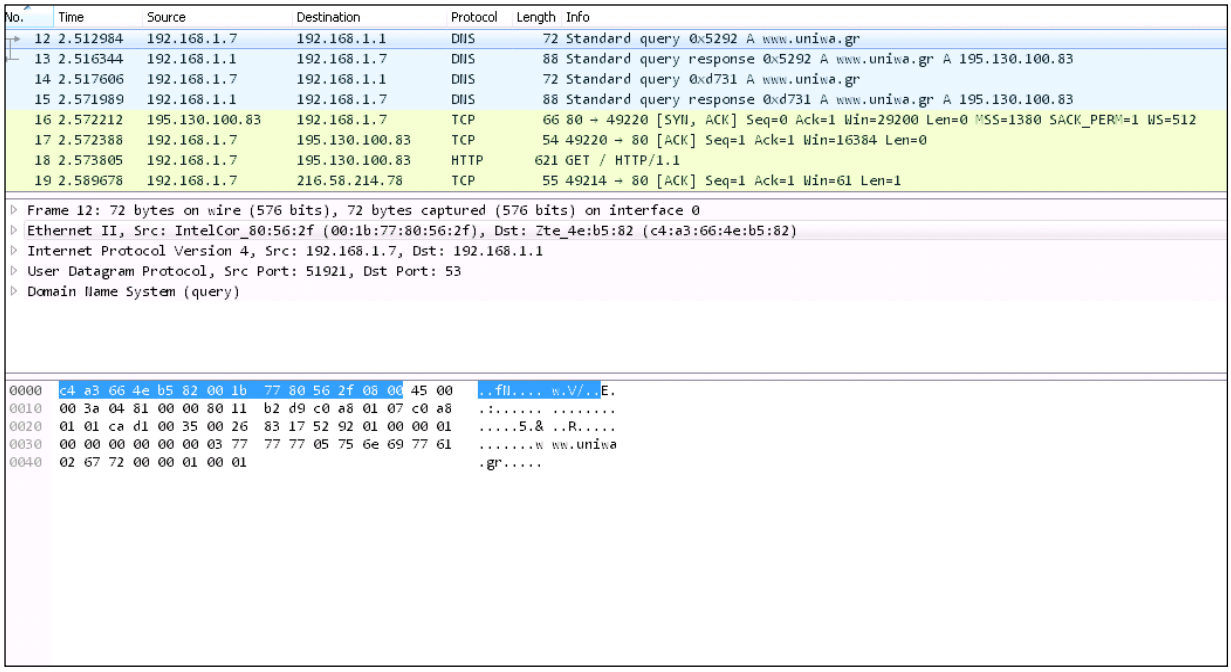
Άσκηση2 για το σπίτι (εξέταση) – ΟΛΟΙ ΟΙ ΦΟΙΤΗΤΕΣ
Χρήση Wireshark – Ανίχνευση εντολών – Πρωτόκολλα – Ενθυλάκωση

Αφού γίνει εκκίνηση του Wireshark, να ρυθμιστεί ώστε να καταγράφει μόνο την κίνηση του PC σας (ή laptop), να καθαριστούν τα παράθυρα και να τεθεί σε αναμονή καταγραφής κίνησης.

Μετά μέσω του browser αναζητείστε μία απλή ιστοσελίδα, π.χ http://www.uniwa.gr
(όχι ασφαλή ιστοσελίδα μέσω https). Μόλις εμφανιστεί η ιστοσελίδα σταματήστε την καταγραφή της κίνησης.



Παράδειγμα: Καταγραφή αναζήτησης ιστοσελίδας http://www.uniwa.gr (Wireshark V2.4.5)

Να απαντηθούν τα ακόλουθα ερωτήματα:

Ερώτημα Α:

Με βάση τη κίνηση που κατέγραψε το wireshark να απαντήσετε στα ακόλουθα:

1. Ποια είναι η IP διεύθυνση του PC σας και ποιά είναι η IP του DNS server που σας εξυπηρέτησε;
2. Ποιό είναι το όνομα (domain name) που χρησιμοποιήθηκε για την ιστοσελίδα και ποιά είναι η IP διεύθυνση που αντιστοιχεί σε αυτό; Αιτιολογήστε ποιο πρωτόκολλο εφαρμογής (application layer) χρησιμοποιήθηκε για την αντιστοιχία αυτή και σε ποιο πακέτο έγινε γνωστή η IP διεύθυνση του web server στο PC σας (ο αριθμός πακέτου είναι στο πάνω παράθυρο η 1η στήλη: No).
3. Ποιά είναι η φυσική διεύθυνση (MAC) του υπολογιστή σας και ποιός είναι ο κατασκευαστής της κάρτας Ethernet του Η/Υ σας; (αιτιολογήστε στην απάντησή σας)
4. Σε ποιό πακέτο από τα αναγραφόμενα γίνεται η **πρώτη** ερώτηση του υπολογιστή σας προς τον DNS server για την εύρεση της IP διεύθυνσης που χρειάζεστε και σε ποιό πακέτο λαμβάνει η κάρτα του δικτύου σας την απάντηση;

Ερώτημα Β:

Επιλέξτε στο πάνω παράθυρο το πακέτο του πρώτου αιτήματος που έκανε το PC σας στον DNS server:

1. Ποιό πρωτόκολλο επιπέδου μεταφοράς (transport layer) χρησιμοποιήθηκε για την εντολή "αίτημα DNS"; (αιτιολογήστε την απάντησή σας).
2. Να εξηγηθεί η ενθυλάκωση των δεδομένων που έγινε στην εντολή αυτή, να παρασταθούν σχηματικά οι πρόσθετες πληροφορίες (headers) που προστίθενται με την ενθυλάκωση μπροστά από τα δεδομένα της εντολής "αίτημα DNS" και να ευρεθεί το μήκος κάθε επικεφαλίδας (header) που προστίθενται από το επίπεδο εφαρμογής μέχρι και το επίπεδο Ethernet.

   Προσοχή: στο μεσαίο παράθυρο τα επίπεδα του TCP/IP αναγράφονται ανάποδα από κάτω προς τα πάνω (bottom-up) ενώ η ενθυλάκωση γίνεται από τα ψηλότερα επίπεδα του TCP/IP προς τα κάτω.

Ερώτημα Γ:

Επιλέξτε στο πάνω παράθυρο το πακέτο του πρώτου αιτήματος (GET) που έκανε το PC σας στον web server για την απόκτηση της ιστοσελίδας (μετά την εγκαθίδρυση της σύνδεσης TCP μεταξύ του PC σας και του web server).

1. Ποιό πρωτόκολλο εφαρμογής (application layer) χρησιμοποιήθηκε για την πρώτη εντολή "αίτημα ιστοσελίδας" του PC σας στον web server; (εντολή: GET / HTTP/1.1)
2. Να εξηγηθεί η ενθυλάκωση των δεδομένων που έγινε στην εντολή αυτή, να παρασταθούν σχηματικά οι πρόσθετες πληροφορίες (headers) που προστίθενται με την ενθυλάκωση μπροστά από τα δεδομένα της εντολής "αίτημα ιστοσελίδας" και να ευρεθεί το μήκος κάθε επικεφαλίδας (header) που προστίθενται από το επίπεδο εφαρμογής μέχρι και το επίπεδο Ethernet.
3. Ποιό πρωτόκολλο επιπέδου μεταφοράς (transport layer) χρησιμοποιήθηκε για το αίτημα εμφάνισης της ιστοσελίδας από τον browser του PC σας.
4. Από όλα τα πακέτα που κατέγραψε το Wireshark από την έναρξη μέχρι την απόκτηση της ιστοσελίδας να συγκεντρωθεί η κίνηση TCP (Analyse → Follow → TCP stream) και να εξηγηθούν τα κυριότερα πεδία των επικεφαλίδων (headers) του πρώτου αιτήματος http και της απάντησης από τον web server.

ΠΑΡΑΤΗΡΗΣΕΙΣ:

1) Κάθε φοιτητής θα καταγράψει μια διαφορετική απλή ιστοσελίδα http (**ΟΧΙ https και ΟΧΙ την ιστοσελίδα του παραδείγματος: http://www.uniwa.gr).**
2) Η αποτύπωση (snapshot) της ιστοσελίδας θα παραδοθεί μαζί με τις απαντήσεις.