Πρωτόκολλα και επικοινωνίες δικτύων
Εργαστήριο 2

Τμήμα Πληροφορικής και τηλεπικοινωνιών
Πανεπιστήμιο Ιωαννίνων, Άρτα

2023-05-03

Περιεχόμενα

1 Εισαγωγή

1.1 Σύνοψη

Το βασικό εργαλείο για την παρατήρηση των μηνυμάτων που ανταλλάσσονται μεταξύ των εκτελούμενων οντοτήτων πρωτοκόλλων καλείται packet sniffer. Όπως υπονοεί και το όνομα, ο packet sniffer συλλαμβάνει ("sniffs") τα μηνύματα τα οποία στέλνονται ή λαμβάνονται από τον υπολογιστή σας. Επίσης, ο packet sniffer συνήθως αποθηκεύει και απεικονίζει τα περιεχόμενα διαφόρων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνονται. Ο ίδιος ο packet sniffer είναι παθητικός. Παρατηρεί τα μηνύματα που στέλνονται και λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που τρέχουν στον υπολογιστή σας αλλά ο ίδιος δεν στέλνει ποτέ πακέτα. Παρόμοια, τα λαμβανόμενα πακέτα δεν απευθύνονται ποτέ με ρητό τρόπο στον packet sniffer. Αντίθετα, ο packet sniffer λαμβάνει ένα αντίγραφο των πακέτων που στέλνονται ή λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στον υπολογιστή σας.

Το δεύτερο συστατικό στοιχείο ενός packet sniffer είναι ο αναλυτής πακέτων (packet analyzer), ο οποίος απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Για το σκοπό

αυτό, ο αναλυτής πακέτων πρέπει να "καταλαβαίνει" τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα. Για παράδειγμα, έστω ότι ενδιαφερόμαστε να απεικονίσουμε τα διάφορα πεδία των μηνυμάτων που ανταλλάσσονται από το πρωτόκολλο HTTP στο Σχήμα 1. Ο αναλυτής πακέτων καταλαβαίνει τη μορφή των πλαισίων Ethernet και επομένως μπορεί να αναγνωρίσει ένα αυτοδύναμο πακέτο IP (IP datagram) μέσα σε ένα πλαίσιο Ethernet. Επίσης, καταλαβαίνει τη μορφή ενός IP datagram, ώστε να είναι σε θέση να εξάγει ένα TCP segment που περιέχεται μέσα σε ένα IP datagram. Επιπλέον, καταλαβαίνει τη δομή ενός TCP segment οπότε μπορεί να εξάγει το μήνυμα HTTP που περιέχεται στο TCP segment. Τέλος, καταλαβαίνει το πρωτόκολλο HTTP και έτσι, για παράδειγμα, γνωρίζει ότι τα πρώτα bytes ενός μηνύματος HTTP θα περιέχουν τις ακολουθίες χαρακτήρων "GET", "POST" ή "HEAD".

1.2 Τι θα δούμε σε αυτό το εργαστήριο:

Οι κάρτες δικτύωσης είναι βασικά στοιχεία των σύγχρονων δικτύων υπολογιστών, παρέχοντας τα μέσα για τη μετάδοση και τη λήψη δεδομένων σε ένα δίκτυο. Οι κάρτες αυτές έχουν σχεδιαστεί για να διασυνδέονται με διαφορετικούς τύπους δικτύων και διαθέτουν μια σειρά χαρακτηριστικών που τους επιτρέπουν να λειτουργούν αποτελεσματικά. Ένα βασικό χαρακτηριστικό των καρτών δικτύωσης είναι η ικανότητά τους να λειτουργούν σε διαφορετικές ταχύτητες. Οι περισσότερες σύγχρονες κάρτες μπορούν να λειτουργούν σε πολλαπλές ταχύτητες, όπως 10 Mbps, 100 Mbps και 1 Gbps. Αυτό τους επιτρέπει να λειτουργούν με διαφορετικούς τύπους δικτύων και να διαχειρίζονται διαφορετικά επίπεδα δικτυακής κίνησης. Ένα άλλο σημαντικό χαρακτηριστικό των καρτών δικτύωσης είναι η υποστήριξή τους για διαφορετικούς τύπους πρωτοκόλλων δικτύου. Αυτά τα πρωτόκολλα καθορίζουν τον τρόπο μετάδοσης και λήψης δεδομένων στο δίκτυο. Παραδείγματα κοινών πρωτοκόλλων δικτύου περιλαμβάνουν τα TCP/IP, NetBIOS και IPX/SPX. Εκτός από αυτά τα χαρακτηριστικά, οι κάρτες δικτύωσης χρησιμοποιούν επίσης τους πίνακες ARP και Ethernet για τη βελτιστοποίηση της απόδοσης του δικτύου. Οι πίνακες ARP χρησιμοποιούνται για την αντιστοίχιση διευθύνσεων IP σε διευθύνσεις MAC, επιτρέποντας στις συσκευές ενός δικτύου να επικοινωνούν μεταξύ τους. Οι πίνακες Ethernet, από την άλλη πλευρά, χρησιμοποιούνται για να παρακολουθούν ποιες συσκευές είναι συνδεδεμένες σε ποιες θύρες ενός μεταγωγέα, επιτρέποντας την αποτελεσματικότερη δρομολόγηση της δικτυακής κίνησης. Τα πλαίσια Ethernet είναι οι βασικές μονάδες δεδομένων που μεταδίδονται μέσω δικτύων Ethernet. Αποτελούνται από μια επικεφαλίδα, ένα ωφέλιμο φορτίο και ένα τρέιλερ και περιλαμβάνουν πληροφορίες όπως οι διευθύνσεις MAC πηγής και προορισμού, το μήκος του πακέτου και πληροφορίες ανίχνευσης σφαλμάτων. Τα πλαίσια Ethernet χρησιμοποιούνται για τη μετάδοση δεδομένων μεταξύ συσκευών σε ένα δίκτυο και είναι απαραίτητα για τη δυνατότητα επικοινωνίας μεταξύ συσκευών στο ίδιο δίκτυο. Συνοπτικά, οι κάρτες δικτύωσης αποτελούν βασικά συστατικά των σύγχρονων δικτύων υπολογιστών και διαθέτουν μια σειρά χαρακτηριστικών που τους επιτρέπουν να λειτουργούν αποτελεσματικά. Οι πίνακες ARP και Ethernet, καθώς και τα πλαίσια Ethernet, αποτελούν βασικά στοιχεία αυτών των δικτύων, επιτρέποντας την αποτελεσματική δρομολόγηση της δικτυακής κίνησης και επιτρέποντας στις συσκευές να επικοινωνούν μεταξύ τους.

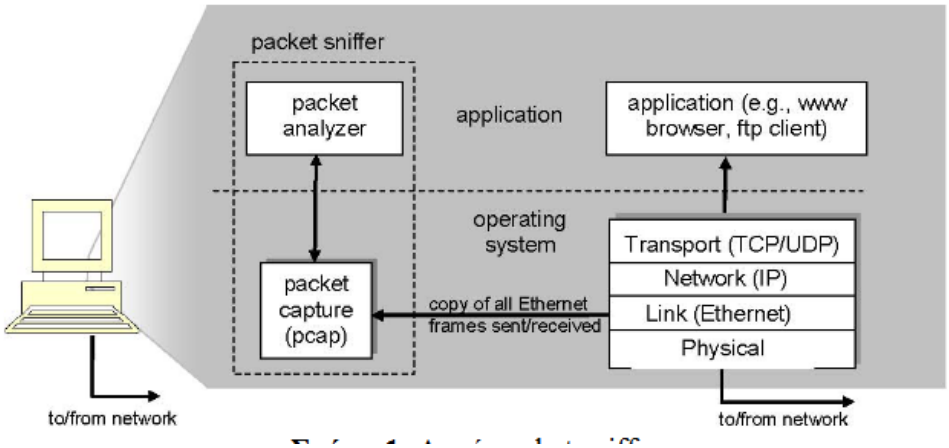

Figure 1: Packet Sniffer Analyzer

2 Βασικές Δικτυακές δυνατότητες

1. **Βασικά χαρακτηριστικά των καρτών δικτύωσης** Η κάρτα δικτύου συνδέει τον υπολογιστή σας στο τοπικό δίκτυο του εργαστηρίου και επιτρέπει την επικοινωνία με άλλους υπολογιστές. Για τον σκοπό αυτό παράγει και λαμβάνει μηνύματα που τα αποκαλούμε πλαίσια (frames). Τα πλαίσια ακολουθούν είτε το πρότυπο Ethernet είτε το IEEE 802.3. Κάθε πλαίσιο αρχίζει με ένα Preamble (Προοίμιο) που επιτρέπει το συγχρονισμό του δέκτη με τον αποστολέα. Το πλαίσιο περιέχει δύο διευθύνσεις 6 byte, μία για τον προορισμό και μία για την πηγή. Ακολουθεί το πεδίο Type (Τύπος) ή το πεδίο Length(Μήκος), ανάλογα με το κατά πόσο πρόκειται για πλαίσιο Ethernet ή IEEE 802.3, αντίστοιχα. Ο Τύπος δείχνει το πρωτόκολλο του ανώτερου στρώματος, συνήθως, το πρωτόκολλο IP. Το μήκος δηλώνει πόσα byte βρίσκονται στο πεδίο δεδομένων, από ένα ελάχιστο 0 μέχρι ένα μέ- γιστο 1.500 byte. Το πεδίο δεδομένων ακολουθείται από το πεδίο CRC (Άθροισμα Ελέγχου) μήκους 4 byte, που ελέγχεται στον δέκτη και αν ανιχνευθεί σφάλμα το πλαίσιο απορρίπτεται. Ένα έγκυρο πλαίσιο έχει μήκος τουλάχιστον 64 byte, από τη διεύθυνση προορισμού μέχρι το άθροισμα ελέγχου. Εάν το τμήμα δεδομένων ενός πλαισίου είναι μικρότερο από 46 byte, το πεδίο παραγεμίζεται (pad) μέχρι το ελάχιστο μέγεθος.

   Χρησιμοποιώντας το τερματικό των windows καταγράψτε:

   - Την ονομασία της κάρτας δικτύωσης (network adapter).
   - Την ταχύτητα σύνδεσης.
   - Τη διεύθυνση υπο-στρώματος MAC σε δεκαεξαδική μορφή
   - Τον κατασκευαστή της κάρτας δικτύωσης.
   - Τα συνδεδεμένα με αυτήν πρωτόκολλα δικτύωσης.
   - Τη διακοπή (interrupt – IRQ) που χρησιμοποιεί.
   - Την έκδοση του οδηγού (driver) της κάρτας και το όνομα του σχετικού αρχείου.
   - Τη θέση της στο PCI bus του υπολογιστή.

2. **ARP (Address Resolution Protocol - Πρωτόκολλο επίλυσης διευθύνσεων)**. Είναι ένα πρωτόκολλο που χρησιμοποιείται για την αντιστοίχιση μιας διεύθυνσης δικτύου (όπως μια διεύθυνση IP) σε μια φυσική διεύθυνση (όπως μια διεύθυνση MAC) σε ένα τοπικό δίκτυο. Το πρωτόκολλο χρησιμοποιείται για την επίλυση της διεύθυνσης επιπέδου 2 μιας συσκευής δικτύου, όπως ένας υπολογιστής, στο τοπικό δίκτυο, όταν είναι γνωστή μόνο η διεύθυνση Layer 3(όπως η διεύθυνση IP).

   Όταν μια συσκευή χρειάζεται να στείλει δεδομένα σε μια άλλη συσκευή στο τοπικό δίκτυο, ελέγχει πρώτα την προσωρινή μνήμη ARP για να δει αν γνωρίζει ήδη τη φυσική διεύθυνση της συσκευής-στόχου. Εάν η διεύθυνση δεν υπάρχει στην προσωρινή μνήμη, η συσκευή εκπέμπει ένα αίτημα ARP σε όλες τις συσκευές του δικτύου, ζητώντας τη φυσική διεύθυνση που σχετίζεται με τη διεύθυνση IP του στόχου. Η συσκευή με την αντίστοιχη διεύθυνση IP απαντά με τη φυσική της διεύθυνση και η ζητούσα συσκευή ενημερώνει την προσωρινή μνήμη ARP με τη νέα αντιστοίχιση.

   Το ARP είναι ένα πρωτόκολλο χωρίς κατάσταση, που σημαίνει ότι δεν αποθηκεύει καμία πληροφορία σχετικά με τις συσκευές με τις οποίες έχει επικοινωνήσει στο παρελθόν. Αντ' αυτού, τα αιτήματα και οι απαντήσεις ARP αποστέλλονται ανάλογα με τις ανάγκες. Αυτό καθιστά το ARP ευάλωτο σε ορισμένους τύπους επιθέσεων, όπως το ARP spoofing, όπου ένας επιτιθέμενος στέλνει πλαστά μηνύματα ARP σε μια συσκευή δικτύου προκειμένου να συσχετίσει τη διεύθυνση MAC του επιτιθέμενου με τη διεύθυνση IP μιας νόμιμης συσκευής δικτύου, επιτρέποντας στον επιτιθέμενο να υποκλέψει την κυκλοφορία δικτύου που προορίζεται για τη νόμιμη συσκευή.

   Το ARP λειτουργεί στο Επίπεδο Σύνδεσης Δεδομένων (Layer 2) του μοντέλου OSI και αποτελεί βασικό στοιχείο της τοπικής δικτύωσης. Υλοποιείται από τα περισσότερα λειτουργικά συστήματα δικτύου και χρησιμοποιείται για τη διευκόλυνση της επικοινωνίας μεταξύ συσκευών σε ένα τοπικό δίκτυο.

   Συνοπτικά

   - Ο πίνακας ARP είναι ένας κατάλογος διευθύνσεων IP και των αντίστοιχων διευθύνσεων MAC που έχει μάθει μια συσκευή μέσω ARP.

- Όταν μια συσκευή χρειάζεται να στείλει δεδομένα σε μια άλλη συσκευή στο τοπικό δίκτυο, ελέγχει πρώτα τον πίνακα ARP για να δει αν γνωρίζει ήδη τη διεύθυνση MAC που σχετίζεται με τη διεύθυνση IP του στόχου.
- Εάν η διεύθυνση MAC δεν υπάρχει στον πίνακα ARP, η συσκευή στέλνει ένα αίτημα ARP σε όλες τις συσκευές του δικτύου ζητώντας τη διεύθυνση MAC που σχετίζεται με τη διεύθυνση IP του στόχου.
- Όταν η συσκευή με την αντίστοιχη διεύθυνση IP απαντήσει με τη διεύθυνση MAC της, η ζητούσα συσκευή ενημερώνει τον πίνακα ARP με τη νέα αντιστοίχιση.
- Ο πίνακας ARP χρησιμοποιείται για την επιτάχυνση της επικοινωνίας στο δίκτυο, επιτρέποντας στις συσκευές να αναζητούν διευθύνσεις MAC χωρίς να χρειάζεται να στέλνουν αιτήσεις ARP για κάθε πακέτο που στέλνουν.
- Ο πίνακας ARP μπορεί να προβληθεί χρησιμοποιώντας την εντολή arp στη γραμμή εντολών ή στο τερματικό.
- Ο πίνακας ARP μπορεί να επεξεργαστεί χειροκίνητα ή να διαγραφεί χρησιμοποιώντας διοικητικές εντολές.
- Ο πίνακας ARP είναι ευάλωτος σε επιθέσεις όπως το ARP spoofing, όπου ένας επιτιθέμενος στέλνει πλαστά μηνύματα ARP σε μια συσκευή δικτύου προκειμένου να συσχετίσει τη διεύθυνση MAC του επιτιθέμενου με τη διεύθυνση IP μιας νόμιμης συσκευής δικτύου, επιτρέποντας στον επιτιθέμενο να υποκλέψει την κυκλοφορία δικτύου που προορίζεται για τη νόμιμη συσκευή.

Χρησιμοποιώντας τον πίνακα ARP table

(a) Δείτε και καταγράψτε τον πίνακα ARP του υπολογιστή σας πληκτρολογώντας arp –a ή arp –g σε ένα παράθυρο εντολών. Ο πίνακας αυτός περιέχει τις διευθύνσεις MAC και IP των υπολογιστών με τους οποίους έχει επικοινωνήσει πρόσφατα ο δικός σας.

(b) Σε ένα παράθυρο εντολών εκτελέστε την εντολή ping <διεύθυνση IP>, όπου <διεύθυνση IP> η διεύθυνση IP του διπλανού σας υπολογιστή. Δείτε πάλι και καταγράψτε τον πίνακα ARP του υπολογιστή σας. Τι παρατηρείτε;

(c) Σημειώστε τις διευθύνσεις IP της προκαθορισμένης πύλης και των εξυπηρετητών DNS του υπολογιστή σας. [Υπόδειξη: Για την εύρεση του default gateway και των εξυπηρετητών DNS μπορείτε να χρησιμοποιήσετε την εντολή ipconfig /all.]

(d) Υπάρχουν οι διευθύνσεις αυτές στον πίνακα ARP του υπολογιστή σας;

Σε ένα παράθυρο εντολών εκτελέστε την εντολή **arp -d** ώστε να αδειάσει ο πίνακας ARP του υπολογιστή σας καθώς και **ipconfig /flushdns** για να διαγραφούν οι γνωστές αντιστοιχήσεις ονομάτων σε διευθύνσεις IP. Στη συνέχεια επισκεφτείτε την κεντρική σελίδα του Πανεπιστημίου **www.dit.uoi.gr** χρησιμοποιώντας κάποιον πλοηγό ιστού. Μιας και η διεύθυνση IP του εξυπηρετητή ιστού του ΕΜΠ δεν είναι γνωστή στον πλοηγό ιστού (ακόμη και εάν ήταν μόλις τη διαγράψατε), θα προηγηθεί επικοινωνία με τον εξυπηρετητή DNS ώστε να προσδιορισθεί. Κατόπιν θα ακολουθήσει η ανταλλαγή μηνυμάτων μεταξύ του πλοηγού ιστού (πελάτης) και του εξυπηρετητή.

(e) Ποιες από τις διευθύνσεις IP που προσδιορίσατε στο ερώτημα 1.3 έχουν τώρα καταχωρηθεί στον πίνακα ARP και γιατί; [**Υπόδειξη:** Εάν πελάτης και εξυπηρετητής βρίσκονται σε διαφορετικά υποδίκτυα, η επικοινωνία στο στρώμα IP γίνεται μέσω της πύλης που υποδεικνύει ο πίνακας δρομολόγησης.]

(f) Ποιες από τις διευθύνσεις IP που προσδιορίσατε στο ερώτημα 1.3 δεν καταχωρήθηκαν στον πίνακα ARP και γιατί;

3 Ασκήσεις

1. **Το πλαίσιο Ethernet** Στην συγκεκριμένη άσκηση θα πραγματοποιηθεί καταγραφή των πλαισίων Ethernet που παράγονται κατά την επίσκεψη μιας ιστοσελίδας. Συνοπτικά το πλαίσιο Ethernet:

   - Το πλαίσιο Ethernet είναι μια θεμελιώδης μονάδα δεδομένων σε ένα δίκτυο Ethernet.

- Αποτελείται από κεφαλίδα, ωφέλιμο φορτίο και ρυμουλκούμενο.
- Η επικεφαλίδα περιέχει διάφορα πεδία, συμπεριλαμβανομένων των διευθύνσεων MAC προορισμού και πηγής και του τύπου ή του μήκους του ωφέλιμου φορτίου.
- Το ωφέλιμο φορτίο είναι τα πραγματικά δεδομένα που μεταδίδονται, τα οποία μπορεί να περιλαμβάνουν από απλό κείμενο έως σύνθετα πρωτόκολλα.
- Το τρέιλερ περιέχει έναν κυκλικό έλεγχο πλεονασμού (CRC), ο οποίος χρησιμοποιείται για την ανίχνευση σφαλμάτων στο πλαίσιο κατά τη μετάδοση.
- Το πλαίσιο Ethernet έχει μέγιστο μέγεθος 1518 bytes, συμπεριλαμβανομένης της επικεφαλίδας και του τρέιλερ.
- Το ελάχιστο μέγεθος του πλαισίου Ethernet είναι 64 bytes.
- Το προοίμιο είναι μια ακολουθία bit που προστίθεται στην αρχή του πλαισίου Ethernet για το συγχρονισμό των ρολογιών των συσκευών αποστολής και λήψης.
- Αποτελείται από 7 bytes εναλλασσόμενων 1s και 0s, ακολουθούμενα από ένα byte οριοθέτησης.
- Το Πλαίσιο Ethernet αποτελεί τη βάση για τη μετάδοση δεδομένων στα περισσότερα τοπικά δίκτυα (LAN).
- Το πρωτόκολλο Ethernet έχει τυποποιηθεί από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) ως το πρότυπο IEEE 802.3.
- Τα Πλαίσια Ethernet μεταδίδονται με τη χρήση ενός πρωτοκόλλου πολλαπλής πρόσβασης με αίσθηση φέροντος και ανίχνευση σύγκρουσης (CSMA/CD) για την αποφυγή συγκρούσεων μεταξύ πολλαπλών συσκευών που επιχειρούν να μεταδώσουν ταυτόχρονα.
- Το Ethernet Frame μπορεί να καταγραφεί και να αναλυθεί με τη χρήση αναλυτών πρωτοκόλλου δικτύου, όπως το Wireshark, που μπορεί να βοηθήσει στην αντιμετώπιση προβλημάτων δικτύου και στη διάγνωση προβλημάτων.

Για την άσκηση, Προτού αρχίσετε την καταγραφή φροντίστε να αδειάσετε την προσωρινή μνήμη (cache) του πλοηγού. Για να πραγματοποιήσετε την ακόλουθη διαδικασία στον chrome ακολουθήστε τα βήματα της εικόνας 2.

In Chrome

1. On your computer, open Chrome.
2. At the top right, click More .
3. Click More tools. Clear browsing data.
4. At the top, choose a time range. To delete everything, select All time.
5. Next to "Cookies and other site data" and "Cached images and files," check the boxes.
6. Click Clear data.

Figure 2: Clear cache in chrome

Αφού ξεκινήσετε το Wireshark, ακολουθήστε από το μενού του κεντρικού παραθύρου, τη διαδρομή **Edit→Preferences...** και από τη λίστα επιλογών στα αριστερά διαλέγετε το Name Resolution. Βεβαιωθείτε ότι κανένα από τα τετραγωνάκια στα αριστερά δεν είναι επιλεγμένο και πατήστε OK.

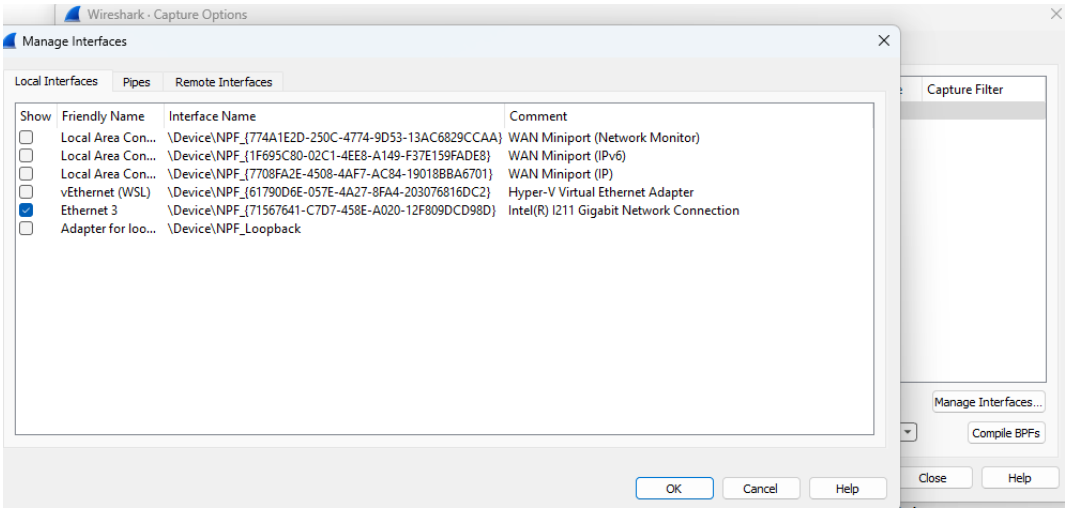

Figure 4: Manage Intefaces

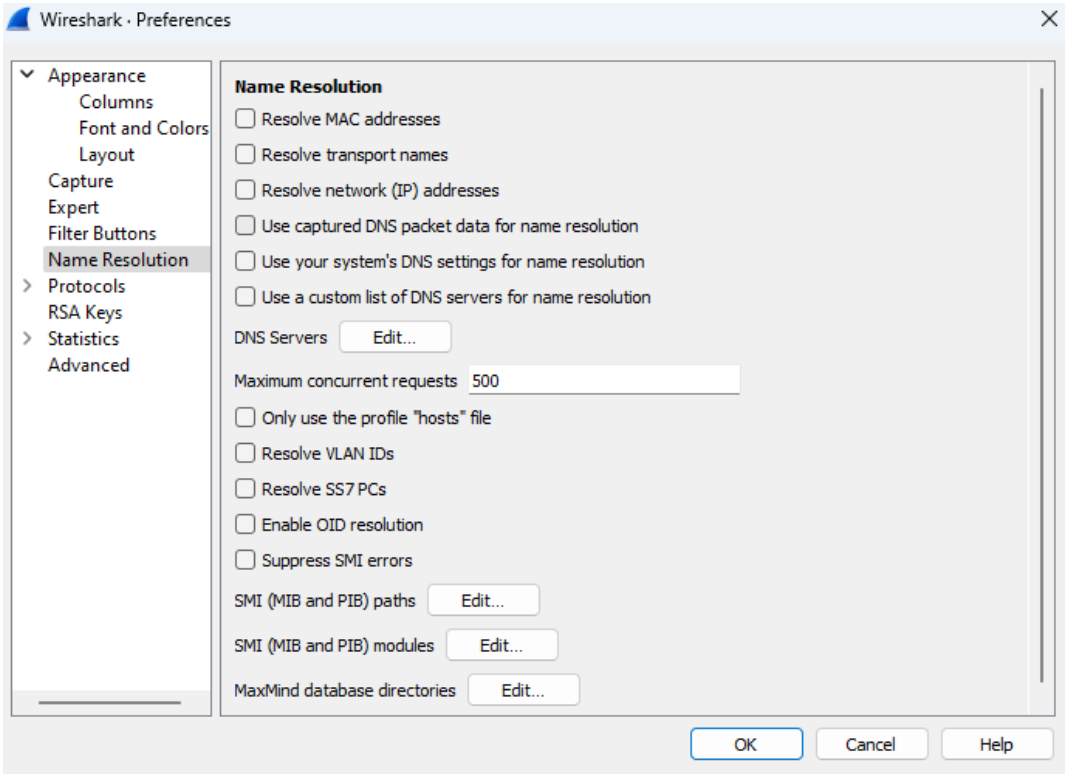

Figure 3: Ρυθμίσεις προτημήσεων για άσκηση 3

Για τη διαδικασία της καταγραφής ακολουθούμε από το μενού επιλογών τη διαδρομή **Capture** → **Options** → **Manage Intefaces**(Εικόνα 4). Στο παράθυρο που εμφανίζεται θα δείτε όλες τις διαθέσιμες κάρτες δικτύου του υπολογιστή σας, την IP διεύθυνση τους και μια ένδειξη για το πλήθος και ρυθμό πακέτων (εφόσον υπάρχει τηλεπικοινωνιακή κίνηση). Επιλέξτε την κάρτα δικτύου του υπολογιστή σας μέσω της οποίας θα γίνει η σύλληψη των πακέτων και ελέγξτε τις επιλογές της Κάρτας δικτύου(Βεβαιωθείται ότι καμία επιλογή του Name Resolution δεν είναι ενεργή. Εικόνα 5).

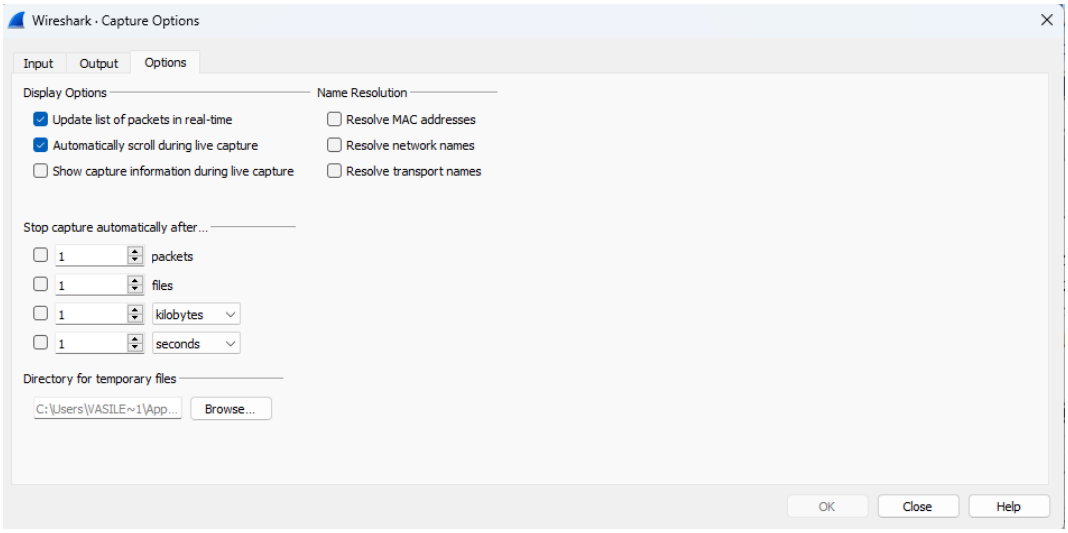

Figure 5: NIC Options

Στη συνέχεια επισκεφτείτε ιστοσελίδα που φιλοξενείται στον υπολογιστή με διεύθυνση IP **195.130.73.235**. Μόλις φορτωθεί πλήρως η σελίδα πατήστε το Stop για να σταματήσει η καταγραφή. Επειδή σε αυτήν την Άσκηση θα συνδυάσουμε το WireShark με το ARP table, θα επιλέξετε από το Μενού **Edit** → **Preferences** → **Appearence** → **Columns** και θα πρέπει η δομή των packet results να είναι η μορφή που παρουσιάζεται στην Εικόνα 6:

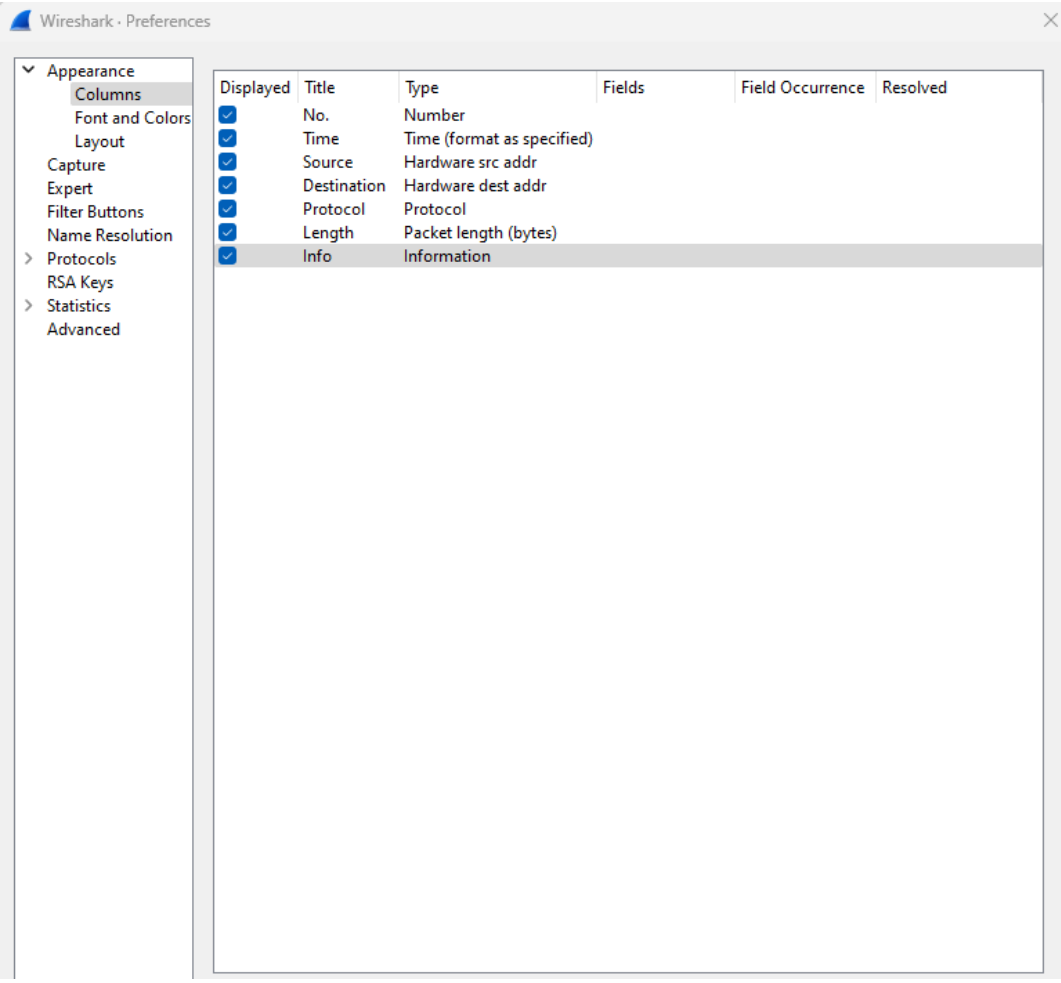

Figure 6: Wireshark Columns

Θα βασίσετε τις απαντήσεις σας για τις επόμενες ερωτήσεις στα στοιχεία της καταγραφής και ειδικότερα στις πληροφορίες που αποτυπώνονται στα παράθυρα με τις λεπτομέρειες της επικεφαλίδας και το περιεχόμενο των πλαισίων. Υπενθυμίζουμε ότι τα πακέτα IP και ARP ενθυλακώνονται σε πλαίσια Ethernet:

- Βρείτε και επιλέξτε το πλαίσιο Ethernet που περιέχει το πρώτο μήνυμα HTTP GET και προσδιορίστε τη διεύθυνση MAC του υπολογιστή σας. [Υπόδειξη: Ακολουθήστε τη διαδρομή **Edit** → **Find Packet...** και στο παράθυρο που θα εμφανιστεί επιλέξτε String. Στο πλαίσιο Filter: πληκτρολογήστε "GET", χωρίς τα εισαγωγικά, και πατήστε το κουμπί Find. Εν ανάγκη συνεχίστε την αναζήτηση από την αρχή της καταγραφής](Εικόνα 7)

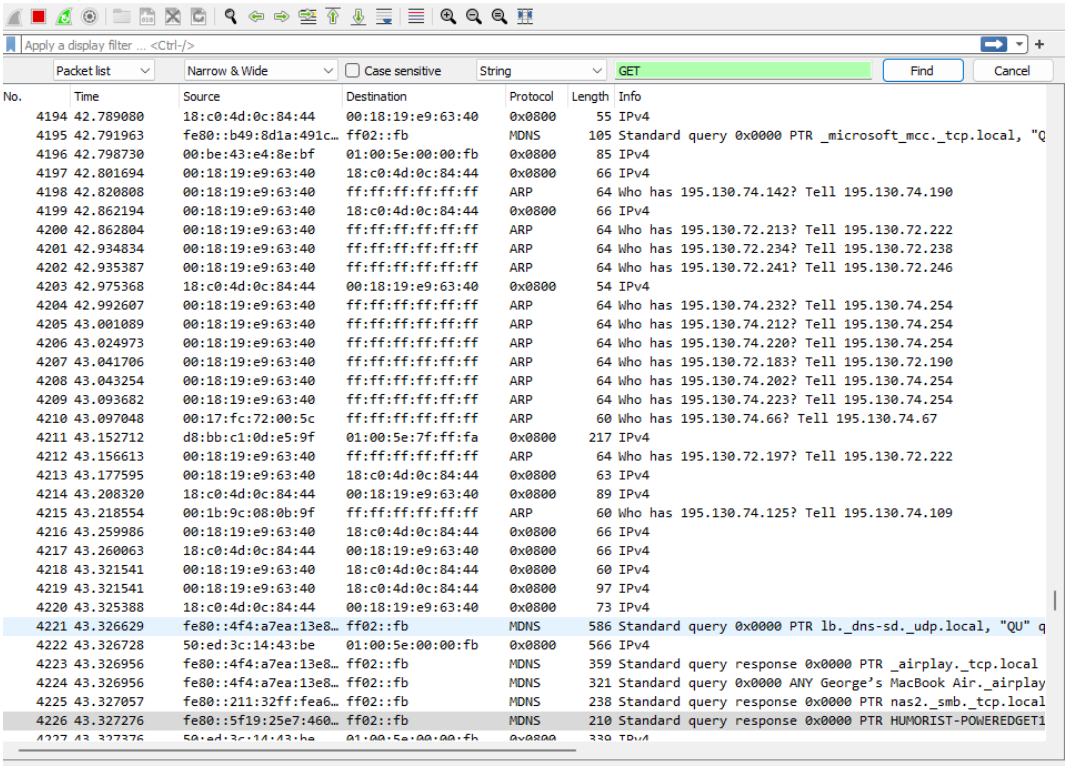

Figure 7: Αποτελέσματα Φίλτρου αλφαριθμητικού GET

- Ποια είναι η διεύθυνση MAC του προορισμού του πλαισίου(Παράδειγμα-Εικόνα 8); **TIP: Κλίκ στο πακέτο → Επιλογή Adapter → Destination**

Figure 8: Εύρεση Mac Adress του προορισμού πλαισίου

- Είναι η παραπάνω διεύθυνση MAC αυτή του **195.130.73.235**;
- Εάν όχι, σε ποια συσκευή ανήκει και γιατί;
- Ποια είναι η δεκαεξαδική τιμή του πεδίου Τύπος (Type) του παραπάνω πλαισίου και ποιο πρωτόκολλο υποδεικνύει;
- Ποιο είναι το μήκος του πλαισίου σε byte;
- Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII "G" της λέξης GET; [Υπόδειξη: επιλέξτε το πεδίο δεδομένων του προηγούμενου αναπτύγματος ώστε να εμφανισθούν στο παράθυρο με τα περιεχόμενα τα αντίστοιχα byte δεδομένων].

Στη συνέχεια βρείτε και επιλέξτε το πλαίσιο Ethernet που περιέχει την απάντηση στο προηγούμενο μήνυμα HTTP [Υπόδειξη: Ακολουθώντας την υπόδειξη του ερωτήματος 2.1, αναζητείστε την ακολουθία "200 OK", χωρίς τα εισαγωγικά, στο περιεχόμενο των αμέσως επόμενων πλαισίων της λίστας καταγεγραμμένων πακέτων.]

- Ποια είναι η διεύθυνση MAC του αποστολέα;

- Είναι η παραπάνω διεύθυνση MAC αυτή του 195.130.73.235
- Σε ποια συσκευή ανήκει η διεύθυνση αυτή;
- Ποια είναι η διεύθυνση MAC του παραλήπτη;
- Σε ποιον υπολογιστή ανήκει;
- Ποια είναι η δεκαεξαδική τιμή του πεδίου Τύπος του παραπάνω πλαισίου;
- Ποιο είναι το μήκος του πλαισίου σε byte; Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII "O" της λέξης OK;
- Ποια από τα πεδία του πλαισίου Ethernet καταγράφει το Wireshark; [Υπόδειξη: συμβουλευθείτε την http://www.techfest.com/networking/lan/ethernet2.htm#2.1 για να δείτε τα πεδία του πλαισίου Ethernet και τα ονόματά τους.]
- Τι συμβαίνει με το CRC; [Υπόδειξη: δείτε http://www.wireshark.org/faq.html#q7.10.]

4 Extra Ασκήσεις

1. Βρείτε τον πίνακα ARP στο Wireshark: Ανοίξτε το Wireshark και καταγράψτε κάποια κίνηση δικτύου. Μεταβείτε στο μενού "Statistics" (Στατιστικά) και επιλέξτε "ARP" από τη λίστα. Θα πρέπει να δείτε τον πίνακα ARP με μια λίστα διευθύνσεων IP και τις αντίστοιχες διευθύνσεις MAC. Καταγράψτε το αποτέλεσμα:

2. Προσδιορίστε τις διευθύνσεις MAC των συσκευών στο δίκτυό σας: Ξεκινήστε μια καταγραφή στο Wireshark και φιλτράρετε για πακέτα ARP χρησιμοποιώντας την έκφραση φίλτρου "arp". Αναζητήστε πακέτα ARP που έχουν μήνυμα "Who has", το οποίο υποδεικνύει ότι η συσκευή προσπαθεί να βρει τη διεύθυνση MAC μιας άλλης συσκευής. Η διεύθυνση MAC της συσκευής που στέλνει το αίτημα ARP θα αναγράφεται στο πεδίο "Source" (Πηγή), ενώ η διεύθυνση MAC της συσκευής που ερωτάται θα αναγράφεται στο πεδίο "Destination" (Προορισμός). Καταγράψτε το απότέλεσμα:

3. Αντιμετώπιση ενός προβλήματος συνδεσιμότητας δικτύου με χρήση του ARP: Ξεκινήστε μια καταγραφή στο Wireshark και φιλτράρετε για πακέτα ARP χρησιμοποιώντας την έκφραση φίλτρου "arp". Αναζητήστε πακέτα ARP που έχουν μήνυμα "Who has" από τη συσκευή που αντιμετωπίζει προβλήματα συνδεσιμότητας. Ελέγξτε το πεδίο "Destination" (Προορισμός) για να δείτε αν η διεύθυνση MAC της συσκευής που ερωτάται είναι σωστή. Εάν δεν είναι, τότε μπορεί να υπάρχει πρόβλημα με τον πίνακα ARP στη συσκευή ή στο δίκτυο. Αναζητήστε πακέτα ARP που έχουν μήνυμα "Gratuitous ARP", το οποίο υποδεικνύει ότι μια συσκευή ανακοινώνει τη δική της διεύθυνση MAC. Αυτό μπορεί να βοηθήσει στον εντοπισμό του εάν η συσκευή είναι σωστά συνδεδεμένη στο δίκτυο. Καταγράψτε πιθανά αποτελέσματα: