Πρωτόκολλα και Αρχιτεκτονικές δικτύων
Εργαστήριο 3

Τμήμα Πληροφορικής και τηλεπικοινωνιών
Πανεπιστήμιο Ιωαννίνων, Άρτα

2023-05-03

Περιεχόμενα

1 Εισαγωγή

Το DNS (Domain Name System) είναι ένα κρίσιμο στοιχείο της υποδομής του Διαδικτύου. Πρόκειται για ένα κατανεμημένο σύστημα που μεταφράζει τα ονόματα τομέων που μπορούν να διαβαστούν από τον άνθρωπο, όπως το **www.example.com**, σε διευθύνσεις IP, οι οποίες απαιτούνται για την επικοινωνία μεταξύ υπολογιστών στο Διαδίκτυο. Το DNS αναφέρεται συχνά ως ο "τηλεφωνικός κατάλογος" του Διαδικτύου. Επιτρέπει στους χρήστες να έχουν πρόσβαση σε δικτυακούς τόπους και άλλους πόρους του Διαδικτύου χρησιμοποιώντας ευκολομνημόνευτα ονόματα αντί για δυσκολομνημόνευτες διευθύνσεις IP. Το nslookup είναι ένα εργαλείο γραμμής εντολών που επιτρέπει στους χρήστες να ζητούν πληροφορίες από διακομιστές DNS για να λαμβάνουν πληροφορίες σχετικά με ονόματα τομέα και διευθύνσεις IP. Είναι ένα ισχυρό διαγνωστικό εργαλείο που μπορεί να χρησιμοποιηθεί για την αντιμετώπιση προβλημάτων που σχετίζονται με το DNS, όπως προβλήματα επίλυσης ονομάτων, προβλήματα συνδεσιμότητας δικτύου και λανθασμένες ρυθμίσεις διακομιστή DNS. Το Nslookup είναι διαθέσιμο στα περισσότερα λειτουργικά συστήματα, συμπεριλαμβανομένων των Windows, macOS και Linux. Το Ipconfig (συντομογραφία του "Internet Protocol Configuration") είναι ένα άλλο εργαλείο γραμμής εντολών που χρησιμοποιείται για την εμφάνιση πληροφοριών σχετικά με τη διαμόρφωση του δικτύου ενός υπολογιστή. Είναι διαθέσιμο στα Windows και επιτρέπει στους χρήστες να προβάλλουν πληροφορίες όπως η διεύθυνση IP του υπολογιστή, η μάσκα υποδικτύου, η προεπιλεγμένη πύλη και οι διευθύνσεις διακομιστών DNS. Το Ipconfig χρησιμοποιείται συχνά για τη διάγνωση προβλημάτων συνδεσιμότητας δικτύου, καθώς μπορεί να παρέχει πολύτιμες πληροφορίες σχετικά με τις ρυθμίσεις δικτύου ενός υπολογιστή. Σε αυτή την εργασία, θα εξερευνήσουμε λεπτομερέστερα τα DNS, nslookup και ipconfig, συμπεριλαμβανομένου του τρόπου λειτουργίας τους, του τρόπου χρήσης τους και του τρόπου με τον οποίο μπορούν να χρησιμοποιηθούν για τη διάγνωση και την αντιμετώπιση προβλημάτων δικτύου.

1.1 DNS - Πώς λειτουργεί

Το DNS είναι ένα ιεραρχικό σύστημα ονοματοδοσίας που βασίζεται σε μια κατανεμημένη βάση δεδομένων. Η βάση δεδομένων συντηρείται από ένα παγκόσμιο δίκτυο διακομιστών DNS, οι οποίοι συνεργάζονται για την παροχή υπηρεσιών επίλυσης ονομάτων για το Διαδίκτυο. Όταν ένας χρήστης εισάγει ένα όνομα τομέα στο πρόγραμμα περιήγησης ιστού, το πρόγραμμα περιήγησης στέλνει ένα αίτημα στον τοπικό επιλυτή DNS (που συνήθως παρέχεται από τον πάροχο υπηρεσιών Διαδικτύου του χρήστη). Στη συνέχεια, ο επιλύτης στέλνει ένα αίτημα στον διακομιστή DNS που είναι υπεύθυνος για τον τομέα ανωτάτου επιπέδου (π.χ. .com, .net, .org). Ο διακομιστής DNS ανωτάτου επιπέδου απαντά με τη διεύθυνση του διακομιστή DNS που είναι υπεύθυνος για τον τομέα δευτέρου επιπέδου (π.χ. example.com). Στη συνέχεια, ο επιλύτης στέλνει ένα αίτημα στον διακομιστή DNS δεύτερου επιπέδου, ο οποίος απαντά με τη διεύθυνση IP του διακομιστή ιστού που φιλοξενεί τον αιτούμενο ιστότοπο. Το DNS λειτουργεί χρησιμοποιώντας δύο τύπους εγγραφών DNS: Εγγραφές A και εγγραφές MX. Οι εγγραφές A αντιστοιχούν ονόματα τομέων σε διευθύνσεις IP, ενώ οι εγγραφές MX αντιστοιχούν ονόματα τομέων σε διακομιστές αλληλογραφίας. Όταν ένας χρήστης εισάγει ένα όνομα τομέα στο πρόγραμμα περιήγησης ιστού, το πρόγραμμα περιήγησης ελέγχει για μια εγγραφή A που σχετίζεται με το όνομα τομέα. Εάν βρεθεί μια εγγραφή A, το πρόγραμμα περιήγησης στέλνει ένα αίτημα στη διεύθυνση IP που σχετίζεται με την εγγραφή A. Εάν δεν βρεθεί καμία εγγραφή A, το πρόγραμμα περιήγησης ελέγχει για μια εγγραφή MX που σχετίζεται με το όνομα τομέα. Εάν βρεθεί μια εγγραφή MX, το πρόγραμμα περιήγησης στέλνει ένα αίτημα στο διακομιστή αλληλογραφίας που σχετίζεται με την εγγραφή MX.

1.2 Nslookup - Πως λειτουργεί

Το Nslookup είναι ένα εργαλείο γραμμής εντολών που χρησιμοποιείται για την υποβολή ερωτημάτων σε διακομιστές DNS για την απόκτηση πληροφοριών σχετικά με ονόματα τομέων και διευθύνσεις IP. Για να χρησιμοποιήσετε το nslookup, ανοίξτε μια γραμμή εντολών ή ένα παράθυρο τερματικού και πληκτρολογήστε "nslookup" ακολουθούμενο από το όνομα τομέα ή τη διεύθυνση IP που θέλετε να αναζητήσετε. Για παράδειγμα, για να λάβετε τη διεύθυνση IP του www.example.com, πληκτρολογήστε "nslookup www.example.com" στη γραμμή εντολών. Το nslookup θα εμφανίσει τη διεύθυνση IP που σχετίζεται με το όνομα τομέα και άλλες πληροφορίες σχετικά με το διακομιστή DNS που παρείχε τις πληροφορίες. Το Nslookup μπορεί να χρησιμοποιηθεί για τη διάγνωση ενός ευρέος φάσματος προβλημάτων δικτύου, συμπεριλαμβανομένων προβλημάτων επίλυσης ονομάτων, προβλημάτων συνδεσιμότητας δικτύου και λανθασμένων ρυθμίσεων διακομιστή DNS. Για παράδειγμα, αν δεν μπορείτε να αποκτήσετε

πρόσβαση σε έναν ιστότοπο, μπορείτε να χρησιμοποιήσετε το nslookup για να προσδιορίσετε αν το πρόβλημα οφείλεται σε ένα ζήτημα που σχετίζεται με το DNS. Ας υποθέσουμε ότι το nslookup είναι σε θέση να επιλύσει το όνομα τομέα σε μια διεύθυνση IP. Στην περίπτωση αυτή, υποδηλώνει ότι ο διακομιστής DNS λειτουργεί σωστά και το πρόβλημα μπορεί να οφείλεται σε άλλο ζήτημα, όπως ένα ζήτημα συνδεσιμότητας δικτύου ή ένα πρόβλημα με τον διακομιστή ιστού που φιλοξενεί τον ιστότοπο. Εκτός από την αναζήτηση διακομιστών DNS, το nslookup μπορεί επίσης να χρησιμοποιηθεί για την εκτέλεση αντίστροφης αναζήτησης DNS, η οποία αντιστοιχίζει διευθύνσεις IP σε ονόματα τομέα. Για να εκτελέσετε μια αντίστροφη αναζήτηση DNS, πληκτρολογήστε "nslookup" ακολουθούμενη από τη διεύθυνση IP που θέλετε να αναζητήσετε. Για παράδειγμα, για να λάβετε το όνομα τομέα που σχετίζεται με τη διεύθυνση **IP 192.168.0.1**, πληκτρολογήστε "**nslookup 192.168.0.1**" στη γραμμή εντολών.

1.3 Ipconfig - Πώς λειτουργεί

Το Ipconfig είναι ένα εργαλείο γραμμής εντολών που εμφανίζει πληροφορίες σχετικά με τη διαμόρφωση δικτύου ενός υπολογιστή. Για να χρησιμοποιήσετε το ipconfig, ανοίξτε μια γραμμή εντολών και πληκτρολογήστε "ipconfig" ακολουθούμενο από την κατάλληλη επιλογή γραμμής εντολών. Για παράδειγμα, για να εμφανίσετε πληροφορίες σχετικά με τη διεύθυνση IP, τη μάσκα υποδικτύου και την προεπιλεγμένη πύλη του υπολογιστή, πληκτρολογήστε "ipconfig /all" στη γραμμή εντολών. Το ipconfig θα εμφανίσει πληροφορίες όπως η διεύθυνση IP του υπολογιστή, η μάσκα υποδικτύου, η προεπιλεγμένη πύλη και οι διευθύνσεις διακομιστών DNS. Το Ipconfig μπορεί να χρησιμοποιηθεί για τη διάγνωση προβλημάτων συνδεσιμότητας δικτύου, όπως προβλήματα με τη διαμόρφωση της διεύθυνσης IP ή προβλήματα με τον προσαρμογέα δικτύου του υπολογιστή. Για παράδειγμα, ας υποθέσουμε ότι δεν μπορείτε να συνδεθείτε στο Διαδίκτυο. Σε αυτή την περίπτωση, μπορείτε να χρησιμοποιήσετε το ipconfig για να διαπιστώσετε αν έχει εκχωρηθεί στον υπολογιστή μια έγκυρη διεύθυνση IP και αν έχει ρυθμιστεί να χρησιμοποιεί τον σωστό διακομιστή DNS. Τα DNS, nslookup και ipconfig είναι βασικά εργαλεία για τη διάγνωση και την αντιμετώπιση προβλημάτων δικτύου. Το DNS είναι ένα ζωτικής σημασίας στοιχείο της υποδομής του Διαδικτύου, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε ιστότοπους και άλλους πόρους του Διαδικτύου χρησιμοποιώντας εύκολα στην απομνημόνευση ονόματα αντί για δύσκολα στην απομνημόνευση διευθύνσεις IP. Το Nslookup είναι ένα ισχυρό διαγνωστικό εργαλείο που μπορεί να χρησιμοποιηθεί για την αντιμετώπιση προβλημάτων που σχετίζονται με το DNS, ενώ το ipconfig παρέχει πολύτιμες πληροφορίες σχετικά με τη διαμόρφωση του δικτύου ενός υπολογιστή. Κατανοώντας πώς λειτουργούν αυτά τα εργαλεία και πώς να τα χρησιμοποιούν αποτελεσματικά, οι διαχειριστές δικτύου μπορούν να διαγνώσουν και να επιλύσουν προβλήματα δικτύου πιο γρήγορα και αποτελεσματικά.

2 Ασκήσεις(Nslookup and Ipconfig)

2.1 Nslookup flags

- **-debug:** Η παράμετρος αυτή ενεργοποιεί την έξοδο εντοπισμού σφαλμάτων, η οποία μπορεί να είναι χρήσιμη κατά την αντιμετώπιση σύνθετων προβλημάτων DNS.
- **-type:** Αυτή η παράμετρος καθορίζει τον τύπο της εγγραφής DNS που θα αναζητηθεί. Για παράδειγμα, το "-type=MX" μπορεί να χρησιμοποιηθεί για να ζητηθεί η εγγραφή ανταλλαγής αλληλογραφίας (MX) για ένα συγκεκριμένο όνομα τομέα.
- **-server:** Αυτή η παράμετρος σάς επιτρέπει να καθορίσετε τον διακομιστή DNS που θα ερωτηθεί. Από προεπιλογή, το nslookup χρησιμοποιεί τον προεπιλεγμένο διακομιστή DNS που έχει ρυθμιστεί στον τοπικό υπολογιστή.
- **-querytype:** Αυτή η παράμετρος σάς επιτρέπει να καθορίσετε τον τύπο ερωτήματος που θα χρησιμοποιείται κατά την αναζήτηση εγγραφών DNS. Για παράδειγμα, το "-querytype=AAAA" μπορεί να χρησιμοποιηθεί για την αναζήτηση εγγραφών IPv6.
- **-timeout:** Αυτή η παράμετρος σας επιτρέπει να καθορίσετε την τιμή χρονικού ορίου για τα ερωτήματα DNS. Από προεπιλογή, το nslookup περιμένει 2 δευτερόλεπτα για μια απάντηση από το διακομιστή DNS.
- **-retry:** Αυτή η παράμετρος σάς επιτρέπει να καθορίσετε τον αριθμό των φορών επανάληψης ενός αποτυχημένου ερωτήματος DNS. Από προεπιλογή, το nslookup επαναλαμβάνει 3 φορές.

- **-nssearch:** Αυτή η παράμετρος ενεργοποιεί ερωτήματα τύπου NSAP[1] για σημεία πρόσβασης υπηρεσιών δικτύου.
- **-ipv4:** Αυτή η παράμετρος αναγκάζει το nslookup να χρησιμοποιεί IPv4 για την υποβολή ερωτημάτων σε διακομιστές DNS.
- **-ipv6:** Αυτή η παράμετρος αναγκάζει το nslookup να χρησιμοποιεί IPv6 για την υποβολή ερωτημάτων σε διακομιστές DNS.
- **-vc:** Αυτή η παράμετρος ενεργοποιεί τη λειτουργία TCP/IP για το ερώτημα nslookup.

2.2 Ipconfig flags

- **/all:** Αυτή η παράμετρος εμφανίζει λεπτομερείς πληροφορίες για όλες τις διασυνδέσεις δικτύου, συμπεριλαμβανομένων των διευθύνσεων IP, των μασκών υποδικτύου, των προεπιλεγμένων πυλών, των διακομιστών DNS, των διευθύνσεων IP του διακομιστή DHCP και άλλων λεπτομερειών διαμόρφωσης.
- **/displaydns:** Αυτή η παράμετρος χρησιμοποιήται, για να βρείτε τις εγγραφές που είναι αποθηκευμένες στην προσωρινή μνήμη (cache)
- **/release:** Αυτή η παράμετρος αποδεσμεύει τη διεύθυνση IP που έχει εκχωρηθεί σε μια διασύνδεση δικτύου από το διακομιστή DHCP.
- **/renew:** Αυτή η παράμετρος ανανεώνει τη διεύθυνση IP που έχει εκχωρηθεί σε μια διασύνδεση δικτύου από το διακομιστή DHCP.
- **/flushdns:** Αυτή η παράμετρος διαγράφει την προσωρινή μνήμη cache του επιλυτή DNS, η οποία μπορεί να είναι χρήσιμη εάν αντιμετωπίζετε προβλήματα επίλυσης DNS.
- **/registerdns:** Αυτή η παράμετρος αναγκάζει τη διασύνδεση δικτύου να καταχωρίσει εκ νέου το όνομα DNS και τη διεύθυνση IP της στο διακομιστή DNS.
- **/displaydns:** Αυτή η παράμετρος εμφανίζει τα περιεχόμενα της κρυφής μνήμης του επιλυτή DNS.
- **/showclassid:** Αυτή η παράμετρος εμφανίζει το αναγνωριστικό κλάσης DHCP που σχετίζεται με τη διασύνδεση δικτύου.
- **/setclassid:** Αυτή η παράμετρος ορίζει το αναγνωριστικό κλάσης DHCP που σχετίζεται με τη διασύνδεση δικτύου.
- **/showclassid6:** Αυτή η παράμετρος εμφανίζει το αναγνωριστικό κλάσης DHCPv6 που σχετίζεται με τη διασύνδεση δικτύου.
- **/setclassid6:** Αυτή η παράμετρος ορίζει το αναγνωριστικό κλάσης DHCPv6 που σχετίζεται με τη διασύνδεση δικτύου.
- **/showclassid6:** Αυτή η παράμετρος εμφανίζει το αναγνωριστικό κλάσης DHCPv6 που σχετίζεται με τη διασύνδεση δικτύου.
- **/setclassid6:** Αυτή η παράμετρος ορίζει το αναγνωριστικό κλάσης DHCPv6 που σχετίζεται με τη διασύνδεση δικτύου.

[1] https://help.sap.com/docs/SAP_NETWEAVER_750/40d2cb3a4f9249d58e9bbc95f4dbaff8/4e56dd962bd54f48e10000000a42189e.html

2.3 Extra εντολές

Υπάρχουν πολλές άλλες εντολές που μπορεί να σας φανούν χρήσιμες όταν μελετάτε το DNS και τις ρυθμίσεις δικτύου. **Ακολουθούν μερικά παραδείγματα:**

- **ping:** στέλνοντας πακέτα σε μια απομακρυσμένη διεύθυνση IP και περιμένοντας απάντηση.
- **tracert - traceroute:** Αυτή η εντολή χρησιμοποιείται για την ανίχνευση της διαδρομής που ακολουθούν τα πακέτα δικτύου από μια συσκευή σε μια άλλη, δείχνοντας τους δρομολογητές ή τις συσκευές δικτύου κατά μήκος της διαδρομής.
- **netstat:** Αυτή η εντολή εμφανίζει πληροφορίες σχετικά με τις ενεργές συνδέσεις δικτύου, συμπεριλαμβανομένων των τοπικών και απομακρυσμένων διευθύνσεων IP και θυρών, του πρωτοκόλλου που χρησιμοποιείται και της κατάστασης της σύνδεσης.
- **route:** Αυτή η εντολή χρησιμοποιείται για την προβολή ή την τροποποίηση του τοπικού πίνακα δρομολόγησης, ο οποίος καθορίζει τον τρόπο δρομολόγησης της κυκλοφορίας δικτύου μεταξύ διαφορετικών τμημάτων δικτύου.
- **nsupdate:** Αυτή η εντολή χρησιμοποιείται για τη διαδραστική ενημέρωση εγγραφών DNS σε έναν διακομιστή DNS.
- **dig:** Αυτή η εντολή είναι παρόμοια με την nslookup, αλλά παρέχει πιο λεπτομερείς πληροφορίες σχετικά με τα ερωτήματα DNS, συμπεριλαμβανομένου του χρόνου που απαιτείται για τη λήψη μιας απάντησης από το διακομιστή DNS.
- **arp:** Αυτή η εντολή χρησιμοποιείται για την εμφάνιση και τη διαχείριση της προσωρινής μνήμης ARP, η οποία χρησιμοποιείται για την αντιστοίχιση διευθύνσεων IP σε διευθύνσεις MAC σε ένα τοπικό δίκτυο.
- **ifconfig - ip:** Αυτές οι εντολές χρησιμοποιούνται για την προβολή και τη διαμόρφωση των διασυνδέσεων δικτύου και των σχετικών διευθύνσεων IP, netmasks και άλλων λεπτομερειών διαμόρφωσης.
- **hostname:** Αυτή η εντολή εμφανίζει το όνομα κεντρικού υπολογιστή του τοπικού μηχανήματος.
- **ssh:** Αυτή η εντολή χρησιμοποιείται για την ασφαλή σύνδεση σε ένα απομακρυσμένο μηχάνημα μέσω δικτύου.

2.4 Εκφωνήσεις

1. Εκτελέστε τα παρακάτω και καταγράψτε τα αποτελέσματα:
   - Χρησιμοποιήστε το nslookup για να αναζητήσετε τη διεύθυνση IP του ονόματος τομέα "google.com".
   - Χρησιμοποιήστε το nslookup για να εκτελέσετε μια αντίστροφη αναζήτηση DNS στη διεύθυνση **IP 8.8.8.8**.
   - Χρησιμοποιήστε nslookup για να ζητήσετε την εγγραφή MX (ανταλλαγή αλληλογραφίας) για το όνομα τομέα **yahoo.com**.
   - Χρησιμοποιήστε το nslookup για να ζητήσετε την εγγραφή NS (διακομιστής ονομάτων) για το όνομα τομέα **amazon.com**.
   - Χρησιμοποιήστε το nslookup για να εκτελέσετε μια αναζήτηση DNS σε ένα όνομα τομέα της επιλογής σας.
2. Εκτελέστε τα παρακάτω και καταγράψτε τα αποτελέσματα:
   - Χρησιμοποιήστε το ipconfig για να εμφανίσετε πληροφορίες σχετικά με τις ρυθμίσεις δικτύου του υπολογιστή σας.
   - Χρησιμοποιήστε το ipconfig για να ανανεώσετε τη διεύθυνση IP του υπολογιστή σας.
   - Χρησιμοποιήστε το ipconfig για να αποδεσμεύσετε τη διεύθυνση IP του υπολογιστή σας.

- Χρησιμοποιήστε το ipconfig για να εμφανίσετε πληροφορίες σχετικά με τους διακομιστές DNS του υπολογιστή σας.
- Χρησιμοποιήστε το ipconfig για να εμφανίσετε πληροφορίες σχετικά με τον προσαρμογέα δικτύου του υπολογιστή σας.
- Εμφάνιση των ρυθμίσεων του προσαρμογέα δικτύου για όλες τις διασυνδέσεις δικτύου στο σύστημα.

3 Άσκηση στο Wireshark

Μετά την εξοικείωση με το nslookup και το ipconfig, θα χρησιμοποιήσουμε το Wireshark για να συλλάβουμε τα πακέτα DNS που δημιουργούνται κατά τη συνηθισμένη δραστηριότητα πλοήγησης του Παγκόσμιου Ιστού.

Πρώτα επιλέξτε το κατάλληλο interface όπως στην εικόνα 1, επιλέγοντας **Capture** → **Options** → **Manage Interfaces**, και έχοντας επιλεγμένα τα τις στήλες της εικόνας 2.

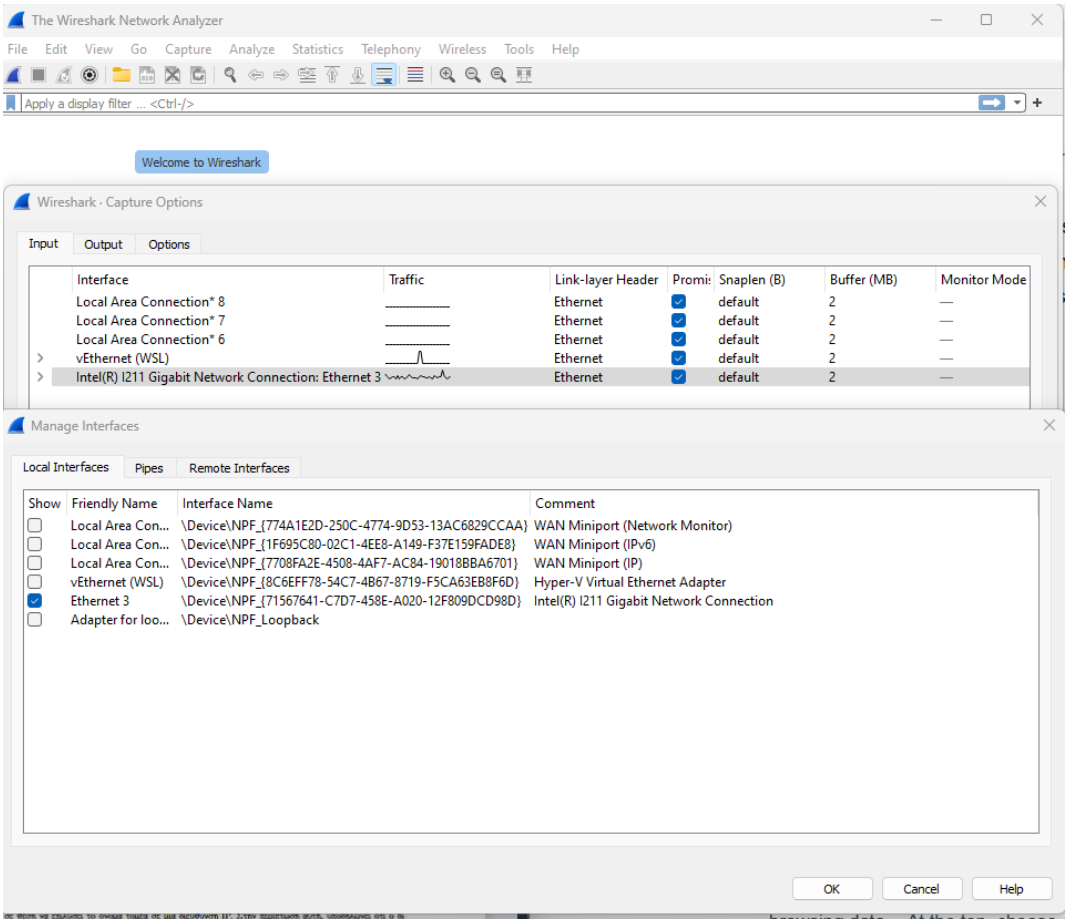

Figure 1: Manage Intefaces

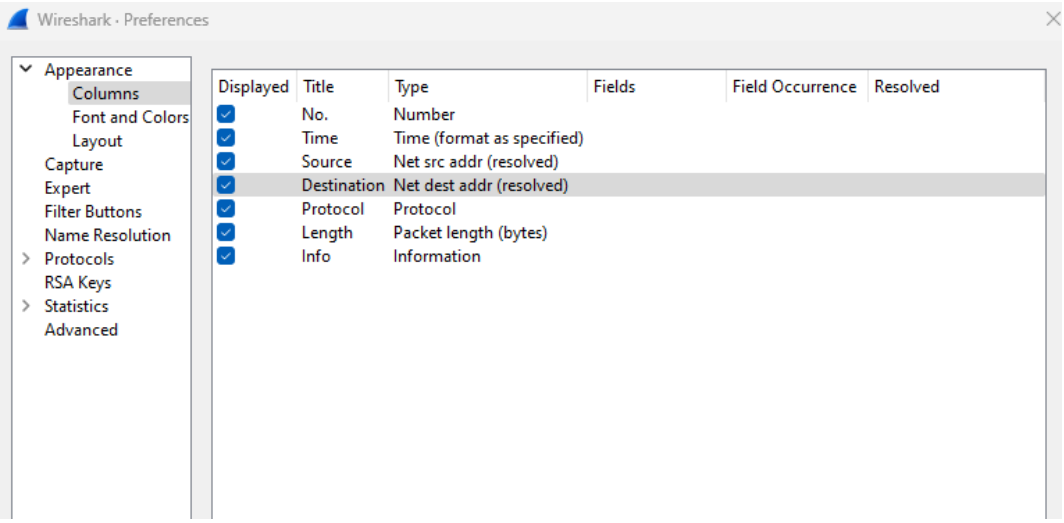

Figure 2: Wireshark selected columns

- Χρησιμοποιήστε το ipconfig για να αδειάσετε την DNS cache του host σας.
- Ανοίξτε το web browser σας και αδειάστε την cache του3.

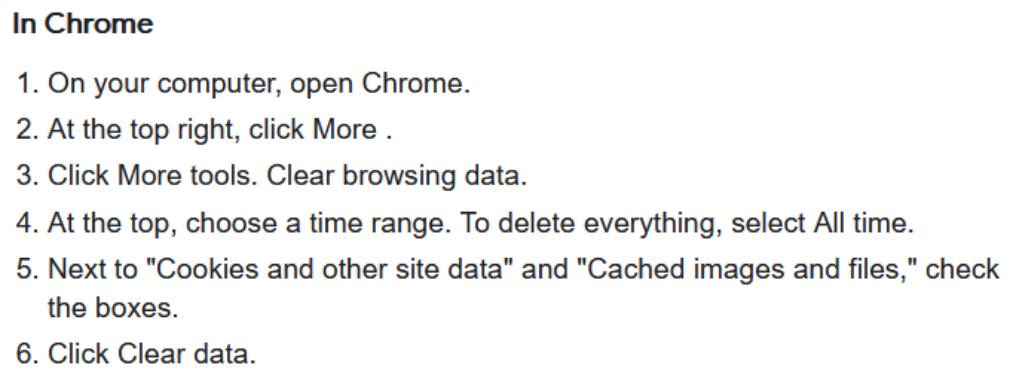

Figure 3: Clear cache

- Ανοίξτε το Wireshark και εισάγετε "ip.addr == διεύθυνση_IP_host" στο φίλτρο. Χρησιμοποιήστε το ipconfig για να βρείτε τη διεύθυνση IP του host σας(διεύθυνση_IP_host). Το φίλτρο αυτό απομακρύνει όλα τα πακέτα που δεν προέρχονται από ούτε προορίζονται για τον host σας.
- Ξεκινήστε τη σύλληψη πακέτων από το Wireshark.
- Με τη βοήθεια του browser, επισκεφθείτε την ιστοσελίδα: http://www.ietf.org
- Σταματήστε τη σύλληψη πακέτων. **Παράδειγμα εκτέλεσης παρουσιάζεται στην εικόνα 4**

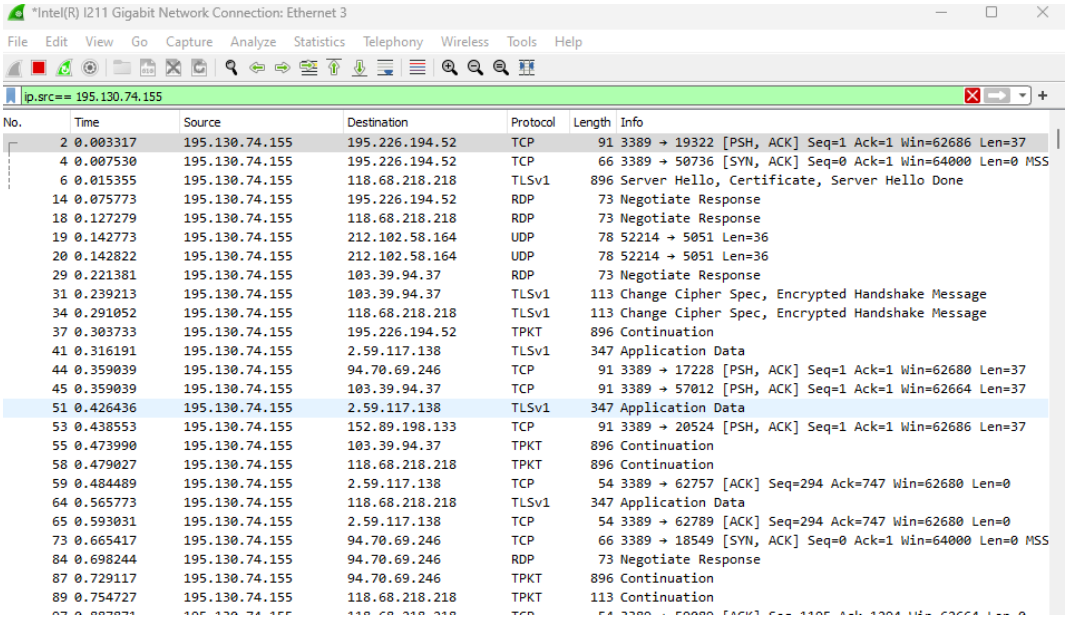

Figure 4: Execute packet capture

3.1 ΣΕΤ 1

Απαντήστε στις ακόλουθες ερωτήσεις:

1. Εντοπίστε τα μηνύματα ερωτημάτων (query) και αποκρίσεων (response) του DNS. Ποιο πρωτόκολλο μεταφοράς χρησιμοποιείται για τη μεταφορά τους, UDP ή TCP;

2. Ποια η θύρα προορισμού (destination port) του μηνύματος ερωτήματος; Ποια η θύρα πηγής (source port) του μηνύματος απόκρισης;

3. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Χρησιμοποιήστε το ipconfig για να προσδιορίσετε τη διεύθυνση IP του τοπικού σας DNS server. Τι σχέση έχουν μεταξύ τους οι δύο διευθύνσεις IP;

4. Εξετάστε το μήνυμα ερωτήματος. Ποιο το "είδος" ("Type") του ερωτήματος; Περιέχονται "απαντήσεις' ("answers') στο μήνυμα ερωτήματος;

5. Εξετάστε το μήνυμα απόκρισης. Πόσες "απαντήσεις" περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;

6. Θεωρείστε το επακόλουθο πακέτο SYN (SYN packet ή SYN segment) που στέλνει το TCP που τρέχει στον host σας. Η διεύθυνση προορισμού αυτού του πακέτου αντιστοιχεί σε καμία από τις διευθύνσεις IP που παρέχονται στο μήνυμα απόκρισης του DNS;

7. . Η ιστοσελίδα http://www.ietf.org περιέχει εικόνες. Χρειάζεται ο host σας να στείλει νέα ερωτήματα DNS πριν από την ανάκτηση κάθε εικόνας;

3.2 ΣΕΤ 2

Ας ασχοληθούμε τώρα με το nslookup

- Ξεκινήστε τη σύλληψη πακέτων.
- Τρέξτε το nslookup για το όνομα host www.mit.edu.

```
Server:  pdns1.grnet.gr
Address:  194.177.210.210

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:11a:396::255e
          2a02:26f0:11a:388::255e
          23.33.6.100
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

Figure 5: Nslookup Mit edu

- Σταματήστε τη σύλληψη πακέτων.

Η ακολουθία των πακέτων (trace) που απεικονίζεται στο Wireshark θα πρέπει να μοιάζει με αυτήν που φαίνεται στην εικόνα 6(Με βάση πάντα τον δικό σας host).

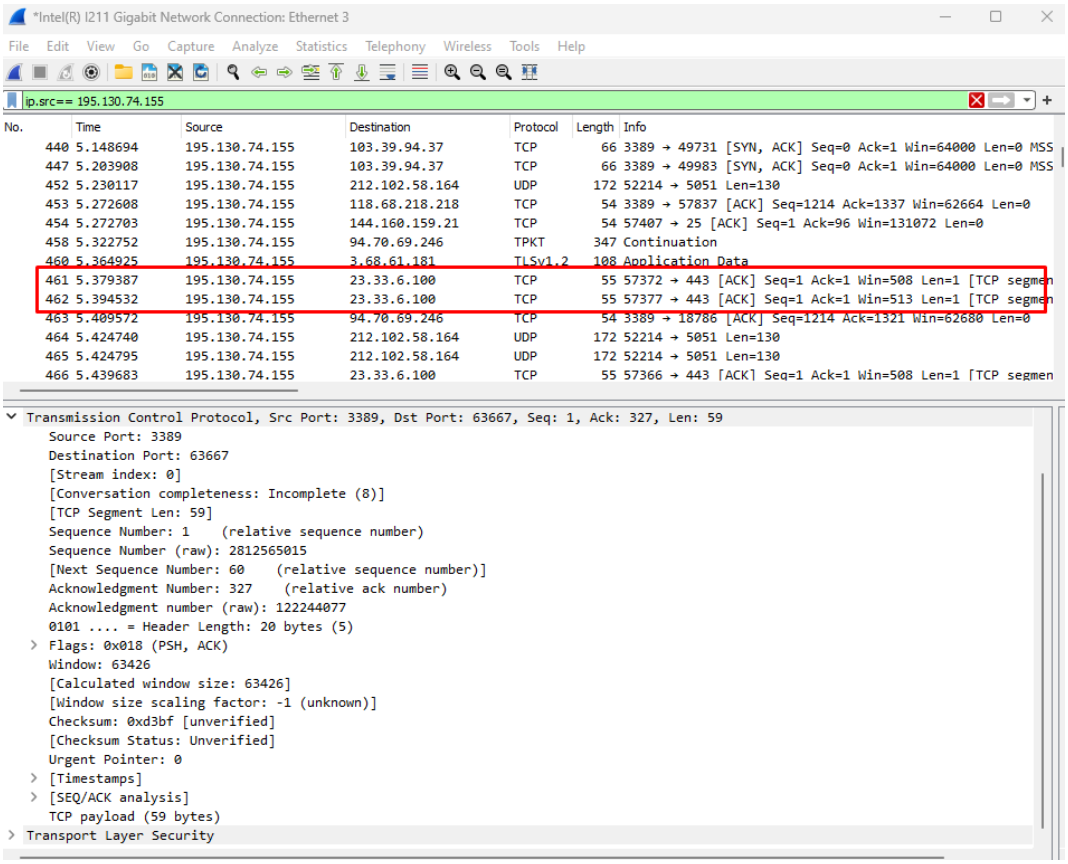

Figure 6: Wireshark Mit_edu

Όπως φαίνεται, το nslookup έστειλε στην πραγματικότητα τρία ερωτήματα DNS και έλαβε, αντίστοιχα, τρεις αποκρίσεις. Για να απαντήσετε στις παρακάτω ερωτήσεις αγνοείστε τα δύο πρώτα ζεύγη ερωτημάτων, αποκρίσεων καθώς αφορούν το nslookup και κατά κανόνα δεν δημιουργούνται από συνήθεις ιαδικτυακές εφαρμογές. Επικεντρωθείτε, λοιπόν, στο τελευταίο ερώτημα και την τελευταία απόκριση DNS.

1. Ποια η θύρα προορισμού (destination port) του μηνύματος ερωτήματος; Ποια η θύρα πηγής(source port) του μηνύματος απόκρισης;

2. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server;

3. Εξετάστε το μήνυμα ερωτήματος. Ποιο το "είδος" ("Type") του ερωτήματος; Περιέχονται "απαντήσεις" ("answers") στο μήνυμα ερωτήματος;

4. Εξετάστε το μήνυμα απόκρισης. Πόσες "απαντήσεις" περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;

5. Παρέχεται εικόνα για το παραπάνω ερώτημα

3.3 ΣΕΤ 3

Επαναλάβετε το προηγούμενο πείραμα για την εντολή: **nslookup –type=NS mit.edu**

Απαντήστε στις παρακάτω ερωτήσεις:

- Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server;
- Εξετάστε το μήνυμα ερωτήματος. Ποιο το "είδος" ("Type") του ερωτήματος; Περιέχονται "απαντήσεις" ("answers") στο μήνυμα ερωτήματος;
- Εξετάστε το μήνυμα απόκρισης. Ποια ονόματα nameservers του MIT παρέχονται στο μήνυμα απόκρισης; Στο μήνυμα απόκρισης παρέχονται και οι διευθύνσεις IP των nameservers του MIT;
- Παρέχεται εικόνα για το παραπάνω ερώτημα.

Επαναλάβετε το προηγούμενο πείραμα για την εντολή: **nslookup** `www.aiit.or.kr` **ip_bitsy.mit.edu**

Απαντήστε στις ακόλουθες ερωτήσεις:

1. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server; Εάν όχι, σε τι αντιστοιχεί η συγκεκριμένη διεύθυνση IP;

2. Εξετάστε το μήνυμα ερωτήματος. Ποιο το "είδος" ("Type") του ερωτήματος; Περιέχονται "απαντήσεις" ("answers") στο μήνυμα ερωτήματος;

3. Εξετάστε το μήνυμα απόκρισης. Πόσες "απαντήσεις" περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;

4. Παρέχεται εικόνα για το παραπάνω ερώτημα.

5. Εάν εκτελέσετε την εντολή nslookup `www.dit.uoi.gr` αφού αδειάσετε την DNS cache, θα περάσετε από τους ίδιους nameservers για να λάβετε την απάντηση;