



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**Εποπτεία δικτύου Ethernet με χρήση Packet Sniffer και ανάλυση της
κίνησης σε επίπεδο πακέτων**

Ρέγγας Λυμπέρης
(Αρ. Μητρώου ais0068)

Εισηγήτρια: Αναστασία Βελώνη, Λέκτορας Εφαρμογών

ΑΘΗΝΑ
ΙΟΥΝΙΟΣ 2018

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εποπτεία δικτύου Ethernet με χρήση Packet Sniffer και ανάλυση της κίνησης σε επίπεδο πακέτων

Λυμπέρης Π. Ρέγγας
(Αρ. Μητρώου ais0068)

Εισηγήτρια:

Αναστασία Βελώνη, Λέκτορας Εφαρμογών

Εξεταστική Επιτροπή:

Ιωάννης Έλληνας, Καθηγητής

Αναστασία Βελώνη, Λέκτορας Εφαρμογών

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Λυμπέρης Ρέγγας του Παναγιώτη, με αριθμό μητρώου ais0068, φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «Εφαρμοσμένα Πληροφοριακά Συστήματα» του Πανεπιστημίου Δυτικής Αττικής, πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

ΕΥΧΑΡΙΣΤΙΕΣ

Στην αρχή κάθε εγχειρήματος, όσο δύσκολο και να είναι, ο τελικός στόχος φαίνεται μακρινός. Στο τέλος κάθε εγχειρήματος υπάρχει η ικανοποίηση της επίτευξης του τελικού στόχου και η απολαβή των συγχαρητηρίων, η βαρύτητα των οποίων μεγαλώνει όσο ο στόχος είναι (αντικειμενικά ή υποκειμενικά) δυσκολότερος. Όμως, αυτό που έχει μείνει σε αυτόν που επιτελεί το εγχείρημα και στους ανθρώπους με τους οποίους συναναστρέφεται καθημερινά, είναι η διαδρομή. Η διαδρομή που έχει διαγραφεί από την αρχή μέχρι το τέλος είναι οι πολλές επιμέρους, μικρές, καθημερινές μάχες που δίνεις, καταρχήν με τον εαυτό σου και έπειτα με τους κοντινούς σου ανθρώπους και είναι γεμάτη από συναισθήματα, καλά και άσχημα, ικανοποίηση και γκρίνια, ξενύχτια και στερήσεις, χαλιά που μαζεύεις τον Αύγουστο, βόλτες με την οικογένεια που μετατίθενται συνεχώς, φίλοι και συγγενείς τους οποίους δεν έχεις «χρόνο» να δεις και ένα μόνιμο αίσθημα ότι «...υπάρχει κάτι που εκκρεμεί και πρέπει να γίνει γιατί τελειώνει ο χρόνος και πάλι δεν θα προλάβω...». Τελικά, ίσως η μεγαλύτερη ικανοποίηση είναι η στιγμή που θα τελειώσουν όλα με επιτυχία και εσύ, μόνος με τον εαυτό σου, θα πάρεις μια βαθιά ανάσα και θα σκεφθείς «πάει και αυτό, τελείωσε, γυρνάω πίσω στην κανονική ζωή...».

Θέλω να ευχαριστήσω από καρδιάς τους συνοδοιπόρους (και συμπάσχοντες) σε αυτή την προσπάθεια, καταρχήν την σύζυγό μου Δώρα και έπειτα τα παιδιά μου Παναγιώτη και Σταύρο, για την συμπαράσταση και την υπομονή που έδειξαν σε όλη αυτή τη διαδρομή, για τις θυσίες που έκαναν και τις στερήσεις που υπέστησαν.

Επίσης, θέλω να ευχαριστήσω όλους αυτούς που δυσκόλεψαν αυτό το έργο γιατί με έκαναν πιο πεισματάρη και πιο δυνατό.

Τέλος, θα ήθελα να ευχαριστήσω τους καθηγητές για όσα μου δίδαξαν αλλά περισσότερο για την αμέριστη συμπαράσταση και υπομονή που έδειξαν σε όλη αυτή την διαδρομή.

Σας ευχαριστώ όλους!

Το έργο αυτό αφιερώνεται στον Πατέρα μου Παναγιώτη. Είμαι βέβαιος ότι θα χαίρεται όταν θα με βλέπει από εκεί, ψηλά, που βρίσκεται...

ΠΕΡΙΛΗΨΗ

Στις μέρες μας ένα δίκτυο υπολογιστικών συσκευών, όπου και εάν βρίσκεται ανεπτυγμένο, ενσύρματο ή ασύρματο, είτε είναι ένα απλό οικιακό δίκτυο είτε ένα εταιρικό όπου συνδέονται εκατοντάδες χρήστες, αποτελεί από μόνο του ένα περίπλοκο σύστημα διακίνησης δεδομένων. Επιπλέον, οι συσκευές που συνδέονται σε αυτό είναι πλέον τόσες πολλές και τόσο διαφορετικές μεταξύ τους (υπολογιστές, τηλεοράσεις, κλιματιστικά κ.τ.λ.) με αποτέλεσμα να δυσκολεύει ακόμα περισσότερο, κατ' αρχήν την κατανόηση, και ακολούθως την εποπτεία και η επιτήρησή του.

Αντικείμενο της παρούσας εργασίας είναι η δημιουργία ενός εγχειριδίου με το οποίο θα είναι δυνατή η εύκολη κατανόηση της δομής των διακινούμενων δεδομένων ενώ παράλληλα θα είναι δυνατή, αρχικά, η καταγραφή της κίνησής τους και σε δεύτερο χρόνο η επεξεργασία τους και η εξαγωγή των ζητούμενων συμπερασμάτων. Τα εργαλεία που θα χρησιμοποιηθούν είναι ένας παθητικός «ακροατής δεδομένων» (Packet Sniffer) και το λογισμικό καταγραφής και επεξεργασίας πακέτων Wireshark.

Η δομή του εγχειριδίου βασίζεται στην συσχέτιση κάθε επιπέδου του μοντέλου OSI με κάθε επίπεδο καταγραφής του λογισμικού Wireshark, με την παράθεση των σχετικών πρωτοκόλλων που κατανέμονται σε αυτό. Για κάθε επίπεδο θα υπάρχει αναλυτική επεξήγηση της χρησιμοποιούμενης μεθοδολογίας για την εξαγωγή των ζητούμενων αποτελεσμάτων.

Η χρησιμότητα της παρούσας εργασίας είναι η εύκολη εφαρμογή της υποδεικνυόμενης μεθοδολογίας στις περιπτώσεις που χρειάζεται άμεση και αναλυτική κατανόηση της συμπεριφοράς ενός δικτύου και των συνδεδεμένων σε αυτό συσκευών.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ

Δίκτυα υπολογιστικών συσκευών, Κυβερνοασφάλεια, Επίλυση προβλημάτων σε δίκτυο

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Ακρόαση πακέτων, Wireshark, Παθητική παγίδα δικτύου, Ανάλυση πακέτων

ABSTRACT

Nowadays, a network of computing devices, whether developed, wired or wireless, whether it's a simple home network or a business network which are connected hundreds of users, is in itself a complicated data-handling system. In addition, the devices connected to this network are so many and so different between them (computers, televisions, air conditioners, etc.), making it even more difficult to understand, to supervise and to monitor it.

The purpose of this paper is to create a user manual which will help to easy comprehension of the structure of the traffic data, while at the same time it will be possible, first, to record the network traffic and then to process them and to extract the desired conclusions. The tools to be used are a passive Packet Sniffer and a packet logging and processing software named Wireshark.

The structure of the manual is based on the correlation of each level of the OSI model with each capture level of Wireshark software, by listing the relevant protocols allocated to it. For each level there will be a detailed explanation of the methodology used to export the desired results.

The usefulness of this paper is the easy implementation of the indicated methodology in cases where the need is the fast and detailed understanding of the behavior of a network and its connected devices.

SCIENTIFIC AREA

Computer networks, Cyber security, Network troubleshooting and debugging

KEY WORDS

Packet sniffing, Wireshark, Passive network tap, Packet analysis

ΠΕΡΙΕΧΟΜΕΝΑ

Πίνακας περιεχομένων

1	ΚΕΦΑΛΑΙΟ 1ο: ΕΙΣΑΓΩΓΗ	19
1.1	Περιγραφή του αντικειμένου της πτυχιακής εργασίας	19
1.2	Δομή της πτυχιακής εργασίας και μεθοδολογία λειτουργίας	19
2	ΚΕΦΑΛΑΙΟ 2ο: ΑΚΡΟΑΤΕΣ ΠΑΚΕΤΩΝ	21
2.1	Γενική περιγραφή.....	21
2.2	Ορισμός ενός συστήματος Ακρόασης Πακέτων	22
2.3	Τοπολογίες συνδεσμολογίας Ακρόασης Πακέτων	23
2.4	Κατηγορίες Ακροατών Πακέτων.....	24
2.5	Παραδείγματα Ακροατών Πακέτων	24
3	ΚΕΦΑΛΑΙΟ 3ο: ΤΟ ΜΟΝΤΕΛΟ OSI	27
3.1	Γενική περιγραφή.....	27
3.2	Επίπεδο 7: Το επίπεδο Εφαρμογών.....	29
3.3	Επίπεδο 6: Το επίπεδο Παρουσίασης.....	30
3.4	Επίπεδο 5: Το επίπεδο Συνόδου	30
3.5	Επίπεδο 4: Το επίπεδο Μεταφοράς.....	30
3.6	Επίπεδο 3: Το επίπεδο Δικτύου.....	30
3.7	Επίπεδο 2: Το επίπεδο Ζεύξης Δεδομένων	31
3.8	Επίπεδο 1: Το Φυσικό επίπεδο.....	31
4	ΚΕΦΑΛΑΙΟ 4ο: WIRESHARK.....	33
4.1	Γενική περιγραφή.....	33
4.2	Το περιβάλλον λειτουργίας του Wireshark	34
4.3	Η γραμμή λειτουργιών (menu) του Wireshark.....	35
4.4	Η κύρια γραμμή εργαλείων (main toolbar) του Wireshark.....	36
4.5	Η γραμμή φίλτρων (filter toolbar)	36
4.6	Το παράθυρο προβολής πακέτων (packet list pane).....	37

4.7	Το παράθυρο προβολής λεπτομερειών πακέτων (packet details pane) .	37
4.8	Το παράθυρο προβολής πακέτων σε bytes (packet bytes pane)	38
4.9	Η γραμμή κατάστασης (statusbar)	38
4.10	Φίλτρα στο Wireshark	38
4.11	Φίλτρα σύλληψης.....	39
4.12	Φίλτρα απεικόνισης	42
5	ΚΕΦΑΛΑΙΟ 5ο: OSI, TCP/IP και WIRESHARK	47
5.1	Συσχέτιση μοντέλου OSI και μοντέλου TCP/IP	47
5.2	Συνδεσμολογία Ακροατή Πακέτων	48
5.3	Επίπεδο 1 TCP/IP :Το επίπεδο Πρόσβασης Δικτύου.....	49
5.3.1	Πρωτόκολλο Ethernet.....	49
5.3.2	Wireshark και Ethernet	50
5.3.3	Πρωτόκολλο MAC	51
5.3.4	Wireshark και MAC.....	51
5.3.5	Πρωτόκολλο ARP.....	52
5.3.6	Wireshark και ARP	53
5.3.7	WiFi	54
5.3.8	Wireshark και WiFi	55
5.4	Επίπεδο 2 TCP/IP: Το επίπεδο Δικτύου	55
5.4.1	Πρωτόκολλο IP.....	55
5.4.2	Wireshark και IP	57
5.4.3	Πρωτόκολλο DHCP	58
5.4.4	Wireshark και DHCP	58
5.4.5	Πρωτόκολλο NAT	59
5.4.6	Πρωτόκολλο ICMP	60
5.4.7	Wireshark και ICMP.....	61
5.5	Επίπεδο 3 TCP/IP :Το επίπεδο Μεταφοράς	61

5.5.1	Πρωτόκολλο TCP	61
5.5.2	Wireshark και TCP	62
5.5.3	Πρωτόκολλο UDP.....	63
5.5.4	Wireshark και UDP	64
5.6	Επίπεδο 4 TCP/IP :Το επίπεδο Εφαρμογής	65
5.6.1	Πρωτόκολλο HTTP.....	65
5.6.2	Wireshark και HTTP	66
5.6.3	Πρωτόκολλο DNS.....	68
5.6.4	Wireshark και DNS	69
5.6.5	Πρωτόκολλο FTP	70
5.6.6	Πρωτόκολλο SSL	71
6	ΚΕΦΑΛΑΙΟ 6° ΕΠΙΛΟΓΟΣ:.....	72
6.1	Σύνοψη Πτυχιακής εργασίας.....	72

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Βασική αρχή λειτουργίας Packet sniffer	21
Εικόνα 2: Δομή ενός συστήματος Ακρόασης Πακέτων	22
Εικόνα 3: USB Packet Sniffer Mercury T2.....	24
Εικόνα 4: Ethernet Packet Sniffer SharkTap.....	25
Εικόνα 5: USB3 Packet Sniffer Profitap	25
Εικόνα 6: Throwing Star LAN Tap.....	26
Εικόνα 7: Συνδεσμολογία Throwing Star LAN Tap	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
Εικόνα 8: Τα επίπεδα κατά OSI και IP/TCP, και η αντιστοιχία τους	28
Εικόνα 9: Το περιβάλλον εργασίας του Wireshark.....	34
Εικόνα 10: Το μενού του Wireshark	35
Εικόνα 11: Η κύρια γραμμή εργαλείων του Wireshark	36
Εικόνα 12: Η γραμμή φίλτρων του Wireshark	36
Εικόνα 13: Το παράθυρο προβολής πακέτων του Wireshark	37
Εικόνα 14: Το παράθυρο προβολής λεπτομερειών πακέτων του Wireshark	37
Εικόνα 15: Το παράθυρο προβολής πακέτων σε bytes του Wireshark.....	38
Εικόνα 16: Η γραμμή κατάστασης του Wireshark	38
Εικόνα 17: Διαδικασία φίλτρων σύλληψης	39
Εικόνα 18: Βήματα και διαδικασίες για την ρύθμιση ενός φίλτρου σύλληψης.....	40
Εικόνα 19 :Διαθέσιμα Πρωτόκολλα φίλτρου απεικόνισης.....	43
Εικόνα 20: Σχέση μοντέλου OSI και μοντέλου TCP/IP	47
Εικόνα 21: Βασικά πρωτόκολλα στα επίπεδα του μοντέλου TCP/IP	48
Εικόνα 22: Συνδεσμολογία για την εκπόνηση των παραδειγμάτων	49
Εικόνα 23: Παράδειγμα Ethernet.....	50
Εικόνα 24: Παράδειγμα MAC	52
Εικόνα 25: Πίνακας ARP	53
Εικόνα 26: Παράδειγμα ARP.....	54
Εικόνα 27: Παράδειγμα WLAN.....	55
Εικόνα 28: Επικεφαλίδα IP.....	57
Εικόνα 29: Παράδειγμα IP.....	58
Εικόνα 30: Παράδειγμα IP.....	59
Εικόνα 31: Παράδειγμα ICMP	61
Εικόνα 32: Επικεφαλίδα TCP	62

Εικόνα 33: Παράδειγμα TCP	63
Εικόνα 34: Επικεφαλίδα UDP	64
Εικόνα 35: Παράδειγμα UDP	65
Εικόνα 36: Πρωτόκολλο HTTP	67
Εικόνα 37: DNS ερωτήματα	69
Εικόνα 38: DNS αποκρίσεις	70

ΚΕΦΑΛΑΙΟ 1ο: ΕΙΣΑΓΩΓΗ

1.1 Περιγραφή του αντικειμένου της πτυχιακής εργασίας

Αντικείμενο της παρούσας εργασίας είναι η δημιουργία ενός εγχειριδίου με το οποίο θα είναι δυνατή η εύκολη κατανόηση της δομής των διακινούμενων δεδομένων ενός δικτύου υπολογιστικών συσκευών ενώ παράλληλα θα είναι δυνατή, αρχικά, η καταγραφή της κίνησής τους και σε δεύτερο χρόνο η επεξεργασία τους και η εξαγωγή των ζητούμενων συμπερασμάτων.

Η δομή του εγχειριδίου βασίζεται στην συσχέτιση κάθε επιπέδου του μοντέλου OSI με κάθε επίπεδο καταγραφής του λογισμικού Wireshark, με την παράθεση των σχετικών πρωτοκόλλων που κατανέμονται σε αυτό. Για κάθε επίπεδο θα υπάρχει αναλυτική επεξήγηση της χρησιμοποιούμενης μεθοδολογίας για την εξαγωγή των ζητούμενων αποτελεσμάτων. Τα εργαλεία που θα χρησιμοποιηθούν είναι ένας παθητικός «ακροατής δεδομένων» (Packet Sniffer) και το λογισμικό καταγραφής και επεξεργασίας πακέτων Wireshark.

Κατά καιρούς έχουν υπάρξει πολλές, ξεχωριστές εργασίες είτε για το μοντέλο OSI, είτε για την εφαρμογή Wireshark, αλλά ποτέ δεν υπήρξε συσχέτιση των δύο αυτών οντοτήτων και παρουσίασή τους σε δομή επιπέδων.

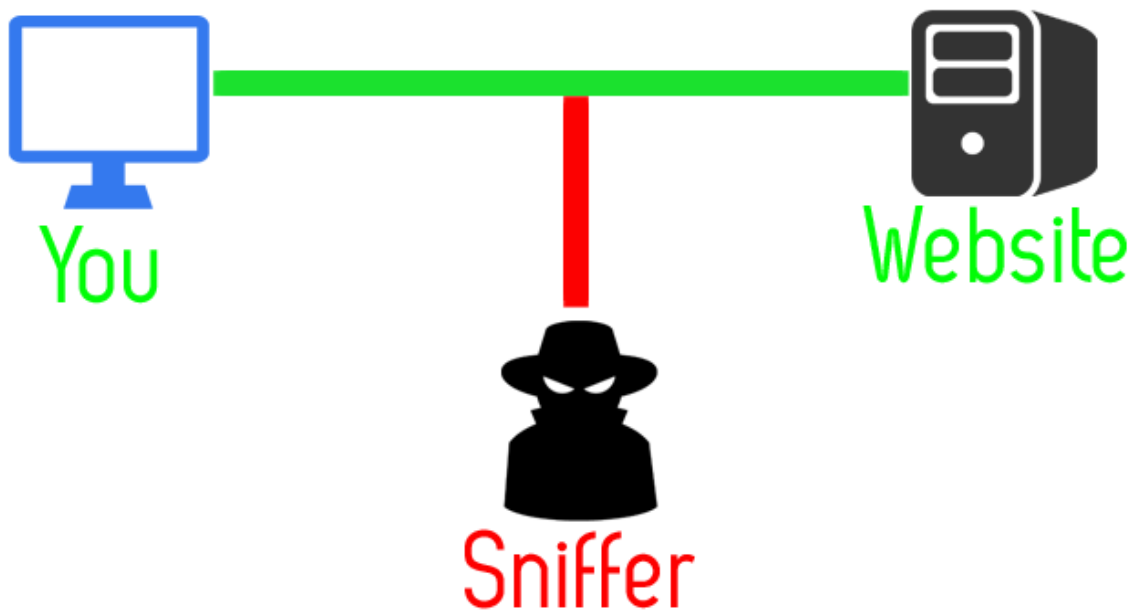
1.2 Δομή της πτυχιακής εργασίας και μεθοδολογία λειτουργίας

Το εγχειρίδιο στα πρώτα κεφάλαια παρουσιάζει εν συντομία τις τρεις βασικές οντότητες με τις οποίες ασχολείται, δηλαδή τους Ακροατές Πακέτων (Packet Sniffers), το μοντέλο OSI και το λογισμικό Wireshark ώστε ο αναγνώστης να κατανοήσει το τεχνικό υπόβαθρο στο οποίο στηρίζετε η εργασία. Στη συνέχεια γίνεται αναλυτική περιγραφή των ενεργειών που πρέπει να πραγματοποιήσει ο αναγνώστης στο λογισμικό Wireshark ώστε να εξάγει τα επιθυμητά αποτελέσματα. Οι εργασίες έχουν και ταξινομηθεί και ομαδοποιηθεί με βάση τη συσχέτιση των επιπέδων του μοντέλου OSI και των επιπέδων καταγραφής του λογισμικού Wireshark και παρουσιάζονται με βάση τα πρωτόκολλα που συσχετίζονται με κάθε επίπεδο καταγραφής του Wireshark. Έτσι, ο αναγνώστης/χρήστης αυτού του εγχειριδίου έχει τη δυνατότητα να ανατρέξει κατευθείαν στο επιθυμητό πρωτόκολλο, όπου μπορεί να βρει και την αντίστοιχη τεχνική τεκμηρίωση.

ΚΕΦΑΛΑΙΟ 2ο: ΑΚΡΟΑΤΕΣ ΠΑΚΕΤΩΝ

2.1 Γενική περιγραφή

Οι Ακροατές Πακέτων (Packet Sniffers) είναι αυτόνομες συσκευές ή λογισμικά τα οποία παρεμβάλλονται σε ένα δίκτυο υπολογιστικών συσκευών χωρίς να είναι ανιχνεύσιμοι και λαμβάνουν, καταγράφουν, και αναλύουν τα διακινούμενα δεδομένα.



Εικόνα 1: Βασική αρχή λειτουργίας Packet sniffer

Εκτός από συσκευές, Ακροατές Πακέτων υπάρχουν και με τη μορφή λογισμικού όπου χρησιμοποιείται η κάρτα δικτύου του υπολογιστή στον οποίο βρίσκονται εγκατεστημένοι. Σε αυτή την περίπτωση ο υπολογιστής είναι ανιχνεύσιμος στο δίκτυο.

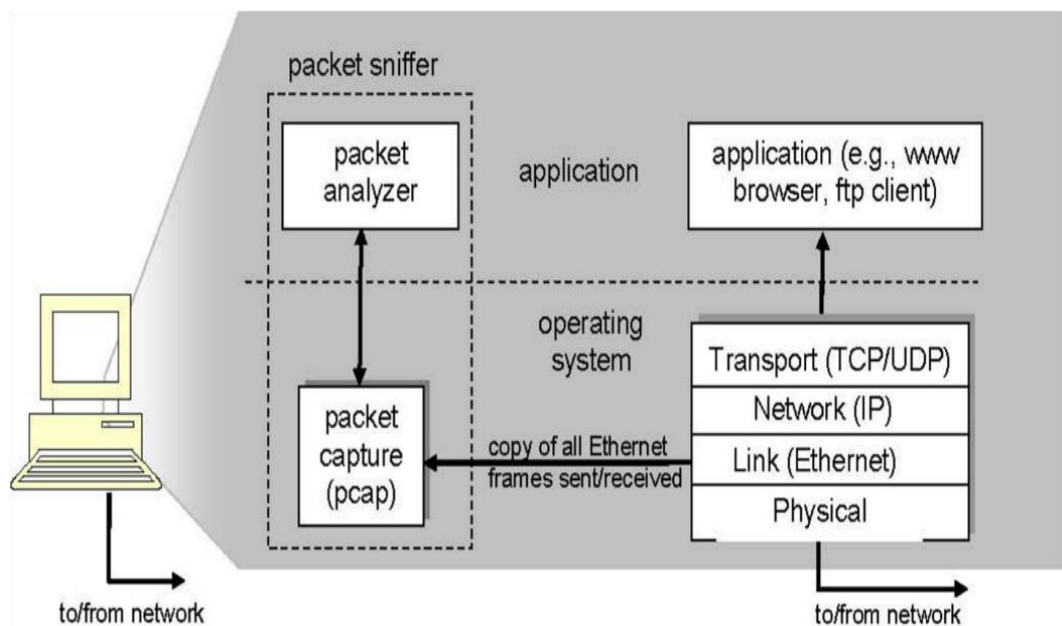
Οι Ακροατές Πακέτων (Packet Sniffers) χρησιμοποιούνται σε εφαρμογές όπου είναι απαραίτητη η εποπτεία και επιτήρηση της δικτυακής κίνησης. Με το κατάλληλο λογισμικό είναι δυνατή η καταγραφή και ανάλυση αυτών των δεδομένων ώστε να ώστε να εξαχθούν οι ζητούμενες πληροφορίες, όπως τα πρωτόκολλα που χρησιμοποιούνται, οι διευθύνσεις MAC και IP, οι συσκευές που είναι συνδεδεμένες και όλα τα δεδομένα που διακινούνται μεταξύ όλων ή της κάθε επιμέρους υπολογιστικής συσκευής και πολλές φορές είναι δυνατή η ανάκτηση κωδικών

πρόσβασης και άλλων προσωπικών δεδομένων. Η λειτουργία Ακρόασης Πακέτων ονομάζεται Packet Sniffing.

2.2 Ορισμός ενός συστήματος Ακρόασης Πακέτων

Το βασικό εργαλείο για την παρατήρηση των πακέτων που ανταλλάσσονται μεταξύ των συσκευών ενός δικτύου καλείται Ακροατής Πακέτων (Packet Sniffer). Όπως υπονοεί και το όνομα, ο Ακροατής Πακέτων συλλαμβάνει τα πακέτα τα οποία στέλνονται ή λαμβάνονται από μία υπολογιστική συσκευή. Επίσης, ο Ακροατής Πακέτων έχει τη δυνατότητα να αποθηκεύει και απεικονίζει τα περιεχόμενα διαφόρων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που καταγράφονται.

Στο παρακάτω σχήμα φαίνεται η δομή ενός Ακροατή Πακέτων. Στο δεξί μέρος του παρακάτω σχήματος φαίνονται τα υποστηριζόμενα δικτυακά πρωτόκολλα και οι εφαρμογές (όπως ένας φυλλομετρητής ή ένα λογισμικό απομακρυσμένης επιφάνειας εργασίας) που λειτουργούν στην υπολογιστική συσκευή. Ο Ακροατής Πακέτων, ο οποίος φαίνεται μέσα στο πλαίσιο των διακεκομμένων γραμμών του συγκεκριμένου σχήματος, είναι είτε μία εξωτερική συσκευή, είτε ένα λογισμικό το οποίο είναι εγκατεστημένο σε έναν υπολογιστή και λαμβάνει ένα αντίγραφο κάθε πλαισίου δεδομένων για κάθε επίπεδο του μοντέλου OSI που στέλνεται ή λαμβάνεται από τον υπολογιστή μας.



Εικόνα 2: Δομή ενός συστήματος Ακρόασης Πακέτων

Το πρώτο συστατικό στοιχείο ενός Ακροατή Πακέτων είναι ο Καταγραφέας Πακέτων (Packet Capture). Σύμφωνα με την αρχή λειτουργίας του μοντέλου OSI, ότι τα πλαίσια που ανταλλάσσονται από τα πρωτόκολλα ανωτέρων επιπέδων, (HTTP, FTP, TCP, UDP IP), ενθυλακώνονται μέσα σε πλαίσια επιπέδου ζεύξης τα οποία τελικά μεταδίδονται μέσω του δικτύου με φυσικά μέσα (καλώδιο UTP). Επομένως, η σύλληψη όλων των πλαισίων ζεύξης μας παρέχει όλα τα δεδομένα που στέλνονται και λαμβάνονται από όλα τα πρωτόκολλα του μοντέλου OSI και όλες τις εφαρμογές που εκτελούνται στον υπολογιστή μας.

Το δεύτερο συστατικό στοιχείο ενός Ακροατή Πακέτων είναι ο Αναλυτής Πακέτων (Packet Analyzer), ο οποίος αναλύει απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο πλαίσιο ενός πακέτου σε οποιοδήποτε πρωτόκολλο ανήκει. Για το σκοπό αυτό, ο Αναλυτής Πακέτων πρέπει να κατανοεί τη δομή όλων των δεδομένων που ανταλλάσσονται από τα πρωτόκολλα.

2.3 Τοπολογίες συνδεσμολογίας Ακρόασης Πακέτων

Η παρεμβολή σε ένα δίκτυο επιτυγχάνεται με τις παρακάτω συνδεσμολογίες:

ΤΟΠΟΛΟΓΙΑ	ΠΕΡΙΓΡΑΦΗ
Κοινόχρηστων Δεδομένων (Shared Media)	Ο Ακροατής χρησιμοποιεί μία από τις εξόδους ενός Κόμβου (Hub)
Διαμοιρασμένων Δεδομένων (Switched media) χωρίς παρεμβολή Ακροατή	Ο Ακροατής είναι ένας από τους υπολογιστές που συνδέονται σε έναν Εναλλάκτη Δικτύου (Switch)
Διαμοιρασμένων Δεδομένων (Switched media) με παρεμβολή Ακροατή	Η έξοδος του Εναλλάκτη (Switch) συνδέεται σε ένα Κόμβο (Hub) όπου παρεμβάλλεται ο Ακροατής
Διαμοιρασμένων Δεδομένων (Switched media) με χρήση εξόδου ακρόασης	Ο Έναλλάκτης (Switch) διαθέτει θύρα ακρόασης όπου συνδέεται ο Ακροατής
Ενδιάμεσος Ακροατής	Ο Ακροατής τοποθετείται μεταξύ δύο συσκευών. Ενεργός (Ακροατής με δύο κάρτες δικτύου) ή Παθητικός

ΤΟΠΟΛΟΓΙΑ	ΠΕΡΙΓΡΑΦΗ
Διαμοιρασμένων Δεδομένων (Switched media) με παρεμβολή κακόβουλου Ακροατή	Ο Ακροατής είναι ένας από τους υπολογιστές που συνδέονται σε έναν Εναλλάκτη Δικτύου (Switch) και χρησιμοποιεί κακόβουλες μεθόδους ώστε να αλλάξει τη διαδρομή των δεδομένων

2.4 Κατηγορίες Ακροατών Πακέτων

Οι Ακροατές Πακέτων χωρίζονται σε δύο μεγάλες κατηγορίες: Ενεργοί και Παθητικοί

Οι Ενεργοί Ακροατές Πακέτων είναι συσκευές ή λογισμικά τα οποία συνδέονται στο εποπτευόμενο δίκτυο, είναι ανιχνεύσιμα και αναλύουν μέρος ή όλα τα δεδομένα που διακινούνται, αναλόγως των προδιαγραφών που έχουν σχεδιαστεί.

Οι Παθητικοί Ακροατές Πακέτων είναι συσκευές οι οποίες διαθέτουν μία είσοδο και δύο εξόδους LAN. Παρεμβάλλονται σε ένα δίκτυο υπολογιστικών συσκευών χωρίς να είναι ανιχνεύσιμοι σαν μία νοητή διχοτόμηση του καλωδίου μεταφοράς των δεδομένων. Στην είσοδο λαμβάνουν όλα τα δεδομένα τα οποία εξάγουν άθικτα στην πρώτη έξοδο ενώ παράλληλα αντιγράφουν και εξάγουν στη δεύτερη έξοδο το σύνολο των αρχικών δεδομένων

2.5 Παραδείγματα Ακροατών Πακέτων

Ορισμένες συσκευές Ακρόασης Πακέτων παρουσιάζονται ενδεικτικά παρακάτω:



Εικόνα 3: USB Packet Sniffer Mercury T2

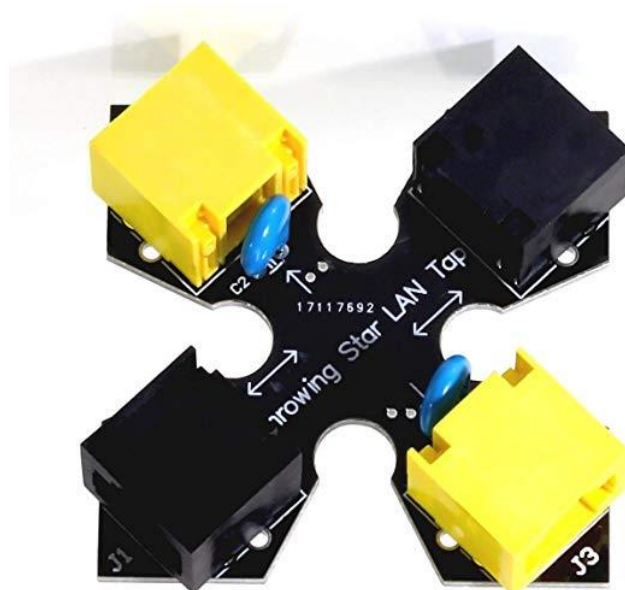


Εικόνα 4: Ethernet Packet Sniffer SharkTap

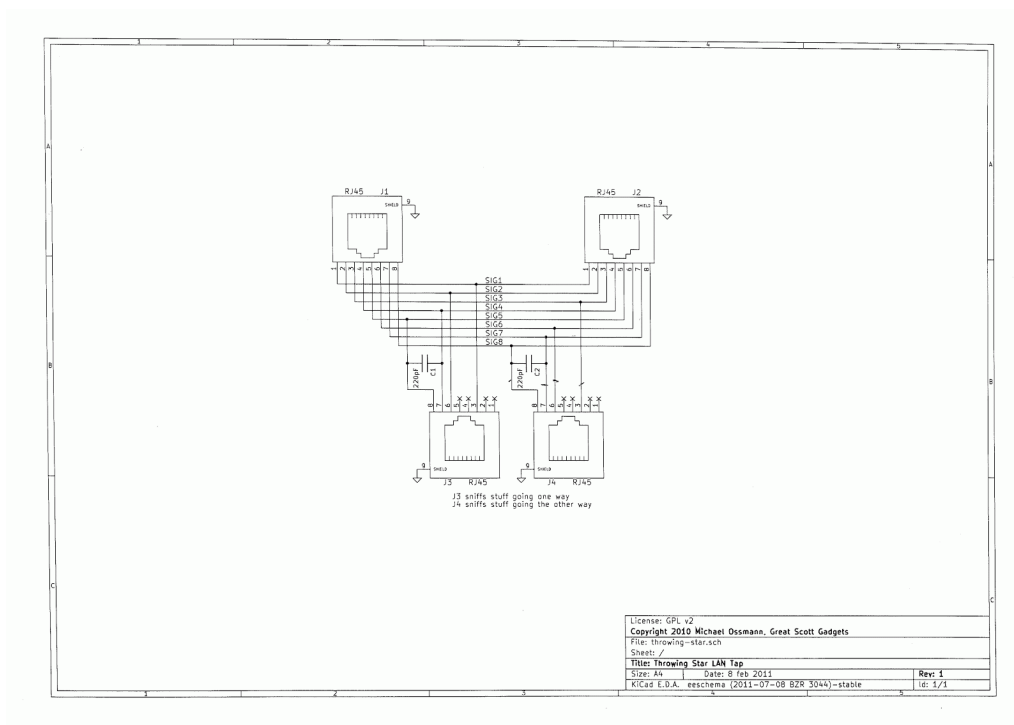


Εικόνα 5: USB3 Packet Sniffer Profitap

Ο Ακροατής Πακέτων που θα χρησιμοποιηθεί στην παρούσα εργασία είναι ένας απλός, παθητικός Ακροατής με την ονομασία Throwing Star LAN Tap 1.5.



Εικόνα 6: Throwing Star LAN Tap



Εικόνα 7: Συνδεσμολογία Throwing Star LAN Tap

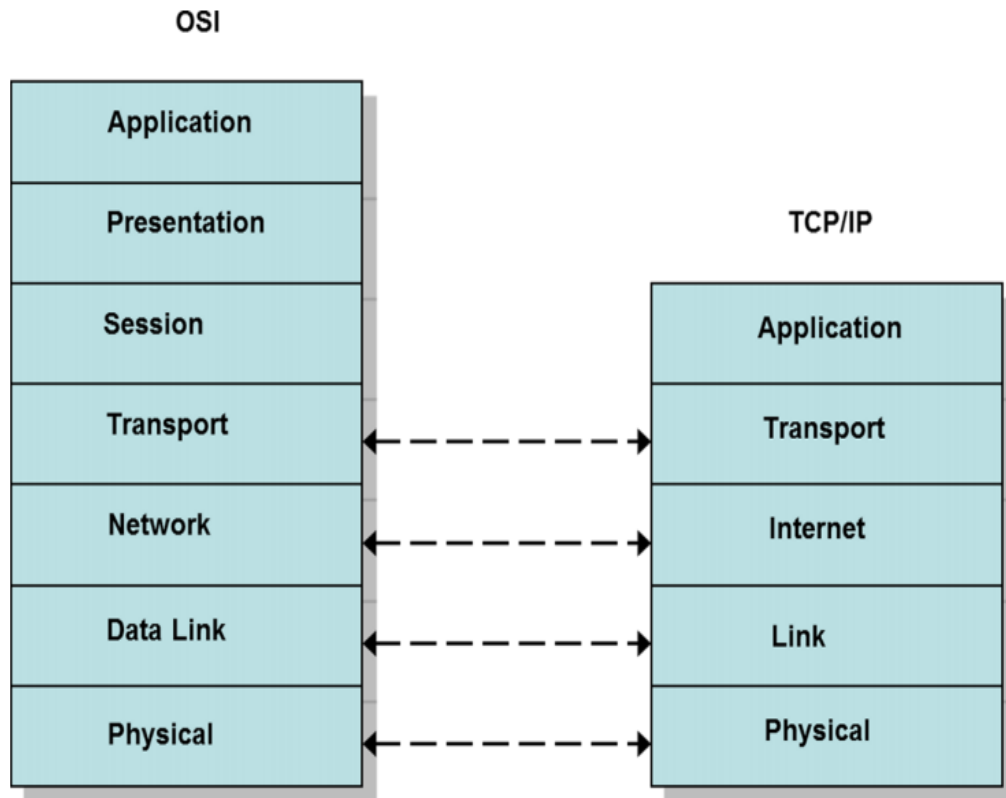
ΚΕΦΑΛΑΙΟ 3ο: ΤΟ ΜΟΝΤΕΛΟ OSI

3.1 Γενική περιγραφή

Ένα μοντέλο δικτύου προσφέρει τις γενικές αρχές για τον διαχωρισμό των δικτυακών λειτουργιών των υπολογιστικών συστημάτων σε διακριτά επίπεδα (Layers). Κάθε ένα από αυτά τα διακριτά επίπεδα παρέχει δυνατότητες στα κάτω επίπεδα και υποστηρίζει τα πάνω επίπεδα. Ένα τέτοιο μοντέλο, διαβαθμισμένης λειτουργικότητας και διακριτής δομής, καλείται στοίβα πρωτοκόλλων ή σουίτα πρωτοκόλλων. Τα πρωτόκολλα λειτουργούν είτε μέσω συσκευών/υλικού είτε μέσω λογισμικού. Στις περισσότερες στοίβες πρωτοκόλλων συνδυάζονται και οι δύο τρόποι λειτουργίας. Συνήθως, στα χαμηλότερα επίπεδα οι λειτουργίες επιτελούνται με υλικό (Hardware) ενώ στα ανώτερα με λογισμικό (Software).

Το 1983 προτάθηκε το OSI (Open Systems Interconnection Reference Model). Αυτό περιλαμβάνει επτά επίπεδα τα οποία προδιαγράφουν τις απαιτήσεις για την επικοινωνία μεταξύ δύο υπολογιστών. Το μοντέλο ορίζεται από το στάνταρντ 7498-1 του οργανισμού ISO. Επιτρέπει τη συνεργασία των συσκευών ενός δικτύου ανεξάρτητα με το ποια πρωτόκολλα χρησιμοποιούνται και από ποιους κατασκευαστές υπολογιστών υποστηρίζονται. Αντιθέτως το παλαιότερο μοντέλο αναφοράς TCP/IP περιλαμβάνει πέντε επίπεδα. Παρά τις προσπάθειες, υπήρξε μεγάλη αντίδραση από την κοινότητα των προγραμματιστών, αλλά και των κατασκευαστών προς το OSI. Παράλληλα, η αυστηρή τυπολατρία του μοντέλου OSI σε σχέση με την πιο «χαλαρή» προσέγγιση του TCP/IP έκαναν την δημιουργία και υιοθέτηση πρωτοκόλλων σύμφωνα με το τελευταίο πολύ πιο εύκολη υπόθεση

Στην πράξη, σήμερα, στο Διαδίκτυο χρησιμοποιείται το μοντέλο αναφοράς TCP/IP. Συνηθίζεται όμως η παρουσίαση του μοντέλου αναφοράς OSI και μετά αντιστοίχιση των επιπέδων του μοντέλου αναφοράς TCP/IP στα κατάλληλα επίπεδα του πρώτου. Η αντιστοιχία μεταξύ των επιπέδων κατά OSI και κατά TCP/IP φαίνεται στην επόμενη εικόνα. Το επίπεδο Εφαρμογής και για τα δύο μοντέλα είναι κοινό, αλλά η λειτουργικότητα των επιπέδων Παρουσιάσεως και Συνόδου μπορεί είτε να μην υλοποιείται στην περίπτωση του TCP/IP, είτε να ενσωματωθεί (εάν υπάρχει ανάγκη) στο επίπεδο Εφαρμογής του TCP/IP. Ενδιαφέρον είναι επίσης να τονισθεί ότι στο Internet Layer του TCP/IP υπάρχει ως δυνατότητα μόνον ένα πρωτόκολλο: το IP.



Εικόνα 8: Τα επίπεδα κατά OSI και IP/TCP, και η αντιστοιχία τους

Τα κύρια πλεονεκτήματα του μοντέλου OSI είναι τα παρακάτω:

- Βοηθάει στην απεικόνιση και καλύτερη κατανόηση του δικτύου από τους χρήστες.
- Βοηθάει στην καλύτερη κατανόηση της συνεργασία μεταξύ του Υλικού (Hardware) και του Λογισμικού (Software).
- Διευκολύνει την επίλυση προβλημάτων κατακερματίζοντας το δίκτυο σε διακριτά, εύκολα διαχειρίσιμα τμήματα.
- Προδιαγράφει τις μεθόδους με τις οποίες είναι δυνατή η σύγκριση των βασικών λειτουργιών και σχέσεων διαφορετικά δίκτυα.
- Βοηθάει τους χρήστες να καταλάβουν νέες τεχνολογίες καθώς αυτές αναπτύσσονται.
- Ενισχύει την λειτουργικότητα των προϊόντων.

Ο παρακάτω πίνακας περιγράφει συνοπτικά τα πλεονεκτήματα που παρουσιάστηκαν και γενικότερα τον τρόπο λειτουργίας.

	Μονάδα δεδομένων	Επίπεδο	Λειτουργία
Λογισμικό	Δεδομένα	Επίπεδο 7 (Εφαρμογών)	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
		Επίπεδο 6 (Παρουσίασης)	Αναπαράσταση δεδομένων και κρυπτογράφηση
		Επίπεδο 5 (Συνόδου)	Έλεγχος του διαλόγου μεταξύ των άκρων της επικοινωνίας
	Τμήμα	Επίπεδο 4 (Μεταφοράς)	Αξιόπιστη επικοινωνία από άκρο σε άκρο
Υλικό	Πακέτο	Επίπεδο 3 (Δικτύου)	Καθορισμός διαδρομών και λογικών διευθύνσεων των κόμβων στα πλαίσια ενός διαδικτύου
	Πλαίσιο	Επίπεδο 2 (Ζεύξης Δεδομένων)	Φυσική διευθυνσιοδότηση (MAC & LLC)
	Bit	Επίπεδο 1 (Φυσικό)	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

Πίνακας 1: Σύνοψη περιγραφή του μοντέλου OSI και των 7 επιπέδων του

3.2 Επίπεδο 7: Το επίπεδο Εφαρμογών

Το επίπεδο εφαρμογών (Application Layer) δίνει τη δυνατότητα στους χρήστες να προσπελάσουν τις πληροφορίες ενός δικτύου, μέσω μιας εφαρμογής. Σε αυτό το επίπεδο επιτυγχάνεται η κύρια διασύνδεση του χρήστη με την εφαρμογή και τελικά με το δίκτυο.

3.3 Επίπεδο 6: Το επίπεδο Παρουσίασης

Το επίπεδο Παρουσίασης (Presentation Layer) είναι υπεύθυνο για το πως μια εφαρμογή θα μετασχηματίσει τα δεδομένα τα οποία είναι να σταλούν στο επίπεδο εφαρμογών. Ουσιαστικά, επιτρέπει στην εφαρμογή να διαβάσει και να κατανοήσει τα μηνύματα δεδομένων. Οι λειτουργίες που περιλαμβάνει είναι:

- Κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων για ασφάλεια.
- Συμπίεση και αποσυμπίεση των δεδομένων με σκοπό την γρηγορότερη μετάδοση
- Μορφοποίηση γραφικών.
- Μετάφραση περιεχομένου.
- Μετάφραση βασισμένη στα χαρακτηριστικά του συστήματος.

3.4 Επίπεδο 5: Το επίπεδο Συνόδου

Το επίπεδο συνόδου προσφέρει ποικίλες υπηρεσίες όπως ο εντοπισμός του πλήθους των bytes που κάθε ένα άκρο της συνόδου λαμβάνει. Το επίπεδο αυτό επιτρέπει στις 8 εφαρμογές να λειτουργούν σε συσκευές για την εγκαθίδρυση, διαχείριση και τερματισμό μιας συνεδρίας μέσω του δικτύου.

3.5 Επίπεδο 4: Το επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς του μοντέλου προσφέρει επικοινωνία από άκρο σε άκρο (end-to-end) μεταξύ των τελικών συσκευών μέσω ενός δικτύου. Ανάλογα με την εφαρμογή, το επίπεδο μεταφοράς προσφέρει αξιόπιστη, συνδεομοστροπής ή ασυνδεσμική, και όσο το δυνατόν βέλτιστη επικοινωνία

3.6 Επίπεδο 3: Το επίπεδο Δικτύου

Το επίπεδο δικτύου του μοντέλου OSI προσφέρει ένα σύστημα από άκρο σε άκρο (end-to-end) λογικής διευθυνσιοδότησης έτσι ώστε ένα πακέτο δεδομένων να μπορεί να δρομολογηθεί διαμέσων διαφορετικών επιπέδων (Συνδέσμου και μετάδοσης δεδομένων) διαφόρων δικτύων (Ethernet, Token Ring, Frame Relay κτλ). Σε αυτό το επίπεδο ανήκει το πρωτόκολλο IP.

3.7 Επίπεδο 2: Το επίπεδο Ζεύξης Δεδομένων

Το επίπεδο διασύνδεσης δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για την μεταφορά δεδομένων από την μια συσκευή του δικτύου στην άλλη, και για τον έλεγχο και την πιθανή διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες στις κάρτες δικτύου των συσκευών από το εργοστάσιο κατασκευής.

3.8 Επίπεδο 1: Το Φυσικό επίπεδο

Το φυσικό επίπεδο του μοντέλου OSI ορίζει τα χαρακτηριστικά της σύνδεσης και της διεπαφής, καθώς και τις μέσες καλωδιακές απαιτήσεις. Ηλεκτρικά, μηχανικά λειτουργικά και διαδικαστικά χαρακτηριστικά παρέχονται για την αποστολή ροής από bits σε ένα δίκτυο υπολογιστών.

ΚΕΦΑΛΑΙΟ 4ο: WIRESHARK

4.1 Γενική περιγραφή

Το Wireshark είναι ένα ελεύθερο και ανοιχτού κώδικα λογισμικό. Χρησιμοποιείται για εποπτεία και επιτήρηση των διακινούμενων δεδομένων ενός δικτύου, καταγραφής αυτής της κίνησης, και επεξεργασία για τον εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα και για εκπαιδευτικούς λόγους. Ουσιαστικά παρακολουθεί την κίνηση των πακέτων. Παρέχει πληροφορίες για το δίκτυο και τα πρωτόκολλα ανώτερου επιπέδου σχετικά με τα δεδομένα που διακινούνται σ' αυτό. Το Wireshark χρησιμοποιεί τη δικτυακή βιβλιοθήκη libpcap για την σύλληψη (ανάλυση) των πακέτων. Προσφέρει τη δυνατότητα χρήσης φίλτρων για διαφορετικούς τύπους πακέτων που θέλουμε να ανιχνεύσουμε καθώς επίσης και στατιστική ανάλυση και ανάλυση με γράφους.

Το Wireshark είναι εργαλείο καταγραφής και επεξεργασίας δεδομένων. Σε καμιά περίπτωση δεν μπορεί ο χρήστης να στείλει δεδομένα με αυτό ούτε μπορεί να χρησιμοποιηθεί ως προειδοποίηση για κάποιο εισβολέα του δικτύου. Το Wireshark ονομαζόταν Ethereal μέχρι το 2006, όταν ο επικεφαλής προγραμματιστής, αποφάσισε την αλλαγή του ονόματός του λόγω δικαιωμάτων χρήσης που προϋπήρχαν για το όνομα Ethereal.

Τα πακέτα δεδομένων μπορούν να συλληφθούν τόσο από ενσύρματο όσο και ασύρματο δίκτυο και αυτές οι πληροφορίες μπορούν να προβληθούν ζωντανά καθώς συλλαμβάνονται. Επίσης υποστηρίζει πολλά ενθέματα (plugins) έχοντας δυνατότητα επέκτασης ώστε να προστεθούν νέα πρωτόκολλα και χαρακτηριστικά. Το Wireshark είναι διαθέσιμο για όλα τα κύρια λειτουργικά συστήματα όπως τα Windows, Linux και Mac, κάτι που το καθιστά ιδανικό για δίκτυα με διαφορετικές πλατφόρμες.

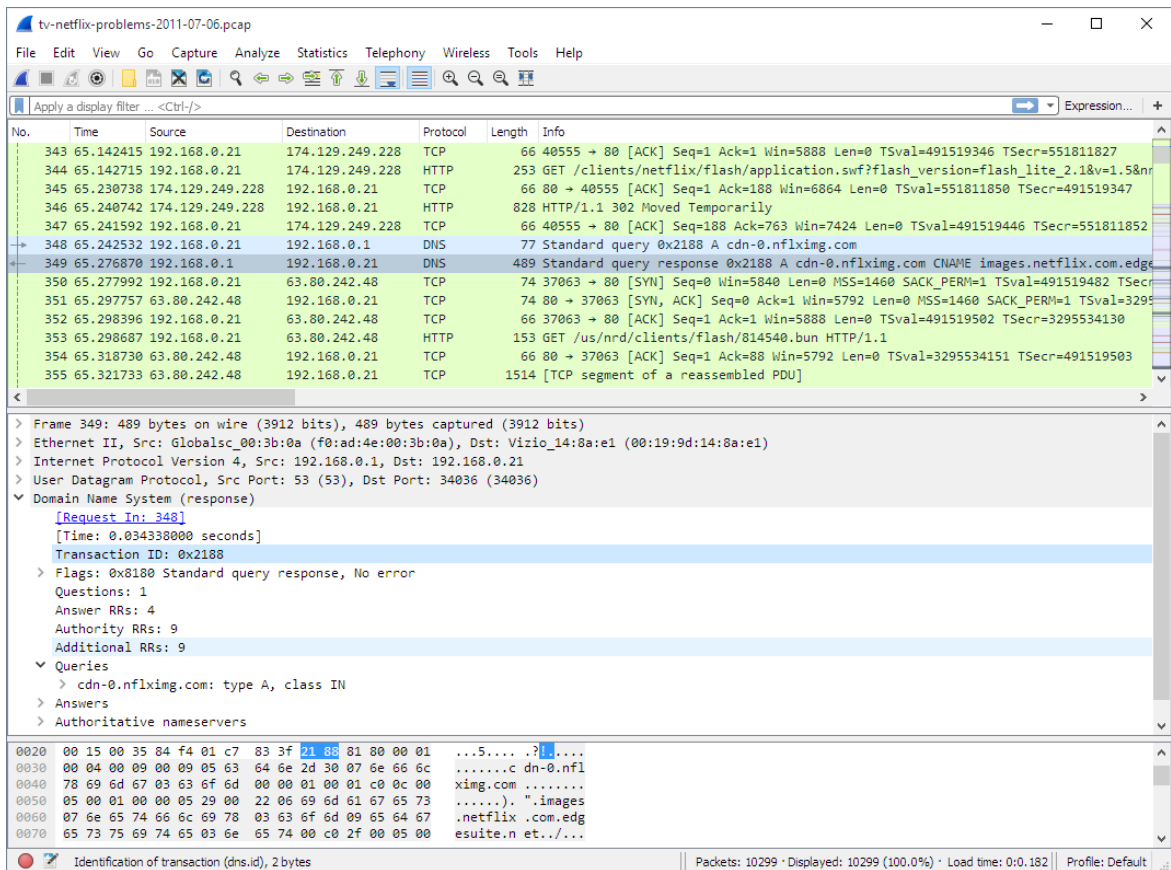
Τα πλεονεκτήματα του Wireshark είναι:

- Η ευκολία εγκατάστασής του.
- Η απλότητα της χρήσης του μέσω του γραφικού περιβάλλοντος (GUI) που το καθιστά ικανό να καταγράψει και να αναλύσει όλη την κυκλοφορία ενός δικτύου, διακριτά ανά ζητούμενο πρωτόκολλο.
- το μεγάλο εύρος της λειτουργικότητας του.

4.2 Το περιβάλλον λειτουργίας του Wireshark

Το περιβάλλον λειτουργίας του Wireshark αποτελείται από:

- την γραμμή λειτουργιών (menu),
- την κύρια γραμμή εργαλείων (main toolbar),
- την γραμμή φίλτρων (filter toolbar),
- το παράθυρο προβολής πακέτων (packet list pane),
- το παράθυρο προβολής λεπτομεριών πακέτων (packet details pane),
- το παράθυρο προβολής πακέτων σε bytes (packet bytes pane),
- την γραμμή κατάστασης (statusbar).



Εικόνα 9: Το περιβάλλον εργασίας του Wireshark

4.3 Η γραμμή λειτουργιών (menu) του Wireshark

Η γραμμή λειτουργιών (menu) του Wireshark περιλαμβάνει έντεκα βασικές ομάδες λειτουργιών (menu) όπως φαίνεται στην επόμενη εικόνα:



Εικόνα 10: Το μενού του Wireshark

Συνοπτική περιγραφή της κάθε ομάδας:

- **(File)** Αυτό το μενού περιέχει στοιχεία για το άνοιγμα και τη συγχώνευση αρχείων καταγραφής, την αποθήκευση, την εκτύπωση ή την εξαγωγή αρχείων καταγραφής ολόκληρων ή μερικών και την έξοδο από την εφαρμογή Wireshark.
- **(Edit)** Αυτό το μενού περιέχει στοιχεία για να βρεθεί ένα πακέτο, αναφορά χρόνου ή να επισημανθεί ένα ή περισσότερα πακέτα, να γίνει διαχείριση του προφίλ διαμόρφωσης και να οριστούν οι προτιμήσεις (αποκοπή, αντιγραφή και επικόλληση δεν εφαρμόζονται επί του παρόντος).
- **(View)** Αυτό το μενού ελέγχει την εμφάνιση των δεδομένων που έχουν ληφθεί, συμπεριλαμβανομένου του χρωματισμού των πακέτων, της μεγέθυνσης της γραμματοσειράς, της εμφάνισης ενός πακέτου σε ένα ξεχωριστό παράθυρο, της επέκτασης και της συμπίεσης των δέντρων σε στοιχεία πακέτου.
- **(Go)** Αυτό το μενού περιέχει στοιχεία για να μεταβείτε σε ένα συγκεκριμένο πακέτο.
- **(Capture)** Αυτό το μενού σας επιτρέπει την έναρξη και τη λήξη της σύλληψης των πακέτων και την επεξεργασία των φίλτρων καταγραφής.
- **(Analyze)** Αυτό το μενού περιέχει στοιχεία που μπορούν να χειριστούν τα φίλτρα οθόνης, να ενεργοποιήσουν ή να απενεργοποιήσουν την ανατομή των πρωτοκόλλων, να διαμορφώσουν τις αποκωδικοποιήσεις που καθορίζονται από το χρήστη και να ακολουθήσουν μια ροή TCP.
- **(Statistics)** Αυτό το μενού περιέχει στοιχεία για την εμφάνιση διαφόρων στατιστικών παραθύρων, όπως μια περίληψη των πακέτων που έχουν

ληφθεί, στατιστικά, στοιχεία ιεραρχίας πρωτοκόλλου προβολής και πολλά άλλα.

- **(Telephony)** Αυτό το μενού περιέχει στοιχεία για την εμφάνιση διαφόρων στατιστικών παραθύρων, συμπεριλαμβανομένης της περίληψης των πακέτων που έχουν ληφθεί, των στατιστικών ιεραρχίας πρωτοκόλλου προβολής και πολλά άλλα
- **(Wireless)** Τα στοιχεία αυτού του μενού εμφανίζουν ασύρματες στατιστικές Bluetooth και IEEE 802.11.
- **(Tools)** Αυτό το μενού περιέχει διάφορα εργαλεία που είναι διαθέσιμα στο Wireshark, όπως η δημιουργία κανόνων ACL Firewall.
- **(Help)** Αυτό το μενού περιέχει στοιχεία που βοηθούν τον χρήστη, π.χ. πρόσβαση σε κάποια βασική βοήθεια, εγχειρίδιο σελίδων των διαφόρων εργαλείων γραμμής εντολών, online πρόσβαση σε ορισμένες από τις ιστοσελίδες και το συνηθισμένο για το παράθυρο διαλόγου.

4.4 Η κύρια γραμμή εργαλείων (main toolbar) του Wireshark

Η κύρια γραμμή εργαλείων (main toolbar) του Wireshark περιλαμβάνει τα εικονίδια των βασικών λειτουργιών όπως φαίνεται στην επόμενη εικόνα:



Εικόνα 11: Η κύρια γραμμή εργαλείων του Wireshark

4.5 Η γραμμή φίλτρων (filter toolbar)

Η γραμμή φίλτρων (filter toolbar) του Wireshark παρέχει την άμεση δυνατότητα επεξεργασίας και εφαρμογής φίλτρων εξαγωγής αποτελεσμάτων.



Εικόνα 12: Η γραμμή φίλτρων του Wireshark

4.6 Το παράθυρο προβολής πακέτων (packet list pane)

Το παράθυρο λίστας πακέτων εμφανίζει όλα τα πακέτα στο τρέχον αρχείο καταγραφής. Κάθε γραμμή στη λίστα πακέτων αντιστοιχεί σε ένα πακέτο στο αρχείο καταγραφής. Όταν επιλεγεί μια γραμμή σε αυτό το παράθυρο, περισσότερες λεπτομέρειες θα εμφανιστούν στα παράθυρα «προβολής λεπτομερειών πακέτων» και «προβολής πακέτων σε bytes».

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.21	192.168.0.1	DNS	84	Standard query 0x403d A moviecontrol.netflix.com
2	0.055880	192.168.0.1	192.168.0.21	DNS	479	Standard query response 0x403d A moviecontrol.netflix.com CNAME nccp-moviecontrol-fro
3	0.057690	192.168.0.21	50.17.249.22	TCP	74	37314->443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491454310 TSecr=0 WS=
4	0.154716	50.17.249.22	192.168.0.21	TCP	74	443->37314 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=2102931926
5	0.155962	192.168.0.21	50.17.249.22	TCP	66	37314->443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491454408 TSecr=2102931926
6	0.163169	192.168.0.21	50.17.249.22	TLSv1	187	Client Hello
7	0.250734	50.17.249.22	192.168.0.21	TCP	66	443->37314 [ACK] Seq=1 Ack=122 Win=5792 Len=0 TSval=2102931950 TSecr=491454416
8	0.252716	50.17.249.22	192.168.0.21	TLSv1	1514	Server Hello
9	0.253826	192.168.0.21	50.17.249.22	TCP	66	37314->443 [ACK] Seq=122 Ack=1449 Win=8768 Len=0 TSval=491454507 TSecr=2102931950
10	0.254730	50.17.249.22	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]
11	0.254778	50.17.249.22	192.168.0.21	TLSv1	349	Certificate
12	0.255853	192.168.0.21	50.17.249.22	TCP	66	37314->443 [ACK] Seq=122 Ack=2897 Win=11648 Len=0 TSval=491454509 TSecr=2102931950
13	0.256102	192.168.0.21	50.17.249.22	TCP	66	37314->443 [ACK] Seq=122 Ack=3180 Win=14528 Len=0 TSval=491454509 TSecr=2102931950
14	0.319870	192.168.0.21	50.17.249.22	TLSv1	264	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
15	0.411795	50.17.249.22	192.168.0.21	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message

Εικόνα 13: Το παράθυρο προβολής πακέτων του Wireshark

4.7 Το παράθυρο προβολής λεπτομερειών πακέτων (packet details pane)

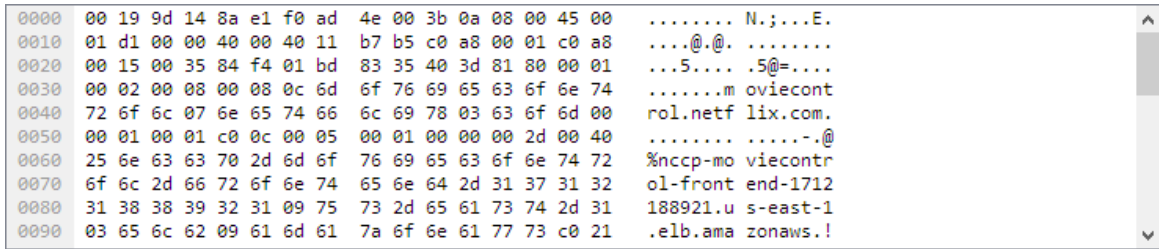
Το παράθυρο λεπτομερειών πακέτου εμφανίζει το τρέχον πακέτο (που έχει επιλεγεί στο παράθυρο «Προβολής πακέτων») σε πιο λεπτομερή μορφή. Τα πρωτόκολλα και τα πεδία του πακέτου που εμφανίζονται σε μορφή δέντρου που μπορεί να επεκταθεί και να συμπυκνωθεί.

>	Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
>	Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
>	User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
>	Domain Name System (response)
>	[Request In: 1]
>	[Time: 0.055880000 seconds]
>	Transaction ID: 0x403d
>	Flags: 0x8180 Standard query response, No error
>	Questions: 1
>	Answer RRs: 2
>	Authority RRs: 8
>	Additional RRs: 8
>	Queries
>	Answers
>	Authoritative nameservers
>	Additional records

Εικόνα 14: Το παράθυρο προβολής λεπτομερειών πακέτων του Wireshark

4.8 Το παράθυρο προβολής πακέτων σε bytes (packet bytes pane)

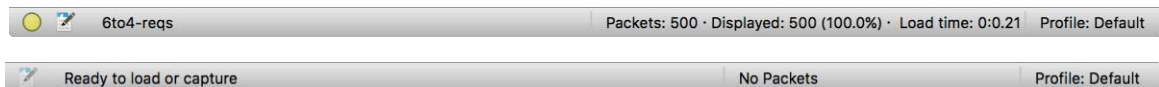
Το παράθυρο bytes πακέτων εμφανίζει τα δεδομένα του τρέχοντος πακέτου (που έχει επιλεγεί στο παράθυρο «Προβολής πακέτων») σε δεκαεξαδική μορφή.



Εικόνα 15: Το παράθυρο προβολής πακέτων σε bytes του Wireshark

4.9 Η γραμμή κατάστασης (statusbar)

Η γραμμή κατάστασης εμφανίζει ενημερωτικά μηνύματα. Στην αριστερή πλευρά θα εμφανιστούν πληροφορίες σχετικές με το περιβάλλον, το μεσαίο τμήμα θα εμφανιστούν πληροφορίες σχετικά με το τρέχον αρχείο καταγραφής και στη δεξιά πλευρά θα εμφανιστεί το επιλεγμένο προφίλ διαμόρφωσης.



Εικόνα 16: Η γραμμή κατάστασης του Wireshark

4.10 Φίλτρα στο Wireshark

Ένα κοινό πρόβλημα κατά την εκκίνηση του Wireshark με τις προεπιλεγμένες ρυθμίσεις είναι ότι καταγράφεται μεγάλη ποσότητα πληροφοριών στην οθόνη με αποτέλεσμα να είναι δύσκολο να βρεθεί η ζητούμενη πληροφορία. Γι' αυτό το λόγο τα φίλτρα είναι τόσο σημαντικά, θα μας βοηθήσουν να αναζητήσουμε, στα χρήσιμα αρχεία καταγραφών, τα δεδομένα που μας ενδιαφέρουν. Τα φίλτρα χωρίζονται σε δύο κατηγορίες:

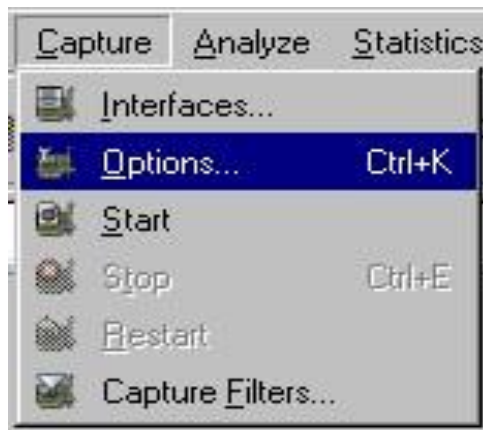
- **Φίλτρα σύλληψης**, τα οποία χρησιμοποιούνται για την επιλογή των δεδομένων που θα καταγραφούν στα αρχεία καταγραφής. Καθορίζονται πριν την εκκίνηση της σύλληψης. Το Wireshark καταγράφει μόνο τα πακέτα που καθορίζονται από τα φίλτρα σύλληψης.

- **Φίλτρα απεικόνισης:** τα οποία χρησιμοποιούνται για την αναζήτηση και εξαγωγή δεδομένων από τα αρχεία καταγραφών. Το Wireshark καταγράφει όλα τα πακέτα, αλλά απεικονίζονται στην οθόνη μόνο τα πακέτα που καθορίστηκαν στα φίλτρα. Τα φίλτρα απεικόνισης μπορούν να τροποποιηθούν κατά τη διάρκεια της σύλληψης των δεδομένων.

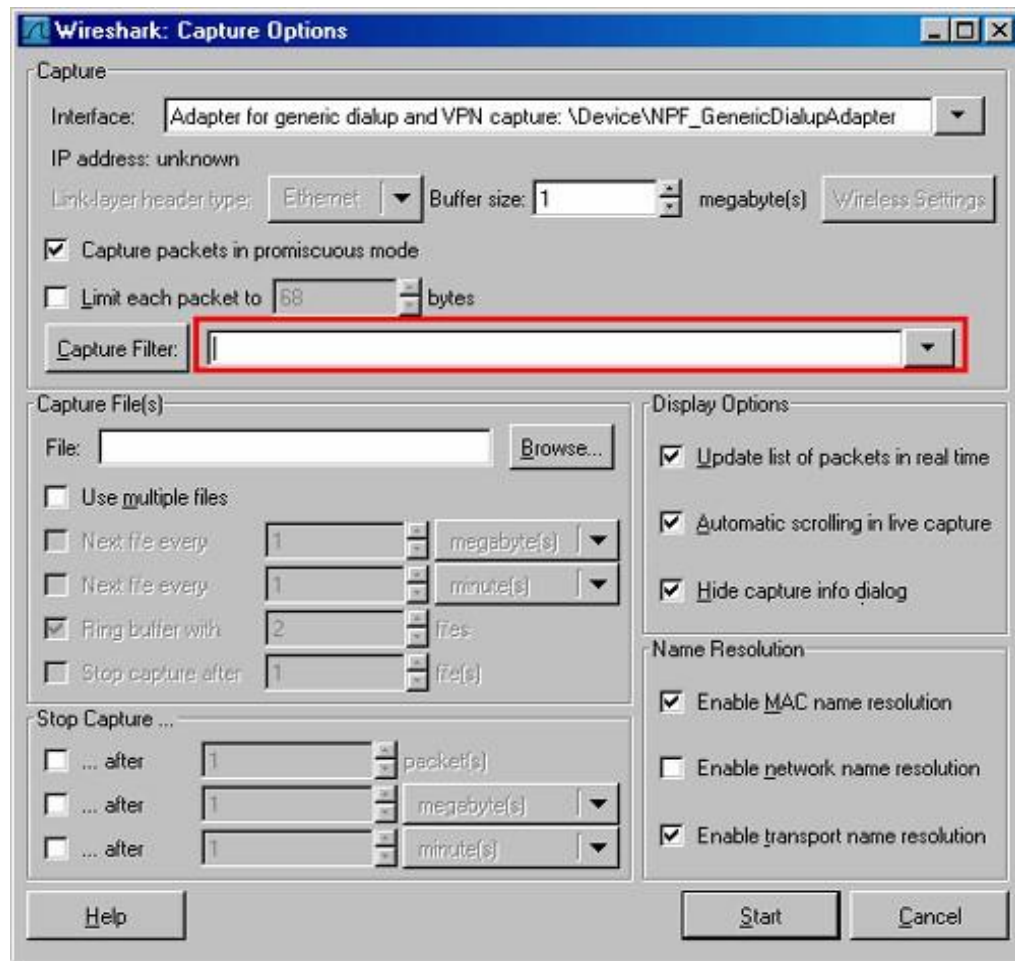
4.11 Φίλτρα σύλληψης

Η σύνταξη του φίλτρου σύλληψης είναι η ίδια που χρησιμοποιείται και στα προγράμματα που χρησιμοποιούν τη βιβλιοθήκη Libcap (Linux) ή τη Winpcap (Windows) όπως το δημοφιλές TCPdump. Το φίλτρο σύλληψης θα πρέπει να οριστεί πριν την έναρξη της σύλληψης με Wireshark. Για να ρυθμίσουμε ένα φίλτρο σύλληψης:

- επιλέγουμε capture > options,
- δίνουμε το όνομα που θέλουμε στο πεδίο capture filter ή πατάμε στο κουμπί capture filter για να επιλέξουμε κάποιο από τα έτοιμα φίλτρα και να το χρησιμοποιήσουμε και για τις καταγραφές μας.
- Πατάμε στο Start για τη σύλληψη των δεδομένων.



Εικόνα 17: Διαδικασία φίλτρων σύλληψης



Εικόνα 18: Βήματα και διαδικασίες για την ρύθμιση ενός φίλτρου σύλληψης

Η σύνταξη του φίλτρου σύλληψης είναι:

Πρωτόκολλο	Κατεύθυνση	Host(s)	Τιμή	Λογικές Πράξεις	Άλλες εκφράσεις
tcp	dst	10.1.1.1	80	and	

Τα φίλτρα σύλληψης μπορούν να πάρουν τις παρακάτω τιμές:

- **Πρωτόκολλο::** ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp, udp.

Εάν δεν δηλωθεί κανένα πρωτόκολλο, χρησιμοποιούνται όλα τα πρωτόκολλα.

- **Κατεύθυνση::** src, dst, src and dst, src or dst

Εάν δεν δηλωθεί ούτε πηγή ούτε προορισμός, οι λέξεις κλειδιά "src ή dst" εφαρμόζονται.

- **Host(s):** net, port, host, portrange.
Εάν δεν δηλωθεί host(s), χρησιμοποιείται η λέξη κλειδί "host".
- **Λογικές Πράξεις:** not, and, or.

Παραδείγματα:

- **tcp dst port 3130**
Δείχνει τα πακέτα με προορισμό την θύρα TCP 3130
- **ip src host 10.10.10.10**
Δείχνει τα πακέτα με τη διεύθυνση πηγής IP που ισούται με το 10.10.10.10.
- **host 10.11.21.31**
Δείχνει τα πακέτα με πηγή ή προορισμό τη διεύθυνση IP η οποία είναι ίση με το 10.11.21.31.
- **src portrange 2100-2459**
Δείχνει τα πακέτα με θύρες πηγής UDP ή TCP μεταξύ του εύρους 2100-2459
- **not icmp**
Δείχνει τα πάντα εκτός από τα πακέτα του icmp (το icmp χρησιμοποιείται τυπικά από το εργαλείο ping)
- **src host 10.8.3.11 and not dst net 10.100.0.0/24**
Δείχνει τα πακέτα με τη διεύθυνση IP πηγής η οποία ισούται με το 10.8.3.11 και την ίδια στιγμή όχι με τη διεύθυνση IP προορισμού του δικτύου 10.100.0.0/24.

- **(src host 10.5.2.11 or src net 10.7.0.0/24) and tcp dst portrange 222-11111 and dst net 10.1.1.1/8**

Δείχνει τα πακέτα με τη διεύθυνση IP πηγής 10.5.2.11 ή το δίκτυο πηγής 10.7.0.0/24, το αποτέλεσμα είναι η αλυσιδωτή σύνδεση των πακέτων τα οποία έχουν προορισμό το εύρος θυρών TCP από 222 έως 11111 και διεύθυνση IP του δικτύου προορισμού 10.1.1.1/8.

Σημειώσεις:

- Η αριστερή πλάγιος "\" χρησιμοποιείται όταν μια λέξη κλειδί χρησιμοποιείται ως τιμή.
- Το "ether proto ip" (ισούται με το "ip"). Αυτό έχει ως στόχο όλα τα πρωτόκολλα IP. Το "ip proto icmp" (ισούται με το "icmp"). Αυτό έχει ως στόχο τα icmp πακέτα τα οποία τυπικά χρησιμοποιούνται από το εργαλείο ping.
- Οι λέξεις κλειδιά "multicast" και "broadcast" μπορούν επίσης να χρησιμοποιηθούν μετά τις λέξεις "ip" ή "ether".
- Η λέξη κλειδί "no broadcast" είναι χρήσιμη όταν θέλουμε να αποκλείσουμε τις αιτήσεις μετάδοσης (broadcast requests).

4.12 Φίλτρα απεικόνισης

Τα φίλτρα απεικόνισης χρησιμοποιούνται για την εξαγωγή και απεικόνιση των ζητούμενων πακέτων από τα δεδομένα τα οποία έχουν συλληφθεί με κάποιο φίλτρο σύλληψης. Οι δυνατότητες αναζήτησης μπορούν να είναι μεγαλύτερες από εκείνες ενός φίλτρου σύλληψης και δεν είναι απαραίτητο να γίνει η επανεκκίνηση της σύλληψης όταν επιθυμήσουμε την αλλαγή του φίλτρου μας.

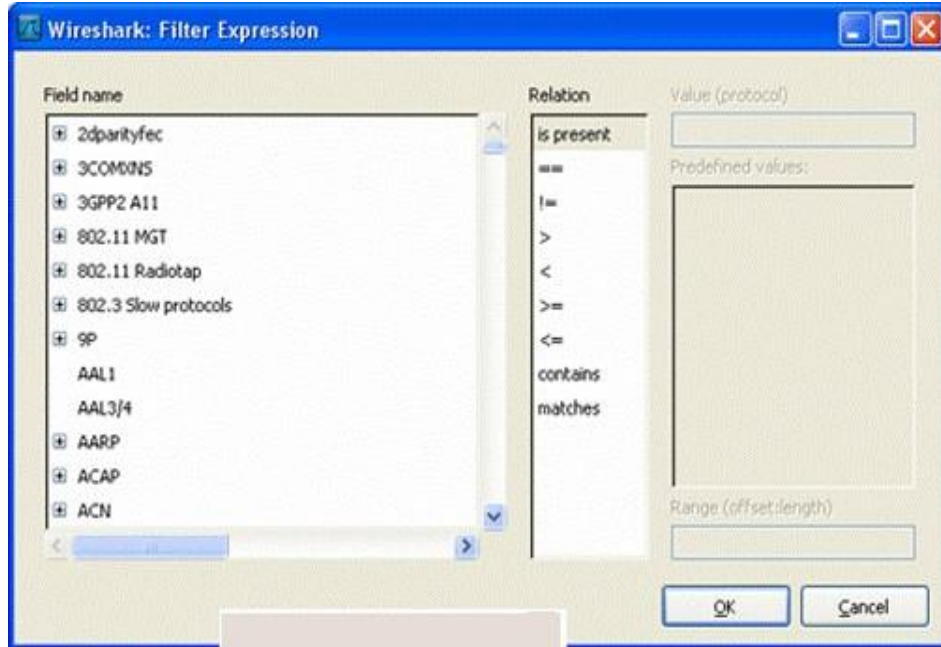
Η σύνταξη του φίλτρου σύλληψης είναι:

Πρωτόκολλο	Ακολουθία 1	Ακολουθία 2	Πράξη Σύγκρισης	Τιμή	Λογικές Πράξεις	Άλλες εκφράσεις
ftp	passive	ip	==	10.1.1.1	or	icmp.type

Τα φίλτρα απεικόνισης μπορούν να πάρουν τις παρακάτω τιμές:

- **Πρωτόκολλο:** IP, TCP, DNS, SSH

και πάρα πολλά άλλα τα οποία βρίσκονται διαθέσιμα μέσω της παρακάτω επιλογής:



Εικόνα 19 :Διαθέσιμα Πρωτόκολλα φίλτρου απεικόνισης

- **Ακολουθία 1, Ακολουθία 2: (προαιρετικές επιλογές)**
Υπό-πρωτόκολλα σύμφωνα με τα αρχικά πρωτόκολλά τους

- **Πράξη σύγκρισης:**

==	!=	>	<	>=	<=
Ίσο	Διάφορο	Μεγαλύτερο	Μικρότερο	Μεγαλύτερο ή Ίσο	Μικρότερο ή Ίσο

- **Λογικές εκφράσεις:**

&&		^^	!
Λογικό AND	Λογικό OR	Λογικό XOR	Λογικό NOT

Παραδείγματα:

- **snmp || dns || icmp**

Εμφάνιση μεταφορών SNMP ή DNS ή ICMP

- **ip.addr == 10.2.3.4**

Εμφανίζει τα πακέτα με διεύθυνση IP πηγής ή προορισμού η οποία ισούται με 10.2.3.4

- **ip.src != 10.7.8.9 or ip.dst != 10.6.5.4**

Εμφανίζει τα πακέτα με διεύθυνση IP πηγής διαφορετική της 10.7.8.9 ή με διεύθυνση IP προορισμού διαφορετική της 10.6.5.4. Με άλλα λόγια, τα εμφανιζόμενα πακέτα θα έχουν:

διεύθυνση IP πηγής: οποιαδήποτε εκτός της 10.7.8.9

διεύθυνση IP προορισμού: οποιαδήποτε

διεύθυνση IP πηγής: οποιαδήποτε

διεύθυνση IP προορισμού: οποιαδήποτε εκτός της 10.4.5.6

- **ip.src != 10.7.8.9 and ip.dst != 10.6.5.4**

Εμφανίζει τα πακέτα με διεύθυνση IP πηγής διαφορετική από την 10.7.8.9 και την ίδια στιγμή με διεύθυνση IP προορισμού διαφορετική της 10.6.5.4. Με άλλα λόγια, τα εμφανιζόμενα πακέτα θα έχουν:

διεύθυνση IP πηγής: οποιαδήποτε εκτός της 10.7.8.9

διεύθυνση IP προορισμού: οποιαδήποτε εκτός της 10.6.5.4

- **tcp.port == 35**

Εμφανίζει τα πακέτα πηγής TCP ή προορισμό την θύρα 35.

- **tcp.dstport == 35**

Εμφανίζει τα πακέτα προορισμού TCP με θύρα προορισμού 35.

- **tcp.flags**

Εμφανίζει τα πακέτα με σημαία TCP.

- **tcp.flags.syn == 0x02**

Εμφανίζει τα πακέτα με σημαία TCP SYN.

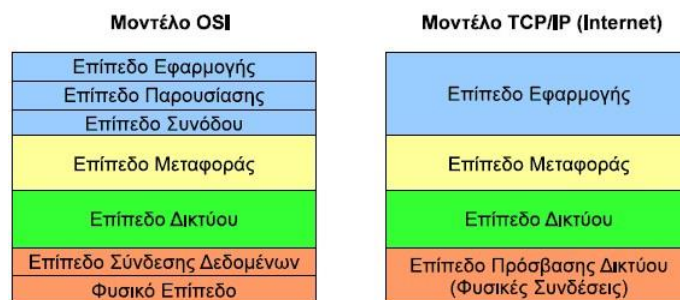
Κατά τη πληκτρολόγηση του φίλτρου το Wireshark ελέγχει την ορθότητα ή όχι της σύνταξης. Εάν η σύνταξη του φίλτρου είναι σωστή, το πλαίσιο σύνταξης θα γίνει πράσινο, ενώ εάν είναι λάθος, το πλαίσιο σύνταξης θα γίνει κόκκινο.

ΚΕΦΑΛΑΙΟ 5ο: OSI, TCP/IP και WIRESHARK

5.1 Συσχέτιση μοντέλου OSI και μοντέλου TCP/IP

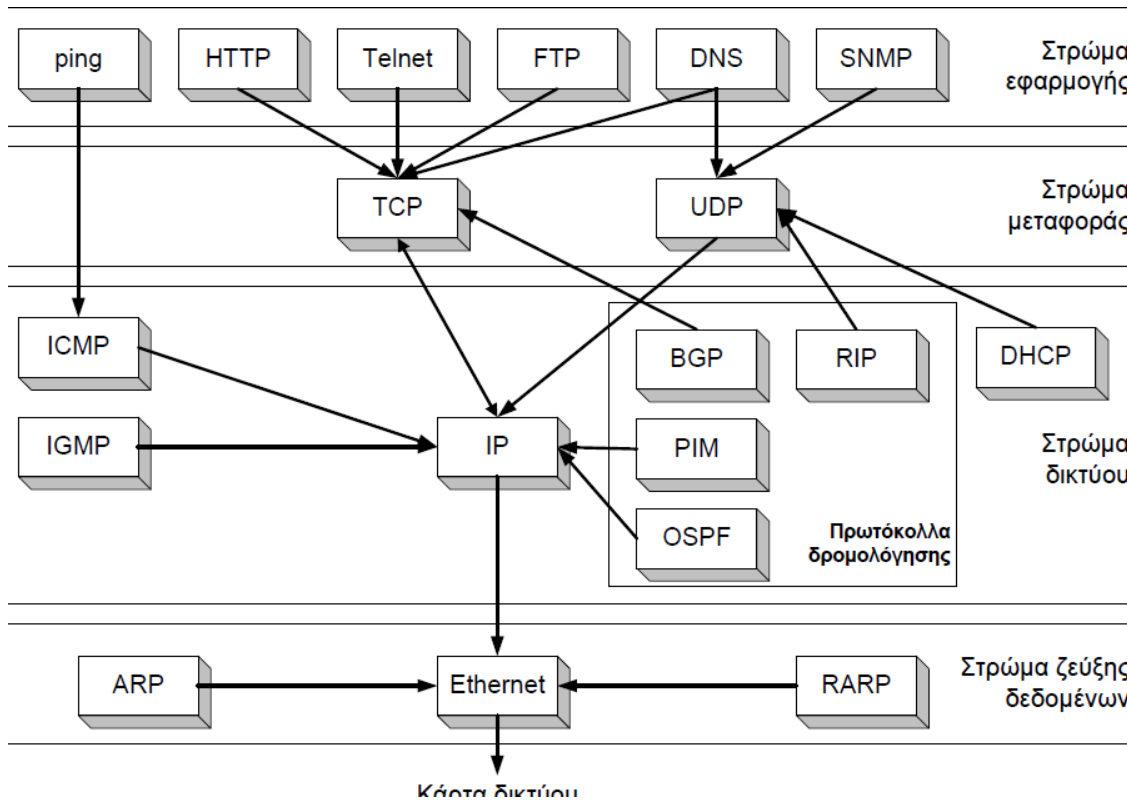
Το λογισμικό Wireshark βασίζεται στην κατανομή των επιπέδων του μοντέλου TCP/IP. Το TCP/IP είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων που περιέχει, το TCP ή Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μετάδοσης) και το IP ή Internet Protocol (Πρωτόκολλο Διαδικτύου).

Αυτή η συλλογή πρωτοκόλλων, είναι οργανωμένη σε 4 στρώματα ή επίπεδα (layers) και αποτελεί εξέλιξη του μοντέλου OSI, το οποίο παραμένει έως σήμερα μόνο θεωρητικό και προτείνει την κατάταξη των πρωτοκόλλων δικτύων σε έναν οργάνωση 7 στρωμάτων. Το καθένα τους απαντά σε συγκεκριμένα προβλήματα μεταφοράς δεδομένων και παρέχει μια καθορισμένη υπηρεσία στα υψηλότερα στρώματα. Τα ανώτερα επίπεδα είναι πιο κοντά στη λογική του χρήστη και εξετάζουν πιο αφηρημένα δεδομένα, στηριζόμενα σε πρωτόκολλα χαμηλότερων στρωμάτων για να μεταφράσουν δεδομένα σε μορφές που μπορούν να διαβιβαστούν με φυσικά μέσα. Στο παρακάτω σχήμα φαίνεται η σχέση των δυο μοντέλων.



Εικόνα 20: Σχέση μοντέλου OSI και μοντέλου TCP/IP

Στο παρακάτω σχήμα φαίνεται η αντιστοίχιση των βασικότερων πρωτοκόλλων στα αντίστοιχα επίπεδα του μοντέλου TCP/IP:

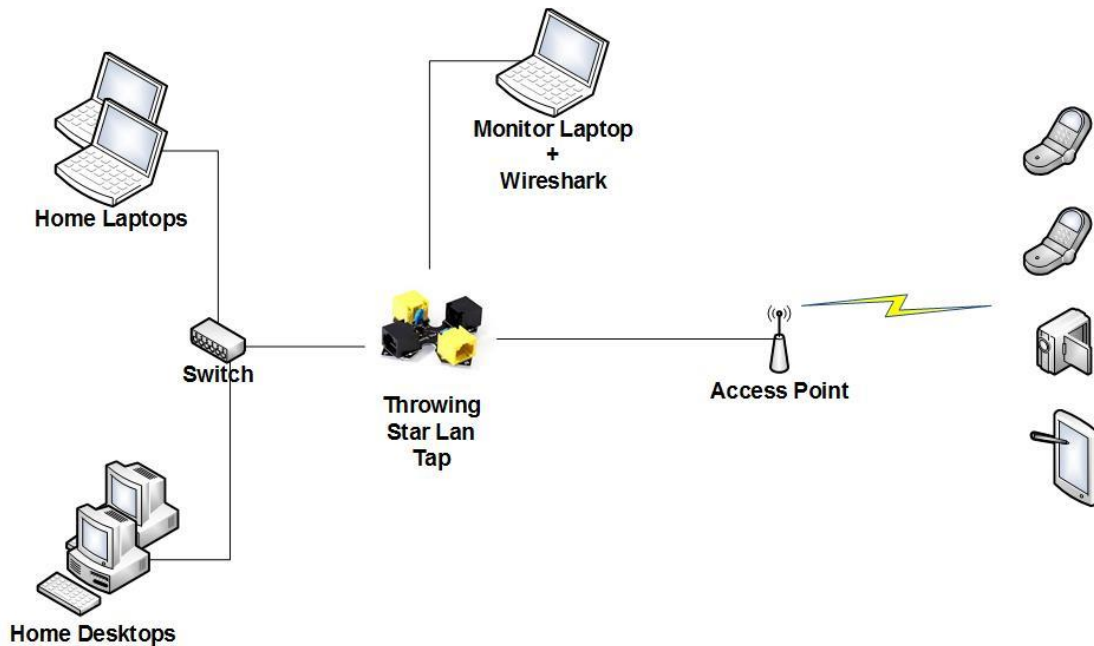


Εικόνα 21: Βασικά πρωτόκολλα στα επίπεδα του μοντέλου TCP/IP

Στον κόσμο των δικτύων και του Internet, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν τον τρόπο που ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα. Τα πρωτόκολλα είναι αυτά που καθορίζουν το πώς διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος, ο χειρισμός των λαθών, κλπ.

5.2 Συνδεσμολογία Ακροατή Πακέτων

Για τις ανάγκες της εκπόνησης των παραδειγμάτων της παρούσας εργασίας θα συνδέσουμε τον Ακροατή Πακέτων Throwing Star LAN Tap μεταξύ ενός switch και ενός ασύρματου Access Point το οποίο εκπέμπει σήμα wifi στην οικία και στο οποίο είναι συνδεδεμένες διάφορες συσκευές (κινητά τηλέφωνα και tablet καθώς και μία ασύρματη κάμερα. Η συνδεσμολογία φαίνεται στο παρακάτω σχήμα:



Εικόνα 22: Συνδεσμολογία για την εκπόνηση των παραδειγμάτων

5.3 Επίπεδο 1 TCP/IP :Το επίπεδο Πρόσβασης Δικτύου

Ο ρόλος του επιπέδου Πρόσβασης Δικτύου είναι η διακίνηση πακέτων του επιπέδου δικτύου μεταξύ δυο οντοτήτων. Το φυσικό επίπεδο, που αποτελείται από τα φυσικά στοιχεία του δικτύου (π.χ. hubs, καλώδια δικτύου, οπτικές ίνες, ομοαξονικά καλώδια, κάρτες δικτύων) και τις προδιαγραφές χαμηλού επιπέδου των σημάτων (τάση, συχνότητα, κλπ.), θεωρείται συχνά ως μέρος του επιπέδου ζεύξης δεδομένων.

Βασικότερα πρωτόκολλα επιπέδου Πρόσβασης Δικτύου: Ethernet, MAC, ARP, WiFi

5.3.1 Πρωτόκολλο Ethernet

Το Ethernet είναι το συνηθέστερο χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα (LAN).

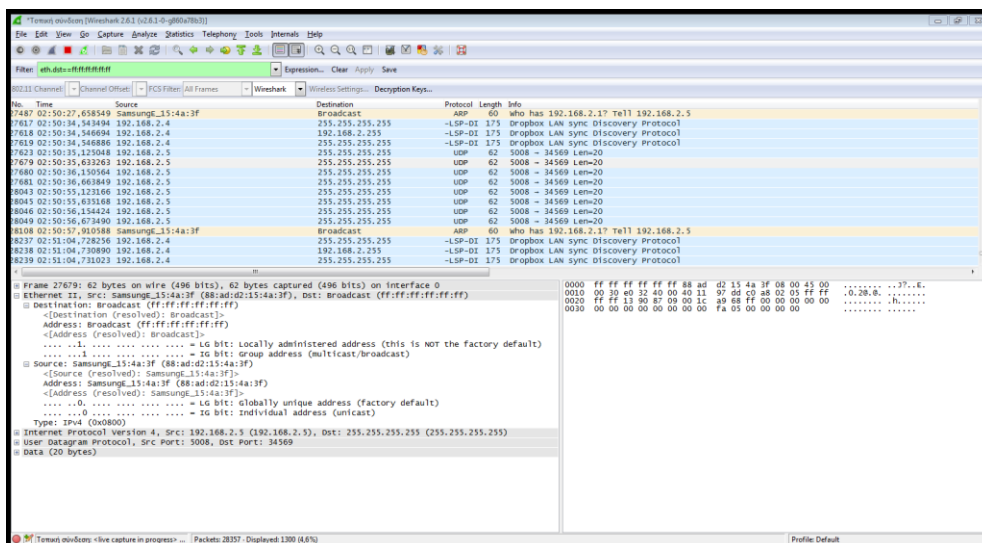
Πρακτικά, το Ethernet χρησιμοποιεί τη μέθοδο μετάδοσης δεδομένων σε μορφή πακέτων (packet switching) μέγιστου μεγέθους (Maximum Transmission Unit, MTU) 1500 bytes και ελάχιστου 46 bytes. Για το σκοπό αυτό, δεδομένα με μήκος μεγαλύτερο των 1500 bytes κατατέμνονται σε πακέτα των 46-1500 bytes (το

λεγόμενο payload) τα οποία αποστέλλονται διαδοχικά στη γραμμή επικοινωνίας. Αν το payload έχει μήκος μικρότερο των 46 bytes, προστίθενται επιπλέον κενά bytes ώστε αυτό να αποκτήσει το επιθυμητό ελάχιστο μήκος. Επιπλέον του payload, προστίθενται πληροφορίες όπως ο σειριακός αριθμός της κάρτας Ethernet, οι φυσικές διευθύνσεις (MAC addresses) αποστολέα και παραλήπτη, το μήκος του payload, καθώς και δεδομένα για έλεγχο σφαλμάτων κατά τη μετάδοση.

5.3.2 Wireshark και Ethernet

Φίλτρα απεικόνισης	
eth	all Ethernet based
eth.addr==08:00:08:15:ca:fe	to and from Ethernet MAC address 08:00:08:15:ca:fe
!(eth.addr==08:00:08:15:ca:fe)	all except to and from Ethernet MAC address 08:00:08:15:ca:fe
eth.dst==ff:ff:ff:ff:ff:ff	Ethernet Broadcast only
eth.dst!=ff:ff:ff:ff:ff:ff	all except Ethernet Broadcast
(eth.dst[0] & 1)	Ethernet Multicast only (least significant bit of first address byte set)
!(eth.dst[0] & 1)	all except Ethernet Multicast (least significant bit of first address byte not set)

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των broadcast μηνυμάτων:



Εικόνα 23: Παράδειγμα Ethernet

5.3.3 Πρωτόκολλο MAC

Κάθε συσκευή που επικοινωνεί σε ένα δίκτυο διαθέτει δύο διευθύνσεις: Η μία είναι η διεύθυνση IP η οποία αποδίδεται από το πρωτόκολλο δικτύου και η άλλη είναι η φυσική διεύθυνση γνωστή και ως διεύθυνση υλικού (hardware address).

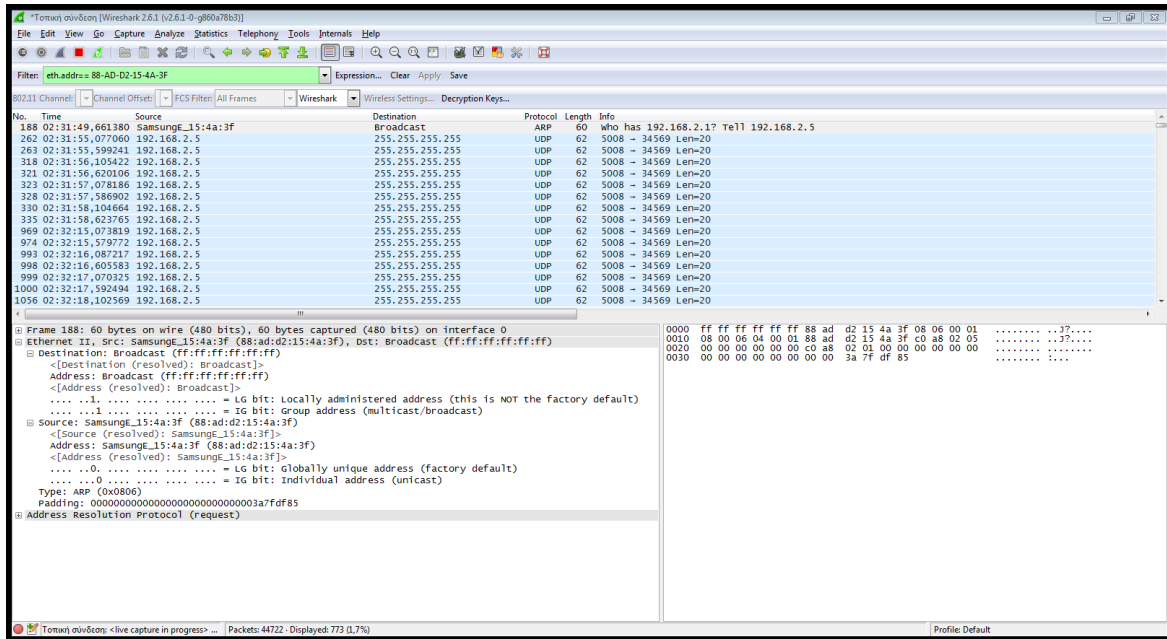
Οι φυσικές διευθύνσεις είναι μοναδικές, γιατί διαφορετικά δεν θα μπορούσαμε να προσδιορίσουμε τις συσκευές στο δίκτυο. Για παράδειγμα μια κάρτα δικτύου (που είναι από τις πλέον κοινές συσκευές σε ένα δίκτυο) διαθέτει μια φυσική διεύθυνση που της έχει αποδοθεί από τον κατασκευαστή της στο στάδιο της κατασκευής της. Σύμφωνα με το μοντέλο OSI, η φυσική διεύθυνση βρίσκεται στο υποεπίπεδο πρόσβασης στο μέσο γνωστό και ως Media Access Control, για το λόγο αυτό ονομάζεται και διεύθυνση MAC.

Μια διεύθυνση MAC (Media Access Control - έλεγχος πρόσβασης σε μέσα) είναι ένας δεκαεξαδικός σειριακός αριθμός (ως προς την αναπαράσταση) ο οποίος είναι μοναδικός για κάθε δικτυακή συσκευή. Ο αριθμός έχει τη μορφή xx:xx:xx:xx:xx:xx, για παράδειγμα 0A:12:A1:B2:AE:04 για την 16-δική αναπαράσταση.

5.3.4 Wireshark και MAC

Φίλτρα απεικόνισης	
eth.addr==08.00.08.15.ca.fe	to and from Ethernet MAC address 08:00:08:15:ca:fe
!(eth.addr==08.00.08.15.ca.fe)	all except to and from Ethernet MAC address 08:00:08:15:ca:fe

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των πακέτων ενός κινητού τηλεφώνου με MAC Address 88-AD-D2-15-4A-3F:



Εικόνα 24: Παράδειγμα MAC

5.3.5 Πρωτόκολλο ARP

Έχουμε πλέον μιλήσει και για τα δύο είδη διευθύνσεων: Τη φυσική (MAC) διεύθυνση που δίνει ο κατασκευαστής του δικτυακού υλικού στις συσκευές του (π.χ. στις κάρτες δικτύου). Τη διεύθυνση IP που ανήκει στην τεχνολογία TCP/IP και αποδίδεται στις συσκευές του δικτύου από τον διαχειριστή του δικτύου.

Η μετατροπή μιας IP διεύθυνσης στην αντίστοιχη φυσική σε ένα περιβάλλον τοπικού δικτύου επιτυγχάνεται με το πρωτόκολλο ARP (Address Resolution Protocol,

Πρωτόκολλο Μετατροπής Διεύθυνσης) που ανήκει στα πρωτόκολλα του χαμηλότερου επιπέδου (Σύνδεσης Δικτύου) στην ιεραρχία του TCP/IP. Αυτό θα μπορούσε και να επιτευχθεί αποθηκεύοντας την αντιστοίχιση αυτή σε ένα πίνακα δύο στηλών (IP Διεύθυνση, Φυσική Διεύθυνση). Ωστόσο αν κάνουμε αυτή τη διαδικασία χειροκίνητα, σύντομα θα έχουμε μεγάλο πρόβλημα ειδικά για μεγάλα δίκτυα. Το πρωτόκολλο ARP κάνει ακριβώς αυτή την αντιστοίχιση από IP διεύθυνση στην φυσική και διατηρεί τον πίνακα *δυναμικά*. Αυτό σημαίνει ότι αναλαμβάνει να ανακαλύψει αρχικά ποια διεύθυνση IP αντιστοιχεί σε ποια διεύθυνση MAC αλλά και να ενημερώνει αυτές τις καταχωρίσεις όταν προστίθενται νέα μηχανήματα (ή όταν γίνεται αλλαγή διευθύνσεων σε υπάρχοντα). Κεντρικό στοιχείο στη λειτουργία του πρωτοκόλλου ARP είναι ο πίνακας δύο στηλών (IP Διεύθυνση, Φυσική Διεύθυνση). Κάθε γραμμή του πίνακα αντιστοιχεί σε μια εγγραφή δηλ. σε μια συσκευή.

IP Διεύθυνση	Ethernet Διεύθυνση
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Εικόνα 25: Πίνακας ARP

Όταν το πρωτόκολλο ARP λάβει μια διεύθυνση IP, αρχικά θα διερευνήσει τον πίνακα ARP για να δει αν υπάρχει η αντίστοιχη εγγραφή:

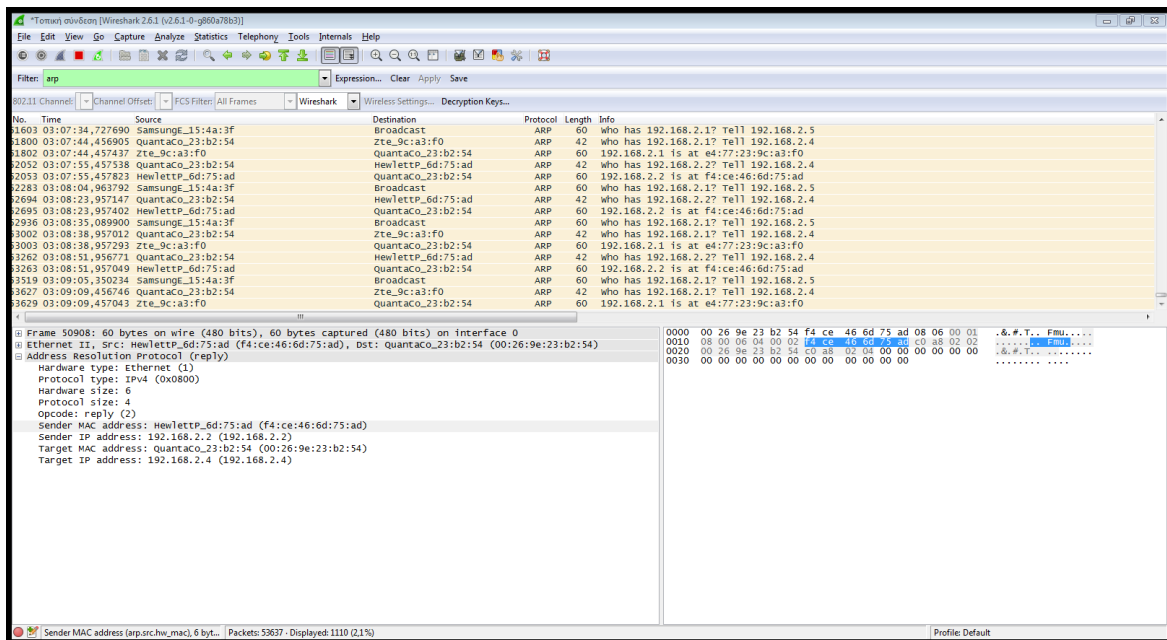
- Αν βρεθεί η εγγραφή στον πίνακα ARP, το πρωτόκολλο θα επιστρέψει την αντίστοιχη φυσική διεύθυνση που αναφέρει ο πίνακας.
- Αν δεν βρεθεί εγγραφή, το πρωτόκολλο θα δημιουργήσει μια αίτηση ARP. Η αίτηση αυτή είναι ένα μήνυμα το οποίο απευθύνεται σε όλα τα μηχανήματα του τοπικού δικτύου. Περιέχει την διεύθυνση IP του υπολογιστή προορισμού. Αν μια συσκευή στο δίκτυο αναγνωρίσει αυτή την IP ως δική της, θα στείλει τη φυσική της διεύθυνση ως απάντηση στη συσκευή που δημιούργησε την αίτηση. Αμέσως μετά τη λήψη της απάντησης, η συσκευή που δημιούργησε την αίτηση θα ενημερώσει τον πίνακα ARP, δημιουργώντας μια νέα εγγραφή με τη διεύθυνση IP και τη φυσική διεύθυνση της συσκευής που μόλις έλαβε. Όταν χρειαστεί ξανά να βρει τη φυσική διεύθυνση αυτής της συσκευής, θα διαβάσει απλώς τον πίνακα και δεν θα χρειαστεί να δημιουργηθεί νέο αίτημα ARP.

Όταν μια ARP εγγραφή δεν έχει χρησιμοποιηθεί για μεγάλο χρονικό διάστημα, στα περισσότερα συστήματα διαγράφεται αυτόματα.

5.3.6 Wireshark και ARP

Φίλτρα απεικόνισης	
arp	Απεικονίζονται μόνο τα ARP μηνύματα

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των πακέτων ενός εκτυπωτή HewlettP_6d:75:ad (f4:ce:46:6d:75:ad) :



Εικόνα 26: Παράδειγμα ARP

5.3.7 WiFi

Το IEEE 802.11 είναι μια οικογένεια προτύπων της IEEE για ασύρματα τοπικά δίκτυα (WLAN) που είχαν ως σκοπό να επεκτείνουν το 802.3 (Ethernet, το συνηθέστερο πρωτόκολλο ενσύρματης δικτύωσης υπολογιστών) στην ασύρματη περιοχή. Τα πρότυπα 802.11 είναι ευρύτερα γνωστά ως «WiFi» επειδή η WiFi Alliance, ένας οργανισμός ανεξάρτητος της IEEE, παρέχει την πιστοποίηση για τα προϊόντα που υπακούουν στις προδιαγραφές του 802.11. Αυτή η οικογένεια πρωτοκόλλων αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων.

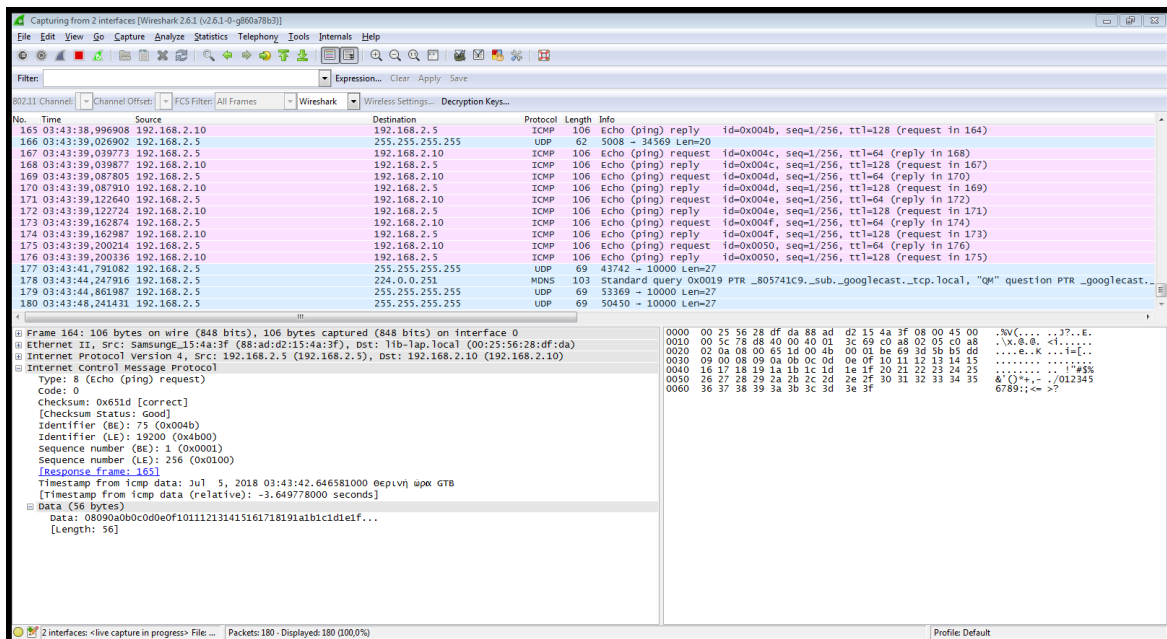
Ο όρος WiFi (Wireless Fidelity) χρησιμοποιείται για να προσδιορίσει τις συσκευές που βασίζονται στην προδιαγραφή IEEE 802.11 b/g/n και εκπέμπουν σε συχνότητες 2.4GHz. Ωστόσο το WiFi (ασύρματη πιστότητα) έχει επικρατήσει και ως όρος αναφερόμενος συνολικά στα ασύρματα τοπικά δίκτυα. Συνήθεις εφαρμογές του είναι η παροχή ασύρματων δυνατοτήτων πρόσβασης στο Internet, τηλεφωνίας μέσω διαδικτύου (VoIP) και διασύνδεσης μεταξύ ηλεκτρονικών συσκευών όπως τηλεοράσεις, ψηφιακές κάμερες, DVD Player και ηλεκτρονικοί υπολογιστές. Σε φορητές ηλεκτρονικές συσκευές το 802.11 βρίσκει εφαρμογές ασύρματης μετάδοσης, όπως π.χ. στη μεταφορά φωτογραφιών από ψηφιακές κάμερες σε υπολογιστές για περαιτέρω επεξεργασία και εκτύπωση, αν και σε αυτόν τον τομέα

έχει υποσκελιστεί από το πρωτόκολλο Bluetooth για τα πολύ μικρότερης εμβέλειας ασύρματα προσωπικά δίκτυα.

5.3.8 Wireshark και WiFi

Φίλτρα καταγραφής
wlan host 88-AD-D2-15-4A-3F

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των πακέτων (μέσω ασύρματου δικτύου) ενός κινητού τηλεφώνου με MAC address 88-AD-D2-15-4A-3F το οποίο κάνει ping:



Εικόνα 27: Παράδειγμα WLAN

5.4 Επίπεδο 2 TCP/IP: Το επίπεδο Δικτύου

Το επίπεδο Διαδικτύου παραλαμβάνει τα πακέτα από το επίπεδο μεταφοράς (πρωτόκολλα TCP και UDP) και παρέχει την υπηρεσία παράδοσης του πακέτου στο επίπεδο μεταφοράς του προορισμού. Επίσης εδώ εκτελούνται τα πρωτόκολλα δρομολόγησης που καθορίζουν τα δρομολόγια που θα ακολουθήσουν τα πακέτα ανάμεσα στον αποστολέα και τον παραλήπτη.

Βασικότερα πρωτόκολλα επιπέδου Δικτύου: IP

5.4.1 Πρωτόκολλο IP

Στο επίπεδο δικτύου της τεχνολογίας TCP/IP, συναντάμε το πρωτόκολλο IP, (Internet Protocol). Η λειτουργία του IP βασίζεται αποκλειστικά στην ιδέα του

αυτοδύναμου πακέτου ή datagram, το οποίο σημαίνει ότι τα πακέτα μεταφέρονται από την πηγή στον προορισμό χωρίς να ακολουθούν συγκεκριμένη διαδρομή (το κάθε ένα μπορεί να ακολουθήσει διαφορετική). Οι έλεγχοι για αξιόπιστη μετάδοση γίνονται από το επίπεδο μεταφοράς, εφόσον χρησιμοποιείται το πρωτόκολλο TCP. Κάθε φορά που το TCP ή το UDP πρωτόκολλο από το επίπεδο μεταφοράς θέλει να μεταδώσει κάποιο τμήμα (θυμηθείτε ότι το TCP και το UDP παράγουν segments), το παραδίδει στο πρωτόκολλο IP. Η μόνη άλλη πληροφορία που χρειάζεται το IP (και η οποία του παρέχεται από το επίπεδο μεταφοράς) είναι η *διεύθυνση του υπολογιστή προορισμού*. Αυτό είναι και το μόνο στοιχείο που ενδιαφέρει το πρωτόκολλο IP.

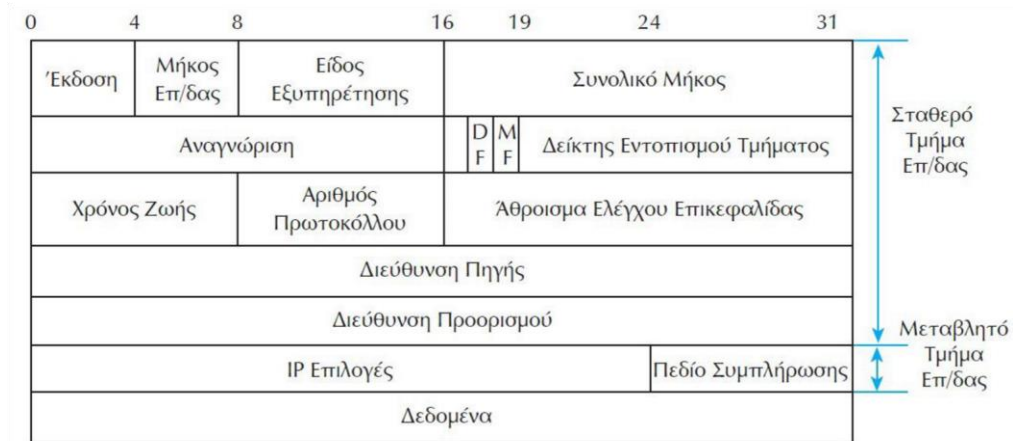
Το IP δεν ενδιαφέρεται καθόλου για το περιεχόμενο του τμήματος ή για το πως (και αν) σχετίζεται με το προηγούμενο ή επόμενο τμήμα που λαμβάνει. Απλώς τα προωθεί στον προορισμό τους. Για να γίνει αυτό βέβαια, θα πρέπει το IP αφού παραλάβει το τμήμα από το επίπεδο μεταφοράς να προσθέσει τη δική του επικεφαλίδα με τα απαραίτητα στοιχεία, σχηματίζοντας έτσι ένα αυτοδύναμο IP πακέτο. Το μέγιστο μήκος του πακέτου αυτού έχει ορισθεί στα 64 Kbytes. Μετά το σχηματισμό του πακέτου, αποστολή του IP είναι να βρει την κατάλληλη διαδρομή που θα το οδηγήσει στον προορισμό του. Μετά τον προσδιορισμό της διαδρομής του πακέτου, γίνεται η μετάδοση του μέσω των φυσικών δικτύων (που αντιστοιχούν στο επίπεδο πρόσβασης δικτύου της τεχνολογίας TCP/IP).

Ένα φυσικό δίκτυο μπορεί ωστόσο να χρησιμοποιεί διαφορετικό μέγιστο μήκος μονάδας μεταφοράς σε σχέση με τα 64 Kbyte που χρησιμοποιεί το IP. Στην περίπτωση που το IP πακέτο “δεν χωράει να περάσει” μέσα από το συγκεκριμένο φυσικό δίκτυο το πρωτόκολλο IP έχει τη δυνατότητα να διασπάσει τα αυτοδύναμα πακέτα σε μικρότερα τμήματα που ονομάζονται κομμάτια ή fragments. Το IP αναλαμβάνει να επανασυνθέσει αυτά τα κομμάτια στον προορισμό τους και να σχηματίσει ξανά το αρχικό αυτοδύναμο IP πακέτο.

Η διάσπαση των πακέτων σε fragments γίνεται όταν το πακέτο φτάσει στον πρώτο δρομολογητή του δικτύου. Ο δρομολογητής αντιλαμβάνεται ότι το φυσικό δίκτυο που συνδέεται σε αυτόν δεν μπορεί να μεταδώσει ολόκληρο το πακέτο που έλαβε και το διασπά σε κομμάτια. (Μη ξεχνάμε ότι ο δρομολογητής είναι μια συσκευή που λειτουργεί στο επίπεδο δικτύου και άρα αντιλαμβάνεται τις πληροφορίες της επικεφαλίδας IP). Τα κομμάτια που δημιουργούνται είναι και αυτά

εντελώς αυτοδύναμα και ανεξάρτητα μεταξύ τους και μπορεί πάλι το καθένα να ακολουθήσει διαφορετική διαδρομή μέχρι τον προορισμό

Έτσι κάθε πακέτο IP, αποτελείται από μια κεφαλίδα και στη συνέχεια ακολουθούν τα δεδομένα. Στη κεφαλίδα αυτή εμπεριέχονται πληροφορίες: πρώτον, για τα δεδομένα που εμπεριέχονται στο πακέτο και δεύτερον, οι διευθύνσεις αφετηρίας και προορισμού. Η διαδικασία προσθήκης της κεφαλίδας σε ένα πακέτο δεδομένων ονομάζεται ενθυλάκωση.

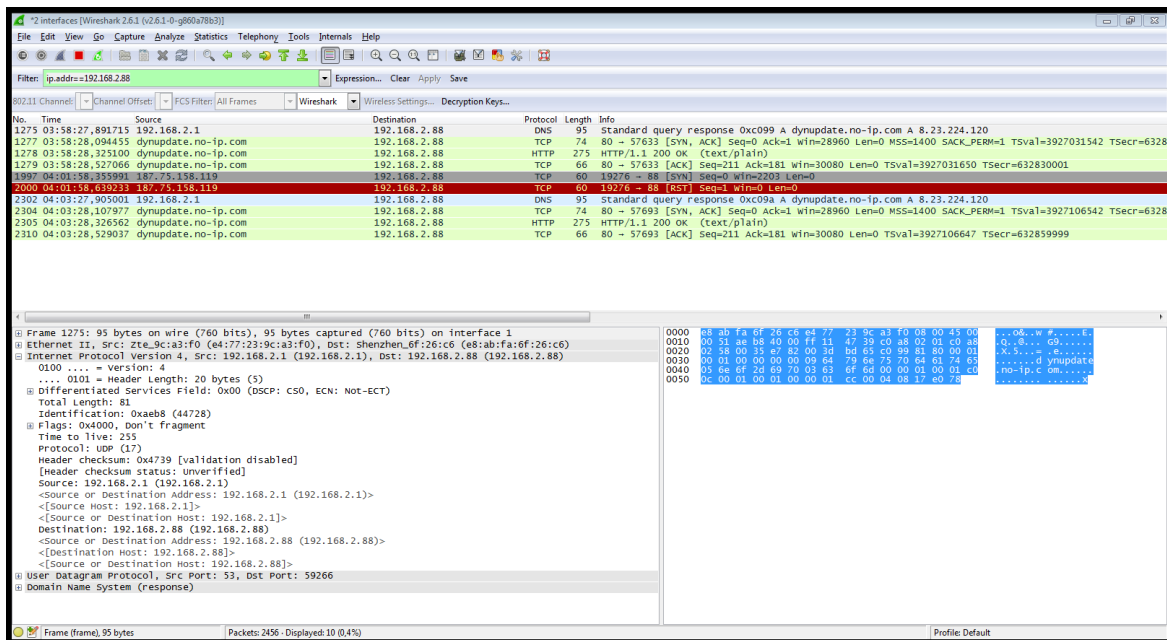


Εικόνα 28: Επικεφαλίδα IP

5.4.2 Wireshark και IP

Φίλτρα απεικόνισης	
ip.addr==192.168.2.88	Απεικονίζονται μόνο τα IP μηνύματα

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των IP πακέτων μίας διαδικτυακής κάμερας με IP 192.168.2.88:



Εικόνα 29: Παράδειγμα IP

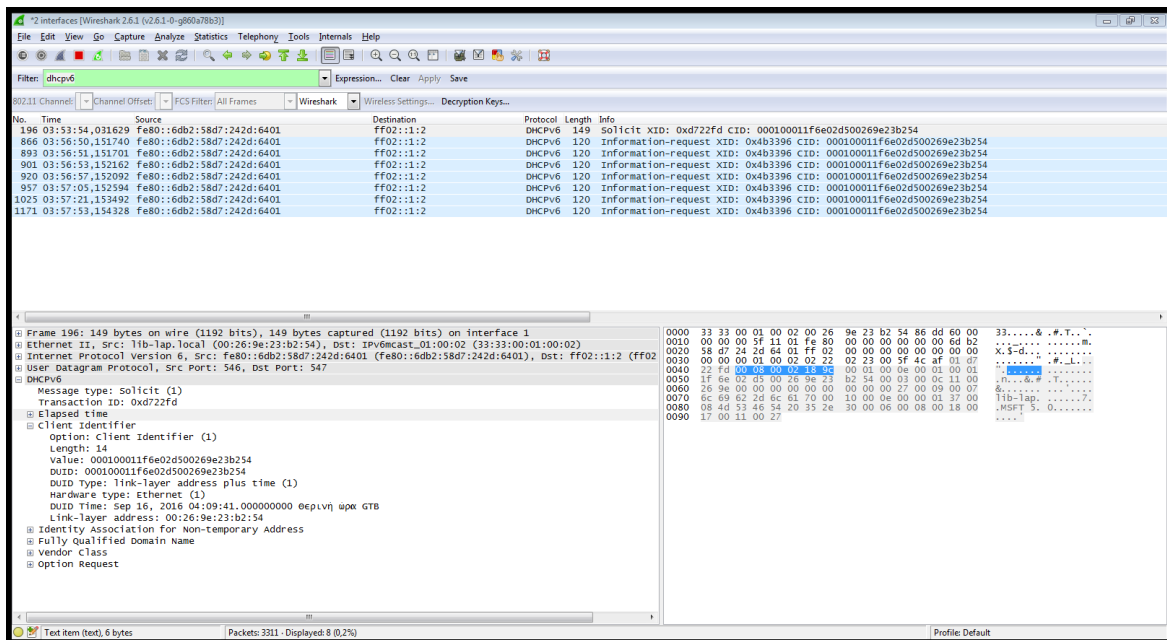
5.4.3 Πρωτόκολλο DHCP

Για να συνδέσουμε έναν υπολογιστή σε ένα δίκτυο, στο συγκεκριμένο υπολογιστή πρέπει να ταξινομηθεί μια μοναδική διεύθυνση. Αυτό επιτυγχάνεται μέσω του **DHCP** (Πρωτοκόλλου Δυναμικής Διαμόρφωσης Κεντρικού Υπολογιστή Δικτύου ή Dynamic Host Configuration Protocol). Το συγκεκριμένο πρωτόκολλο, γνωστό και ως αυτόματη διευθυνσιοδότηση δικτύου, αντιστοιχεί αυτόματα τις ρυθμίσεις παραμέτρων του δικτύου σε έναν εξυπηρετητή (Client). Με τον τρόπο αυτό δεν χρειάζεται να ασχοληθούμε εμείς με την παραμετροποίηση που θα καταστήσουν την επικοινωνία δυνατή. Η εφαρμογή του πρωτοκόλλου DHCP σε ένα δίκτυο, λαμβάνει χώρα ως μια αρχιτεκτονική πελάτη διακομιστή (client server) στην οποία ο υπολογιστής που ζητά να του χορηγηθεί μια δυναμική IP διεύθυνση είναι ο υπολογιστής πελάτης (DHCP client) ενώ ο υπολογιστής που θα του χορηγήσει τη διεύθυνση είναι ο διακομιστής (DHCP server) της υπηρεσίας

5.4.4 Wireshark και DHCP

Φίλτρα απεικόνισης	
dhcpv6	Απεικονίζονται μόνο τα IPv6 μηνύματα

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των DHCP πακέτων της κάρτας δικτύου:



Εικόνα 30: Παράδειγμα IP

5.4.5 Πρωτόκολλο NAT

Γενικά δεν μπορεί να αποδοθεί αυθαίρετα ένας οποιοσδήποτε 32-bit αριθμός σε έναν υπολογιστή – υπάρχουν διάφορες **κλάσεις IP διευθύνσεων** και ο κάθε υπολογιστής μπορεί να έχει ως διεύθυνση κάποιον αριθμό της κλάσης στην οποία ανήκει μόνο. Ειδικά για τα ιδιωτικά δίκτυα, όπου ο αριθμός τους ανά τον κόσμο είναι συντριπτικά μεγάλος (ας αναλογιστούμε για παράδειγμα ότι σε κάθε απλό εργαστήριο Πληροφορικής σε ένα σχολείο υπάρχει ένα τοπικό ιδιωτικό δίκτυο), οι IP διευθύνσεις που μπορούν να έχουν οι υπολογιστές μπορούν να ανήκουν μόνο σε κάποια από τις τρεις επόμενες κλάσεις:

- 10.0.0.0 - 10.255.255.255 (Class A)
- 172.16.0.0 - 172.31.255.255 (Class B)
- 192.168.0.0 - 192.168.255.255 (Class C)

Έτσι, μπορούν ταυτόχρονα δύο διαφορετικοί υπολογιστές που ανήκουν σε διαφορετικά δίκτυα να έχουν την ίδια IP διεύθυνση (στο τοπικό ιδιωτικό του δίκτυο ο καθένας). Από την άλλη πλευρά όμως, αυτό το χαρακτηριστικό γίνεται μειονέκτημα όταν χρειαστεί να συνδεθούν δύο τέτοια δίκτυα – στο νέο μεγαλύτερο δίκτυο που δημιουργείται, είναι πιθανό να βρεθούν δύο υπολογιστές με την ίδια IP διεύθυνση - αυτό βέβαια δεν πρέπει να επιτραπεί να συμβεί. Το παραπάνω λοιπόν πρόβλημα αντιμετωπίζεται με το πρωτόκολλο **NAT** (Network Address Translation), ένα ειδικό πρωτόκολλο που εκτελούν οι πύλες (gateways) και έχει σαν αποτέλεσμα

να αλλάζει την IP διεύθυνση ενός πακέτου που ξεκινά από έναν υπολογιστή εντός του τοπικού δικτύου και προωθείται εκτός του δικτύου.

Πιο συγκεκριμένα, το NAT δουλεύει ως εξής: Κάθε υπολογιστής ενός ιδιωτικού δικτύου που ζητάει να συνδεθεί με κάποιον εκτός δικτύου, κάνει αίτηση στον NAT (που υπάρχει στην πύλη (gateway ή firewall)) για να πάρει μία νέα διεύθυνση. Ο NAT διαθέτει ένα σύνολο διαθέσιμων IP διευθύνσεων (address pool) και μία από αυτές τις αναθέτει στον υπολογιστή. Ταυτόχρονα, κρατάει μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή (διαδικασία MAP). Έτσι, κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «ταξιδεύει» στο Internet έχει σαν διεύθυνση αποστολέα τη νέα αυτή διεύθυνση.

Αντίστροφα, κάθε υπολογιστής που θέλει να στείλει δεδομένα στον συγκεκριμένο υπολογιστή του ιδιωτικού δικτύου, στέλνει πακέτα με διεύθυνση παραλήπτη τη νέα διεύθυνση. Ο NAT είναι πάλι υπεύθυνος σε αυτήν την περίπτωση για να παραλάβει ο υπολογιστής τα πακέτα που προορίζονται για αυτόν. Δηλαδή, ο NAT κοιτάει τη βάση δεδομένων και βλέπει ποια είναι η πραγματική IP διεύθυνση του υπολογιστή (δηλαδή η διεύθυνση που έχει στο ιδιωτικό του δίκτυο) και, με βάση αυτήν την πληροφορία, δρομολογεί τα εισερχόμενα πακέτα.

5.4.6 Πρωτόκολλο ICMP

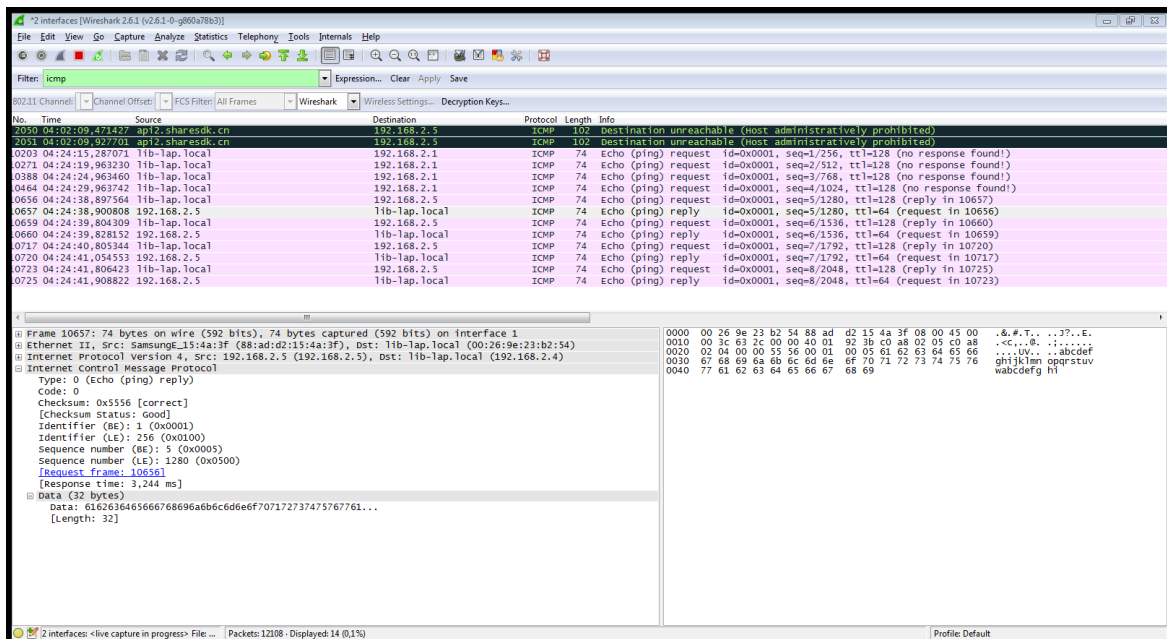
Το πρωτόκολλο Internet Control Message Protocol (**ICMP**) είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο.

Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Εξαίρεση σε αυτό τον κανόνα αποτελεί το εργαλείο **ping**, το οποίο στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να διαπιστώσει εάν ο υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response.

5.4.7 Wireshark και ICMP

Φίλτρα απεικόνισης	
icmp	Απεικονίζονται μόνο τα ICMP μηνύματα

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των ICMP πακέτων της κάρτας δικτύου:



Εικόνα 31: Παράδειγμα ICMP

5.5 Επίπεδο 3 TCP/IP :Το επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς είναι υπεύθυνο για τη μεταφορά μηνυμάτων εφαρμογής, δηλαδή παρέχει στο επίπεδο εφαρμογής έτοιμα μηνύματα όπως αυτά απεστάλησαν, σαν να μην είχε μεσολαβήσει το δίκτυο.

Βασικότερα πρωτόκολλα επιπέδου Μεταφοράς: TCP, UDP

5.5.1 Πρωτόκολλο TCP

Το πρωτόκολλο TCP (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς) αποτελεί το βασικό πρωτόκολλο που βρίσκεται στο επίπεδο μεταφοράς της τεχνολογίας TCP/IP. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να

μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά.

Το TCP μεταδίδει μόνο όταν το πλήθος των δεδομένων που έχει λάβει είναι επαρκές για να συμπληρωθεί το μέγεθος του πακέτου που έχει συμφωνηθεί κατά την εγκατάσταση της σύνδεσης. Από την άλλη όταν λάβει δεδομένα τα οποία υπερβαίνουν αυτό το μέγεθος πακέτου, τα σπάει σε μικρότερα. Τα πακέτα του πρωτοκόλλου TCP καλούνται segments (τμήματα). Ένα από τα κυριότερα μέρη ενός segment είναι η TCP επικεφαλίδα (TCP header) και τα προς μετάδοση Δεδομένα (Data), η οποία παρέχει συγκεκριμένες πληροφορίες για το πρωτόκολλο TCP. Η επικεφαλίδα γενικά αποτελείται από τα βοηθητικά δεδομένα που προσθέτει το TCP και είναι απαραίτητα για τη μετάδοση. Τα δεδομένα είναι φυσικά κομμάτι των πραγματικών δεδομένων του χρήστη που θα μεταφερθούν από το συγκεκριμένο τμήμα.

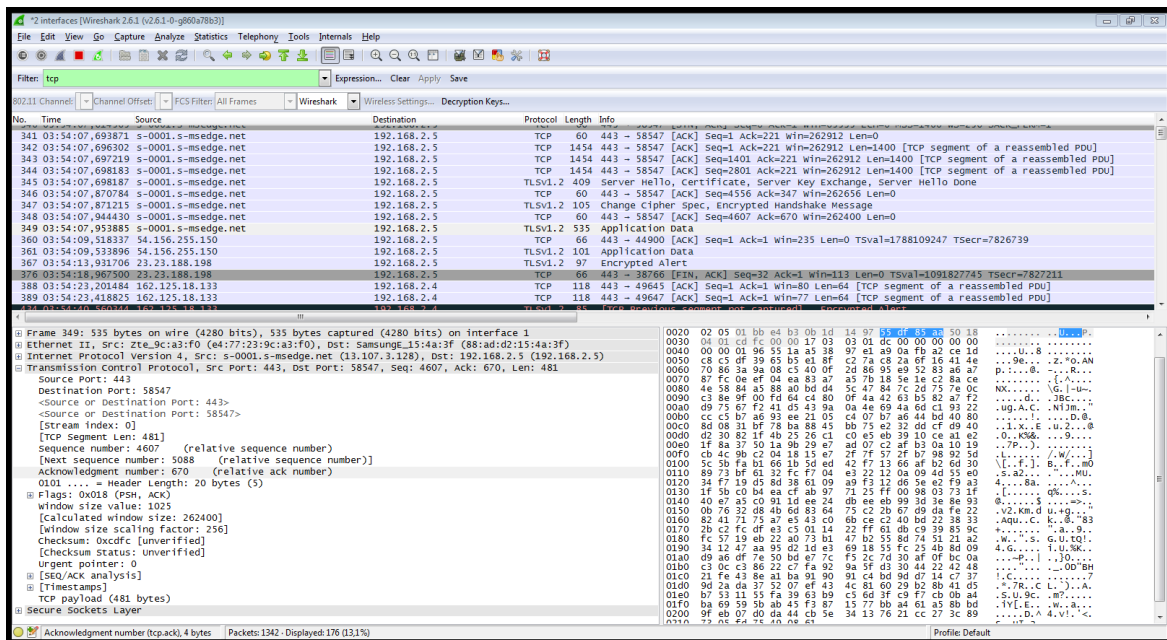
+	Bits 0 - 3	4 - 9	10 - 15	16 - 31
0	Source Port Θύρα Προέλευσης			Destination Port Θύρα Προορισμού
32	Sequence Number Αριθμός ακολουθίας			
64	Acknowledgment Number Αριθμός επιβεβαίωσης			
96	Data Offset	Reserved	Flags Σημαίες	Window Παράθυρο
128	Checksum Άθροισμα ελέγχου			Urgent Pointer Επείγοντα δεδομένα
160	Options Επιλογές (προαιρετικές)			
160/192+	Data Δεδομένα			

Εικόνα 32: Επικεφαλίδα TCP

5.5.2 Wireshark και TCP

Φίλτρα απεικόνισης	
tcp	Απεικονίζονται μόνο τα TCP μηνύματα

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των πακέτων TCP ενός κινητού τηλεφώνου με IP 192.168.2.5:



Εικόνα 33: Παράδειγμα TCP

5.5.3 Πρωτόκολλο UDP

Το πρωτόκολλο TCP είναι σχετικά πολύπλοκο πρωτόκολλο στη λειτουργία του. Ένα αποτέλεσμα αυτής της πολυπλοκότητας είναι ότι εισάγει κάποιες καθυστερήσεις στην επικοινωνία. Υπάρχουν όμως εφαρμογές που ένα πιο απλό πρωτόκολλο θα μας εξυπηρετούσε καλύτερα. Τέτοια είδη εφαρμογών είναι:

- Εφαρμογές που τα μηνύματα τους χωράνε κάθε φορά σε ένα μόνο τμήμα και δεν χρειαζόμαστε τη λειτουργία τεμαχισμού που μας παρέχει το TCP.
- Εφαρμογές που δεν έχει σημασία αν χαθούν κάποια δεδομένα στη μετάδοση, ή δεν έχει νόημα η επαναμετάδοση τους αλλά μια ενδιαφέρει ωστόσο η μετάδοση να προχωράει όσο το δυνατόν πιο γρήγορα και χωρίς καθυστερήσεις. (πχ εφαρμογές φωνής)
- Γενικά εφαρμογές που έχει περισσότερη σημασία να μπορούμε να μεταδώσουμε με τις μικρότερες δυνατές καθυστερήσεις και μεγαλύτερη ταχύτητα παρά με ακρίβεια και αξιοπιστία.

Για τις περιπτώσεις αυτές, έχει σχεδιαστεί ένα ακόμα πρωτόκολλο στο επίπεδο μεταφοράς, το **UDP** (User Datagram Protocol ή Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη).

Το UDP είναι πολύ απλούστερο από το TCP. Δεν διαθέτει τεμαχισμό και για το λόγο αυτό κάθε μήνυμα που μεταδίδεται από μια εφαρμογή μέσω UDP πρέπει να

χωράει εξ' ολοκλήρου σε ένα τμήμα UDP. Είναι πρωτόκολλο αυτοδύναμου πακέτου χωρίς σύνδεση: Η αποστολή ξεκινάει αμέσως χωρίς να γίνει επικοινωνία με την άλλη μεριά και δεν έχει έτσι επιπλέον καθυστερήσεις. Δεν διαθέτει έλεγχο λαθών. Δεν κάνει επαναμετάδοση δεδομένων και δεν κρατάει αντίγραφο των δεδομένων που στάλθηκαν για επιβεβαίωση. Δεν εξασφαλίζει επίσης ότι τα τμήματα θα φτάσουν στον προορισμό τους με τη σωστή σειρά. Αν μια εφαρμογή που χρησιμοποιεί UDP χρειάζεται να εξασφαλίσει ότι τα δεδομένα της δεν έχουν επηρεαστεί από τα παραπάνω προβλήματα, θα πρέπει να τα ελέγξει η ίδια. Μεταφέρεται δηλ. ο έλεγχος λαθών από το επίπεδο μεταφοράς στο επίπεδο εφαρμογής.

Όπως και με το πρωτόκολλο TCP, το UDP χρησιμοποιεί θύρες (ports), τα UDP ports. Η χρήση τους είναι ακριβώς ίδια με του πρωτοκόλλου TCP και προσδιορίζονται από ένα ακέραιο αριθμό 16 bits (παίρνουν δηλ. τιμές από 0 – 65535). Ο αριθμός αυτός γράφεται στην επικεφαλίδα του UDP τμήματος. Το κάθε UDP τμήμα αποτελείται από δύο βασικά κομμάτια, την επικεφαλίδα και τα δεδομένα

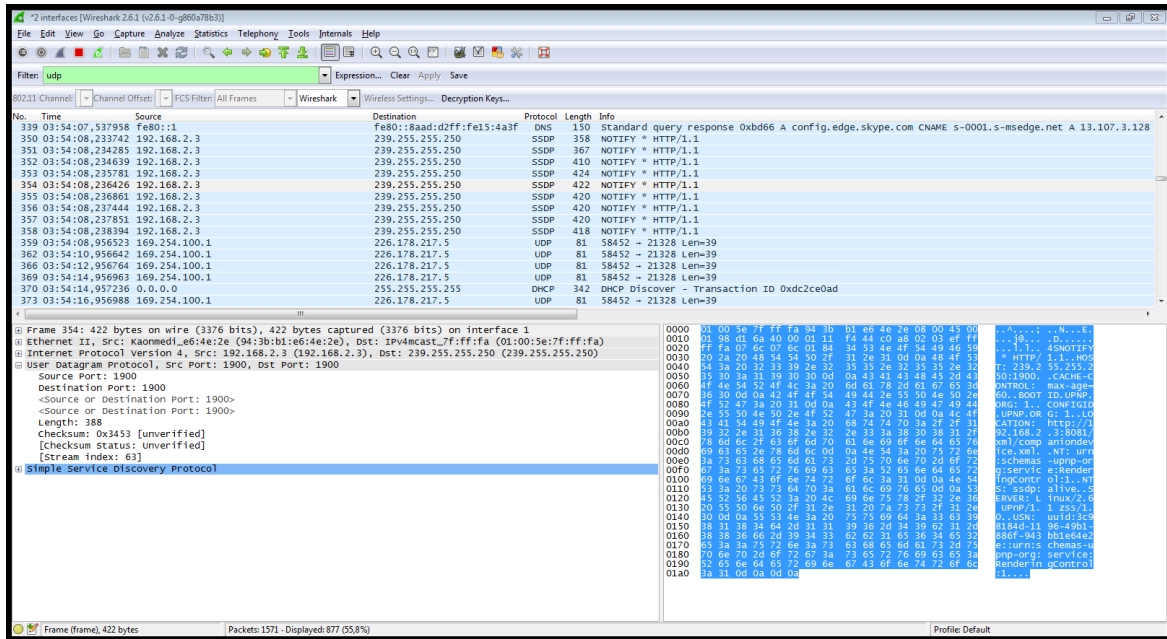
+	Bits 0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Εικόνα 34: Επικεφαλίδα UDP

5.5.4 Wireshark και UDP

Φίλτρα απεικόνισης	
udp	Απεικονίζονται μόνο τα UDP μηνύματα

Στο παρακάτω παράδειγμα φαίνεται η απεικόνιση των πακέτων UDP ενός δέκτη Ote TV:



Εικόνα 35: Παράδειγμα UDP

5.6 Επίπεδο 4 TCP/IP :Το επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής είναι το μέρος όπου βρίσκονται οι εφαρμογές του δικτύου και τα πρωτόκολλα του επιπέδου εφαρμογής.

Βασικότερα πρωτόκολλα επιπέδου Εφαρμογής: HTTP, DNS, FTP, SSL

5.6.1 Πρωτόκολλο HTTP

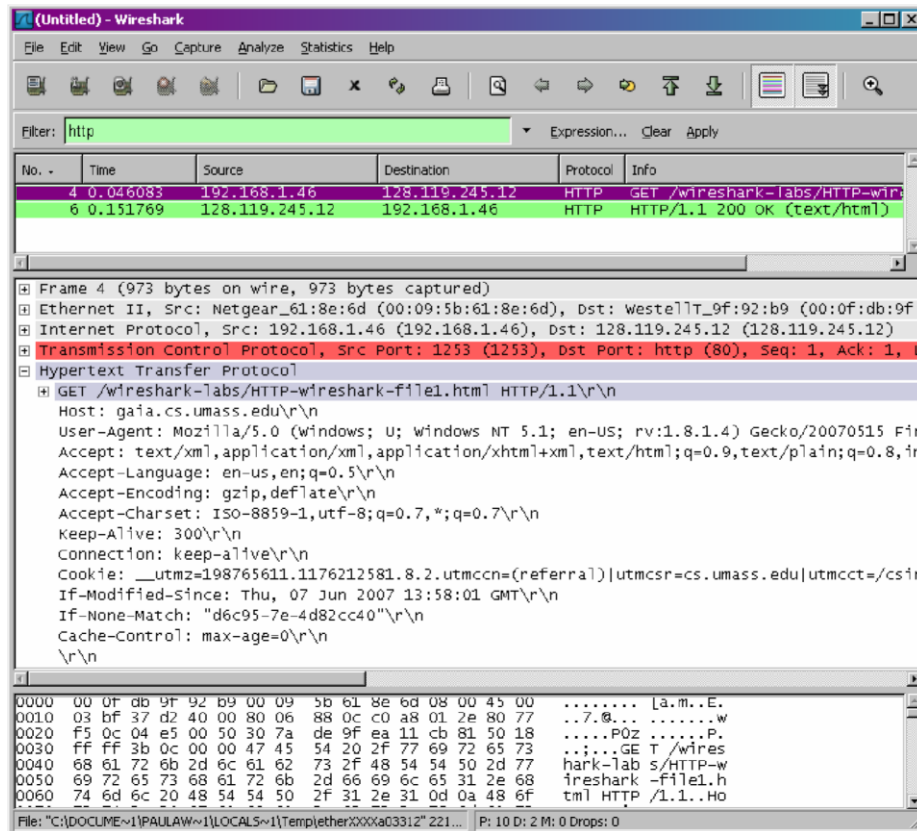
Το Πρωτόκολλο Μεταφοράς Υπερκειμένου HTTP (HyperText Transfer Protocol) λειτουργεί στο επίπεδο Εφαρμογής και αποτελεί το κύριο πρωτόκολλο που χρησιμοποιείται στους φυλλομετρητές του Παγκοσμίου Ιστού για να μεταφέρει δεδομένα (αρχεία κειμένου, γραφικών, εικόνες, ήχου, video ή οποιουδήποτε multimedia αρχείου) ανάμεσα σε έναν διακομιστή (server) και έναν πελάτη (client). Σήμερα το πρωτόκολλο αυτό είναι πλέον καθιερωμένο και διαδεδομένο σε σημείο που σχεδόν όλοι οι φυλλομετρητές να το θεωρούν δεδομένο και να το χρησιμοποιούν σε περίπτωση που ο χρήστης δεν καθορίσει ποιο πρωτόκολλο θέλει να χρησιμοποιήσει. Αν δηλαδή ο χρήστης δεν γράψει `http://my.url` αλλά γράψει σκέτο το: `my.url` σχεδόν όλοι οι φυλλομετρητές θεωρούν σαν δεδομένο το πρωτόκολλο `http` και όχι κάποιο άλλο.

Το HTTP υλοποιείται σε δυο προγράμματα: ένα πρόγραμμα πελάτη (φυλλομετρητής - browser) και ένα πρόγραμμα εξυπηρέτη. Το πρόγραμμα πελάτη και το πρόγραμμα εξυπηρέτη, που εκτελούνται σε διαφορετικά τερματικά συστήματα, συνομιλούν μεταξύ τους ανταλλάσσοντας μηνύματα HTTP. Το HTTP ορίζει την δομή αυτών των μηνυμάτων και το πώς ο πελάτης και ο εξυπηρέτης ανταλλάσσουν τα μηνύματα. Όταν ο χρήστης ζητάει μια ιστοσελίδα, το πρόγραμμα περιήγησης στέλνει μηνύματα αίτησης HTTP για τα αντικείμενα της σελίδας, στον εξυπηρέτη. Ο εξυπηρέτης δέχεται αιτήσεις και αποκρίνεται με μηνύματα απόκρισης HTTP, τα οποία περιέχουν τα αντικείμενα. Το HTTP χρησιμοποιεί το TCP ως υποκείμενο πρωτόκολλο μεταφοράς που παρέχει μια αξιόπιστη μεταφορά δεδομένων στο HTTP. Αυτό σημαίνει ότι κάθε μήνυμα αίτησης HTTP που εκπέμπεται από μια διεργασία πελάτη φτάνει τελικά ανέπαφο στον εξυπηρέτη. Εδώ βλέπουμε ένα από τα μεγαλύτερα πλεονεκτήματα μιας αρχιτεκτονικής οργανωμένης σε διαδοχικά επίπεδα – το HTTP δεν χρειάζεται να ασχολείται για χαμένα δεδομένα ή για λεπτομέρειες περί του πώς το TCP επανορθώνει από την απώλεια ή από την αλλαγή σειράς δεδομένων στο δίκτυο

5.6.2 Wireshark και HTTP

Για να διερευνήσουμε το πρωτόκολλο HTTP ακολουθούμε τα παρακάτω βήματα:

- Ξεκινάμε τον browser μας
- Ξεκινάμε το Wireshark χωρίς να ξεκινήσουμε την σύλληψη πακέτων ακόμη. Εισάγουμε 'http' (χωρίς τα εισαγωγικά) στο παράθυρο προδιαγραφών του φίλτρου παρουσίασης ώστε στο παράθυρο καταλόγου πακέτων να παρουσιάζονται αργότερα μόνο τα συλλαμβανόμενα μηνύματα HTTP.
- Περιμένουμε λίγο περισσότερο από ένα λεπτό και μετά αρχίζουμε τη σύλληψη πακέτων από το Wireshark
- Εισάγουμε το ακόλουθο URL στον browser:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> .
Στον browser θα πρέπει να εμφανιστεί ένα πολύ απλό αρχείο HTML με μια γραμμή μόνο.
- Διακόπτουμε τη σύλληψη πακέτων από το Wireshark



Εικόνα 36: Πρωτόκολλο HTTP

Στην παραπάνω εικόνα φαίνεται ότι συνελήφθησαν δύο μηνύματα http, το μήνυμα GET (από τον browser στον web server gaia.cs.umass.edu) και το μήνυμα απόκρισης από τον server στον browser. Στο παράθυρο περιεχομένων πακέτου φαίνονται λεπτομέρειες του επιλεγμένου μηνύματος HTTP GET. Υπενθυμίζεται ότι, αφού το μήνυμα μεταφέρθηκε μέσα σε ένα TCP segment (τα πακέτα TCP καλούνται τμήματα, τομείς ή τεμάχια), το οποίο μεταφέρθηκε μέσα σε ένα IP datagram μέσα σε πλαίσιο Ethernet, το Wireshark παρουσιάζει πληροφορίες και για τα πακέτα Frame, Ethernet, IP και TCP. Επειδή θέλουμε να ελαχιστοποιήσουμε το ποσό των πληροφοριών που παρουσιάζονται για δεδομένα που δεν σχετίζονται με το HTTP (στο εργαστήριο αυτό ενδιαφερόμαστε για το HTTP, θα εξετάσουμε τα άλλα πρωτόκολλα σε επόμενα εργαστήρια, βεβαιωθείτε ότι τα κουτάκια που βρίσκονται αριστερά των πληροφοριών για τα πακέτα Frame, Ethernet, IP και TCP έχουν το σύμβολο (+) (που σημαίνει ότι υπάρχει κρυμμένη πληροφορία η οποία δεν εμφανίζεται) και ότι η γραμμή HTTP έχει το σύμβολο (-) (που σημαίνει πως εμφανίζονται όλες οι πληροφορίες σχετικά με το μήνυμα HTTP. (Σημείωση- αγνοήστε τα μηνύματα HTTP GET και αποκρίσεων για το Favicon.ico).

5.6.3 Πρωτόκολλο DNS

Μια διεύθυνση IP έχει μέγεθος 32 bit και τυπικά την γράφουμε με τη μορφή τεσσάρων δεκαδικών αριθμών τα οποία χωρίζονται μεταξύ τους με τελείες. Για παράδειγμα μια έγκυρη διεύθυνση IP είναι: 94.86.87.83. Οι χρήστες όμως βρίσκουν αρκετά δύσκολο να απομνημονεύσουν αυτούς τους αριθμούς. Για το σκοπό αυτό, κρίθηκε σκόπιμο να χρησιμοποιούνται στους υπολογιστές συμβολικά ονόματα. Το **DNS** (Domain Name System ή Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών, που χρησιμοποιούν το πρωτόκολλο IP. Το σύστημα DNS μπορεί και αντιστοιχίζει ονόματα με διευθύνσεις IP ή άλλα ονόματα στο Διαδίκτυο ή κάποιο άλλο δίκτυο.

Ένας απλός τρόπος να γίνει αυτό είναι κάθε υπολογιστής να διαθέτει ένα αρχείο το οποίο να περιέχει την αντιστοιχία συμβολικών ονομάτων και IP διευθύνσεων. Για να δουλέψει αυτό το σύστημα, θα πρέπει αυτό το αρχείο να περιέχει τα ονόματα και τις διευθύνσεις όλων των υπολογιστών του δικτύου, να υπάρχει σε όλους τους υπολογιστές και να διατηρείται ενημερωμένο όταν γίνονται αλλαγές. Ο υπολογιστής που ξεκινάει μια αποστολή δεδομένων, θα ψάξει μέσα σε αυτό το αρχείο να βρει το όνομα του υπολογιστή προορισμού και από την ίδια γραμμή θα διαβάσει την διεύθυνση IP που πρέπει να χρησιμοποιήσει. Η μέθοδος αυτή με το αρχείο αντιστοίχισης διευθύνσεων – ονομάτων δουλεύει καλά όταν το δίκτυο είναι μικρό. Τα βασικά προβλήματα για να το χρησιμοποιήσουμε σε ένα μεγάλο δίκτυο είναι:

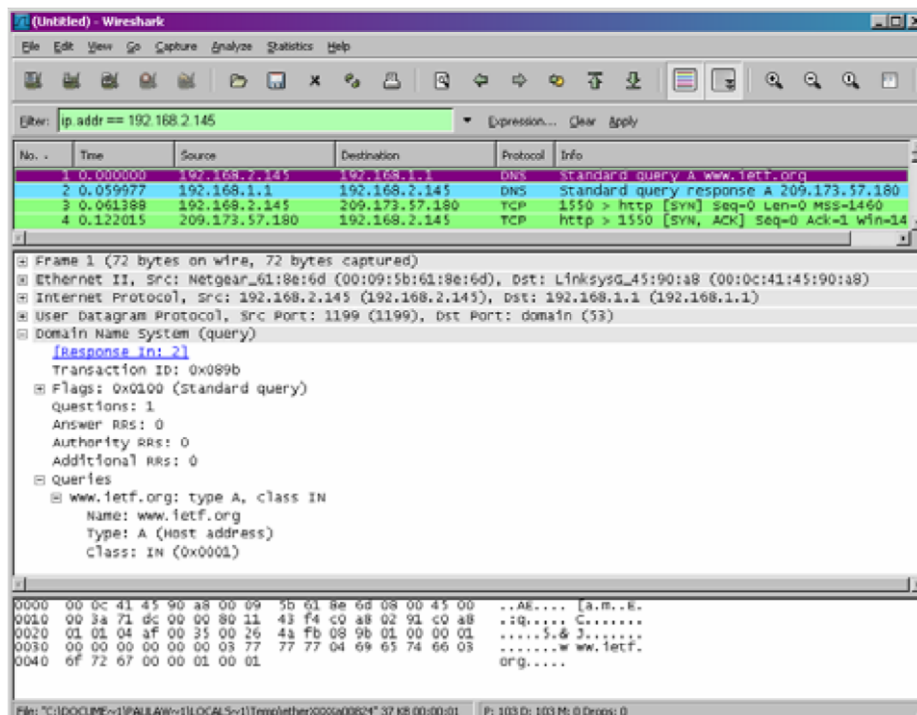
- Κάθε υπολογιστής του δικτύου πρέπει να έχει ένα αντίγραφο αυτού του αρχείου.
- Το αρχείο πρέπει να διατηρείται ενημερωμένο κάθε φορά που γίνεται κάποια αλλαγή στο δίκτυο. Για παράδειγμα όταν προσθέτουμε ή αφαιρούμε ένα υπολογιστή, ή όταν αλλάζουμε ένα όνομα ή διεύθυνση. Επίσης πρέπει να κρατάμε ενημερωμένα όλα τα αντίγραφα του αρχείου.
- Αν το πλήθος των υπολογιστών είναι μεγάλο, η αναζήτηση σε ένα απλό αρχείο κειμένου θα είναι πολύ αργή. Σε κάθε περίπτωση θα σπαταλήσουμε πολύ χρόνο και κόπο για να ενημερώσουμε όλα τα αντίγραφα. Το DNS περιέχει ένα χώρο ονομάτων οργανωμένο ιεραρχικά και η λειτουργία του βασίζεται σε μια κατανομημένη βάση δεδομένων. Ο χώρος διαιρείται σε ένα

σύνολο περιοχών που μπορούν να διαιρεθούν ξανά σε περισσότερες περιοχές.

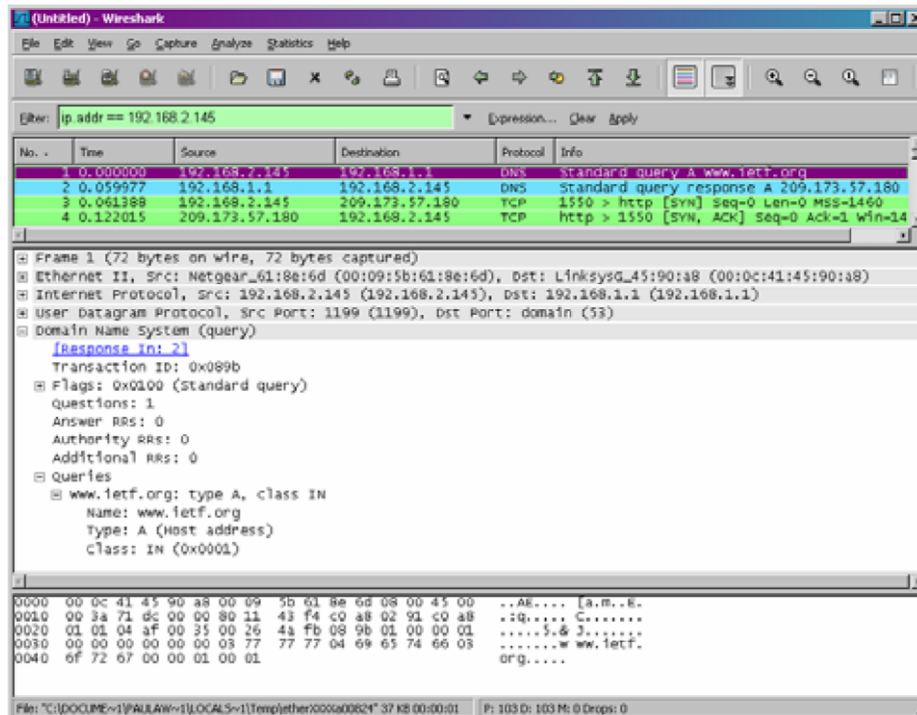
5.6.4 Wireshark και DNS

Για να διερευνήσουμε το πρωτόκολλο DNS ακολουθούμε τα παρακάτω βήματα:

- Χρησιμοποιούμε το `ipconfig /flushdns` για να αδειάσουμε την DNS cache του host μας
- Ανοίγουμε τον browser μας και αδειάζουμε την cache του. (Στην περίπτωση του Internet Explorer, πηγαίνουμε στο μενού Tools και επιλέγουμε Internet Options, στη συνέχεια επιλέγουμε Delete Files στην καρτέλα General)
- Ανοίγουμε το Wireshark και εισάγουμε 'ip.addr == διεύθυνση_IP_host' στο φίλτρο.
- Χρησιμοποιούμε το `ipconfig` για να βρούμε τη διεύθυνση IP του host μας (διεύθυνση _IP_host). Το φίλτρο αυτό απομακρύνει όλα τα πακέτα που δεν προέρχονται από και δεν προορίζονται για τον host μας.
- Ξεκινάμε τη σύλληψη πακέτων από το Wireshark
- Με τη βοήθεια του browser, πάμε στην ιστοσελίδα <http://www.ietf.org>
- Σταματάμε τη σύλληψη πακέτων



Εικόνα 37: DNS ερωτήματα



Εικόνα 38: DNS αποκρίσεις

5.6.5 Πρωτόκολλο FTP

Το πρωτόκολλο μεταφοράς αρχείων **FTP** (File Transfer Protocol) επιτρέπει τη μεταφορά αρχείων μεταξύ υπολογιστών που χρησιμοποιούν την τεχνολογία TCP/IP. Το πρωτόκολλο αυτό χρησιμοποιεί το γνωστό μας μοντέλο πελάτη-εξυπηρετητή. Το πρωτόκολλο FTP χρησιμοποιεί, στο επίπεδο μεταφοράς, το πρωτόκολλο TCP για την μεταφορά των δεδομένων του. Ουσιαστικά το FTP μας επιτρέπει να δημιουργούμε αντίγραφα αρχείων ενός απομακρυσμένου εξυπηρετητή και μας επιτρέπει για παράδειγμα να δουλέψουμε στο σπίτι μας αφού λάβουμε το κατάλληλο αρχείο από τον εξυπηρετητή του γραφείου μας. Για να εξασφαλιστεί η ασφάλεια του συστήματος και να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες η πρόσβαση στα αρχεία ενός εξυπηρετητή, υλοποιείται ένα σύστημα ελέγχου εξουσιοδότησης.

Το σύστημα αυτό βασίζεται στην χρήση ονόματος πρόσβασης και κωδικού τα οποία πρέπει να πληκτρολογήσει ο χρήστης για την είσοδο του στο σύστημα. Τα στοιχεία αυτά δημιουργούνται από το διαχειριστή του εξυπηρετητή FTP και ελέγχονται κάθε φορά. Ο όρος “μεταφορά” στο FTP δηλώνει ότι το αρχείο μεταφέρεται από τον ένα υπολογιστή (εξυπηρετητή) στον άλλο (πελάτη). Ωστόσο

το πρωτότυπο αρχείο δεν επηρεάζεται από αυτή τη διαδικασία (πρόκειται για αντιγραφή, και όχι για μετακίνηση).

5.6.6 Πρωτόκολλο SSL

Το πρωτόκολλο **SSL** λειτουργεί έχει σχεδιαστεί για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης για την αντιμετώπιση όλων των διαφορετικών αναγκών και εξασφαλίζει την ακεραιότητα των δεδομένων ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός.

Όλα τα παραπάνω γίνονται με τρόπο διαφανές και απλό. Αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζητήσει. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους.

ΚΕΦΑΛΑΙΟ 6^ο ΕΠΙΛΟΓΟΣ

6.1 Σύνοψη Πτυχιακής εργασίας

Ο συνδυασμός ενός Ακροατή Πακέτων και ενός λογισμικού το οποίο καταγράφει και αποθηκεύει όλη τη δικτυακή κίνηση σε επίπεδο πακέτων και έχει τη δυνατότητα αποθήκευση των αποτελεσμάτων για περαιτέρω χρήση και επεξεργασία, είναι ο καλύτερος συνδυασμός για την αποτελεσματική εποπτεία ενός δικτύου Ethernet.

Οι δυνατότητες και το βάθος ανάλυσης που προσφέρει το λογισμικό Wireshark με τη χρήση των φίλτρων καταγραφής και απεικόνισης το καθιστούν ικανό για να γίνει αποτελεσματική εξαγωγή των ζητούμενων κάθε φορά δεδομένων.

Η ευκολία εγκατάστασης και η μη ορατότητα του Ακροατή Πακέτων που χρησιμοποιήσαμε κάνει εφικτή τη χρήση του σε οποιοδήποτε δίκτυο καθώς το μόνο που χρειάζεται είναι απλά να παρεμβληθεί στο δίκτυο αυτό, σαν μια νοητή διχοτόμηση του καλωδίου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] <http://www.cnc.uom.gr/services/pdf/section1%282%29.pdf>
- [2]. <http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-TCP-IP-Introduction.html>
- [3]. <http://el.wikipedia.org/wiki/Broadcast>
- [4]. <http://www.diktyas.gr/index.php/2012-01-22-20-45-27/2012-01-22-22-33-47/lan>
- [5]. <http://www.diktyas.gr/index.php/2013-03-13-19-12-51/2012-01-22-21-57-40/-bit->
- [6]. <http://www.diktyas.gr/index.php/2013-03-13-19-12-51/2012-01-22-21-57-40/-utp>
- [7]. <http://www.diktyas.gr/index.php/2013-03-13-19-12-51/2012-01-22-21-57-40/2012-01-22-21-55-31>
- [8]. <http://dide.flo.sch.gr/Plinet/Meetings/Meeting23/VirtualBox-WhatItIs.pdf>
- [9].
https://eclass.teicrete.gr/modules/document/file.php/TP129/%CE%95%CE%A1%CE%93%CE%91%CE%A3%CE%A4%CE%97%CE%A1%CE%99%CE%91_%CE%9C%CE%91%CE%9D%CE%99%CE%A6%CE%91%CE%92%CE%91/01.%CE%A3%CE%B7%CE%BC%CE%B5%CE%B9%CF%8E%CF%83%CE%B5%CE%B9%CF%82/OS-Lab-1-VirtualBox-Ubuntu-Installation-130601.pdf
- [10]. <http://dide.flo.sch.gr/Plinet/Tutorials-STEMP/Linux-Ubuntu.pdf>
- [11]. <http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-NetworkTerminology.html>
- [12]. http://en.wikipedia.org/wiki/Network_Convergence
- [13]. http://en.wikipedia.org/wiki/Optical_fiber
- [14].
<ftp://120.105.184.208/soft/Router%20%AB%FC%A5O%A5%DC%BDd/Cisco%20Router%20Configuration%20Commands.pdf>
- [15]. <http://www.techrepublic.com/blog/data-center/10-commands-you-should-master-when-working-with-the-cisco-ios-104071/>
- [16].
http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf001.pdf
- [17]. <http://www.perle.com/downloads/software/833is/ciscocmdmanual.pdf>
- [18]. <https://perso.ens-lyon.fr/christophe.crespelle/enseignements/ASR/cisco-config.pdf>

- [19]. <http://computernetworkingnotes.com/switching-vlan-stp-vtp-dtp-ether-channels/basic-switch-configurations.html>
- [20]. <http://www.perle.com/downloads/software/833is/ciscocmdmanual.pdf>
- [21]. <http://gonda.nic.in/swangonda/pdf/ccnaguide.pdf>
- [22]. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/data_sheet_c78-720918.html
- [23]. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html
- [24]. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.html
- [25]. http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html
- [26]. www.cisco.com/c/en/us/products/collateral/wireless/aironet-700-series/data_sheet_c78-726725.html
- [27]. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-c-series-switches/data_sheet_c78-639705.html
- [28]. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html>
- [29]. <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html>
- [30]. <http://el.wikipedia.org/wiki/SSH>
- [31]. <https://www.siteground.com/tutorials/email/pop3-imap-smtp-ports.htm>
- [32]. http://diktia.weebly.com/uploads/6/4/5/1/6451366/_protokolla_epikoinonias.pdf
- [33]. <http://pages.cs.aueb.gr/~xgeorge/MTMC/slides/16-Protocols.pdf>
- [34]. <http://el.wikipedia.org/wiki/UDP>
- [35]. <http://el.wingwit.com/Networking/internet-networking/69755.html>
- [36]. http://diktya-epal-g.ggia.info/wp-content/uploads/2009/12/Kefalaio_7_Diadiktywsh_internet_7_4_Prwtokollo_UDP.pdf
- [37]. http://web.teipir.gr/new/ecs/pelab_1/tcp/inter4.htm
- [38]. <http://www.dmst.aueb.gr/dds/norma/internet/udp.htm>
- [39]. <http://vivliothmmy.ee.auth.gr/187/1/diplomatiki.pdf>
- [40]. caclab.csd.auth.gr/askisi2.doc
- [41]. <http://el.wikipedia.org/wiki/EIGRP>
- [42]. http://en.wikipedia.org/wiki/Cisco_Discovery_Protocol

- [43]. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html>
- [44] http://el.wikipedia.org/wiki/Πρωτόκολλο_Μεταφοράς_Υπερκειμένου
- [45] http://el.wikipedia.org/wiki/Domain_Name_System
- [46] http://el.wikipedia.org/wiki/Transmission_Control_Protocol
- [47] <http://el.wikipedia.org/wiki/UDP>
- [48] http://el.wikipedia.org/wiki/Internet_Protocol
- [49] <http://el.wikipedia.org/wiki/ICMP>
- [50] <http://el.wikipedia.org/wiki/Ethernet>
- [51] http://el.wikipedia.org/wiki/Address_Resolution_Protocol
- [52] <http://el.wikipedia.org/wiki/DHCP>
- [53] http://el.wikipedia.org/wiki/IEEE_802.11
- [54] <http://el.wikipedia.org/wiki/SSL>
- [55] <http://el.wikipedia.org/wiki/TCP/IP>
- [56] http://el.wikipedia.org/wiki/Διεύθυνση_MAC
- [57] http://el.wikipedia.org/wiki/Κατάλογος_των_TCP_και_UDP_ports
- [58] <https://foss.ntua.gr/wiki/> (τελευταία επίσκεψη στις 1.3.2013)
- [59] <http://www.neural.uom.gr/Documents/Networks/chapter5.pdf>
- [60] <http://conta.uom.gr/conta/ekpaideysh/seminaria/common/networks/osi.html>
- [61] http://el.wikipedia.org/wiki/Δίκτυο_υπολογιστών
- [62] http://el.wikipedia.org/wiki/Μοντέλο_αναφοράς_OSI
- [63] <http://networking-basics.wikispaces.com/>
- [64] <http://www.diktyas.gr/>
- [65] http://el.wikipedia.org/wiki/Τοπικό_δίκτυο_υπολογιστών
- [66] <http://diktia.weebly.com/>
- [67] <http://www.ece.ntua.gr/>
- [68] http://openmaniak.com/gr/wireshark_stat.php
- [69] <http://www.wireshark.org/>
- [70] <http://el.wikipedia.org/wiki/Wireshark>
- [71] <http://www.techrepublic.com/blog/products/review-wireshark-network-analyzer/642>

