σε κάθε περιοχή στο διαδίκτυο (π.χ. ntua.gr) υπάρχει ένας ή περισσότεροι εξυπηρετητές DNS. Αυτοί περιέχουν μια βάση δεδομένων που αντιστοιχίζει τα ονόματα των κόμβων της συγκεκριμένης περιοχής (π.χ. achilles.ntua.gr) σε διευθύνσεις IPv4 και/ή IPv6. Επίσης μπορεί να περιέχει πληροφορίες για τις διευθύνσεις άλλων εξυπηρετητών DNS «υπεύθυνων» για την περιοχή (name servers – NS), διευθύνσεις εξυπηρετητών ηλεκτρονικού ταχυδρομείου (mail exchangers – MX), επίσημα ονόματα υπολογιστών (canonical names – CNAME), κλπ. Οι εξυπηρετητές DNS απαντούν σε αιτήσεις άλλων εξυπηρετητών DNS,

καθώς και χρηστών του διαδικτύου για την αντιστοιχία ενός ονόματος σε διεύθυνση IP και το αντίστροφο, ερευνώντας την παγκόσμια ιεραρχία DNS γι' αυτά.

Διευθύνσεις MAC

Τυπικά οι δικτυακές διεπαφές των κόμβων υλοποιούν κάποια έκδοση του Ethernet. Στο Ethernet κάθε κάρτα δικτύου διαθέτει μία μοναδική φυσική διεύθυνση, αυτήν του υποστρώματος MAC. Έχει μήκος 48 bit ή 6 byte και η δομή της ορίζεται στο πρότυπο IEEE 802. Το πρώτο bit της διεύθυνσης ορίζει το κατά πόσο πρόκειται για Ομαδική (τιμή 1) ή Ατομική (τιμή 0) διεύθυνση. Το δεύτερο bit της διεύθυνσης 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.

Θύρες

Όταν ο ένας υπολογιστής (πελάτης – client) ζητά μια υπηρεσία από τον άλλο (εξυπηρετητής – server), το όνομα και/ή διεύθυνση IP δεν αρκούν. Θα πρέπει με κάποιο τρόπο να υποδειχθεί και η ζητούμενη υπηρεσία[1]. Οι θύρες είναι αριθμοί 16 bit που προσδιορίζουν διεργασίες (εφαρμογές) εντός ενός host. Ονοματίζουν τα λογικά άκρα της επικοινωνίας στο πρωτόκολλο UDP (User Datagram Protocol) ή των συνδέσεων στο πρωτόκολλο TCP (Transmission Control Protocol) μεταξύ δύο υπολογιστών. Πρόκειται για έναν αριθμό μήκους 16 bit, επομένως ορίζονται συνολικά 65536 θύρες (0 έως 65535).

Για να δοθούν υπηρεσίες προς άγνωστους καλούντες (πελάτες), ορίζεται μια θύρα (port) ως σημείο πρώτης επαφής, όπου η εφαρμογή ή ο εξυπηρετητής «ακούει». Οι πρώτες 1024 θύρες (0 έως 1023) θεωρούνται πασίγνωστες (well known ports) και αντιστοιχούν σε γνωστές εφαρμογές. Οι θύρες 1024 έως 49151 χρησιμοποιούνται από διάφορες εφαρμογές, αλλά προηγείται δέσμευσή τους μέσω διαδικασίας εγγραφής (Registered Ports), ενώ οι θύρες 49152 έως 65535 χρησιμοποιούνται ελεύθερα (Dynamic ή Private Ports).Για παράδειγμα, οι εξυπηρετητές ιστού ακούνε συνήθως στη θύρα 80. Έτσι για την επίσκεψη σε μια ιστοσελίδα θα πρέπει να γίνει μια πρώτη επαφή με τον εξυπηρετητή ιστού στη θύρα 80 και να ζητηθεί η συγκεκριμένη σελίδα με το όνομά της. Όμως, εάν η διεύθυνση IP του εξυπηρετητή ιστού δεν είναι γνωστή, θα πρέπει να προηγηθεί μια αίτηση στον τοπικό εξυπηρετητή DNS (που ακούει στη θύρα 53) για την αντιστοίχηση του ονόματος της ιστοθέσης (web site) σε διεύθυνση IP. Για την εξυπηρέτηση της αίτησης μπορεί να γίνουν διαδοχικές ερωτήσεις σε άλλους εξυπηρετητές, ακολουθώντας την παγκόσμια ιεραρχία DNS, με αποτέλεσμα αυξημένη καθυστέρηση. Για την αποφυγή του παραπάνω οι εξυπηρετητές DNS διαθέτουν μια προσωρινή μνήμη (cache) όπου κρατούν τις απαντήσεις στις πιο πρόσφατες αιτήσεις. Τελικά, το λογισμικό του χρήστη μαθαίνει τη διεύθυνση IP της ιστοθέσης (την οποία συνήθως τοποθετεί σε τοπική προσωρινή μνήμη για την περίπτωση που θα τη χρειαστεί και πάλι σύντομα). Για να μεταδώσει πακέτα IP προς τα εκεί, πρέπει να τα περάσει στο στρώμα ζεύξης δεδομένων (data link) της κάρτας δικτύου του, όπου θα ενθυλακωθούν σε πλαίσια προτού μεταδοθούν.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

Άσκηση 1: Βρείτε την κάρτα δικτύου

Αρχικά θα αναζητήσετε πληροφορίες σχετικές με τις δικτυακές ρυθμίσεις του προσωπικού σας υπολογιστή. Οι πληροφορίες αυτές μπορούν να αντληθούν είτε από το γραφικό περιβάλλον του υπολογιστή σας είτε μέσω εντολών φλοιού (shell) σε παράθυρο γραμμής εντολών (command line

[1] Ένας υπολογιστής μπορεί να είναι ταυτόχρονα πελάτης και εξυπηρετητής

interface). Ο τρόπος ανεύρεσης εξαρτάται από το λειτουργικό σύστημα που χρησιμοποιείτε. Για το λόγο αυτό να είστε προετοιμασμένοι να αναζητήσετε βοήθεια στο περιβάλλον του λειτουργικού σας συστήματος είτε στο διαδίκτυο.

Χρησιμοποιώντας το γραφικό περιβάλλον του προσωπικού σας υπολογιστή ή εντολές φλοιού, όντας συνδεδεμένοι στο διαδίκτυο, βρείτε και καταγράψτε τον τρόπο με τον οποίο βρήκατε:

1.1 Την ονομασία της κάρτας δικτύου (network adapter) μέσω της οποίας συνδέστε στο διαδίκτυο.
1.2 Το είδος της σύνδεσης, ενσύρματη (Ethernet) ή ασύρματη (WiFi).
1.3 Την ταχύτητα σύνδεσης αυτής σε Mbps.
1.4 Τη διεύθυνση υπο-στρώματος MAC σε δεκαεξαδική μορφή. ***[Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]***
1.5 Τη διεύθυνση IPv4 της διεπαφής Ethernet ή WiFi του υπολογιστή σας. ***[Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]***
1.6 Εάν έχει ορισθεί, τη διεύθυνση IPv6 της διεπαφής Ethernet ή WiFi του υπολογιστή σας;
1.7 Τη διεύθυνση IPv4/IPv6 του εξυπηρετητή DNS.
1.8 Τη διεύθυνση IPv4 της προκαθορισμένης πύλης (default gateway/route).

Άσκηση 2: Ρυθμίσεις και στατιστικά

Στη συνέχεια θα αντλήσετε αντίστοιχα στοιχεία σχετικά με τις παραμέτρους δικτύωσης του υπολογιστή σας μέσω εντολών φλοιού. Οι συγκεκριμένες εντολές εξαρτώνται από το λειτουρικό σύστημα και χρησιμεύουν τόσο για να δείτε όσο και για να ρυθμίσετε τις παραμέτρους δικτύωσης. Σε περιβάλλον Unix/Linux χρήσιμες τέτοιες εντολές φλοιού είναι οι hostname, ifconfig και netstat. Σε περιβάλλον Windows οι εντολές hostname, ipconfig, και netstat παρέχουν αντίστοιχη πληροφόρηση, αν και δεν έχουν ακριβώς την ίδια λειτουργικότητα. Σε νεώτερες εκδόσεις του Linux οι εντολές ip και ss μεταξύ άλλων επιτελούν λειτουργίες ανάλογες των ifconfig και netstat. Δείτε περισσότερες πληροφορίες στις ιστοσελίδες https://en.wikipedia.org/wiki/Ifconfig, https://en.wikipedia.org/wiki/Netstat και https://en.wikipedia.org/wiki/Iproute2.

Χρησιμοποιώντας εντολές φλοιού σε παράθυρο εντολών γραμμής του λειτουργικού σας συστήματος βρείτε τις πληροφορίες που ζητούνται παρακάτω. Μαζί με την απάντησή να καταγράψετε την ***ακριβή*** σύνταξη της εντολής[2] φλοιού που χρησιμοποιήσατε.

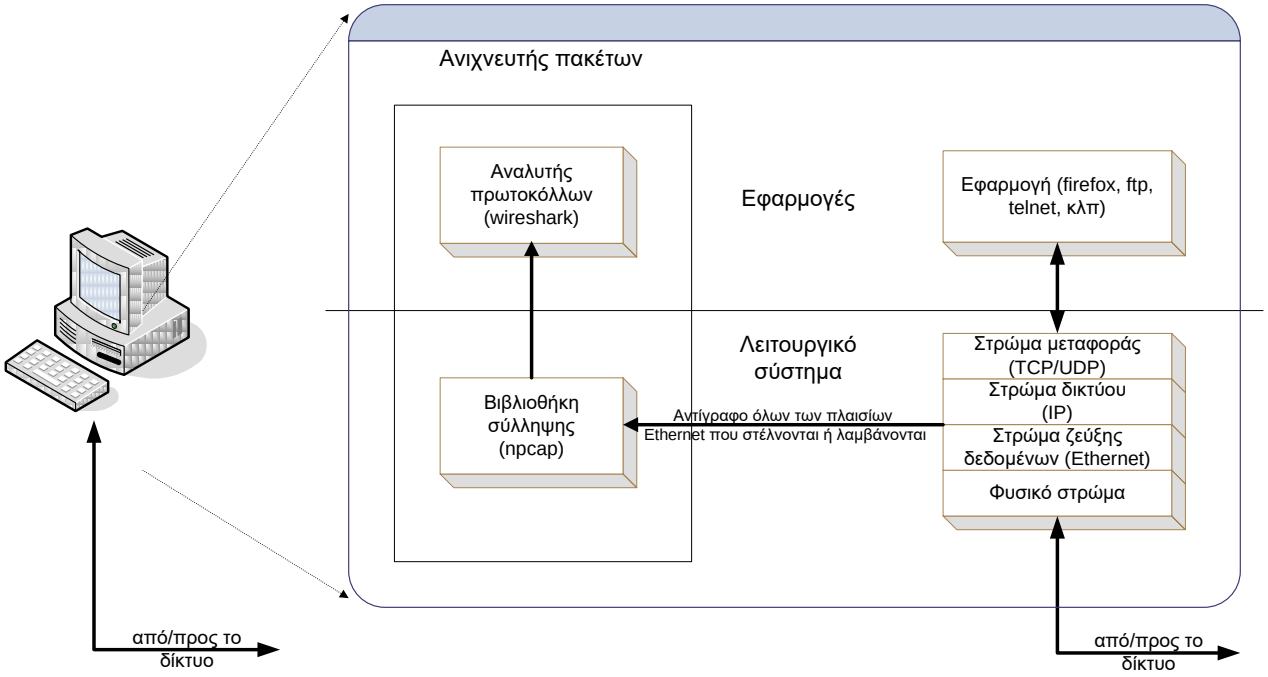
2.1 Το όνομα του υπολογιστή σας. ***[Συμπληρώστε το όνομα μαζί με το είδος λειτουργικού συστήματος το αντίστοιχο πεδίο της επικεφαλίδας του φύλλου απαντήσεων.]***
2.2 Τα ονόματα των καρτών δικτύου (φυσικών και/ή εικονικών) που διαθέτει ο υπολογιστής;
2.3 Τη διεύθυνση υπο-στρώματος MAC της κάρτας δικτύου μέσω της οποίας συνδέστε στο διαδίκτυο.
2.4 Την ταχύτητα σύνδεσης αυτής σε Mbps.
2.5 Τη διεύθυνση IPv4 της διεπαφής Ethernet ή WiFi του υπολογιστή σας.
2.6 Τη μάσκα υποδικτύου και χωρίς την εκτέλεση επιπλέον εντολών:
  i. το μέγεθος σε bit του τμήματος δικτύου της διεύθυνσης IP του υπολογιστή σας, και
  ii. τη διεύθυνση του υποδικτύου.
2.7 Εάν έχει ορισθεί, τη διεύθυνση IPv6 της διεπαφής Ethernet ή WiFi του υπολογιστή σας.
2.8 Τη διεύθυνση IPv4/IPv6 της προκαθορισμένης πύλης (default gateway). *[Υπόδειξη: Στο οικιακό περιβάλλον προκαθορισμένη πύλη είναι ο δρομολογητής (router).]*
2.9 Τη διεύθυνση IPv4/IPv6 των εξυπηρετητών DNS.
2.10 Τη διεύθυνση IPv4 του εξυπηρετητή DHCP. *[Υπόδειξη: Στο οικιακό περιβάλλον τυπικά ταυτίζεται με τον δρομολογητή.]*

[2] Μελετήστε προσεκτικά τη βοήθεια (help) των σχετικών εντολών και ανατρέξτε στην τεκμηρίωση του λειτουργικού σας συστήματος για περισσότερες πληροφορίες.

2.11 Τον αριθμό πλαισίων Ethernet (πακέτων) και το πλήθος byte που έστειλε και έλαβε η κάρτα δικτύου του υπολογιστή σας.
2.12 Τον αριθμό πακέτων IPv4 που έστειλε και έλαβε η κάρτα δικτύου του υπολογιστής σας.
2.13 Τον αριθμό εγκατεστημένων (established) συνδέσεων TCP του υπολογιστή σας με άλλους υπολογιστές. *[Υπόδειξη. Η διεύθυνση 127.0.0.1 είναι ο ίδιος ο υπολογιστής σας.]*
2.14 Για δύο από τις παραπάνω συνδέσεις TCP, τις θύρες πηγής και προορισμού.

Άσκηση 3: Αναλυτής Πρωτοκόλλων Wireshark

Οι βασικές λειτουργίες ενός ανιχνευτή πακέτων (packet sniffer) είναι: α) η καταγραφή – σύλληψη (capture) και β) η ανάλυση της δικτυακής κίνησης του υπολογιστή. Ο ρόλος του είναι παθητικός, με την έννοια ότι απλά παρατηρεί τα πακέτα που στέλνονται και λαμβάνονται από την κάρτα δικτύου, χωρίς ο ίδιος να παράγει δικτυακή κίνηση. Στο σχήμα φαίνεται η τυπική δομή ενός ανιχνευτή πακέτων στην περίπτωση υπολογιστή με μία κάρτα Ethernet. Βλέπετε τη στοίβα πρωτοκόλλων TCP/IP, καθώς επίσης, και διάφορες συνήθεις δικτυακές εφαρμογές που εκτελούνται σε ένα υπολογιστή, όπως ένας πλοηγός ιστού ή πελάτης FTP.



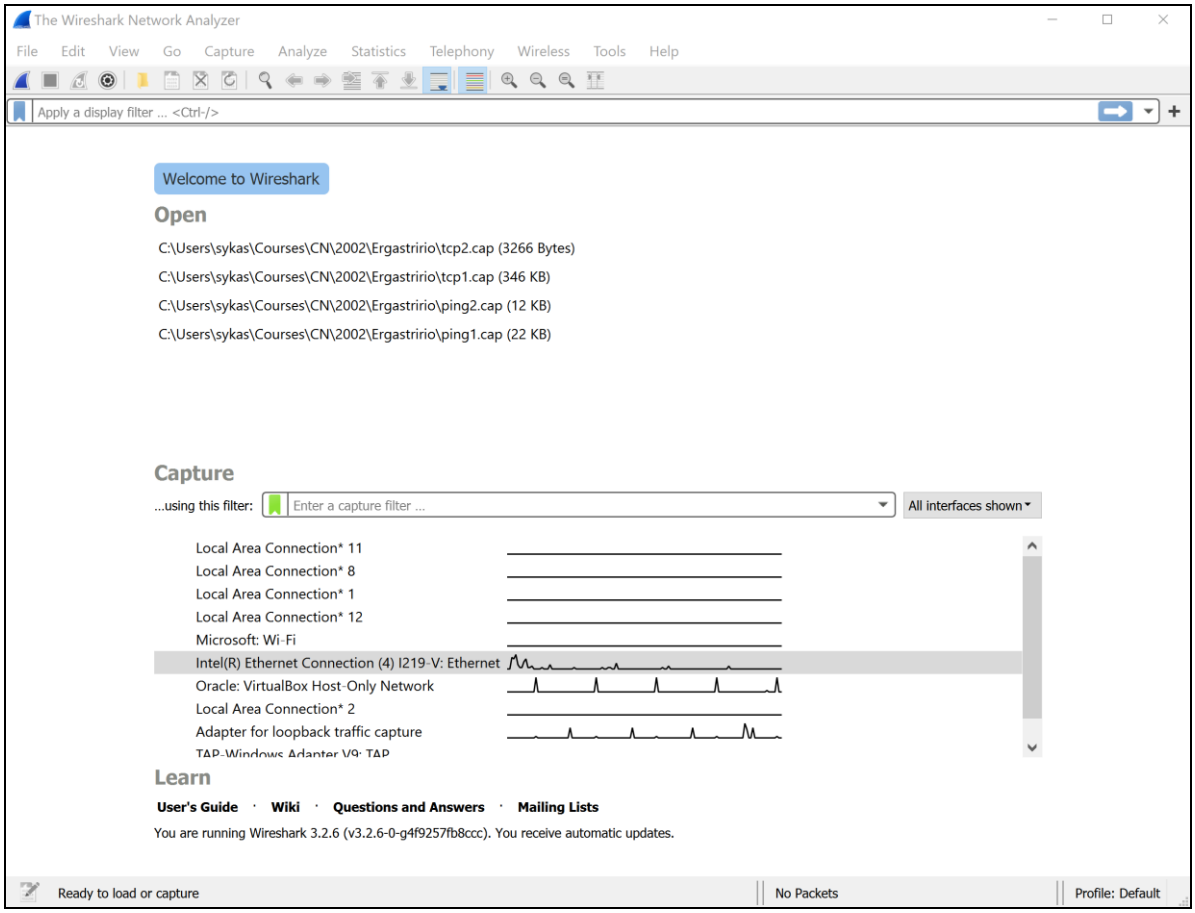
Ο ανιχνευτής πακέτων, που παριστάνεται με το διαγραμμισμένο πλαίσιο στο σχήμα, αποτελεί προσθήκη στο λογισμικό συστήματος και αποτελείται από δύο τμήματα: α) τη βιβλιοθήκη σύλληψης και β) τον αναλυτή πρωτοκόλλων. Η λειτουργία της σύλληψης συνίσταται στην αντιγραφή των πλαισίων (frames), που στέλνονται ή λαμβάνονται από την κάρτα δικτύου, από μια βιβλιοθήκη pcap στον πυρήνα του λειτουργικού συστήματος και τη διάθεσή τους σε εφαρμογές χρήστη. Τα πλαίσια ανήκουν στο επίπεδο ζεύξης δεδομένων του προτύπου OSI και περιέχουν πακέτα[3] του στρώματος δικτύου με ενθυλακωμένα μηνύματα πρωτοκόλλων ανώτερων στρωμάτων. Το δεύτερο τμήμα του ανιχνευτή πακέτων, ο αναλυτής πρωτοκόλλων, αποκωδικοποιεί και εμφανίζει τα περιεχόμενα των πλαισίων. Για τον σκοπό αυτό, πρέπει να γνωρίζει τη δομή των μηνυμάτων *όλων* των πρωτοκόλλων. Για παράδειγμα, στην περίπτωση ενός μηνύματος HTTP, απαιτείται, κατ' αρχήν, 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

[3] Οι όροι «πλαίσιο» (frame) και «πακέτο» (packet), δεν είναι ταυτόσημοι αλλά χρησιμοποιούνται πολλές φορές ο ένας αντί του άλλου.

του μηνύματος HTTP, ενώ περαιτέρω ανάλυση οδηγεί στο συγκεκριμένο τύπο του μηνύματος HTTP, δηλαδή GET, POST κ.ά.

Η άσκηση αυτή αποτελεί εισαγωγή στη χρήση του Wireshark, ενός αναλυτή πρωτοκόλλων που διατίθεται ως ανοικτό λογισμικό (https://www.wireshark.org/) σε πληθώρα λειτουργικών συστημάτων. Θα το εγκαταστήσετε στον προσωπικό σας υπολογιστή κατεβάζοντας, ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείτε, το αντίστοιχο αρχείο από την ιστοσελίδα https://www.wireshark.org/download.html. Μέρος της αρχικής εγκατάστασης του Wireshark είναι και η εγκατάσταση της κατάλληλης βιβλιοθήκης σύλληψης (pcap) ανάλογα με το λειτουργικό σύστημα. Για να λειτουργήσει το Wireshark η βιβλιοθήκη σύλληψης πακέτων pcap πρέπει να έχει δικαιώματα διαχειριστή συστήματος. Στα Windows χρησιμοποιείται η βιβλιοθήκη Npcap, δείτε περισσότερα στην ιστοσελίδα https://nmap.org/npcap/, αντικαταστάτης της WinPcap, η ανάπτυξη της οποίας τερματίστηκε, δείτε https://www.winpcap.org/, και η οποία με τη σειρά της ήταν μεταφορά της libpcap που χρησιμοποιείται σε συστήματα Unix, δείτε https://www.tcpdump.org/. Περισσότερες πληροφορίες σχετικά με τον αναλυτή πρωτοκόλλων Wireshark μπορείτε να βρείτε στην ιστοσελίδα https://www.wireshark.org/docs/ όπου υπάρχουν σύνδεσμοι για το εγχειρίδιο χρήσης σε διάφορες μορφές (html, pdf, κλπ) καθώς και στην ιστοσελίδα https://www.wireshark.org/faq.html σε περίπτωση που συναντήσετε δυσκολίες.

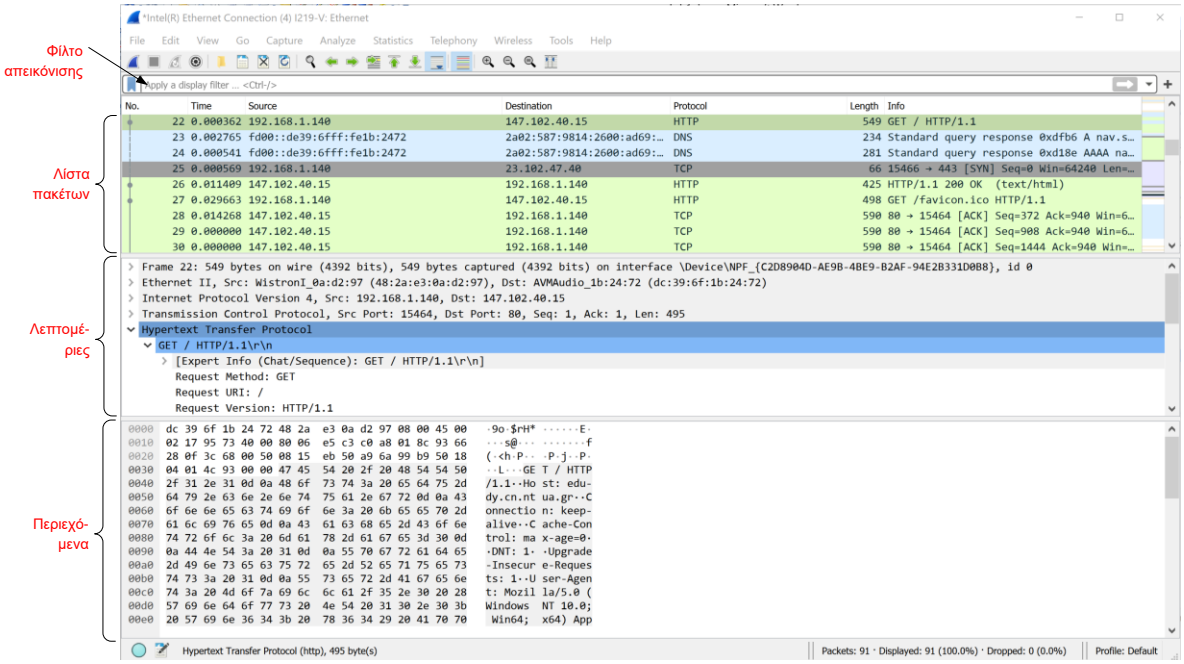
Όταν ξεκινήσετε το Wireshark θα εμφανισθεί το ένα γραφικό περιβάλλον όπως το ακόλουθο[4].



Στο άνω μέρος υπάρχει το μενού των διαθέσιμων εντολών για την έναρξη διαφόρων λειτουργιών, η κύρια εργαλειοθήκη (main toolbar) με συντομεύσεις για τις πιο συχνά χρησιμοποιούμενες εντολές του μενού καθώς και το πεδίο ορισμού φίλτρων απεικόνισης. Το κάτω μέρος χωρίζεται σε τρεις περιοχές. Η πρώτη περιοχή (Open) περιέχει τη λίστα πρόσφατων αρχείων καταγραφής που έχει ανοίξει ο χρήστης. Η τρίτη περιοχή (Learn) περιέχει χρήσιμους συνδέσμους για γρήγορη πρόσβαση στις οδηγίες χρήσης. Το μεγαλύτερο ενδιαφέρον παρουσιάζει η δεύτερη (κεντρική) περιοχή όπου

[4] Σε παλαιότερες εκδόσεις του Wireshark η αρχική σελίδα είναι διαφορετική, παρέχει όμως την ίδια λειτουργικότητα.

εμφανίζονται σε μορφή λίστας οι κάρτες δικτύου του υπολογιστή σας καθώς και το πεδίο ορισμού φίλτρων σύλληψης[5]. Εκεί μπορείτε να επιλέξετε την επιθυμητή κάρτα καθώς και να ορίσετε τα αντίστοιχα φίλτρα σύλληψης. Η καταγραφή ξεκινά με κλικ στο μπλε σύμβολο (Start capturing packets) της εργαλειοθήκης, είτε με διπλό κλικ στην γραμμή της κάρτας δικτύου είτε με δεξί κλικ και Start capture. Εναλλακτικά, μπορείτε να επιλέξετε τις επιθυμητές διεπαφές και φίλτρα από τη διαδρομή *Capture → Options…* στο μενού και η καταγραφή θα ξεκινήσει πατώντας το *Start*. Αμέσως μετά θα παρουσιαστεί το κύριο γραφικό περιβάλλον του Wireshark με τα πακέτα που συλλαμβάνονται να εμφανίζονται σε πραγματικό χρόνο υπό τη μορφή κυλιόμενης λίστας πακέτων. Μπορείτε να σταματήσετε την καταγραφή είτε κάνοντας κλικ στο κόκκινο σύμβολο (Stop capturing packets) της εργαλειοθήκης, είτε ακολουθώντας από το μενού τη διαδρομή *Capture → Stop…* είτε πληκτρολογώντας Ctrl+E.



Στο σχήμα φαίνεται γραφικό περιβάλλον του Wireshark μετά το τέλος μιας καταγραφής. Μπορείτε να διακρίνετε τέσσερα βασικά μέρη:

- Το πεδίο όπου μπορεί να οριστεί το **φίλτρο απεικόνισης (display filter)**. Κάνοντας κλικ στο *Apply* εφαρμόζετε το φίλτρο απεικόνισης και στο επόμενο παράθυρο εμφανίζονται τα πλαίσια που σας ενδιαφέρουν ενώ αποκρύπτονται τα υπόλοιπα.
- Το παράθυρο με τη **λίστα πακέτων (packet list)**, όπου εμφανίζονται περιληπτικές πληροφορίες για τα καταγεγραμμένα πακέτα. 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 (packet details)**, όπου εμφανίζονται περισσότερες πληροφορίες σχετικά με την ενθυλάκωση των πρωτοκόλλων στο επιλεγμένο πακέτο από τη λίστα. Στο παράθυρο εμφανίζονται, ένα ανά γραμμή, όλα τα πρωτόκολλα που περιλαμβάνει το πλαίσιο με τη σειρά ενθυλάκωσής τους καθώς και άλλες σχετικές πληροφορίες που προσθέτει το Wireshark. Τα περιεχόμενα των επικεφαλίδων μπορούν να αντληθούν πατώντας το σύμβολο '>' οπότε αναπτύσσονται οι επικεφαλίδες του εκάστοτε πρωτοκόλλου. Κάνοντας κλικ σε κάποια γραμμή ελέγχετε το τι θα εμφανισθεί με υπογραμμισμένο (highlighted) στο επόμενο παράθυρο.

[5] Σύμφωνα με την ορολογία του Wireshark διακρίνουμε τα *capture* και τα *display filters*. Ο χρήστης μέσω των φίλτρων σύλληψης/απεικόνισης περιορίζει σύμφωνα με τα κριτήριά του την κίνηση που καταγράφεται/απεικονίζεται.

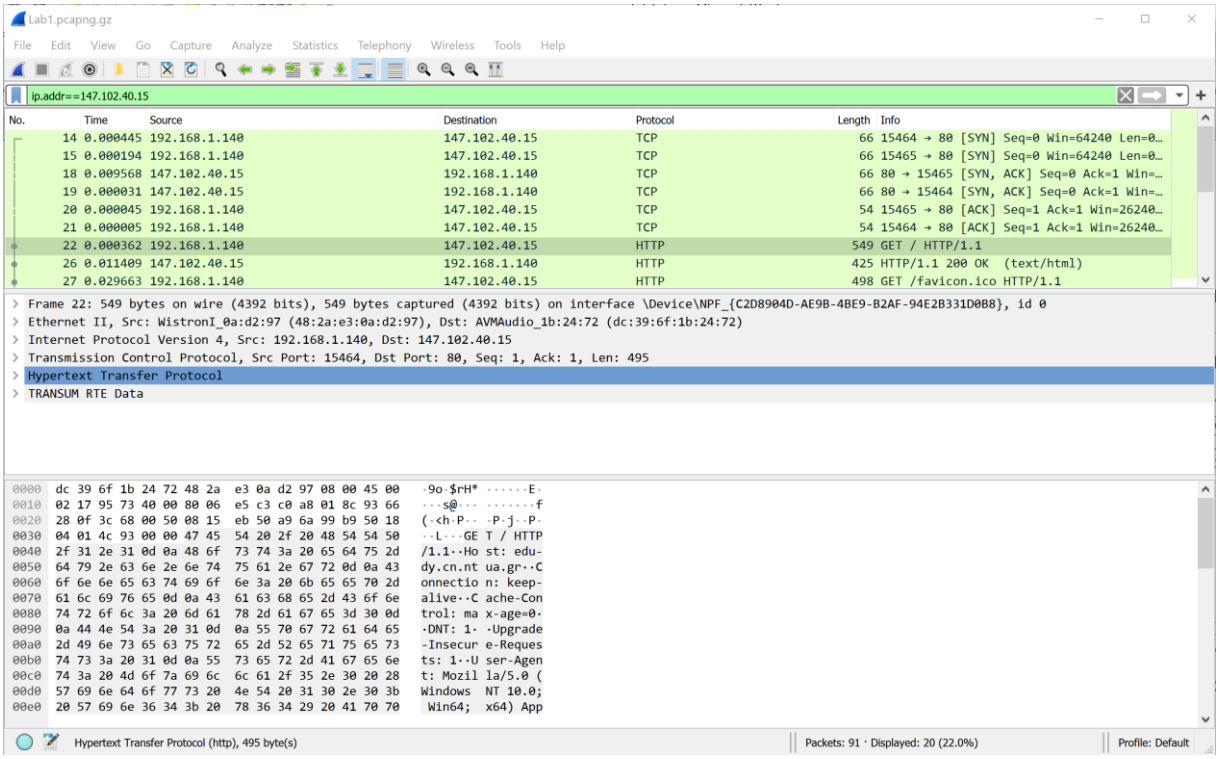
- Το παράθυρο με τα **περιεχόμενα (packet bytes)** εμφανίζει σε δεκαεξαδική μορφή και μορφή ASCII όλα τα byte του επιλεγμένου πακέτου με υπογραμμισμένα τα byte που αντιστοιχούν στις επικεφαλίδες του επιλεγμένου πρωτόκολλο στο παράθυρο με τις λεπτομέρειες.

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 σε μια ιστοσελίδα. Ανοίξτε πρώτα τον φυλλομετρητή της αρεσκείας σας και από το σχετικό μενού εκκαθαρίστε την προσωρινή του μνήμη (cache). Μετά ξεκινήσετε μια καταγραφή στο Wireshark επιλέγοντας τη διεπαφή της κάρτας δικτύου του υπολογιστή σας με την οποία συνδέεστε στο διαδίκτυο. Επισκεφτείτε την ιστοσελίδα http://edu-dy.cn.ntua.gr και μόλις αυτή φορτωθεί πλήρως σταματήστε την καταγραφή. Στο κύριο παράθυρο του Wireshark φαίνεται η καταγεγραμμένη δικτυακή κίνηση. Στη λίστα πακέτων και κάτω από την επικεφαλίδα Protocol εμφανίζεται το εκάστοτε πρωτόκολλο υψηλότερου στρώματος που περιέχει το κάθε πλαίσιο. Κάνοντας κλικ στην επικεφαλίδα Protocol, τα πλαίσια θα ταξινομηθούν ανά είδος πρωτοκόλλου. Παρατηρήστε ότι η αύξουσα (ή φθίνουσα) σειρά ταξινόμησης υποδηλώνεται με ένα μικρό βέλος προς τα πάνω ή κάτω.

3.1 Καταγράψτε τα διαφορετικά πρωτόκολλα που εμφανίζονται στη λίστα.

Στη λίστα πακέτων περιλαμβάνεται κίνηση που δε σχετίζεται με την επίσκεψη στην ιστοσελίδα. Τα πακέτα που ανταλλάχθηκαν με τον εξυπηρετητή ιστού edu-dy.cn.ntua.gr μπορεί να απομονωθούν με την εφαρμογή φίλτρου απεικόνισης. Στο αντίστοιχο πεδίο του κυρίου παραθύρου του Wireshak γράψτε την έκφραση ip.addr==147.102.40.15. Εάν η σύνταξη της έκφρασης είναι σωστή το πεδίο θα χρωματισθεί πράσινο, όπως στο παρακάτω σχήμα, αλλιώς θα είναι ροζ. Πατήστε το πλήκτρο Enter για να εφαρμοσθεί το φίλτρο που μόλις ορίσατε. Θα διαπιστώσετε ότι η κίνηση είναι περιορισμένη σε σχέση με την παρατήρηση χωρίς φίλτρο.



Ταξινομήστε και πάλι τα πλαίσια με αύξουσα αριθμητική σειρά και εντοπίστε το πρώτο μήνυμα HTTP με την εντολή GET που έστειλε ο υπολογιστής σας για να κατεβάσει τη σελίδα καθώς και την αντίστοιχη απόκριση 200 OK του εξυπηρετητή. Με βάση τα στοιχεία της καταγραφής σας απαντήστε τις επόμενες ερωτήσεις.

3.2 Ποια είναι η διεύθυνση MAC του υπολογιστή σας σε δεκαεξαδική μορφή;

3.3 Ποιος είναι ο κατασκευαστής της κάρτας δικτύου; *[Υπόδειξη: Δείτε επικεφαλίδες πλαισίου Ethernet.]*
3.4 Ποια είναι η διεύθυνση IPv4 του υπολογιστή σας;
3.5 Ποια είναι η διεύθυνση IPv4 του edu-dy.cn.ntua.gr;

Στη συνέχεια τοποθετήστε τον δείκτη (pointer) στο πρώτο πλαίσιο που περιέχει τεμάχιο TCP. Με δεξί κλικ θα εμφανισθεί ένα μενού εντολών σχετικών με ενέργειες που μπορείτε να κάνετε. Επιλέξτε το *Follow → TCP Stream*. Στην οθόνη που θα εμφανισθεί βλέπετε το περιεχόμενο της συγκεκριμένης ροής TCP, δηλαδή, την ανταλλαγή μηνυμάτων HTTP μεταξύ του φυλλομετρητή και του εξυπηρετητή ιστού. Τα μηνύματα (εντολές) του φυλλομετρητή 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 Ποια είναι η σύνταξη του φίλτρου που εμφανίζεται τώρα στο πεδίο του φίλτρου απεικόνισης;
3.7 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 φυλλομετρητή εμφανίζεται αυτός ο τίτλος;
3.8 Με εφαρμογή κατάλληλου φίλτρου εμφανίστε τώρα μόνο τα μηνύματα HTTP. Ποια είναι η σύνταξή του;
3.9 Πόσα μηνύματα HTTP στάλθηκαν και πόσα λήφθηκαν;
3.10 Πόσος χρόνος πέρασε από τη στιγμή που στάλθηκε το πρώτο αίτημα GET μέχρι να ληφθεί η απόκριση 200 OK; *[Υπόδειξη: Από το μενού View επιλέξτε Time Display Format → Seconds Since Previous Displayed Packet.]*

Με το δεύτερο αίτημα GET ζητείται το κατέβασμα της εικόνας favicon.ico. Το μέγεθός της είναι αρκετά μεγάλο με αποτέλεσμα η απόκριση να μην χωρά σε ένα πακέτο IPv4 και να πρέπει να αποσταλούν περισσότερα του ενός ώστε να ολοκληρωθεί η μετάδοσή της. Το Wireshark το αντιλαμβάνεται κατά την αποκωδικοποίηση και εμφανίζει το πλήρες αποκωδικοποιημένο μήνυμα HTTP και το μέγεθός του στο Reassembled TCP tab μαζί με το τελευταίο πλαίσιο και αντίστοιχο μέγεθος πλαισίου στο Frame tab.

3.11 Πόσα πακέτα χρειάστηκαν για την ολοκλήρωση της μετάδοσης;
3.12 Πόσος χρόνος πέρασε μέχρι να ληφθεί το πρώτο εξ αυτών, πόσος από την προηγούμενη στιγμή μέχρι να ολοκληρωθεί η μετάδοση των επόμενων και πόσος για να ολοκληρωθεί η

απόκριση στο αίτημα GET; *[Υπόδειξη: Ακυρώστε το φίλτρο απεικόνισης και αναζητήστε τα τεμάχια TCP.]*

Το Wireshark μπορεί να υπολογίζει αυτόματα τους χρόνους απόκρισης που σχετίζονται με τη λειτουργία διαφόρων πρωτοκόλλων. Από το κεντρικό μενού, διαδρομή *Analyze → Enabled Protocols…*, αναζητήστε TRANSUM και ενεργοποιήστε το. Στη συνέχεια, επιλέξτε το πλαίσιο με το δεύτερο GET και αναπτύξτε την τελευταία γραμμή TRANSUM RTE Data στο παράθυρο με τις λεπτομέρειες. Αυτή δεν αντιστοιχεί στα δεδομένα κάποιου πρωτοκόλλου, αλλά αποτελεί πληροφορία που έχει εξάγει το Wireshark κατά την ανάλυση.

3.13 Συγκρίνατε τους χρόνους Service Time, Response Spread και Application PDU (APDU) Response Time με αυτούς που καταγράψατε προηγουμένως.

3.14 Θέλετε τώρα να δείτε μόνο τα μηνύματα HTTP που έστειλε ο υπολογιστής σας. Ποια είναι η σύνταξή του; *[Υπόδειξη: Θα πρέπει να σχηματίσετε μια έκφραση με τον λογικό τελεστή ΚΑΙ (and ή &&) εμπλέκοντας και τη διεύθυνση IPv4 πηγής αυτών.]*

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

Εργαστηριακή Άσκηση 1
Αναλυτής Πρωτοκόλλων Wireshark

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 .....

.....

Άσκηση 3