Αναλυτής Πρωτοκόλλων Wireshark

Η άσκηση αυτή αποτελεί εισαγωγή στη χρήση του αναλυτή πρωτοκόλλων Wireshark, του οποίου οι βασικές λειτουργίες είναι οι εξής: α) καταγραφή – σύλληψη (capture) και β) ανάλυση της δικτυακής κίνησης του υπολογιστή.

Για κάθε λειτουργία ο χρήστης μπορεί να ορίσει κατάλληλα φίλτρα καταγραφής/ανάλυσης τα οποία περιορίζουν την κίνηση που καταγράφεται/αναλύεται σύμφωνα με τα κριτήριά του. Έτσι, σύμφωνα με την ορολογία του Wireshark διακρίνουμε τα capture και τα display filters αντίστοιχα, τα οποία θα αναλυθούν στις επόμενες σειρές ασκήσεων.

Ως εισαγωγικό παράδειγμα θα παρατηρήσετε την κίνηση που παράγεται από την επίσκεψη μιας ιστοσελίδας. Αφού ξεκινήσετε το Wireshark, οι διάφορες επιλογές που αφορούν τη λειτουργίας της καταγραφής ρυθμίζονται ακολουθώντας από το μενού επιλογών τη διαδρομή Capture | Options…). Στο παράθυρο που εμφανίζεται βεβαιωθείτε ότι στο πεδίο Interface αναφέρεται το όνομα της κάρτας δικτύου του υπολογιστή σας και επιπλέον ότι η επιλογή Enable network name resolution είναι ενεργοποιημένη. Πατώντας το Start αρχίζει η καταγραφή και εμφανίζεται σχετικό ενημερωτικό παράθυρο. Χρησιμοποιήστε ένα πλοηγό διαδικτύου (π.χ., firefox) για να επισκεφτείτε κάποια ιστοσελίδα, π.χ., http://www.teimes.gr Μόλις φορτωθεί πλήρως η σελίδα πατήστε το Stop για να σταματήσει η καταγραφή. Στο κύριο παράθυρο του Wireshark, όπου φαίνεται η καταγεγραμμένη δικτυακή κίνηση, μπορεί ενδεχομένως να παρατηρήσετε κίνηση που δε σχετίζεται με την επίσκεψη της ιστοσελίδας. Η ζητούμενη κίνηση μπορεί να απομονωθεί με την εφαρμογή φίλτρου παρατήρησης ως εξής: πηγαίνετε Analyze | Display Filters… και πατήστε το πλήκτρο Expression. Από το πεδίο Field name βρείτε την επιλογή IP, πατήστε το +, διαλέγετε την επιλογή ip.addr, από το πεδίο Relation διαλέξτε το ==, στο πεδίο Value (IPv4 address) πληκτρολογήστε την διεύθυνση IP που σας ενδιαφέρει (π.χ., 194.42.10.196) και πατήστε OK. Το φίλτρο ενεργοποιείται με το πάτημα του Apply. Κλείνοντας το παράθυρο διαλόγου (με OK) θα διαπιστώσετε ότι η κίνηση είναι ενδεχομένως περιορισμένη σε σχέση με την παρατήρηση χωρίς φίλτρο.

Καταγράψτε:

1. Ποια είναι η διεύθυνση IP του www.teimes.gr;
2. Τα πρωτόκολλα που παρατηρείτε ότι χρησιμοποιούνται για την επικοινωνία με την ιστοσελίδα.
3. Για καθένα από τα πρωτόκολλα του προηγούμενου ερωτήματος να γραφεί το επίπεδο που ανήκει σύμφωνα με το πρότυπο OSI.