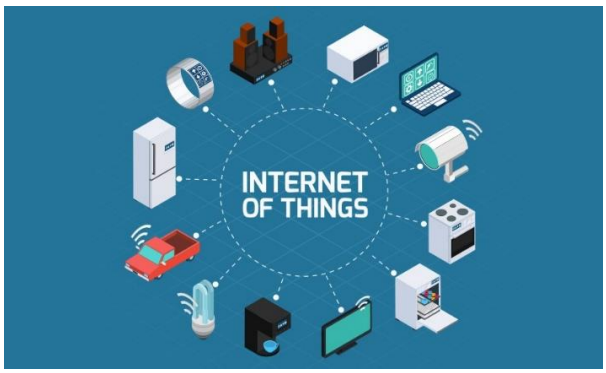
ΕΝΟΤΗΤΑ Ι

1. ΕΙΣΑΓΩΓΗ ΣΤΑ ΕΦΑΡΜΟΣΜΕΝΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

1.1 Εισαγωγή σε βασικές έννοιες

1.1.1 Η σημασία της δικτύωσης στην Πανταχού Παρούσα Υπολογιστική (Ubiquitous Computing)

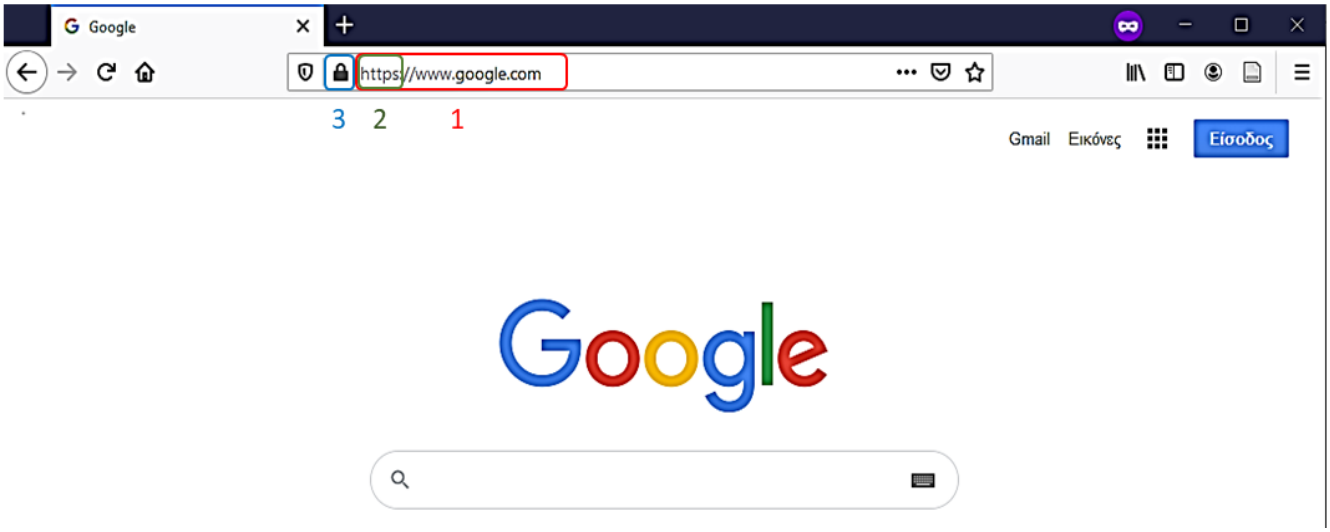
Το διαδίκτυο αποτελεί ένα τμήμα της καθημερινής ζωής και είναι αναγκαία η κατανόηση της λειτουργίας του από κάθε επιστήμονα/μηχανικό που δραστηριοποιείται στους τομείς της Πληροφορικής. Τα τελευταία χρόνια παρατηρούμε την σταδιακή μετάβαση σε μια κατάσταση όπου η υπολογιστική (computing) θα διαχέεται σε κάθε σημείο του περιβάλλοντος του ανθρώπου και είναι διαθέσιμη σε κάθε στιγμή της ζωής του. Η ιδέα της *Πανταχού Παρούσας Υπολογιστικής (Ubiquitous Computing)* είναι μια σκέψη που ξεκινάει στα τέλη του περασμένου αιώνα από τον Mark Weiser και βλέπουμε την υλοποίηση της στον 21ο αιώνα, κυρίως με την έλευση των φορητών συσκευών που λειτουργούν σε ασύρματα δίκτυα. Αυτά διευκολύνουν το κοινωνικό διαδίκτυο (social web), που θεωρείται ως το διαδίκτυο 2.0. Στο κοντινό μέλλον η σημασία των δικτύων υπολογιστών θα παίξει κρίσιμο ρόλο στην δημιουργία του *Ευφυούς Διαδικτύου (Intelligent Web)*, ή διαδικτύου 4.0. Σε αυτό θα συνδέονται μεταξύ τους, εκτός από τους ανθρώπους, και τα αντικείμενα δημιουργώντας το *Διαδίκτυο των Πραγμάτων - Internet of Things (IoT).*



Εικόνα **1.1**: Το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT)

1.1.2 Η εμπειρία του χρήστη που παρέχεται από μια διαδικτυακή εφαρμογή και η έννοια του πρωτοκόλλου δικτύου

Αντιλαμβανόμαστε την δικτύωση μέσα από την εμπειρία χρήση - user experience (UX) την οποία μας δίνουν οι διάφορες εφαρμογές που λειτουργούν στο διαδίκτυο. Θα αναλύσουμε τι υπάρχει πίσω από την αντίληψη της δικτύωσης ως μια παρεχόμενη υπηρεσία, ξεκινώντας από την επισκόπηση της επικοινωνίας που γίνεται όταν φορτώνουμε την αρχική ιστοσελίδα από έναν ιστότοπο (website).



Εικόνα 1.2: Πλοήγηση στον ιστότοπο της Google με χρήση ενός διαδικτυακού συνδέσμου *Uniform Resource Locator (URL)* μέσα από πλοηγό (ή φυλλομετρητή ή browser). Παρατηρούμε: 1. Το URL που περιλαμβάνει το 2. Πρόθεμα πρωτοκόλλου εφαρμογής, εδώ το https και 3. Ένδειξη για ασφαλή επικοινωνία με χρήση κρυπτογράφησης.

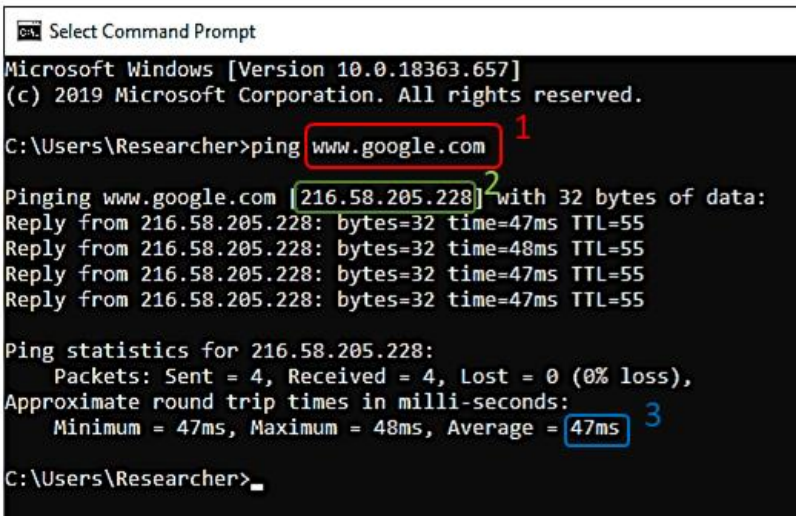
1.1.3 Η διευθυνσιοδότηση στο διαδίκτυο

Όπως το σύστημα του ταχυδρομείου χρειάζεται διεύθυνση αποστολέα και διεύθυνση παραλήπτη για να παραδώσει έναν φάκελο ή πακέτο, έτσι και στα δίκτυα χρειαζόμαστε μια τοπική διεύθυνση αποστολέα και μια απομακρυσμένη διεύθυνση παραλήπτη για κάθε *μονάδα πληροφορίας (data unit)* που αποστέλλεται.

ΑΣΚΗΣΗ 1.1: Εύρεση διεύθυνσης IPv4 μιας απομακρυσμένης διαδικτυακής τοποθεσίας

Ανοίξτε μια γραμμή εντολών του λειτουργικού συστήματος. Στα Windows χρησιμοποιήστε την συντόμευση κουμπί **Win+R**, πληκτρολογήστε **cmd** και πατήστε **Enter**.

- Εκτελέστε την εντολή **ping** αντικαθιστώντας την ονομασία που εμφανίζεται στην θέση 1 της εικόνας 1.3, με αυτήν που χρησιμοποιείτε πιο συχνά.



Εικόνα 1.3: Έλεγχος επικοινωνίας μεταξύ του τοπικού συστήματος μας και απομακρυσμένης τοποθεσίας. Παρατηρούμε: 1. Την ονομασία του τομέα (domain name), 2. Την διεύθυνση IPv4 που αντιστοιχεί στο domain name, 3. Τον μέσο όρο της καθυστέρησης επικοινωνίας σε milliseconds

- Δοκιμάστε οποιαδήποτε ονομασία τομέα θέλετε με την εντολή ping. Παρατηρήστε την επιστροφή της αντίστοιχης **απομακρυσμένης διεύθυνσης IPv4**. Σκεφτόμαστε ως απομακρυσμένο οποιοδήποτε άλλο σύστημα εκτός από αυτό που βρισκόμαστε το οποίο είναι το τοπικό.
- Ανάλογα με την κατεύθυνση της επικοινωνίας το τοπικό σύστημα μπορεί να είναι **είτε αποστολέας είτε παραλήπτης.**

ΑΣΚΗΣΗ 1.2: Εύρεση διεύθυνσης IPv4 με την οποία φαίνεται το σύστημα μας στο διαδίκτυο

Αναζητήστε στο διαδίκτυο με την πρόταση “what is my IP”. Επιλέξτε μια από τις ιστοσελίδες που εμφανίζονται στα αποτελέσματα.

- Παρατηρήστε την διεύθυνση που εμφανίζεται για το τοπικό σας **σύστημα (host)** και αυτήν που εμφανίζεται στο σύστημα ενός συναδέλφου σας. Σε ποιο συμπέρασμα οδηγείστε;

Για την πληρότητα της κατανόησης σας αναφέρεται ότι μπορεί να υπάρξουν πολλές διαφορετικές IPv4 για το ίδιο host. Όταν η ίδια IPv4 χρησιμοποιείται για πολλούς hosts τότε για να καθοριστεί ποιος από αυτούς πρέπει να παραλάβει τις πληροφορίες πρέπει να υπάρχει ένα πρωτόκολλο αποσαφήνισης.

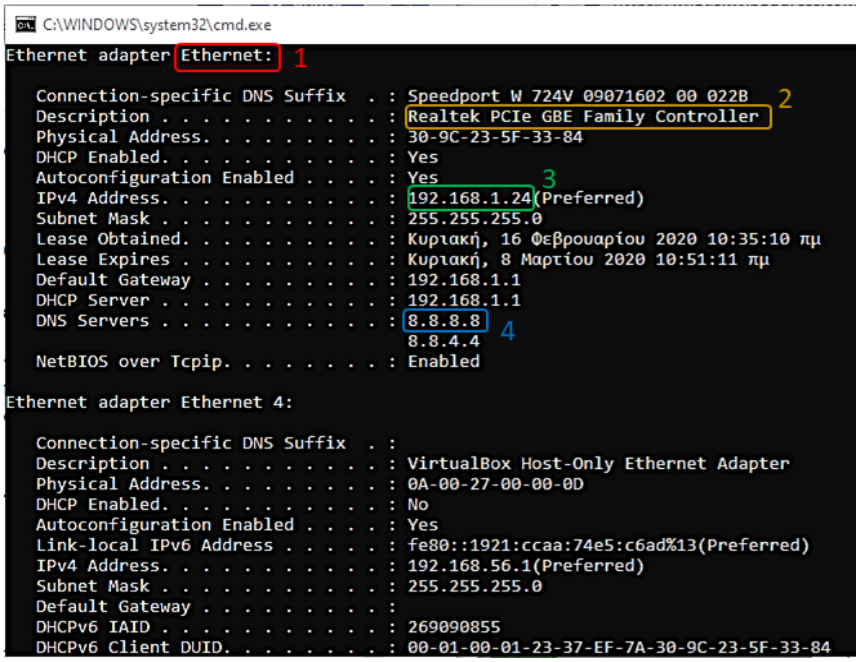
1.1.4 Οι δικτυακές ρυθμίσεις σύνδεσης ενός συστήματος

Οποιοδήποτε υπολογιστικό σύστημα για το οποίο θα χρησιμοποιούμε τον όρο *host,* είτε σταθερό (smart sensor, embedded, desktop, server, κ.α.), είτε φορητό (laptop, tablet, smartphone, wearable, *carputer*, κ.α.) περιλαμβάνει στο υλισμικό του (hardware) ολοκληρωμένα κυκλώματα που υλοποιούν την σύνδεση σε ένα δίκτυο. Η ορολογία κάρτα δικτύου (network card) είναι γνωστή από τους σταθερούς υπολογιστές, επειδή στο παρελθόν το εξειδικευμένο hardware για δικτύωση ήταν μια αυτόνομη κάρτα μέσα στην συναρμολόγηση. Σήμερα μπορεί να το αντιληφθούμε όταν χρησιμοποιούμε μια αποσπώμενη συσκευή usb (usb dongle), για να συνδέσουμε το laptop μας στο 4G δίκτυο κινητής τηλεφωνίας ή να αναβαθμίσουμε την ταχύτητα WiFi του υπολογιστή μας. Στα σύγχρονα PC και στα smartphones το ίδιο hardware είναι ενσωματωμένο στο ίδιο circuit board (all-in-one) και σε όλες τις περιπτώσεις που αναφέραμε ονομάζεται *Ελεγκτής Διεπαφής Δικτύου - Network Interface Controller (NIC).* Σε έναν host υπάρχουν πολλά NICs και το κάθε ένα έχει τις δικές του ρυθμίσεις σύνδεσης στο δίκτυο.

ΑΣΚΗΣΗ 1.3: Εύρεση διεύθυνσης IPv4 του συστήματος μας στο εσωτερικό ενσύρματο τοπικό δίκτυο (LAN)

Εκτελέστε την εντολή **ipconfig /all** σε γραμμή εντολών Windows ή την **ifconfig -a** σε Linux.

- Κινηθείτε με την κάθετη ράβδο κύλισης (vertical scrollbar) του παραθύρου στα αποτελέσματα που έχουν εμφανιστεί. Ανάμεσα στις επιστρεφόμενες πληροφορίες εντοπίστε αυτές που αντιστοιχούν στην ενσύρματη κάρτα δικτύου, η οποία έχει το πρόθεμα “Ethernet adapter” πριν την ονομασία της.
- Επικεντρωθείτε στις πληροφορίες που σημειώνονται στην παρακάτω εικόνα:



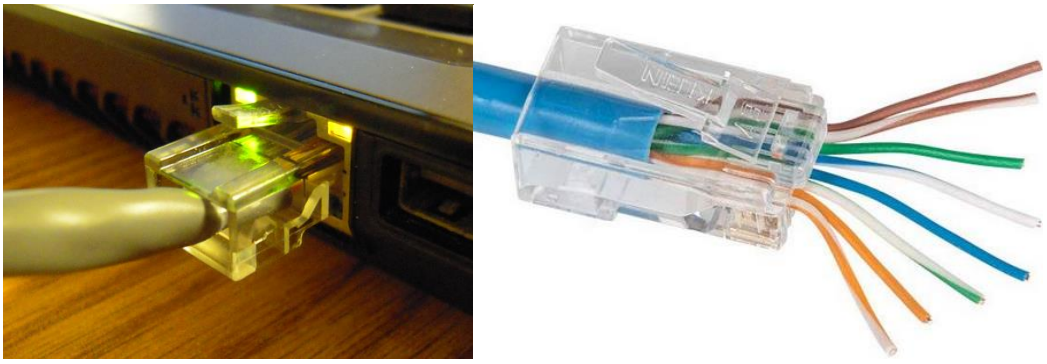
Εικόνα 1.4: Έλεγχος ρυθμίσεων δικτύου τοπικού συστήματος. Παρατηρούμε: 1. Την ονομασία του NIC για το λειτουργικό σύστημα, 2. Την ονομασία του σχετικού hardware του NIC, 3. Την διεύθυνση IPv4 του συστήματος μας που εδώ αντιστοιχεί σε τοπικό δίκτυο λόγω της μορφής 192.168.x.x και 4. Την διεύθυνση IPv4 ενός host που έχει εγκατεστημένο ένα λογισμικό εφαρμογής εξυπηρετητή (server software) το οποίο διαχειρίζεται αιτήματα DNS.

- Θυμηθείτε την IPv4 που βρήκατε στην άσκηση 1.2 και συγκρίνετε την με αυτήν που υπάρχει στις ρυθμίσεις. Μπορείτε να κάνετε την αντιστοιχία με τα αριθμημένα δωμάτια ενός ξενοδοχείου που χρησιμοποιούν οι επισκέπτες που διαμένουν και την διεύθυνση της οδού που φαίνεται εξωτερικά;
- Όπως υπάρχει μια κεντρική πύλη στο ξενοδοχείο, αντίστοιχα μπορείτε να εντοπίσετε μια ρύθμιση δικτύου που δείχνει την πιο κοντινή έξοδο προς το διαδίκτυο από το τοπικό μας δίκτυο.

1.2 Η “αόρατη” λειτουργία του διαδικτύου

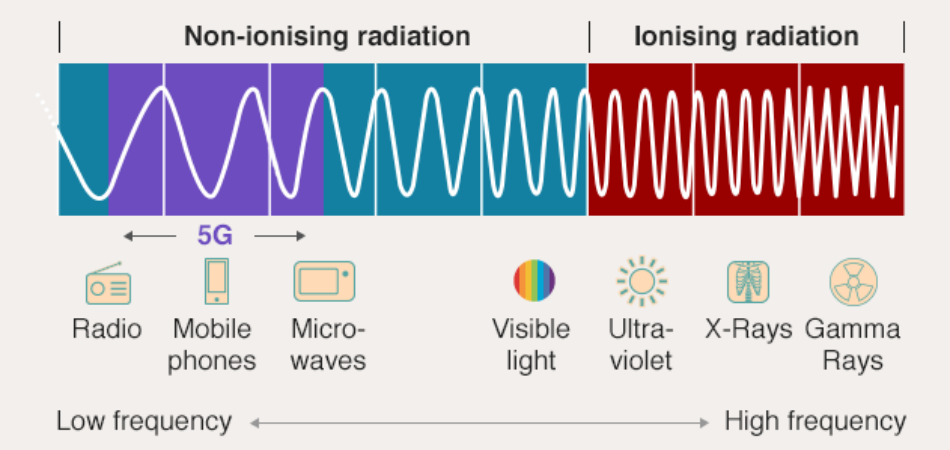
1.2.1 Η φυσική σύνδεση στο δίκτυο του εργαστηρίου

Στο πίσω μέρος του υπολογιστή που χρησιμοποιείτε υπάρχει συνδεδεμένο ένα χάλκινο (copper) καλώδιο σε μια υποδοχή του ενσύρματου NIC, το οποίο αποτελεί το *φυσικό μέσο* που μας συνδέει στο τοπικό δίκτυο - local area network (LAN). Μέσα από το καλώδιο περνάει ένας ηλεκτρομαγνητικός παλμός με ταχύτητα περίπου 200000 Km/sec. Σε περίπτωση που είχαμε *οπτική ίνα (fiber)* η ταχύτητα αγγίζει τα 300000 Km/sec. Υπάρχουν τυποποιημένες κατηγορίες καλωδίων για χρήστη σε τοπικά δίκτυα Ethernet που συμβολίζονται με **Cat {αριθμός}{σύμβολο}**, π.χ. Cat 5e.



Εικόνα 1.5: Σύνδεση χάλκινου καλωδίου (αριστερά)με βύσμα RJ-45 (δεξιά).

Στο φορητό υπολογιστή του τηλεφώνου σας δεν είναι ορατή η κεραία του ασύρματου NIC, που συνδέει την συσκευή με το ασύρματο τοπικό δίκτυο - wireless LAN (WLAN), χρησιμοποιώντας ως φυσικό μέσο τον αέρα. Η δικτύωση στο φυσικό μέσο γίνεται με συγκεκριμένο εύρος συχνοτήτων του ηλεκτρομαγνητικού φάσματος ανάλογα με το είδος δικτύου (WiFi, Bluetooth, 5G)



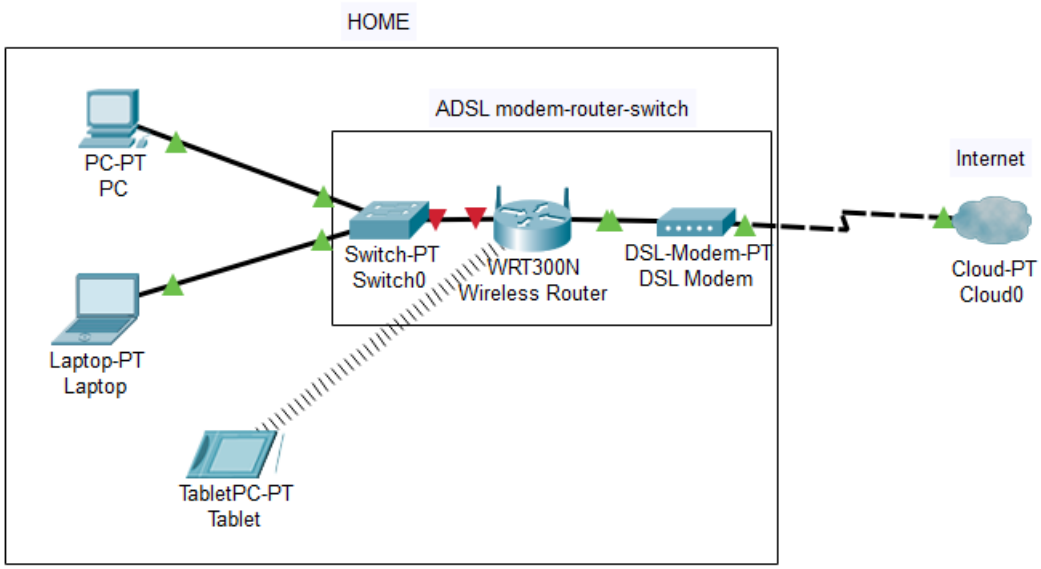
Εικόνα 1.6: Το ηλεκτρομαγνητικό φάσμα[1]. Μεγαλύτερες συχνότητες ασυρμάτων δικτύων παρέχουν μεγαλύτερες ταχύτητες. Μικρότερες συχνότητες μπορούν να αυξήσουν το εύρος του δικτύου και να διαπερνούν φυσικά εμπόδια.

[1]Προέλευση εικόνας: BBC, SCAMP/Imperial College London/EBU

1.2.2 Ο δικτυακός εξοπλισμός που συναντάμε στο περιβάλλον του σπιτιού μας

Μια συνηθισμένη διάταξη ενός οικιακού τοπικού δικτύου περιλαμβάνει ένα desktop και ένα laptop που συνδέονται καλωδιακά με μια πολυσυσκευή που εμπορικά ονομάζεται “modem-router” ή σκέτο “router”. Σε αυτόν συνδέεται ασύρματα ένα smartphone και μια Smart TV. Στην πραγματικότητα η πολυσυσκευή εσωκλείει διαφορετικά συστατικά που εμφανίζονται στην εικόνα 1.8 και ανήκουν στα παρακάτω είδη δικτυακού εξοπλισμού:

- Τα desktop και laptop συνδέονται σε ένα *switch*.
- Το smartphone, το tablet ή η smart TV συνδέονται σε ένα *wireless access point (WAP).*
- Το switch και το WAP συνδέονται με έναν *router*.
- Ο router συνδέεται με ένα *modem*.
- Το modem συνδέεται με ένα άλλο modem που έχει τοποθετήσει ο *πάροχος υπηρεσιών διαδικτύου - internet service provider (ISP).*



Εικόνα 1.8: Τυπικό οικιακό δίκτυο

Από το δικό μας modem και μετά θεωρούμε ότι “μπαίνουμε σε ένα σύννεφο” που δεν γνωρίζουμε σε ποια άκρη θα βγούμε. Με αυτήν την μεταφορά αναπαριστούμε το τμήμα του διαδικτύου που δεν είναι γνωστό και ορατό σε εμάς, και από το οποίο προκύπτει ο όρος *cloud.*

1.2.3 Ο μηχανισμός δικτύωσης που λειτουργεί στο παρασκήνιο

Από την άσκηση 1.3 είδαμε το Default Gateway (προκαθορισμένη πύλη) του τοπικού μας δικτύου. Για να φτάσει τελικά το αίτημά μας στον εξυπηρετητή που θα μας απαντήσει μπορεί να χρειάζεται να επικοινωνήσει ο δικός μας τοπικός δρομολογητής με άλλους δρομολογητές που ενώνονται μεταξύ τους και αποτελούν το δίκτυο. Κάθε φορά που ένας δρομολογητής δεν γνωρίζει να μας δώσει την απάντηση στο ερώτημά μας, θέτει το ερώτημα στον αμέσως επόμενο δρομολογητή που έχει αυτός ως gateway. Αυτό το άλμα από δρομολογητή σε δρομολογητή ονομάζεται **hop**. Με την εντολή TRACERT σε γραμμή εντολών Windows ή την TRACEROUTE σε Linux μπορούμε να δούμε αυτά τα άλματα που έχουν γίνει μέχρι τον τελικό παραλήπτη.

Υπάρχουν εργαλεία για οπτικοποιημένη ανάλυση των αλμάτων αλλά και online ανάλυση της εντολής. Σε κάθε υπολογιστή υπάρχει και η απλή ανάλυση σε μορφή κειμένου.

ΑΣΚΗΣΗ 1.4: Έλεγχος της αλληλουχίας των hops με την εντολή TRACERT

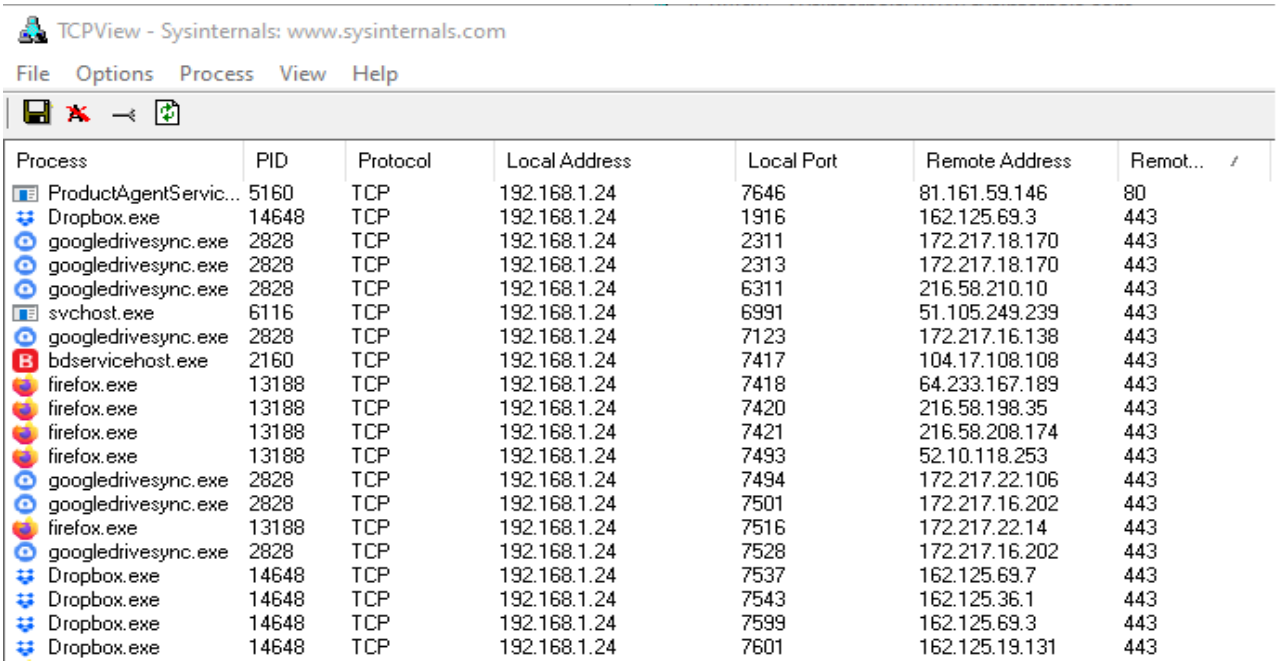
Ανοίξτε μια γραμμή εντολών του λειτουργικού συστήματος όπως είδατε στην Άσκηση 1.3 και εκτελέστε την εντολή **tracert www.iee.ihu.gr**. Περιμένετε να ολοκληρωθεί.

- Εκτελέστε **tracert www.google.com**. Συγκρίνετε τα πρώτα hop σε σχέση με αυτά που εμφανίστηκαν λίγο παραπάνω στην **tracert www.iee.ihu.gr.** Μπορείτε να εντοπίσετε σε ποιο hop φεύγουμε από τον διαδικτυακό πάροχο προς κάποιο κεντρικότερο δίκτυο;

1.2.4 Δικτυακή δραστηριότητα διεργασιών του λειτουργικού συστήματος

Σε έναν host μπορούν να δραστηριοποιούνται πολλές εφαρμογές. Η διευθυνσιοδότηση IPv4 δείχνει απλά τον host αποστολέα και τον host παραλήπτη. Χρειάζεται όμως ένα διαφορετικό σχήμα ώστε η διεργασία προέλευσης στο σύστημα Α να μεταφέρει δεδομένα στην διεργασία προορισμού στο σύστημα Β. Την μεταφορά αναλαμβάνει κυρίως το πρωτόκολλο *Transmission Control Protocol (TCP)* στο οποίο διευθυνσιοδοτούνται οι διεργασίες με την χρήση των *sockets.* Το socket είναι μια υποδοχή στο λειτουργικό σύστημα που αναγνωρίζεται με την διεύθυνση IPv4 και έναν αριθμό *θύρας (port),* μεγέθους 16bit. Η μορφή αναπαράσταση είναι {IPv4}:{Port}.

Στο παρακάτω παράδειγμα βλέπουμε ότι ο απομακρυσμένος εξυπηρετητής 172.217.18.170 αποστέλλει απαντήσεις από την θύρα του με αριθμό 443 σε δύο διαφορετικά sockets της διεργασίας googledrivesync.exe (PID:2828) στο i) 192.168.1.24:2311 και ii) 192.168.1.24:2313.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remot...
ProductAgentServic...	5160	TCP	192.168.1.24	7646	81.161.59.146	80
Dropbox.exe	14648	TCP	192.168.1.24	1916	162.125.69.3	443
googledrivesync.exe	2828	TCP	192.168.1.24	2311	172.217.18.170	443
googledrivesync.exe	2828	TCP	192.168.1.24	2313	172.217.18.170	443
googledrivesync.exe	2828	TCP	192.168.1.24	6311	216.58.210.10	443
svchost.exe	6116	TCP	192.168.1.24	6991	51.105.249.239	443
googledrivesync.exe	2828	TCP	192.168.1.24	7123	172.217.16.138	443
bdservicehost.exe	2160	TCP	192.168.1.24	7417	104.17.108.108	443
firefox.exe	13188	TCP	192.168.1.24	7418	64.233.167.189	443
firefox.exe	13188	TCP	192.168.1.24	7420	216.58.198.35	443
firefox.exe	13188	TCP	192.168.1.24	7421	216.58.208.174	443
firefox.exe	13188	TCP	192.168.1.24	7493	52.10.118.253	443
googledrivesync.exe	2828	TCP	192.168.1.24	7494	172.217.22.106	443
googledrivesync.exe	2828	TCP	192.168.1.24	7501	172.217.16.202	443
firefox.exe	13188	TCP	192.168.1.24	7516	172.217.22.14	443
googledrivesync.exe	2828	TCP	192.168.1.24	7528	172.217.16.202	443
Dropbox.exe	14648	TCP	192.168.1.24	7537	162.125.69.7	443
Dropbox.exe	14648	TCP	192.168.1.24	7543	162.125.36.1	443
Dropbox.exe	14648	TCP	192.168.1.24	7599	162.125.69.3	443
Dropbox.exe	14648	TCP	192.168.1.24	7601	162.125.19.131	443

Εικόνα 1.9: Παρακολούθηση δικτυακής δραστηριότητας διεργασιών (με TCPview). Στήλες από αριστερά το όνομα του εκτελέσιμου της διεργασίας, το αναγνωριστικό Process ID, το πρωτόκολλο μεταφοράς, η τοπική διεύθυνση ακολουθούμενη από την τοπική θύρα, η απομακρυσμένη διεύθυνση ακολουθούμενη από την απομακρυσμένη θύρα.

ΑΣΚΗΣΗ 1.5: Παρακολούθηση λειτουργίας εφαρμογών και αντιστοίχιση θυρών επικοινωνίας με πρωτόκολλα εφαρμογών

Για να παρακολουθήσουμε την δικτυακή λειτουργία των εφαρμογών στον υπολογιστή μας θα χρειαστούμε ένα εργαλείο από την συλλογή εργαλείων Windows Sysinternals. Κατεβάστε την Sysinternals Suite από το https://docs.microsoft.com/en-us/sysinternals/downloads και αποσυμπιέστε το αρχείο .zip σε κάποιον φάκελο της αρεσκείας σας.

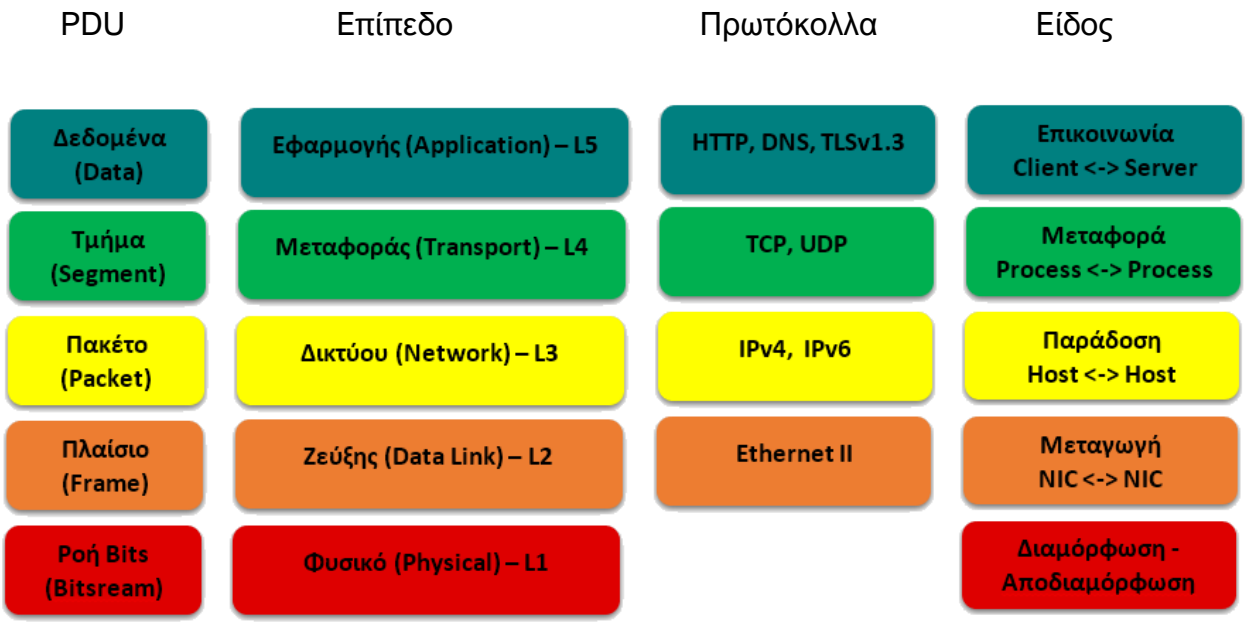
- Εκτελέστε το **tcpview.exe** μέσα από τον φάκελο.
- Ταξινομήστε με κλικ στην στήλη Remote Port. Παρατηρείτε κάποια θύρα που επαναλαμβάνεται σε διαφορετικές γραμμές των Process, ιδιαίτερα αν έχετε ανοικτό τον browser σας σε πολλές ιστοσελίδες;
- Ταξινομήστε με κλικ στην στήλη Sent Packets από τα περισσότερα προς τα λιγότερα. Βλέπετε κάποια εφαρμογή να στέλνει συνέχεια πληροφορίες από τον υπολογιστή σας; Σε ποια απομακρυσμένη διεύθυνση τις στέλνει;

1.3 Τοποθετώντας τα όλα στην στοίβα πρωτοκόλλων TCP/IP

1.3.1 Η στοίβα πρωτοκόλλων TCP/IP

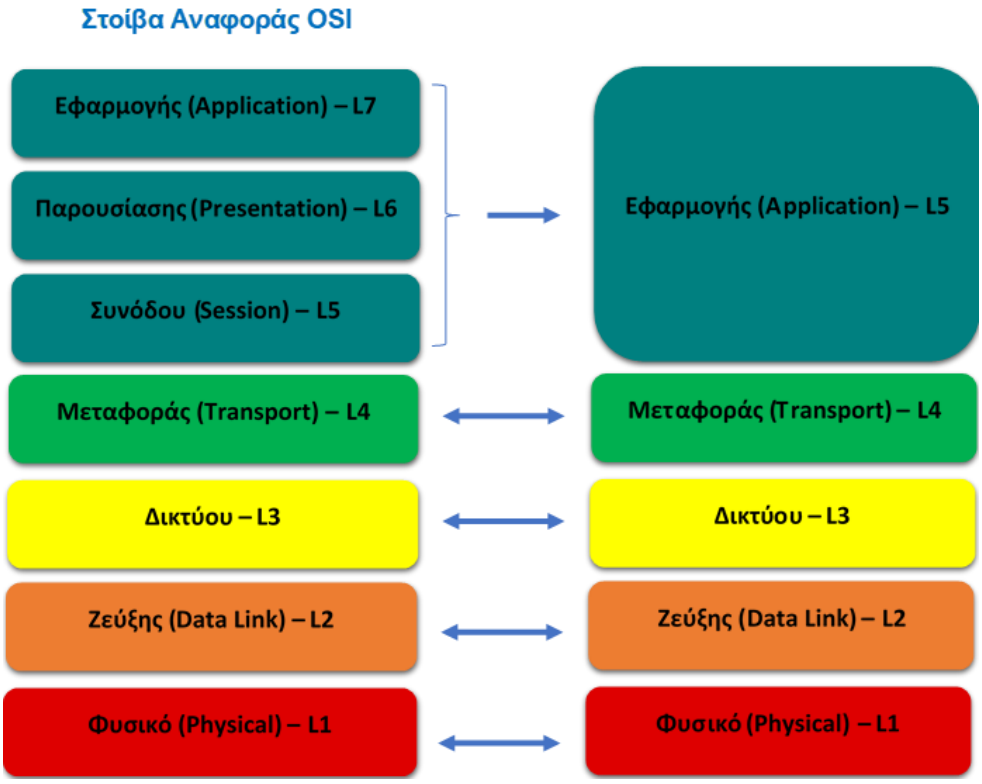
Για να μπορέσουμε να εντάξουμε και να μελετήσουμε τις δικτυακές διαδικασίες και διαφορετικές διαμορφώσεις της πληροφορίας, χρησιμοποιούμε την στοίβα πρωτοκόλλων TCP/IP που είναι μια ιεραρχία επιπέδων, που έχει στην κορυφή τον χρήστη και στην βάση το

φυσικό μέσο με το οποίο λειτουργεί το δίκτυο. Στο μοντέλο πρωτοκόλλων του TCP/IP για κάθε ένα από τα επίπεδα του, υπάρχει η μονάδα πληροφορίας η οποία ανταλλάσσεται μεταξύ των πρωτοκόλλων που θέλουν να επικοινωνήσουν. Αυτή η μονάδα πληροφορίας ονομάζεται Protocol Data Unit (PDU).



Εικόνα 1.10: TCP Protocol Stack

1.3.2 Σύγκριση στοίβας πρωτοκόλλων TCP/IP με την στοίβα αναφοράς OSI



Εικόνα 1.11: Σύγκριση στοίβας OSIμε στοίβα TCP

2. ΤΟ ΣΥΣΤΗΜΑ DNS, ΤΑ ΕΡΓΑΛΕΙΑ ΚΑΤΑΓΡΑΦΗΣ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗΣ ΔΙΚΤΥΩΝ

2.1 Η αντιστοίχιση ονομασιών με διευθύνσεις IPv4 και η λειτουργία του συστήματος DNS.

Είδαμε ότι η διευθυνσιοδότηση του δικτύου γίνεται με χρήση των διευθύνσεων IPv4 και ότι δίνοντας μια ονομασία ενός ιστότοπου, αυτή μετατρέπεται σε διεύθυνση IPv4 που χρησιμοποιείται εσωτερικά. Ο μηχανισμός που εκτελεί αυτήν την "μετάφραση", είναι το Domain Name System (DNS). Ως προς την λειτουργία του διαδικτύου, είναι από τους πιο κρίσιμους. Η μη λειτουργία αυτού του μηχανισμού θα δίνει την εντύπωση στον τελικό χρήστη ότι ένας ιστότοπος δεν λειτουργεί, ενώ αυτός θα συνέχιζε να αποκρίνεται σε έλεγχο με ping. Αυτό δείχνει ότι η υλοποίηση του DNS δεν γίνεται σε επίπεδο δικτύου (L3) αλλά πιο πάνω από κάποια εφαρμογή εξυπηρετητή που αναλαμβάνει να διαχειριστεί αιτήματα από έναν υπολογιστή στέλνοντας του απαντήσεις. Στις δικτυακές ρυθμίσεις του υπολογιστή μας υπάρχει το πεδίο DNS servers που δείχνει την διεύθυνση των hosts, στους οποίους τρέχουν διεργασίες που θα ακούσουν τα αιτήματα DNS σε συγκεκριμένα sockets.

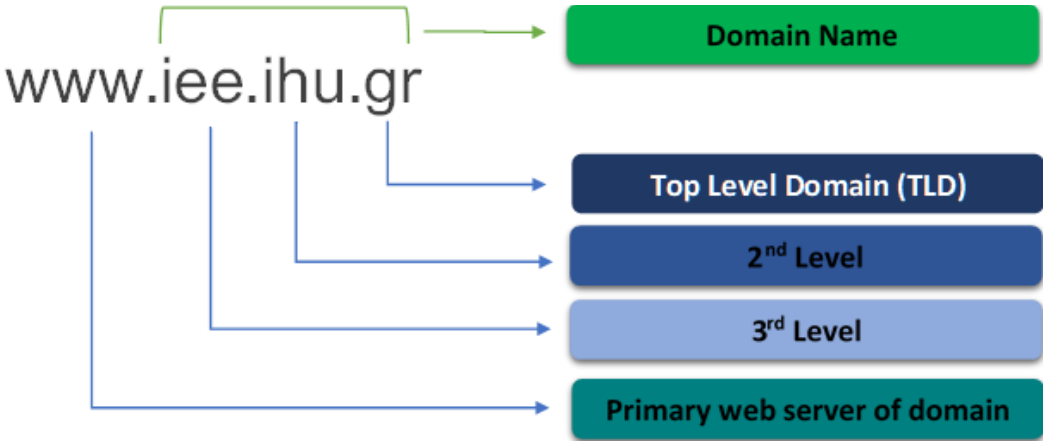
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : Speedport_W_724V_09071602_00_023B
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 30-9C-23-5F-33-84
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.24(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Πέμπτη, 15 Οκτωβρίου 2020 5:40:06 μμ
   Lease Expires . . . . . . . . . . : Πέμπτη, 5 Νοεμβρίου 2020 5:40:07 μμ
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       208.67.222.220
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Εικόνα 2.1: Ρυθμίσεις DNS. Παρατηρούμε ότι η πρώτη IPv4 address8.8.8.8 ανήκει σε αυτές του Google Public DNS και η δεύτερη 208.67.222.220 ανήκει Open DNS.

Μια τέτοια διεργασία ακούει για αιτήματα στο socket `{IPv4 Address του DNS Server}:53` και μεταφέρει την απάντηση χρησιμοποιώντας το πρωτόκολλο μεταφοράς User Datagram Protocol (UDP) το οποίο πλεονεκτεί έναντι του TCP από πλευράς ταχύτητας.

Το πρώτο από τα δεξιά τμήμα μιας ονομασίας όπως .gr, .eu, .com ονομάζεται Top-Level Domain (TLD) και υπάρχουν συγκεκριμένα TLDs για κάθε χώρα ενώ για τις ΗΠΑ υπάρχουν διαφορετικά ανά σκοπό όπως .edu για ακαδημαϊκά ιδρύματα, .gov για κυβερνητικούς οργανισμούς κ.α. Τα TLDs .com και .org που αρχικά ήταν για τις ΗΠΑ, χρησιμοποιούνται σε όλο το κόσμο από εταιρίες και μη κερδοσκοπικούς οργανισμούς αντίστοιχα.



Εικόνα 2.2: Ανάλυση τμημάτων ονομασίας τομέα (domain name)

Το δεύτερο από τα δεξιά είναι το Second-Level Domain (SLD) που σε συνδυασμό με το TLD συνήθως δίνει το κεντρικό domain name (ονομασία τομέα), ενός οργανισμού. Για το πανεπιστήμιο μας αυτό είναι το ihu.gr ενώ σε άλλες περιπτώσεις όπως στο Ηνωμένο Βασίλειο χρησιμοποιείται και τρίτο επίπεδο όπως ox.ac.uk για το πανεπιστήμιο της Οξφόδης και bbc.co.uk για τον δημοσιογραφικό οργανισμό BBC. Πάνω στο κεντρικό domain name μπορούν να υπάρξουν πολλά domains με οποιοδήποτε επίπεδο, το οποίο όμως πρακτικά χρησιμοποιείται μέχρι 3 ή 4 τμήματα. Συνήθης πρακτική είναι το πρώτο από αριστερά τμήμα να δείχνει και το είδος της υπηρεσίας που παρέχεται όπως www που δείχνει έναν εξυπηρετητή web.

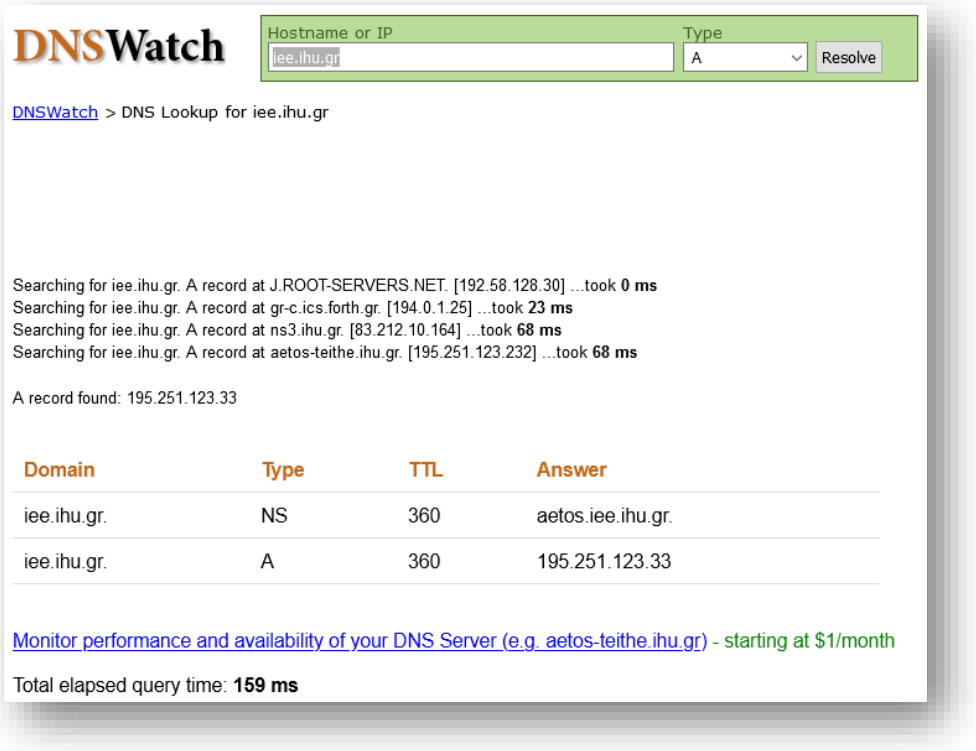
Όταν προμηθευόμαστε μια κεντρική ονομασία domain, δηλώνουμε διάφορα στοιχεία για αυτήν σε ειδικά μητρώα των διαχειριστικών αρχών, για την Ελλάδα στον hostmaster.gr του Ινστιτούτου Τεχνολογίας και Έρευνας (ΙΤΕ). Περισσότερα μπορείτε να βρείτε στο κεφάλαιο 2.4 του βιβλίου της θεωρίας.

Στην περίπτωση που ξεκινούμε μια νέα διαδικτυακή παρουσία, υπάρχουν μηχανές αναζήτησης που εμφανίζουν αν η ονομασία που επιθυμούμε για το domain μας είναι ήδη δεσμευμένη. Η αναζήτηση μπορεί να είναι διαθέσιμη στο ίδιο το μητρώο της διαχειριστικής αρχής, σε εταιρίες που διαμεσολαβούν για την δήλωση στο μητρώο μεταπωλώντας τα domain names, ή σε σελίδες όπως το https://instantdomainsearch.com/. Η επιλογή της κεντρικής ονομασίας domain είναι πολύ σημαντική για την επιτυχία της διαδικτυακής παρουσίας. Υπάρχουν εμπορικά σήματα που πρέπει να γίνουν σεβαστά αλλά και καλύτερες πρακτικές, π.χ. να μην υπάρχει τμήμα του domain που να δημιουργεί σύγχυση με υπαρκτή ονομασία ή ως αυτόνομη λέξη να δημιουργεί αρνητικές εντυπώσεις στον επισκέπτη, κ.α.

ΑΣΚΗΣΗ 2.1: Το εργαλείο dnswatch.info

- Ανοίξτε την ιστοσελίδα https://www.dnswatch.info/ και στο hostname βάλτε το domain name του τμήματος **iee.ihu.gr.**
- Επαναλάβετε για την ονομασία του εξυπηρετητή ιστού του τμήματος **www.iee.ihu.gr .** Συγκρίνετε τα αποτελέσματα. Τι παρατηρείτε;
- Επαναλάβετε και συγκρίνετε τα αποτελέσματα μεταξύ του α) κεντρικού domain του Ελληνικού κράτους **gov.gr** και του εξυπηρετητή ιστού του ίδιου domain β) κεντρικού domain της Google και του εξυπηρετητή ιστού του ίδιου domain.

Σε αυτά παρατηρούμε την αλληλουχία αναζήτησης μεταξύ των name servers, από τους κεντρικούς του διαδικτύου μέχρι αυτόν στον οποίο είναι δηλωμένο το domain. Επίσης υπάρχουν διαφορετικοί τύποι εγγραφών (type) που έρχονται στις απαντήσεις(A, NS, MX, CNAME), όπως και ο συνολικός χρόνος εκτέλεσης του ερωτήματος.



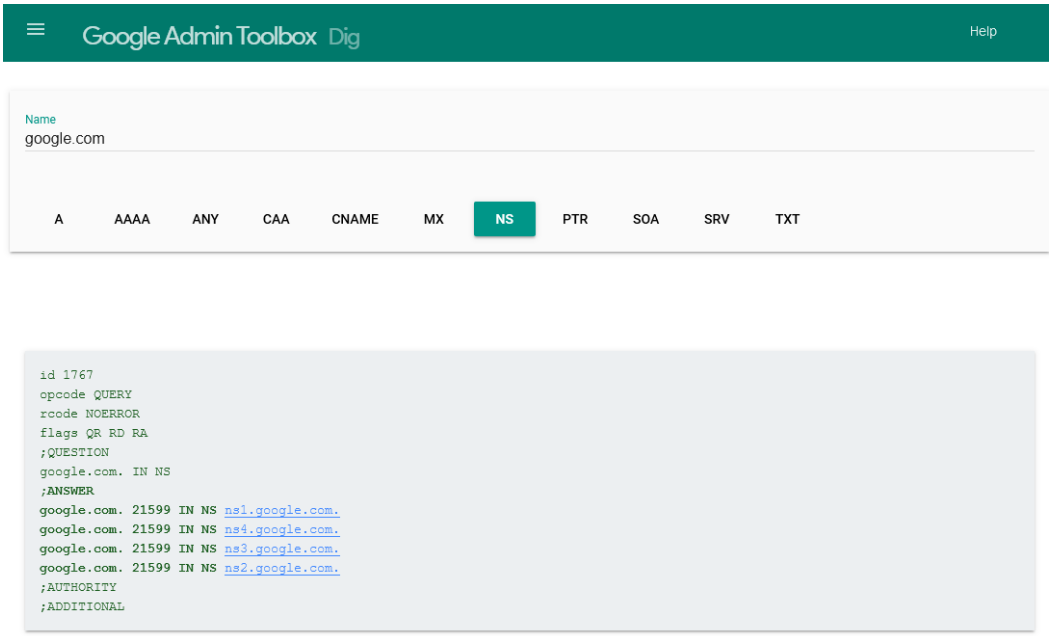
Εικόνα 2.3: Αποτελέσματα εκτέλεση ερωτήματος DNS για τον τομέα iee.ihu.gr

ΑΣΚΗΣΗ 2.2: Το εργαλείο dig για την επιστροφή των name servers που εξυπηρετούν ένα domain

Με το εργαλείο dig μπορούμε να εκτελέσουμε ερωτήματα προς το σύστημα dns. Θα χρησιμοποιήσουμε την online υλοποίηση που υπάρχει στο Google Admin Toolbox. https://toolbox.googleapps.com/apps/dig/ ή εναλλακτικά την https://www.digwebinterface.com/.

- Επιλέξτε τον τύπο εγγραφής NS, που ισοδυναμεί με την εντολή **dig ns** και γράψτε το domain **google.com**. Επιστρέφεται η ερώτηση κάτω από το `;QUESTION` και η σχετική απάντηση κάτω από το `;ANSWER` που μας δείχνει τους name servers στο οποίο είναι δηλωμένο το domain της google.

- Επαναλάβετε για α) το κεντρικό domain του πανεπιστημίου μας και β) για το κεντρικό domain του Εθνικού Μετσόβιου Πολυτεχνείου και γ) για το κεντρικό domain του πανεπιστημίου της Οξφόρδης.(Προσοχή όχι για τον εξυπηρετητή ιστού του domain)



Εικόνα 2.4: Αποτελέσματα εκτέλεσης εντολής dig ns google.com στο online εργαλείο του Google Admin Toolbox

2.2 Εισαγωγή στα εργαλεία του εργαστηρίου

Στο εργαστηριακό κομμάτι του μαθήματος για ενότητα 2 και την ενότητα 3, θα χρησιμοποιηθούν τα εξής εργαλεία:

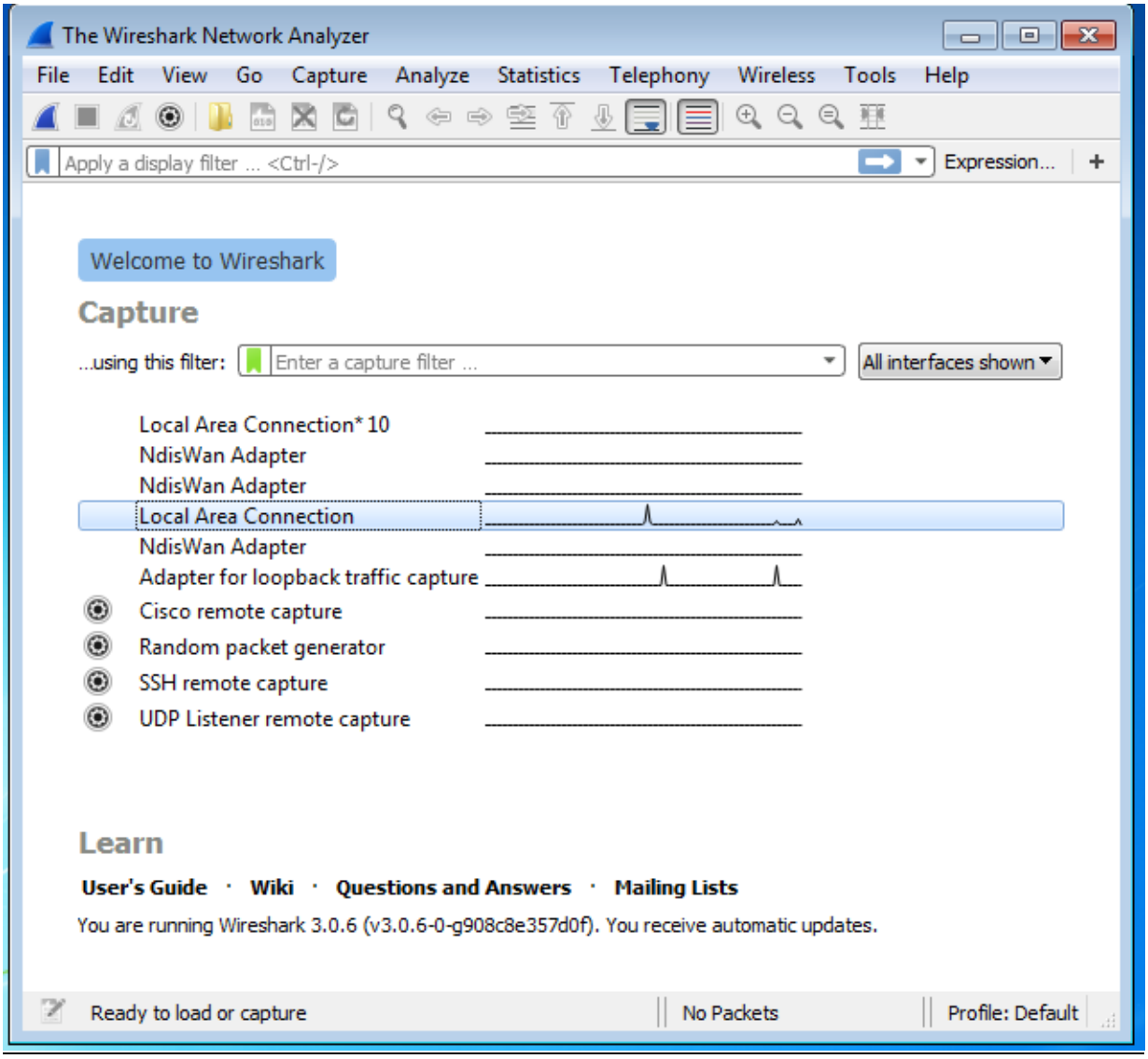
- Wireshark http://www.wireshark.org
- Cisco Packet Tracer https://www.netacad.com/courses/packet-tracer

Το **Wireshark** είναι ένα λογισμικό ανάλυσης πρωτοκόλλων δικτύου υπολογιστών. Διατίθεται από την γενική άδεια δημόσιας χρήσης GNU και είναι ελεύθερο λογισμικό ανοιχτού κώδικα. Είναι διαθέσιμο για όλα τα κύρια λειτουργικά συστήματα όπως Windows, Linux, Mac OS X, Solaris και BSD. Σε Unix περιβάλλοντα χρησιμοποιεί το GTK+ για το γραφικό περιβάλλον και το Pcap για σύλληψη πακέτων και σε Windows το WinPcap. Με την βοήθεια του Wireshark θα εστιάσουμε τελικά στην διαδικασία της ενθυλάκωσης της πληροφορίας που στέλνει ένας πομπός αλλά και στην διαδικασία της απενθυλάκωσης της στον παραλήπτη.

Το **Cisco Packet Tracer** είναι ένα λογισμικό προσομοίωσης δικτύου. Θα σας επιτρέψει να πειραματιστείτε πάνω στην λειτουργία δικτύων, εστιάζοντας στην λειτουργία του 3ου επιπέδου του μοντέλου αναφοράς του OSI. Με το Packet Tracer θα μπορείτε να δημιουργήσετε δίκτυα 1ου και 2ου επιπέδου, λογικών ομάδων, δηλαδή IP δικτύων, στατική δρομολόγηση IP πακέτων καθώς και την χρήση πρωτοκόλλων δρομολόγησης.

2.2.1 Εισαγωγή στο εργαλείο Wireshark

Στα Windows βρείτε και εκκινήστε το Wireshark από το εικονίδιο του. *Το αντίστοιχο στο λειτουργικό σύστημα Linux είναι το "wireshark network analyzer for studin".* Αρχικά εμφανίζει μια λίστα με τις διεπαφές δικτύου (network interfaces) που έχει ο υπολογιστής σας. Παρατηρήστε ότι υπάρχει κίνηση δεδομένων σε κάποιες από αυτές. Σε Windows επιλέξτε την "Local Area Connection" που αντιστοιχεί στην ενσύρματη κάρτα δικτύου και *στο Linux το "Any".*



Εικόνα 2.5: Αρχική οθόνη του Wireshark

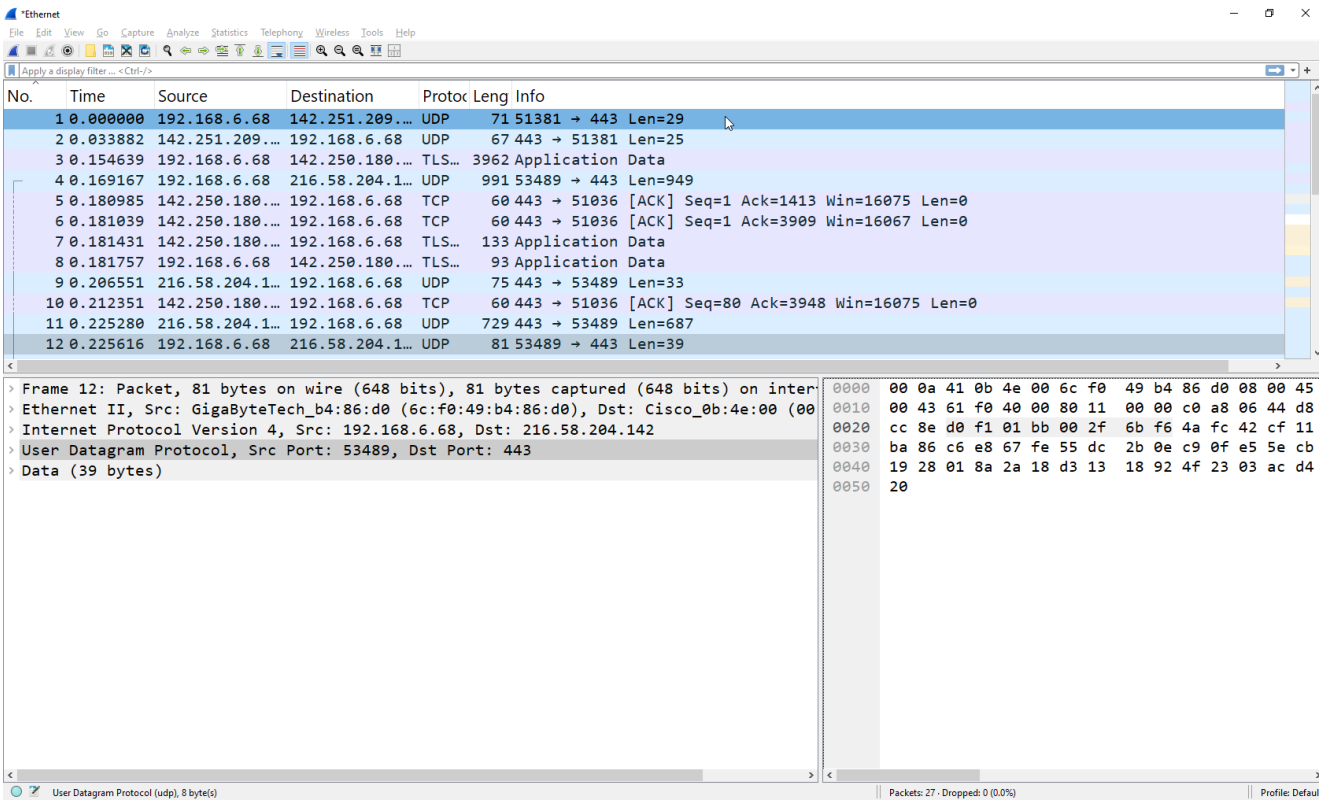
Μπορείτε να διαβάσετε τον οδηγό στο https://www.wireshark.org/docs/wsug_html_chunked/ ξεκινώντας από το Introduction. Μπορείτε να βρείτε επίσης και πολλά χρήσιμα βίντεο με οδηγίες στο διαδίκτυο.

Με την επιλογή του interface, που είναι ένα από τα διαθέσιμα NIC στο σύστημα σας, το Wireshark αρχίζει απευθείας να καταγράφει δεδομένα που διέρχονται από αυτό, προς ή από το φυσικό μέσο του δικτύου σας. Η γραφική διεπαφή χρήστη (GUI) του Wireshark είναι

χωρισμένη σε διάφορες περιοχές. Επάνω υπάρχει η γραμμή Menu (File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help) και αμέσως από κάτω η γραμμή με εικονίδια που χρησιμοποιούνται πιο συχνά (συντομεύσεις από τις επιλογές των μενού). Παρακάτω βλέπουμε τη γραμμή για τη δημιουργία φίλτρου (θα εξηγηθεί αργότερα) και κυριαρχούν στο υπόλοιπο της οθόνης τρία panels:

1. Στο επάνω panel, το πρώτο μέρος δηλαδή, είναι η λίστα όλων των μηνυμάτων όλων των πρωτοκόλλων που κατεγράφησαν.
2. Αν επιλέξετε κάτι από το πρώτο μέρος τότε στο δεύτερο panel (κάτω αριστερά) φαίνεται η ενθυλάκωση των πρωτοκόλλων καθώς και η ανάλυση τους, αν πατήσετε το > .
3. Στο τρίτο panel (κάτω δεξιά) φαίνεται σε δεκαεξαδικούς αριθμούς μια ροή bits (bitstream) που αντιστοιχεί στο **PDU** (εξηγείται αμέσως παρακάτω) που έχετε επιλέξει από την λίστα που εμφανίζεται στο δεύτερο panel.

Στο μοντέλο πρωτοκόλλων του TCP/IP (όπως είδαμε στο 1ο εργαστήριο) για κάθε ένα από τα επίπεδα του, υπάρχει η μονάδα πληροφορίας η οποία ανταλλάσσεται μεταξύ των πρωτοκόλλων που θέλουν να επικοινωνήσουν. Αυτή η μονάδα πληροφορίας ονομάζεται **Protocol Data Unit (PDU)**. Στο L5 (**Application**) η μονάδα ονομάζεται **Data**. Στο L4 (**Transport**) η μονάδα ονομάζεται **Segment**. Στο L3 (**Network**) η μονάδα ονομάζεται **Packet**. Στο L2 (**Data Link**) η μονάδα ονομάζεται **Frame** και στο L1 (**Physical**) η μονάδα είναι το **Bit**. Υπενθυμίζεται ότι ανάλογα με την βιβλιογραφία το μοντέλο πρωτοκόλλων του TCP/IP μπορεί να εμφανίζεται με 4 ή 5 επίπεδα. Στην εκδοχή των τεσσάρων επιπέδων τα ονόματα είναι Application, Transport, Internet, Network Access. Το βιβλίο σας έχει την εκδοχή των πέντε επιπέδων με τα αντίστοιχα ονόματα. Για παράδειγμα, το πρωτόκολλο IP είναι ένα πρωτόκολλο επιπέδου δικτύου. Το PDU του ονομάζεται IP Packet και εναλλακτικά μπορεί να το δείτε ως IP Datagram.



Εικόνα 2.6: Η γραφική διεπαφή χρήστη (GUI) της καταγραφής στο Wireshark.

Στο πρώτο panel βλέπουμε τις στήλες **No**. (έχει κάποια βελάκια) **Time** (χρόνος συνήθως σε δευτερόλεπτα) **Source** (η διεύθυνση αποστολέα 2ου ή 3ου επιπέδου) **Destination** (η διεύθυνση παραλήπτη 2ου ή 3ου επιπέδου) **Protocol** (ποιο πρωτόκολλο επικοινωνίας χρησιμοποιήθηκε) **Length** (το μέγεθος που καταγράφηκε συνήθως σε bytes) **Info** (παρέχει σημαντικές πληροφορίες για αυτό που καταγράφηκε).

Στο δεύτερο panel (κάτω αριστερά) μπορούμε να έχουμε μεταβλητό αριθμό εγγραφών και αυτό εξαρτάται από το πρωτόκολλο επικοινωνίας που χρησιμοποιήθηκε. Όσο πιο κοντά είναι στο επίπεδο εφαρμογής τόσο περισσότερες εγγραφές θα υπάρχουν.

Στο τρίτο panel (κάτω δεξιά) βλέπουμε τα δεδομένα που έχουν καταγραφεί σε δεκαεξαδική μορφή και σε ASCII 7-bit.

2.2.2 Δημιουργία καταγραφής PDUs με το Wireshark

Για να κατανοήσετε την λειτουργία του εκτελέστε τα παρακάτω βήματα αν έχετε την οθόνη σας ίδια με την εικόνα 2.5 :

- Στην περιοχή του φίλτρου γράψτε icmp (για να ελέγξουμε και πάλι αυτά που είδαμε στο προηγούμενο εργαστήριο) και πατήστε το πρώτο εικονίδιο της έναρξης καταγραφής (αυτό με το μπλε πτερύγιο).
- Ανοίξτε ένα παράθυρο με Command Prompt και κάντε **`ping www.google.com`**

- Μόλις τελειώσει η εμφάνιση της εντολής με τα περιεχόμενά της, πατήστε το δεύτερο εικονίδιο (αυτό με το κόκκινο τετράγωνο) για να σταματήσετε την καταγραφή.

Παρατηρούμε ότι έχουν καταγραφεί σε 8 γραμμές στο πρώτο panel η επικοινωνία που μόλις ολοκληρώθηκε. Στη στήλη Info βλέπουμε ποιο είναι request και ποιο reply (και ποια χρονική στιγμή έχει γίνει το reply ή το request). Στις στήλες Source βλέπουμε την IPv4 διεύθυνση αυτού που στέλνει το request και στη Destination την IPv4 διεύθυνση αυτού που το παραλαμβάνει. Ομοίως και αντίστροφα γίνεται στα reply.

Επιλέγοντας κάποια από τις 8 γραμμές μπορούμε να δούμε με λεπτομέρεια το περιεχόμενο στο δεύτερο panel. Συγκεκριμένα, με επιλεγμένη την πρώτη γραμμή, βλέπουμε το Frame X (όπου X ο αριθμός της χρονικής αλληλουχίας) και το πλήθος των bytes που έχουν καταγραφεί (αποτελεί την περίληψη όσων έχουν καταγραφεί -συνήθως δεν το αναλύουμε). Από κάτω υπάρχει το Ethernet II μαζί με τις φυσικές διευθύνσεις των NIC του αποστολέα και του παραλήπτη. Στην 3η γραμμή βλέπουμε το Internet Protocol Version 4 μαζί με τις IPv4 διευθύνσεις του αποστολέα και του παραλήπτη. Πατώντας στο {>} επεκτείνει προς τα κάτω περισσότερες πληροφορίες σχετικά με το συγκεκριμένο πρωτόκολλο. Στην τελευταία γραμμή βρίσκουμε το Internet Control Message Protocol που περιλαμβάνει τα δεδομένα του συγκεκριμένου πρωτοκόλλου.

ΑΣΚΗΣΗ 2.3: Καταγραφή και ανάλυση της εντολής ping προς μια απομακρυσμένη διαδικτυακή τοποθεσία

- Εκτελέστε τα βήματα της καταγραφής για την εντολή **ping** αντικαθιστώντας την διαδικτυακή τοποθεσία με μια της αρεσκείας σας.
- Τι παρατηρείτε ως προς το πλήθος των γραμμών; Ποια δεδομένα παραμένουν ίδια με το παράδειγμα που εκτελέσαμε; Δοκιμάστε ξανά οποιαδήποτε ονομασία τομέα θέλετε με την εντολή ping. Παρατηρήστε ότι σε κάθε σωστά ολοκληρωμένη εντολή ping οι γραμμές των requests έχουν πάντα την διεύθυνση του Η/Υ σας στις αποστολές και διαφορετικές διευθύνσεις στη στήλη του παραλήπτη.
- Δοκιμάστε να πληκτρολογήσετε μια λανθασμένη διεύθυνση στην εντολή **ping** (όπως όταν πληκτρολογείτε εσφαλμένα ένα site). Τι καταγράφηκε;

ΑΣΚΗΣΗ 2.4: Καταγραφή και ανάλυση της εντολής tracert

- Εκτελέστε τα βήματα της καταγραφής για την εντολή **tracert** *(όπως την είδαμε στο προηγούμενο εργαστήριο με κείμενο)* αντικαθιστώντας την διαδικτυακή τοποθεσία με μια της αρεσκείας σας. Τι παρατηρείτε ως προς το πλήθος των γραμμών; Τι κοινό έχει με την εκτέλεση της προηγούμενης άσκησης;
- Μπορείτε να βρείτε τη φυσική διεύθυνση του παραλήπτη που υπάρχει στο 7ο hop της εντολής; Ποιά βήματα πρέπει να κάνετε και σε ποια panel;