Εργαστηριακή Άσκηση 3
Ενθυλάκωση και Επικεφαλίδες

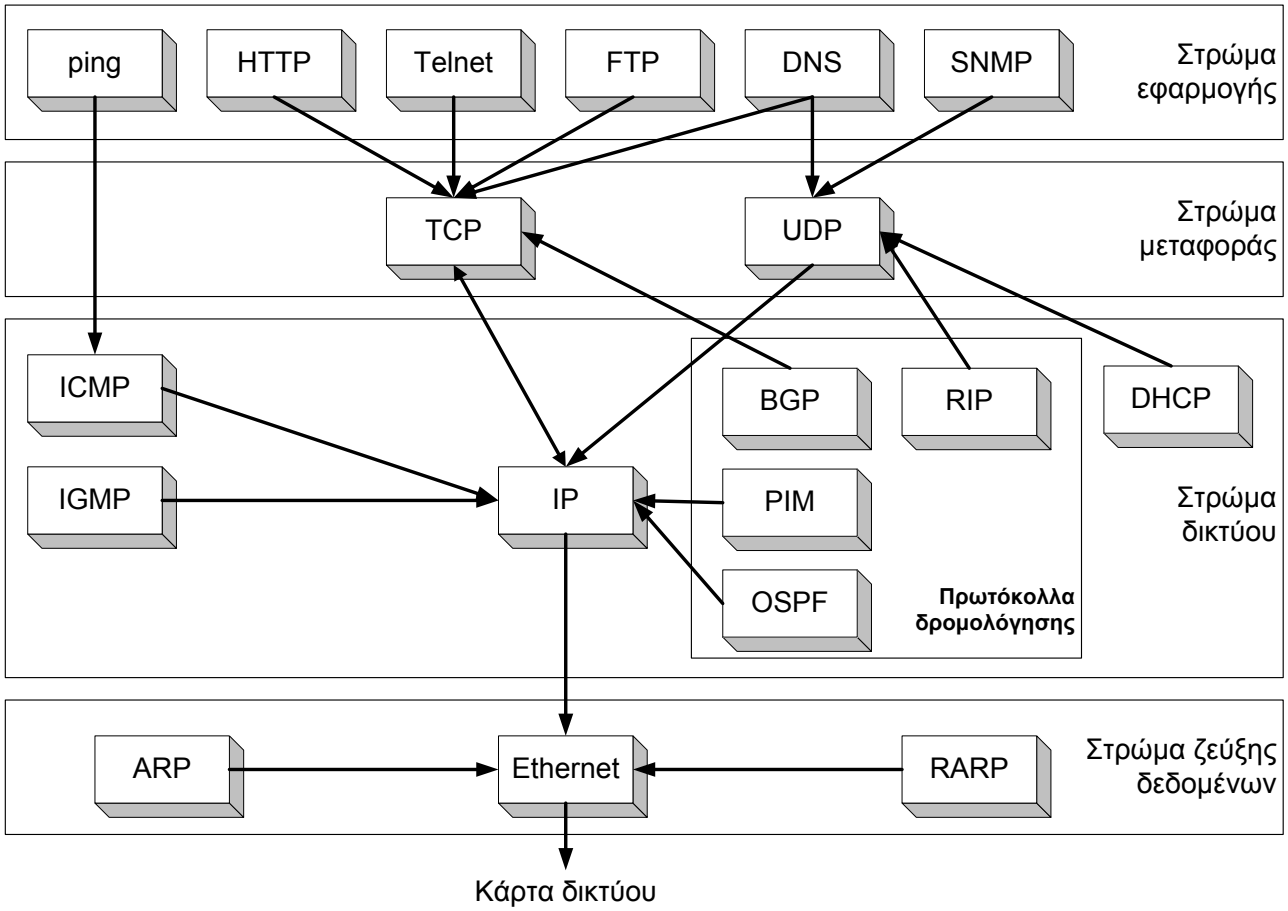
Όπως γνωρίζετε και από προηγούμενα μαθήματα, για να μειωθεί η πολυπλοκότητα σχεδίασης και να βελτιωθεί η συμβατότητα μεταξύ κατασκευαστών, τα περισσότερα πρωτόκολλα δικτύων οργανώνονται σε στρώματα (layers) ή επίπεδα (levels), το καθένα από τα οποία κτίζεται πάνω στο κατώτερό του. Ο αριθμός των στρωμάτων, 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 χρησιμοποιείται ένα άλλο μοντέλο αναφοράς, γνωστό ως η στοίβα πρωτοκόλλων TCP/IP (TCP/IP protocol stack), που περιλαμβάνει τέσσερα στρώματα: το φυσικό στρώμα, το στρώμα δικτύου, το στρώμα μεταφοράς και το στρώμα εφαρμογής. 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 φυσικό στρώμα μπορεί να είναι οποιοδήποτε τηλεπικοινωνιακό σύστημα. Η θέση ενός πρωτοκόλλου στην ιεραρχία της σουίτας TCP/IP ορίζεται μέσω της ενθυλάκωσης. Π.χ. τα δεδομένα ενός πρωτοκόλλου που τοποθετείται στο στρώμα δικτύου ενθυλακώνονται σε πλαίσια του φυσικού στρώματος. Περισσότερα για τη θέση των πρωτοκόλλων του Internet στην ιεραρχία αυτή μπορείτε να βρείτε στην ιστοσελίδα http://www.networksorcery.com/enp επιλέγοντας από το menu στα αριστερά τον υπερσύνδεσμο "*IP protocol suite*".

Παρατηρείστε 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, δεν αφορά τη 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 σχήμα της επόμενης σελίδας, 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 φυσικού στρώματος, "πακέτο" τη μονάδα δεδομένων πρωτοκόλλου του στρώματος δικτύου, "τεμάχιο" ή "δεδομενόγραμμα" (TCP segment ή UDP datagram) τη μονάδα δεδομένων πρωτοκόλλου του στρώματος μεταφοράς, ανά περίσταση, και "μήνυμα" τη μονάδα δεδομένων πρωτοκόλλου του στρώματος εφαρμογής.



Ο σκοπός αυτού του εργαστηρίου είναι η μελέτη της ενθυλάκωσης της πληροφορίας ανάμεσα στα στρώματα πρωτοκόλλων της σουίτας TCP/IP. Όπως και στα προηγούμενα εργαστήρια θα εργαστείτε με το πρόγραμμα Wireshark. Τα πλαίσια που καταγράφονται από το Wireshark εμφανίζονται έγχρωμα[1] στο παράθυρο με τη λίστα καταγεγραμμένων πακέτων στο επάνω μέρος της οθόνης. Κάθε γραμμή αντιστοιχεί σε ένα πλαίσιο που συλλαμβάνεται. Η επιλογή ενός οποιουδήποτε από τα πλαίσια που καταγράφηκαν γίνεται κάνοντας κλικ στην αντίστοιχη γραμμή της λίστας. Μεταξύ των στοιχείων που εμφανίζονται για κάθε πλαίσιο, στο πεδίο με τίτλο Protocol εμφανίζεται το ανώτατης τάξης ενθυλακωμένο πρωτόκολλο που αποκωδικοποιεί το Wireshark. Για κάθε πρωτόκολλο, που ενθυλακώνεται στα δεδομένα του πλαισίου που έχει επιλεγεί, τα βασικά πεδία της επικεφαλίδας του εμφανίζονται με γραφικό τρόπο στο παράθυρο με τις λεπτομέρειες επικεφαλίδας στο μεσαίο τμήμα της οθόνης. Πιο συγκεκριμένα, υπάρχει μία γραμμή για την επικεφαλίδα κάθε πρωτοκόλλου που είναι ενθυλακωμένο στα δεδομένα του πλαισίου. 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.

Στο παράθυρο με τα περιεχόμενα (κάτω τμήμα της οθόνης) εμφανίζονται τα δεδομένα του επιλεγμένου πλαισίου σε δεκαεξαδική και ASCII μορφή. Μπορείτε να δείτε όλο το περιεχόμενο της επικεφαλίδας ενός πρωτοκόλλου με διπλό κλικ στην αντίστοιχη γραμμή ή κάνοντας κλικ επάνω της και πιέζοντας το πλήκτρο + ή με κλικ στο σύμβολο στα αριστερά της. Όταν κάνετε κλικ πάνω σε κάποια επικεφαλίδα ή σε κάποιο πεδίο μιας επικεφαλίδας (στο παράθυρο με τις λεπτομέρειες επικεφαλίδας), τότε εμφανίζεται με αντιστροφή χρώματος (highlighted) το αντίστοιχο κομμάτι του

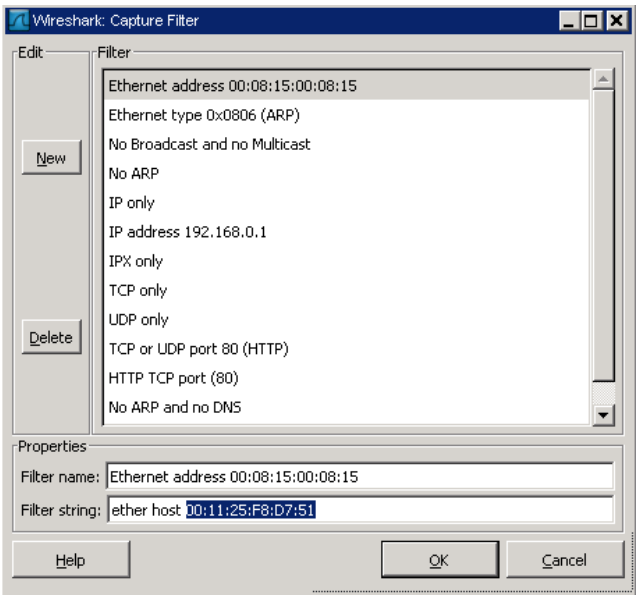
[1] Μπορείτε να δείτε τους προκαθορισμένους κανόνες χρωματισμού πακέτων του Wireshark στο *View→Coloring rules*, από όπου μπορείτε να αλλάξετε τους κανόνες, να προσθέσετε νέους και να εισάγετε νέους από αρχεία. Αν δεν είναι ήδη, μπορείτε να ενεργοποιήστε τους κανόνες επιλέγοντας *View→Coloring Rules*….

πλαισίου στο παράθυρο με τα περιεχόμενα του πλαισίου. Τέλος, το μέγεθος και των τριών παραθύρων (καταγεγραμμένα πλαίσια, λεπτομέρειες επικεφαλίδας, 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 ανάλυσης. Ο μηχανισμός σύλληψης υλοποιείται στη βιβλιοθήκη WinPcap.(που αποτελεί μεταφορά σε περιβάλλον Windows της libpcap του Unix). Τα πλαίσια που συλλαμβάνονται πρέπει να ικανοποιούν μια λογική (Boolean) έκφραση, το *φίλτρο σύλληψης*. Η σύνταξή της λογικής έκφρασης περιγράφεται στην ιστοσελίδα http://www.tcpdump.org/tcpdump_man.html. Η ίδια περιγραφή επαναλαμβάνεται και στην τεκμηρίωση της βιβλιοθήκης WinPcap στην ιστοθέση http://www.winpcap.org/docs/docs_40_2/html/group__language.html. Μια πιο επεξηγηματική περιγραφή όμως μπορείτε να βρείτε στο help του Wireshark (*§4.8 Filtering while capturing*), ενώ στην ιστοσελίδα http://wiki.wireshark.org/CaptureFilters θα βρείτε πολλά ενδιαφέροντα παραδείγματα.

Για να καταγράφονται μόνο πλαίσια που παράγονται ή απευθύνονται στον υπολογιστή σας, εφαρμόστε ένα φίλτρο καταγραφής ως εξής: από το παράθυρο *Capture → Options…* πιέστε το κουμπί "*Capture Filter*" και επιλέξτε τη γραμμή Ethernet address 00:08:15:00:08:15 (το όνομα του φίλτρου). Στη συνέχεια στο πεδίο *Filter string* (ο ορισμός της λογικής έκφρασης) διορθώστε τη διεύθυνση ώστε να είναι ίδια με τη διεύθυνση MAC της κάρτας δικτύου του υπολογιστή σας. Το φίλτρο ενεργοποιείται με το πάτημα του *OK*.



Προσοχή: Σε αντίθεση με τα φίλτρα παρατήρησης δεν υπάρχει οπτική ένδειξη (πράσινο χρώμα) για την ορθότητα της σύνταξης. Εάν η σύνταξη είναι λάθος θα εμφανισθεί σχετικό μήνυμα όταν προχωρήσετε στην καταγραφή.

1. Φυσικό στρώμα

Ξεκινήστε να καταγράφετε τη διερχόμενη κίνηση με τη βοήθεια του φίλτρου που περιγράφτηκε παραπάνω. Σιγουρευτείτε ότι στο πεδίο *Interface* αναφέρεται το όνομα της κάρτας δικτύου του υ-

πολογιστή σας και επιπλέον ότι καμιά από τις επιλογές της κατηγορίας *Name Resolution* δεν είναι ενεργοποιημένη. Ανοίξτε ένα παράθυρο εντολών και εκτελέστε την εντολή `arpclear` προκειμένου να καθαρίσετε τον πίνακα arp του υπολογιστή σας. Κάντε `ping` σε διπλανό υπολογιστή και σταματήστε την καταγραφή. Υπενθυμίζεται ότι για τη χρήση της εντολής ping πρέπει να πληκτρολογήσετε `ping <διεύθυνση IP>`, όπου `<διεύθυνση IP>` η διεύθυνση IP του διπλανού υπολογιστή, ενώ ο πίνακας arp του υπολογιστή σας εμφανίζεται με την εκτέλεση της εντολής `arp -a` από γραμμή εντολών. Με βάση τα δεδομένα που καταγράψατε να απαντηθούν τα παρακάτω ερωτήματα, αφού πρώτα εφαρμόσετε το φίλτρο απεικόνισης *arp or icmp*:

1.1 Ποια η σημασία του φίλτρου απεικόνισης που εφαρμόσατε;
1.2 Ποια είναι τα ονόματα και το μήκος των πεδίων της επικεφαλίδας του Ethernet;
1.3 Ποιο είναι το συνολικό μήκος αυτής της επικεφαλίδας;
1.4 Ποιο πεδίο του πλαισίου Ethernet καθορίζει το πρωτόκολλο δικτύου;
1.5 Ποια είναι η θέση που καταλαμβάνει μέσα στην επικεφαλίδα το πεδίο αυτό;
1.6 Ποια είναι η τιμή του πεδίου αυτού για πακέτα IP; *[Υπόδειξη: Για να εντοπίσετε πλαίσια που περιέχουν πακέτα IP, βεβαιωθείτε ότι στη σειρά ενθυλάκωσης πρωτοκόλλων, που εμφανίζεται στο παράθυρο με τις λεπτομέρειες επικεφαλίδας, περιλαμβάνεται επικεφαλίδα 'Internet Protocol']*
1.7 Ποια είναι η τιμή του πεδίου αυτού για πακέτα ARP;

2. Στρώμα Δικτύου

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

2.1 Ποια πρωτοκόλλα στρώματος δικτύου παρατηρείτε;
2.2 Εξηγείστε γιατί η τιμή του πεδίου Hardware size που εμφανίζεται στα πακέτα ARP έχει την τιμή 6. *[Υπόδειξη: Για τη δομή της επικεφαλίδας του πρωτοκόλλου ARP συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ARP στο δεξιό της μέρος].*

Επιλέξτε ένα πλαίσιο όπου ενθυλακώνεται ένα πακέτο IP.

2.3 Ποιο είναι το συνολικό μήκος της επικεφαλίδας IP με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα πλαισίου;
2.4 Ποια είναι τα ονόματα των πρώτων δύο πεδίων της επικεφαλίδας IP;
2.5 Ποιο είναι το μήκος σε bit και ποια η τιμή των πεδίων αυτών; *[Υπόδειξη: Για την δομή της επικεφαλίδας του πρωτοκόλλου IP μπορείτε να συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο IP στο δεξιό της μέρος]*
2.6 Πώς προκύπτει το μήκος που προσδιορίσατε στην ερώτηση 2.3 από την τιμή του αντίστοιχου πεδίου της επικεφαλίδας IP;
2.7 Ποιο είναι το μήκος των διευθύνσεων IP;
2.8 Εξηγείστε γιατί η τιμή του πεδίου Protocol size που εμφανίζεται στα πακέτα ARP έχει την τιμή 4.
2.9 Ποιο είναι το συνολικό μήκος του πακέτου IP με βάση τα δεδομένα της καταγραφής που εμφανίζονται στο παράθυρο με τα περιεχόμενα του επιλεγμένου πλαισίου;
2.10 Ποιο είναι το μήκος δεδομένων (payload) του πακέτου IP;
2.11 Υπάρχει πεδίο σχετικό με το μήκος του πακέτου IP στην επικεφαλίδα του και ποια η τιμή του;
2.12 Πώς προκύπτει το μήκος των δεδομένων (payload) του πακέτου IP από τα στοιχεία της επικεφαλίδας;
2.13 Ποιο πεδίο της επικεφαλίδας IP καθορίζει το πρωτόκολλο στρώματος μεταφοράς;
2.14 Ποια είναι η θέση του (σε σχέση με την αρχή της επικεφαλίδας IP);
2.15 Ποια είναι η τιμή του για το πρωτόκολλο ICMP;

3. Στρώμα Μεταφοράς

Στη συνέχεια αρχίστε νέα καταγραφή της διερχόμενης κίνησης χρησιμοποιώντας το πρόγραμμα ανάλυσης πακέτων Wireshark με το ίδιο φίλτρο σύλληψης όπως και πριν. Επισκεφθείτε τον ιστότοπο http://edu-dy.cn.ntua.gr/lab3 και σταματήστε την καταγραφή των πακέτων αφού έχει ολοκληρωθεί το κατέβασμα της σελίδας. *[Προσοχή: Δεν πρέπει να έχετε επισκεφτεί το συγκεκριμένο ιστότοπο πριν την καταγραφή! Διαφορετικά εκτελέστε την εντολή* `ipconfig /flushdns` *προηγουμένως]*. Με βάση τα δεδομένα που καταγράψατε να απαντηθούν τα παρακάτω ερωτήματα, αφού πρώτα ενεργοποιήσετε το φίλτρο απεικόνισης *ip*:

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 για το πρωτόκολλο TCP;
3.4 Ποια είναι η τιμή του πεδίου Protocol για το πρωτόκολλο UDP;
3.5 Ποια είναι τα ονόματα των πεδίων της επικεφαλίδας των τεμαχίων TCP και δεδομενογραμμάτων UDP που είναι κοινά και στα δύο πρωτόκολλα;
3.6 Ποιο είναι το μήκος της επικεφαλίδας των δεδομενογραμμάτων UDP;
3.7 Ποιο πεδίο καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP;
3.8 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/default0604.htm επιλέγοντας το "TCP/UDP ports" από το αριστερό της μέρος]*.
3.9 Αναφέρατε τα πρωτόκολλα στρώματος εφαρμογής που 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: Για τη δομή της επικεφαλίδας του πρωτοκόλλου DNS συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm 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 *[Υπόδειξη: κάντε κλικ στο αντίστοιχο μήνυμα 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 *[Υπόδειξη: κάντε κλικ στο αντίστοιχο μήνυμα HTTP]*.
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, δηλαδή, την ανταλλαγή μηνυμάτων μεταξύ του πλοηγού και του εξυπηρετητή ιστού. Τα μηνύματα (εντολές) του πλοηγού ιστού εμφανίζονται σε ροζ φόντο, ενώ τα μηνύματα (αποκρίσεις) του εξυπηρετητή ιστού εμφανίζονται σε γαλάζιο φόντο, όπως στο ακόλουθο παράδειγμα:

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Accept-Language: el
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.mit.edu
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 05 Nov 2004 08:25:08 GMT
Server: MIT Web Server Apache/1.3.26 Mark/1.4 (Unix) mod_ssl/2.8.9 OpenSSL/0.9.6g
Last-Modified: Fri, 05 Nov 2004 04:59:29 GMT
ETag: "71d07dc-40a9-418b08b1"
Accept-Ranges: bytes
Content-Length: 16553
Keep-Alive: timeout=15, max=400
Connection: Keep-Alive
Content-Type: text/html
```

Παρατηρείστε 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 την δομή της επικεφαλίδας του πρωτοκόλλου HTTP συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.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 που επιστρέφει ο εξυπηρετητής ιστού;

Επαναλάβετε την καταγραφή της διερχόμενης κίνησης με το Wireshark όταν επισκέπτεστε τον ιστότοπο http://edu-dy.cn.ntua.gr/lab3 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 επισκευθεί την παραπάνω ιστοσελίδα. *[Υπόδειξη: ανατρέξατε στη βοήθεια για την εντολή* `ipconfig`*]*.

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 3
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 .....

1.2 .....

.....

1.3 .....

1.4 .....

1.5 .....

1.6 .....

1.7 .....

2

2.1 .....

2.2 .....

.....

2.3 .....

2.4 .....

2.5 .....

2.6 .....

.....

2.7 .....

2.8 .....

.....

2.9 .....

2.10 .....

2.11 .....

2.12 .....

.....

2.13 .....

2.14 .....