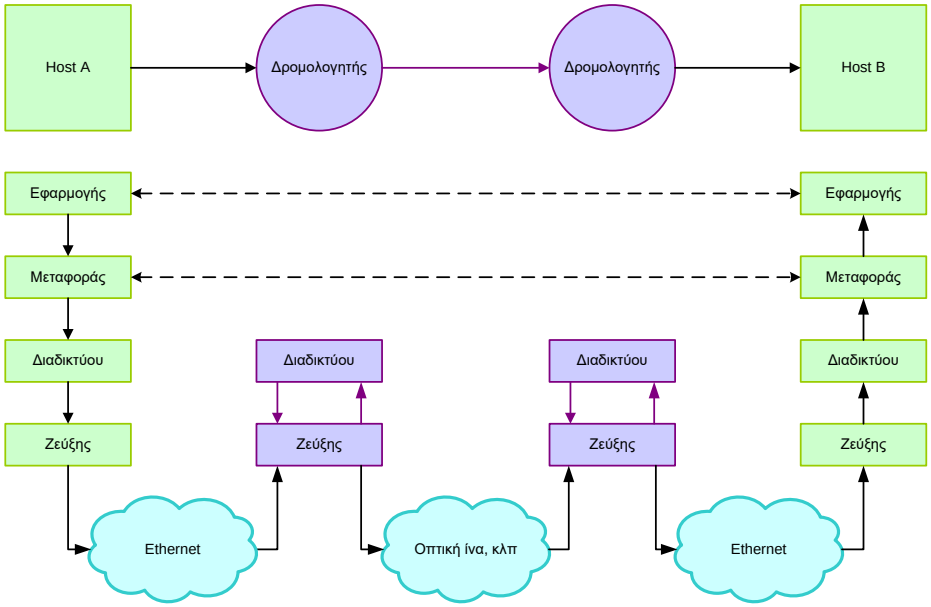
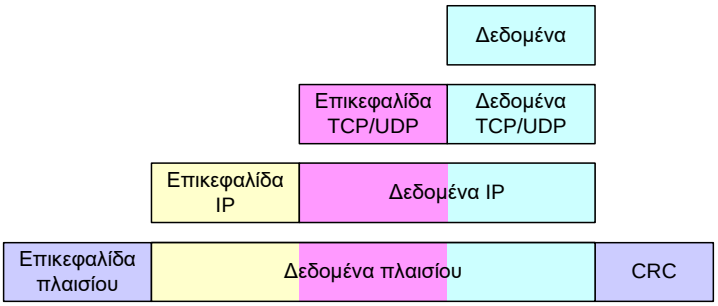
Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Όπως γνωρίζετε και από προηγούμενα μαθήματα, για να μειωθεί η πολυπλοκότητα σχεδίασης και να βελτιωθεί η συμβατότητα μεταξύ κατασκευαστών, τα περισσότερα πρωτόκολλα δικτύων οργανώνονται σε στρώματα (layers), το καθένα από τα οποία κτίζεται πάνω στο κατώτερό του. Ο αριθμός των στρωμάτων, τα περιεχόμενά τους και η λειτουργία τους διαφέρουν από δίκτυο σε δίκτυο, αλλά σε όλα τα δίκτυα ο σκοπός του κάθε στρώματος είναι να προσφέρει συγκεκριμένες υπηρεσίες στα ανώτερα στρώματα, απομονώνοντάς τα έτσι από τις λεπτομέρειες υλοποίησης των προσφερομένων υπηρεσιών. Το στρώμα *n* μιας μηχανής διεξάγει συζήτηση με το στρώμα *n* μιας άλλης μηχανής, είτε άμεσα, είτε έμμεσα (μέσω τρίτων). Άμεσο αποτέλεσμα της δόμησης των πρωτοκόλλων σε στρώματα είναι η ενθυλάκωση (*encapsulation*), η τοποθέτηση δηλαδή της μονάδας πληροφορίας πρωτοκόλλου (Protocol Data Unit – PDU) κάθε στρώματος εντός του τμήματος δεδομένων του επόμενου προς τα κάτω στρώματος.

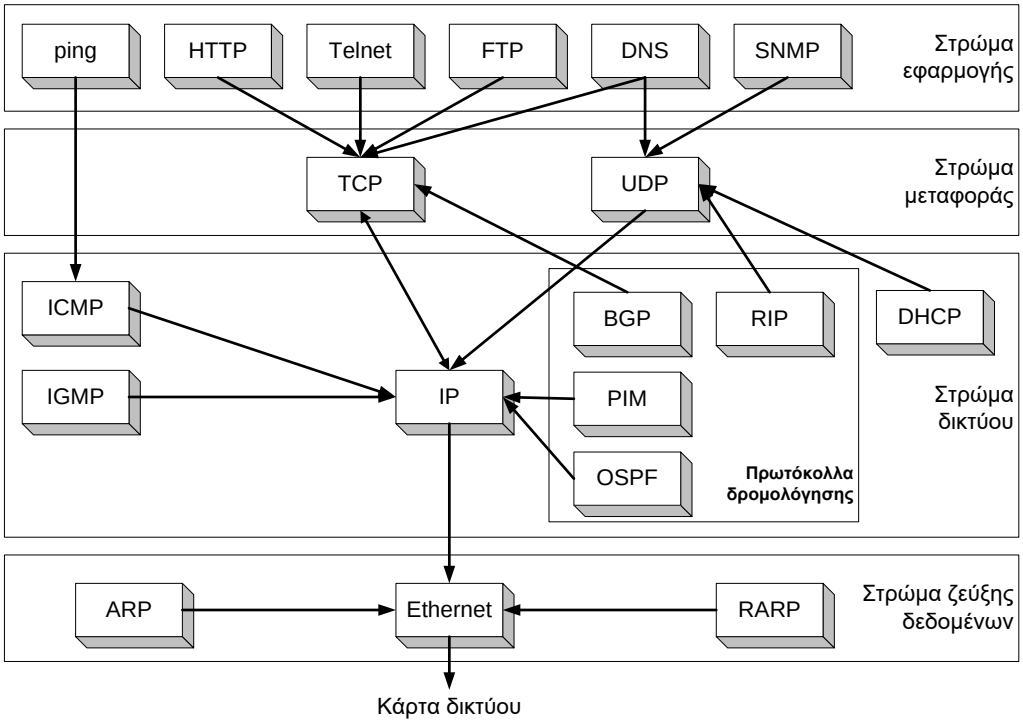
Το μοντέλο OSI βασίζεται σε μια πρόταση που ανέπτυξε ο διεθνής οργανισμός προτύπων ISO (International Standards Organization), ως ένα πρώτο βήμα προς την κατεύθυνση της διεθνούς προτυποποίησης των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα στρώματα. Το μοντέλο αποκαλείται μοντέλο αναφοράς OSI (Open Systems Interconnection) του ISO, επειδή αφορά ανοιχτά συστήματα, δηλαδή, συστήματα που είναι ανοιχτά στην επικοινωνία με άλλα συστήματα. Στο Internet όμως χρησιμοποιείται ένα άλλο μοντέλο αναφοράς, γνωστό ως στοίβα πρωτοκόλλων TCP/IP (TCP/IP protocol stack), που περιλαμβάνει τέσσερα στρώματα: το στρώμα ζεύξης (link) δεδομένων, το στρώμα διαδικτύου (internet), το στρώμα μεταφοράς (transport) και το στρώμα εφαρμογής (application). Τα ακραία συστήματα (hosts) περιλαμβάνουν και τα τέσσερα στρώματα, ενώ οι ενδιάμεσοι κόμβοι (δρομολογητές) υλοποιούν μόνο τα δύο κατώτερα στρώματα. Η IETF (Internet Engineering Task Force) είναι η αρμόδια ομάδα εργασίας για την προτυποποίηση των πρωτοκόλλων του Internet. Η προτυποποίηση σε σχέση με τη σουίτα πρωτοκόλλων TCP/IP αφορά μόνο τα ανώτερα τρία στρώματα της αρχιτεκτονικής. Το στρώμα ζεύξης μπορεί να είναι οποιοδήποτε τηλεπικοινωνιακό σύστημα.



Η θέση ενός πρωτοκόλλου στην ιεραρχία της σουίτας TCP/IP ορίζεται μέσω της ενθυλάκωσης (δείτε σχήμα στην επόμενη σελίδα). Π.χ. τα δεδομένα ενός πρωτοκόλλου που τοποθετείται στο στρώμα δικτύου ενθυλακώνονται σε πλαίσια του στρώματος ζεύξης δεδομένων. Περισσότερα για τη θέση των πρωτοκόλλων του Internet στην ιεραρχία αυτή (στοίβα πρωτοκόλλων TCP/IP) μπορείτε να βρείτε στην ιστοσελίδα http://www.networksorcery.com/enp/default.htm επιλέγοντας από το menu στα αριστερά τον υπερσύνδεσμο "*IP protocol suite*".



Παρατηρήστε όμως ότι, από λειτουργικής πλευράς, η αντιστοιχία των πρωτοκόλλων TCP/IP σε στρώματα κατά OSI δεν είναι προφανής και άμεση. Αυτό συμβαίνει διότι το TCP/IP προηγήθηκε χρονικά του μοντέλου OSI. Για παράδειγμα, η λειτουργία του πρωτοκόλλου ARP, αυτή της ανεύρεσης διευθύνσεων Ethernet που αντιστοιχούν σε διευθύνσεις IPv4, δεν αφορά στη μετάδοση πακέτων από το ένα άκρο του δικτύου στο άλλο και για αυτό, κατά OSI, βρίσκεται στο στρώμα ζεύξης δεδομένων, ενώ αντίθετα θεωρείται πρωτόκολλο του στρώματος δικτύου στο Internet, επειδή τα δεδομένα του ARP ενθυλακώνονται απ' ευθείας σε πλαίσια Ethernet. Στο επόμενο σχήμα, για λόγους πληρότητας, παρουσιάζεται η αντιστοίχηση μερικών βασικών πρωτοκόλλων του Internet στα στρώματα του μοντέλου αναφοράς OSI.



Στο υπόλοιπο του κειμένου θα θεωρούμε την ιεραρχία πρωτοκόλλων σύμφωνα με τη σουίτα TCP/IP. Για διάκριση των μονάδων πληροφορίας ανά στρώμα της ιεραρχίας αυτής, στη συνέχεια, θα αποκαλούμε ***πλαίσιο*** τη μονάδα δεδομένων πρωτοκόλλου του στρώματος ζεύξης δεδομένων, ***πακέτο*** τη μονάδα δεδομένων πρωτοκόλλου του στρώματος δικτύου, ***τεμάχιο TCP*** ή ***δεδομενόγραμμα UDP*** (TCP segment ή UDP datagram) τη μονάδα δεδομένων πρωτοκόλλου του στρώματος μεταφοράς, ανά περίσταση (πρωτόκολλο TCP ή UDP), και ***μήνυμα*** τη μονάδα δεδομένων πρωτοκόλλου του στρώματος εφαρμογής.

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η μελέτη της ενθυλάκωσης της πληροφορίας ανάμεσα στα στρώματα πρωτοκόλλων της σουίτας TCP/IP. Όπως και στις προηγούμενες ασκήσεις θα εργαστείτε με το πρόγραμμα Wireshark. Τα πλαίσια που καταγράφονται από το Wireshark

εμφανίζονται έγχρωμα[1] στο παράθυρο με τη λίστα πακέτων στο επάνω μέρος της οθόνης. Κάθε γραμμή αντιστοιχεί σε ένα πλαίσιο που συλλαμβάνεται και στο πεδίο με τίτλο Protocol εμφανίζεται το ανώτατης τάξης ενθυλακωμένο πρωτόκολλο που αποκωδικοποιεί το Wireshark. Η επιλογή ενός οποιουδήποτε από τα πλαίσια που καταγράφηκαν γίνεται κάνοντας κλικ στην αντίστοιχη γραμμή της λίστας. Για το επιλεγμένο πλαίσιο εμφανίζονται όλα τα ενθυλακωμένα πρωτόκολλα στο παράθυρο με τις λεπτομέρειες (μεσαίο τμήμα της οθόνης) καθώς και το σύνολο των δεδομένων του σε δεκαεξαδική και ASCII μορφή στο παράθυρο με τα περιεχόμενα (κάτω τμήμα της οθόνης). Συνεπώς, δεδομένης της δομής ενός πακέτου IP για παράδειγμα, μπορεί να αναλυθεί το τεμάχιο (segment) TCP που εμπεριέχεται μέσα στο IP. Ομοίως, η δομή του τεμαχίου TCP επιτρέπει την αποκωδικοποίηση του μηνύματος HTTP, ενώ περαιτέρω ανάλυση οδηγεί στο συγκεκριμένο τύπο του μηνύματος HTTP, δηλαδή, GET, POST κ.ά.

Για κάθε ενθυλακωμένο πρωτόκολλο, τα βασικά πεδία της επικεφαλίδας του εμφανίζονται στο παράθυρο με τις λεπτομέρειες. Μπορείτε να δείτε όλες τις επικεφαλίδες και το περιεχόμενο τους με διπλό κλικ στην αντίστοιχη γραμμή ή κάνοντας κλικ στο σύμβολο '>' στα αριστερά της. Τα δεδομένα που αντιστοιχούν στις επικεφαλίδες του επιλεγμένου πρωτοκόλλου εμφανίζονται υπογραμμισμένα (highlighted) στο παράθυρο με τα περιεχόμενα (κάτω μέρος της οθόνης). Κάνοντας κλικ σε κάποια επικεφαλίδα (ή σε κάποιο πεδίο της) υπογραμμίζεται το αντίστοιχο μέρος δεδομένων στα περιεχόμενα, ενώ τα δεδομένα των άλλων επικεφαλίδων εμφανίζονται σκιασμένα. Τέλος, το μέγεθος και των τριών παραθύρων (λίστα, λεπτομέρειες αι περιεχόμενα πλαισίου) μπορεί να μεταβληθεί επιλέγοντας και σύροντας τις οριζόντιες μπάρες που τα διαχωρίζουν.

Στο σημερινό εργαστήριο θα χρησιμοποιήσετε τη λειτουργία σύλληψης *(Capture)* με φίλτρο, ώστε να καταγράφονται πλαίσια με κάποια συγκεκριμένα χαρακτηριστικά. Σημειώνεται ότι το φίλτρο απεικόνισης *(Display)* που επιλέγετε από το μενού *Analyze*, ενεργοποιείται είτε κατά τη διάρκεια της καταγραφής είτε αφού αυτή έχει ολοκληρωθεί προκειμένου να περιορίσει τον αριθμό των συλληφθέντων πλαισίων που εμφανίζονται στο παράθυρο του Wireshark. Αντίθετα το φίλτρο σύλληψης που επιλέγετε από το μενού *Capture*, ενεργοποιείται πριν ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων.

Η σύνταξη του φίλτρου σύλληψης στο Wireshark είναι διαφορετική από τη σύνταξη του φίλτρου απεικόνισης. Ο μηχανισμός σύλληψης υλοποιείται στη βιβλιοθήκη npcap σε περιβάλλον Windows ή libpcap σε περιβάλλον Linux/Unix. Τα πλαίσια που συλλαμβάνονται πρέπει να ικανοποιούν μια λογική (Boolean) έκφραση, το *φίλτρο σύλληψης*. Δείτε σχετικά παραδείγματα στην ιστοσελίδα https://www.tcpdump.org/manpages/tcpdump.1.html, το εγχειρίδιο (man page) της εντολής γραμμής tcpdump του Unix. Η πλήρης τεκμηρίωση της σύνταξης των φίλτρων υπάρχει στο εγχειρίδιο του pcap-filter https://www.tcpdump.org/manpages/pcap-filter.7.html. Μια πιο συνοπτική περιγραφή όμως μπορείτε να βρείτε στον οδηγό χρήσης (User Guide) του Wireshark (§*4.10 Filtering while capturing*), ενώ στην ιστοσελίδα https://gitlab.com/wireshark/wireshark/-/wikis/CaptureFilters θα βρείτε πολλά ενδιαφέροντα παραδείγματα.

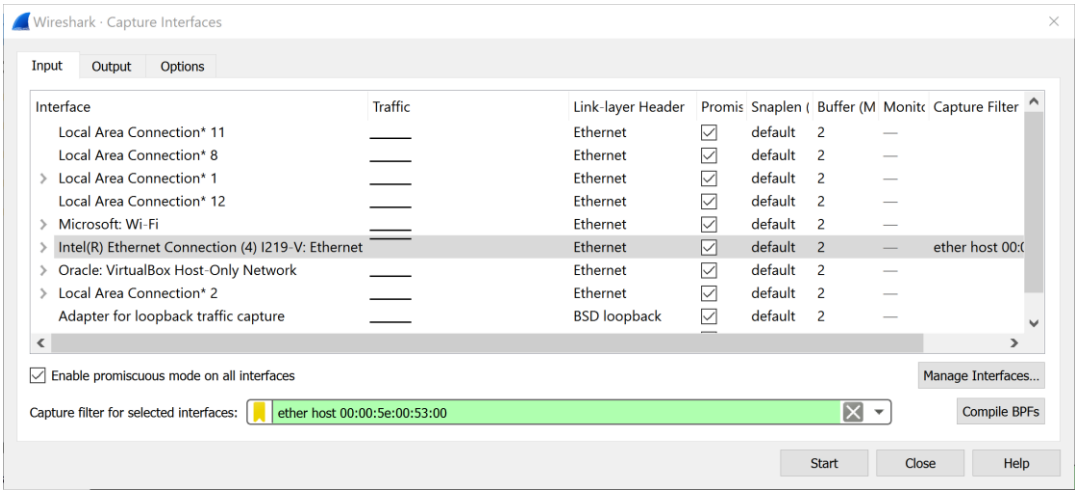
Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

1. Στρώμα ζεύξης δεδομένων

Για να καταγράφονται μόνο πλαίσια που παράγονται ή απευθύνονται στον υπολογιστή σας, εφαρμόστε ένα φίλτρο σύλληψης ως εξής: ακολουθήστε τη διαδρομή *Capture→ Options…*, κάντε κλικ στο όνομα της κάρτας δικτύου στην οποία θέλετε να ορίσετε φίλτρο σύλληψης και μετά στο

[1] Μπορείτε να δείτε τους προκαθορισμένους κανόνες χρωματισμού πακέτων του Wireshark στο *View→Coloring rules*, από όπου μπορείτε να αλλάξετε τους κανόνες, να προσθέσετε νέους και να εισάγετε νέους από αρχεία.

πράσινο σύμβολο (bookmark) πλάι από το πεδίο ορισμού φίλτρων σύλληψης. Στο παράθυρο με προκαθορισμένα φίλτρα που θα εμφανιστεί επιλέξτε τη γραμμή Ethernet address 00:00:5e:00:53:00 (το όνομα του φίλτρου). Αυτόματα θα συμπληρωθεί ένα συντακτικά σωστό φίλτρο σύλληψης για τη MAC διεύθυνση 00:00:5e:00:53:00. Στη συνέχεια διορθώστε τη διεύθυνση MAC ώστε να είναι ίδια με τη διεύθυνση MAC της κάρτας δικτύου του υπολογιστή σας. Η σύνταξη του φίλτρου είναι σωστή όταν το πεδίο έχει πράσινο χρώμα και η καταγραφή ξεκινά πατώντας Enter ή Start.



Ανοίξτε ένα παράθυρο εντολών, εκτελέστε την εντολή ping 1.1.1.1 και μόλις ολοκληρωθεί η σταματήστε την καταγραφή. Με βάση τα δεδομένα που καταγράψατε να απαντηθούν τα παρακάτω ερωτήματα, αφού πρώτα εφαρμόσετε το φίλτρο απεικόνισης *arp or ip*:

1.1 Ποια η σημασία του φίλτρου απεικόνισης που εφαρμόσατε;
1.2 Ποια είναι τα ονόματα των πεδίων της επικεφαλίδας του πλαισίου Ethernet;
1.3 Υπάρχει πεδίο για το συνολικό μήκος του πλαισίου ή των δεδομένων που μεταφέρει;
1.4 Ποιο είναι το μήκος των διευθύνσεων Ethernet σε byte;
1.5 Ποιο είναι το συνολικό μήκος της επικεφαλίδας Ethernet σε byte;
1.6 Ποιο πεδίο του πλαισίου Ethernet καθορίζει το πρωτόκολλο δικτύου;
1.7 Ποια είναι η θέση που καταλαμβάνει μέσα στην επικεφαλίδα Ethernet;
1.8 Ποια είναι η τιμή του πεδίου αυτού για πακέτα IPv4;
1.9 Εάν καταγράφηκαν, ποια είναι η τιμή του πεδίου αυτού για πακέτα ARP.

2. Στρώμα Δικτύου

Με βάση την προηγούμενη καταγραφή και με το φίλτρο απεικόνισης *icmp* ενεργοποιημένο, να απαντηθούν τα παρακάτω ερωτήματα:

2.1 Ποια η σημασία του φίλτρου απεικόνισης που εφαρμόσατε;
2.2 Ποιο είναι το μήκος των διευθύνσεων IPv4 σε byte;
2.3 Ποια είναι τα ονόματα των πρώτων δύο πεδίων της επικεφαλίδας IPv4;
2.4 Ποιο είναι το μήκος σε bit και ποια η τιμή των πεδίων αυτών; *[Υπόδειξη: Για τη δομή της επικεφαλίδας του πρωτοκόλλου IPv4 μπορείτε να συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο IP στο δεξιό της μέρος]*
2.5 Επιλέξτε ένα πακέτο IPv4. Ποιο είναι το συνολικό μήκος σε byte της επικεφαλίδας IPv4 με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα;
2.6 Πώς προκύπτει αυτό το μήκος από την τιμή του αντίστοιχου πεδίου της επικεφαλίδας IPv4;
2.7 Ποιο είναι το συνολικό μήκος σε byte αυτού του πακέτου IPv4 με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα;
2.8 Υπάρχει πεδίο σχετικό με το μήκος του πακέτου IPv4 στην επικεφαλίδα του; Συμφωνεί η τιμή του με το μήκος που βρήκατε προηγουμένως;
2.9 Ποιο είναι το μήκος δεδομένων (payload) του πακέτου IPv4 σε byte;

2.10 Πώς προκύπτει το μήκος των δεδομένων (payload) του πακέτου IPv4 από τα στοιχεία της επικεφαλίδας;
2.11 Ποιο πεδίο της επικεφαλίδας IPv4 καθορίζει το πρωτόκολλο στρώματος μεταφοράς της σουίτας TCP/IP;
2.12 Ποια είναι η θέση του (σε σχέση με την αρχή της επικεφαλίδας IPv4);
2.13 Ποια είναι η τιμή του για το πρωτόκολλο ICMP;

3. Στρώμα Μεταφοράς

Στη συνέχεια αρχίστε μια νέα καταγραφή της κίνησης με το ίδιο φίλτρο σύλληψης όπως και πριν. Εάν χρησιμοποιείτε Windows, σε ένα παράθυρο εντολών εκτελέστε την εντολή ipconfig /flushdns για να διαγραφούν οι αντιστοιχήσεις ονομάτων DNS σε διευθύνσεις IP. Σε Ubuntu εκτελέστε την εντολή sudo systemd-resolve --flush-caches. Σε συστήματα Unix/Linux, εν γένει δεν χρησιμοποιείται προσωρινή αποθήκευση για την επίλυση ονομάτων. Εάν όμως την έχετε ενεργοποιήσει, διαγράψτε με τα περιεχόμενά της επανεκκινώντας την αντίστοιχη υπηρεσία, π.χ. nscd, unbound, κλπ. Μετά επισκεφθείτε την ιστοσελίδα http://edu-dy.cn.ntua.gr/lab2/ και σταματήστε την καταγραφή των πακέτων αφού έχει ολοκληρωθεί το κατέβασμα της σελίδας. Με βάση τα δεδομένα που καταγράψατε να απαντηθούν τα παρακάτω ερωτήματα, αφού πρώτα ενεργοποιήσετε το φίλτρο απεικόνισης *tcp or udp*:

3.1 Ποια η σημασία του παραπάνω φίλτρου απεικόνισης;
3.2 Ποια πρωτοκόλλα του στρώματος μεταφοράς παρατηρείτε;
3.3 Ποια είναι η τιμή του πεδίου *Protocol* στην επικεφαλίδα IPv4 για το πρωτόκολλο TCP και ποια για το UDP; *[Υπόδειξη: Εάν τα δεδομενογράμματα UDP μεταφέρθηκαν ως πακέτα IPv6, καταγράψτε την τιμή του πεδίου Next Header.]*
3.4 Ποια είναι τα ονόματα των πεδίων της επικεφαλίδας των τεμαχίων TCP και δεδομενογραμμάτων UDP που είναι κοινά και στα δύο πρωτόκολλα;
3.5 Ποιο είναι το μήκος σε byte της επικεφαλίδας των δεδομενογραμμάτων UDP;
3.6 Υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος των δεδομενογραμμάτων UDP;
3.7 Ποιο πεδίο καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP και ποια η θέση του στην επικεφαλίδα;
3.8 Υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος τεμαχίων TCP; Εάν όχι, πώς προκύπτει αυτό; *Προσοχή, οι γραμμές εντός αγκυλών [και] στο παράθυρο με τις λεπτομέρειες δεν αντιστοιχούν σε επικεφαλίδες αλλά προκύπτουν από την ανάλυση που κάνει το Wireshark.*
3.9 Υπάρχει πεδίο στην επικεφαλίδα TCP ή UDP που να προσδιορίζει τον τύπο του πρωτοκόλλου εφαρμογής; Αιτιολογήστε την απάντησή σας. *[Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm επιλέγοντας το "TCP/UDP ports" από το αριστερό της μέρος.]*
3.10 Αναφέρετε άλλα πρωτόκολλα στρώματος εφαρμογής που τυχόν παρατηρήσατε.

4. Στρώμα Εφαρμογής

Με βάση την τελευταία καταγραφή και τώρα με φίλτρο απεικόνισης *http or dns* ενεργοποιημένο, να απαντηθούν τα παρακάτω ερωτήματα:

4.1 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το DNS;
4.2 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το HTTP;
4.3 Ποιο bit της σημαίας (flag) στην επικεφαλίδα DNS καθορίζει το κατά πόσον πρόκειται για ερώτηση ή απάντηση και ποια η αντίστοιχη τιμή; *[Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm για τη δομή της επικεφαλίδας του πρωτοκόλλου DNS επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο DNS στο δεξιό της μέρος.]*
4.4 Καταγράψτε τη θύρα προορισμού των ερωτήσεων DNS.
4.5 Καταγράψτε τις θύρες πηγής (προέλευσης) των ερωτήσεων DNS.

4.6 Καταγράψτε τη θύρα πηγής (προέλευσης)των απαντήσεων DNS.
4.7 Καταγράψτε τις θύρες προορισμού των απαντήσεων DNS.
4.8 Τι παρατηρείτε για τη σχέση των θυρών προέλευσης των ερωτήσεων με τις θύρες προορισμού των απαντήσεων;
4.9 Ποια είναι η πασίγνωστη θύρα όπου ακούει ο εξυπηρετητής DNS;
4.10 Καταγράψτε τη θύρα προορισμού των μηνυμάτων HTTP που παράγει ο υπολογιστής σας.
4.11 Καταγράψτε τις θύρες πηγής (προέλευσης) των μηνυμάτων HTTP που έστειλε ο υπολογιστής σας.
4.12 Καταγράψτε τη θύρα πηγής (προέλευσης) των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού.
4.13 Καταγράψτε τις θύρες προορισμού των απαντήσεων αυτών.
4.14 Ποια είναι η πασίγνωστη θύρα όπου ακούει ο εξυπηρετητής HTTP;
4.15 Τι παρατηρείτε για τη σχέση των θυρών προέλευσης των μηνυμάτων HTTP με τις θύρες προορισμού των αντίστοιχων απαντήσεων του εξυπηρετητή ιστού;

Στη συνέχεια κάντε κλικ στο πρώτο μήνυμα πρωτοκόλλου HTTP και από το μενού "*Analyze*" επιλέξτε "*Follow TCP Stream*". Στην οθόνη που θα εμφανισθεί, βλέπετε το περιεχόμενο της συγκεκριμένης ροής TCP. Παρατηρήστε ότι σε αντίθεση με όλες τις προηγούμενες περιπτώσεις τα ονόματα των πεδίων περιγράφονται ρητά και μετά ακολουθεί η τιμή τους. Με βάση τα αποτελέσματα της προηγούμενης καταγραφής να απαντηθούν τα ερωτήματα:

4.16 Ποια είναι η ονομασία του πρώτου μηνύματος HTTP από τον υπολογιστή σας προς τον εξυπηρετητή ιστού; *[Υπόδειξη: Για τη δομή της επικεφαλίδας του πρωτοκόλλου HTTP συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο HTTP στο δεξιό της μέρος.]*
4.17 Ποιος είναι ο κωδικός απάντησης που επιστρέφει ο εξυπηρετητής ιστού;

Επαναλάβετε την καταγραφή της διερχόμενης κίνησης με το Wireshark όταν επισκέπτεστε τον ιστότοπο http://edu-dy.cn.ntua.gr/lab2/ και σταματήστε την καταγραφή των πακέτων αφού έχει ολοκληρωθεί το κατέβασμα της σελίδας. Με βάση τα δεδομένα που καταγράψατε, συγκρινόμενα με αυτά που είδατε στην προηγούμενη καταγραφή, και το φίλτρο απεικόνισης *http or dns* ενεργοποιημένο, να απαντηθεί το παρακάτω ερώτημα:

4.18 Γιατί χρειάζονταν η εκτέλεση της εντολής ipconfig /flushdns σε περίπτωση που είχατε ήδη επισκεφθεί την παραπάνω ιστοσελίδα.

Όνοματεπώνυμο: Νίκος Μπέλλος	**Ομάδα:** 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3 / Windows OS	**Ημερομηνία:** 25 / 10 / 2021
Διεύθυνση IP: 192 . 168 . 1 . 6	**Διεύθυνση MAC:** 7C - 2A - 31 - 40 - C9 - AF

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Εμφανίζονται όλα τα πακέτα που περιέχουν επικεφαλίδες ARP (Address Resolution Protocol) ή IP (Internet Protocol)

1.2 Destination, Source, Type

1.3 Όχι, δεν υπάρχει

1.4 6 bytes

1.5 14 bytes (6 → Destination, 6 → Source, 2 → Type)

1.6 Το πεδίο type του πλαισίου Ethernet

1.7 Καταλαμβάνει τα δύο τελευταία bytes

1.8 HEX τιμή για IPv4 : 08 00

1.9 HEX τιμή για IPv4 (με πακέτα ARP) : 08 06

2

2.1 Εμφανίζονται όλα τα πακέτα με πρωτόκολλο ICMP (Internet Control Message Protocol)

2.2 Μία διεύθυνση IPv4 εχει μήκος 4 bytes

2.3 Πρώτο πεδίο : Version, Δεύτερο πεδίο : Header Length

2.4 Τα πεδία έχουν μήκος 4 bit το καθένα. Το πρώτο έχει τιμή 4 (τύπος πρωτοκόλου) και το δεύτερο τιμή 5

2.5 Μήκος επικεφαλίδας IPv4 : 20 bytes

2.6 Ταυτίζεται με τη τιμή που αναγράφεται στο πεδίο Header Length της επικεφαλίδας IPv4

2.7 Μήκος πακέτου IPv4 (με βάση τα περιεχόμενα) : 74 bytes

2.8 Το μήκος του πακέτου αναγράφεται και στη λίστα πακέτων και στην επικεφαλίδα Frame και ναι συμφωνεί με αυτό που βρίκαμε παραπάνω

2.9 Μήκος δεδομένων / Data : 32 bytes

2.10 Από την επικεφαλίδα Internet Control Message Protocol κοιτάμε το πεδίο Data στο οποιο αναγράφεται δίπλα το μήκος του

2.11 Το πεδίο που λέγεται `Protocol`

2.12 Βρίσκεται στο 10 byte από την αρχή της επικεφαλίδας IPv4

2.13 Τιμή Protocol για ICMP : 01 (HEX)

3

3.1 Εμφανίζει όλα τα πακέτα που περιέχουν επικεφαλίδες TCP ή UDP

3.2 UDP, TCP, QUIC, TLS

3.3 Για TCP : 06 (HEX), για UDP : 11 (HEX)

3.4 Source Port, Destination Port, Checksum

3.5 8 bytes

3.6 Υπάρχει το πεδίο Length

3.7 Υπάρχει το πεδίο Header Length (1 byte) το οποίο είναι το 13ο byte από την αρχή της επικεφαλίδας

3.8 Οχι, δεν υπάρχει. Προκύπτει από το άθροισμα σε bytes του Header Length και του TCP Payload

3.9 Το Destination ή το Source Port μπορεί να αποκαλύπτει το τύπο πρωτοκόλλου εφαρμογής (πχ. η πόρτα 443 υποδηλώνει το HTTPS)

3.10 DNS, HTTP

4.1 Το UDP πρωτόκολλο

4.2 Το TCP πρωτόκολλο

4.3 Το πρώτο bit. 0 για ερώτηση και 1 για απάντηση

4.4 Destination port (DNS query) : 53

4.5 Source port (DNS query) : 59374

4.6 Source port (DNS reponse) : 53

4.7 Destination port (DNS response) : 59374

4.8 Η DNS ερώτηση με την DNS απάντηση "περνάνε" από την ίδια πόρτα

4.9 DNS Port : 53

4.10 Destination Port : 80

4.11 Source Port : 49451

4.12 Source Port : 80

4.13 Destination Port : 49451

4.14 HTTP Port : 80

4.15 Οι δύο πόρτες αυτες (source και destination) ταυτίζονται

4.16 GET /lab2/ HTTP/1.1

4.17 HTTP/1.1 200 OK (ο κωδικός είναι ο 200 ο οποίος συνεπάγεται απάντηση επιτυχής σύνδεσης με το web server)

4.18 Η εντολή ipconfig /flushdns χρειάζεται για το καθαρισμό της cache από DNS αρχεία, διότι αν έχουμε επισκευτεί ήδη τη σελίδα τα DNS requests θα απαντηθούν από τη cache και όχι από το DNS server.