Εργαστήριο Wireshark: Εισαγωγή

Computer Networking: A Top-Down Approach Featuring the Internet

Έκδοση:2.0

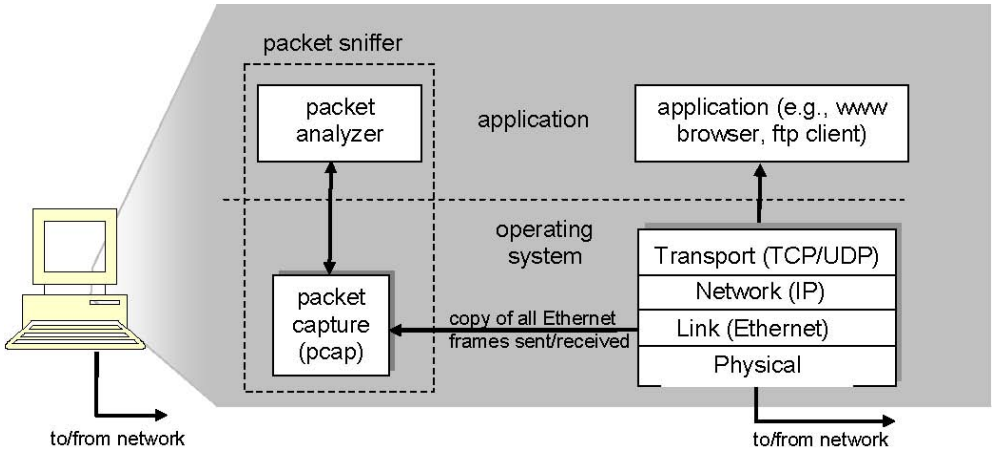
Μετάφραση - Απόδοση: Σ. Τσακιρίδου

Συχνά, μπορούμε να κατανοήσουμε καλύτερα τα δικτυακά πρωτοκόλλα "παρατηρώντας τα σε δράση" ή "παίζοντας μαζί τους", δηλαδή παρατηρώντας την ακολουθία των μηνυμάτων που ανταλλάσσονται μεταξύ δύο οντοτήτων πρωτοκόλλων, εισχωρώντας στις λεπτομέρειες λειτουργίας των πρωτοκόλλων, αναγκάζοντάς τα να εκτελέσουν συγκεκριμένες ενέργειες και στη συνέχεια παρατηρώντας αυτές τις ενέργειες και τις συνέπειές τους. Αυτό μπορεί να γίνει σε προσομοιωμένα σενάρια ή σε ένα περιβάλλον "πραγματικού" δικτύου όπως το Διαδίκτυο. Τα εφαρμογίδια Java (Java applets) που συνοδεύουν αυτό το βιβλίο ακολουθούν την πρώτη προσέγγιση. Στα εργαστήρια Wireshark[1] θα ακολουθήσουμε τη δεύτερη προσέγγιση. Θα τρέξετε διάφορες δικτυακές εφαρμογές σε διαφορετικά σενάρια χρησιμοποιώντας έναν υπολογιστή στο γραφείο, στο σπίτι ή σε ένα εργαστήριο. Θα παρατηρήσετε τα δικτυακά πρωτόκολλα στον υπολογιστή σας "σε δράση", να αλληλεπιδρούν και να ανταλλάσσουν μηνύματα με οντότητες πρωτοκόλλων που εκτελούνται αλλού στο Διαδίκτυο. Έτσι, εσείς και ο υπολογιστής σας θα αποτελέσετε μέρος αυτών των "ζωντανών" εργαστηρίων. Θα παρατηρήσετε και θα μάθετε πράττοντας.

Το βασικό εργαλείο για την παρατήρηση των μηνυμάτων που ανταλλάσσονται μεταξύ των εκτελούμενων οντοτήτων πρωτοκόλλων καλείται **packet sniffer**. Όπως υπονοεί και το όνομα, ο packet sniffer συλλαμβάνει ("sniffs") τα μηνύματα τα οποία στέλνονται ή λαμβάνονται από τον υπολογιστή σας. Επίσης, ο packet sniffer συνήθως αποθηκεύει και απεικονίζει τα περιεχόμενα διαφόρων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνονται. Ο ίδιος ο packet sniffer είναι παθητικός. Παρατηρεί τα μηνύματα που στέλνονται και λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που τρέχουν στον υπολογιστή σας αλλά ο ίδιος δεν στέλνει ποτέ πακέτα. Παρόμοια, τα λαμβανόμενα πακέτα δεν απευθύνονται ποτέ με ρητό τρόπο στον packet sniffer. Αντίθετα, ο packet sniffer λαμβάνει ένα *αντίγραφο* των πακέτων που στέλνονται ή λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στον υπολογιστή σας.

[1] Προηγούμενες εκδόσεις αυτών των εργαστηρίων χρησιμοποιούσαν τον αναλυτή πακέτων Ethereal. Το Μάιο του 2006, ο σχεδιαστής του Ethereal προσχώρησε σε μία νέα εταιρεία οπότε αναγκάστηκε να εγκαταλείψει το σήμα κατατεθέν Ethereal®. Στη συνέχεια δημιούργησε το διάδοχο του Ethereal®, τον αναλυτή δικτυακών πρωτοκόλλων Wireshark. Επειδή το Ethereal® δε συντηρείται, ούτε αναπτύσσεται, πλέον, ενεργά χρησιμοποιούμε το Wireshark για τα εργαστήρια αυτά.

Στο Σχήμα 1 φαίνεται η δομή ενός packet sniffer. Στα δεξί μέρος του Σχήματος 1 φαίνονται τα πρωτόκολλα (στην προκειμένη περίπτωση τα πρωτόκολλα του Διαδικτύου) και οι εφαρμογές (όπως ένας web browser ή ένας ftp client) που τρέχουν κανονικά στον υπολογιστή σας. Ο packet sniffer, ο οποίος φαίνεται μέσα στο παραλληλόγραμμο διακεκομμένων γραμμών του Σχήματος 1, είναι μία προσθήκη στο σύνηθες λογισμικό του υπολογιστή σας και αποτελείται από δύο μέρη. Η **βιβλιοθήκη σύλληψης πακέτων** (**packet capture library)** λαμβάνει ένα αντίγραφο κάθε πλαισίου επιπέδου ζεύξης που στέλνεται ή λαμβάνεται από τον υπολογιστή σας. Υπενθυμίζεται ότι τα μηνύματα που ανταλλάσσονται από τα πρωτόκολλα ανώτερων επιπέδων, όπως το HTTP, FTP, TCP, UDP ή το IP, τελικά ενθυλακώνονται όλα μέσα σε πλαίσια επιπέδου ζεύξης τα οποία μεταδίδονται μέσω φυσικών μέσων όπως ένα καλώδιο Ethernet. Επομένως, η σύλληψη όλων των πλαισίων επιπέδου ζεύξης σας παρέχει όλα τα μηνύματα που στέλνονται και λαμβάνονται από όλα τα πρωτόκολλα και όλες τις εφαρμογές που εκτελούνται στον υπολογιστή σας.



Σχήμα 1: Δομή packet sniffer

Το δεύτερο συστατικό στοιχείο ενός packet sniffer είναι ο **αναλυτής πακέτων** (**packet analyzer**), ο οποίος απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Για το σκοπό αυτό, ο αναλυτής πακέτων πρέπει να "καταλαβαίνει" τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα. Για παράδειγμα, έστω ότι ενδιαφερόμαστε να απεικονίσουμε τα διάφορα πεδία των μηνυμάτων που ανταλλάσσονται από το πρωτόκολλο HTTP στο Σχήμα 1. Ο αναλυτής πακέτων καταλαβαίνει τη μορφή των πλαισίων Ethernet και επομένως μπορεί να αναγνωρίσει ένα αυτοδύναμο πακέτο IP (IP datagram) μέσα σε ένα πλαίσιο Ethernet. Επίσης, καταλαβαίνει τη μορφή ενός IP datagram, ώστε να είναι σε θέση να εξάγει ένα TCP segment που περιέχεται μέσα σε ένα IP datagram. Επιπλέον, καταλαβαίνει τη δομή ενός TCP segment οπότε μπορεί να εξάγει το μήνυμα HTTP που περιέχεται στο TCP segment. Τέλος, καταλαβαίνει το πρωτόκολλο HTTP και έτσι, για παράδειγμα, γνωρίζει ότι τα πρώτα bytes ενός μηνύματος HTTP θα περιέχουν τις ακολουθίες χαρακτήρων "GET", "POST" ή "HEAD", όπως φαίνεται στο Σχήμα 2.8 του βιβλίου σας.

Στα εργαστήρια αυτά θα χρησιμοποιήσουμε τον packet sniffer Wireshark

(http://www.wireshark.org), ο οποίος θα μας δώσει τη δυνατότητα να απεικονίσουμε τα περιεχόμενα των μηνυμάτων που στέλνονται ή λαμβάνονται από τα πρωτόκολλα σε διαφορετικά επίπεδα της στοίβας πρωτοκόλλων. (Σε τεχνική γλώσσα, το Wireshark είναι ένας αναλυτής πακέτων που χρησιμοποιεί μία βιβλιοθήκη σύλληψης πακέτων στον υπολογιστή σας.) Το Wireshark είναι ένας ελεύθερος χρέωσης αναλυτής δικτυακών πρωτοκόλλων ο οποίος τρέχει σε υπολογιστές Windows, Linux/Unix και Mac. Είναι ένας ιδανικός αναλυτής πακέτων για τα εργαστήριά μας: είναι ευσταθής, έχει μία μεγάλη βάση χρηστών και καλά στοιχειοθετημένη υποστήριξη που περιλαμβάνει έναν οδηγό χρήστη (http://www.wireshark.org/docs/wsug_html_chunked/), σελίδες εγχειριδίου χρήστη (man pages) (http://www.wireshark.org/docs/man-pages/) και ένα λεπτομερή κατάλογο συχνών ερωτημάτων (Frequently Asked Questions, FAQ) (http://www.wireshark.org/faq.html), είναι πλούσιος σε λειτουργίες που περιλαμβάνουν τη ικανότητα να αναλύει περισσότερα εκατοντάδες πρωτοκόλλων και έχει μία καλά σχεδιασμένη διεπαφή χρήστη (user interface). Λειτουργεί σε υπολογιστές που χρησιμοποιούν Ethernet, Token-Ring, FDDI, σειριακές συνδέσεις (PP και SLIP), ασύρματα τοπικά δίκτυα 802.11 και συνδέσεις ATM (ανάλογα με το λειτουργικό σύστημα).

Πως να λάβετε το Wireshark

Για να τρέξετε το Wireshark θα χρειαστείτε πρόσβαση σε έναν υπολογιστή που να υποστηρίζει και το Wireshark και τη βιβλιοθήκη σύλληψης πακέτων *libpcap ή WinPCap*. Εάν το λογισμικό *libpcap* δεν είναι ήδη εγκατεστημένο στο λειτουργικό σας σύστημα, θα εγκατασταθεί για σας όταν εγκαταστήσετε το Wireshark. Για ένα κατάλογο των υποστηριζόμενων λειτουργικών συστημάτων και των ιστοτόπων από όπου μπορείτε να φορτώσετε το απαραίτητο λογισμικό, επισκεφθείτε την ιστοσελίδα http://www.wireshark.org/download.html.

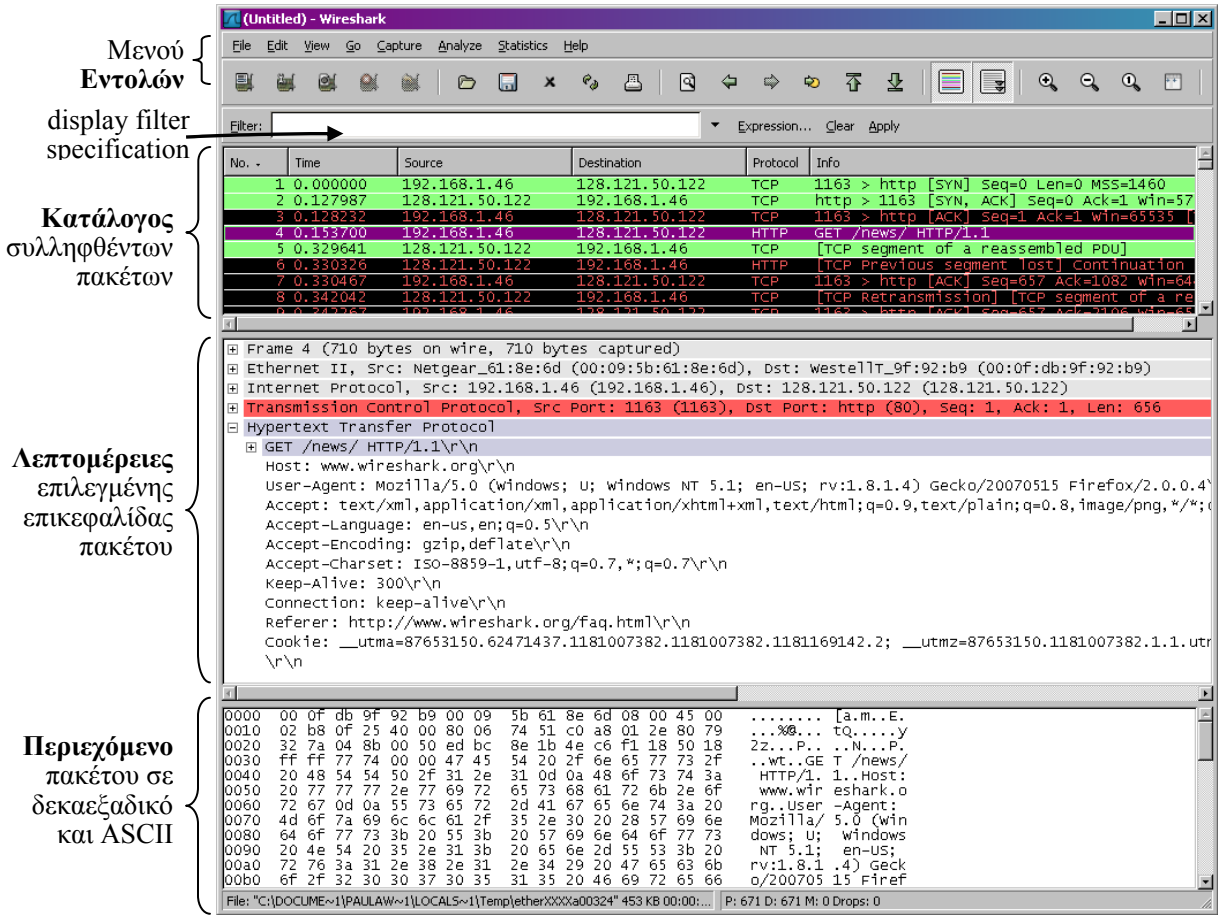
Φορτώστε και εγκαταστήστε το λογισμικό Wireshark:

- Πηγαίνετε στην ιστοσελίδα http://www.wireshark.org/download.html, φορτώστε και εγκαταστήστε το δυαδικό αρχείο Wireshark που είναι κατάλληλο για τον υπολογιστή σας.
- Φορτώστε τον οδηγό χρήστη του Wireshark.

Ο κατάλογος FAQ του Wireshark περιλαμβάνει έναν αριθμό από χρήσιμες υποδείξεις και ενδιαφέρουσες πληροφορίες, ειδικά εάν αντιμετωπίσετε προβλήματα με την εγκατάσταση ή την εκτέλεση του Wireshark.

Εκτέλεση του Wireshark

Κατά την εκτέλεση του προγράμματος Wireshark εμφανίζεται στην οθόνη η γραφική διεπαφή χρήστη (graphical user interface, GUI) του Wireshark που φαίνεται στο Σχήμα 2. Αρχικά, τα διάφορα παράθυρα δεν περιέχουν δεδομένα.



Σχήμα 2: Γραφική Διεπαφή Χρήστη (Graphical User Interface) του Wireshark

Η διεπαφή του Wireshark περιλαμβάνει πέντε κύρια στοιχεία:

- Τα **μενού των εντολών** (**command menus**) είναι συνηθισμένα πτυσσόμενα (pulldown) μενού που βρίσκονται στο επάνω μέρος του παραθύρου. Προς το παρόν μας ενδιαφέρουν τα μενού File και Capture. Το μενού File επιτρέπει την αποθήκευση δεδομένων για πακέτα που έχουν συλληφθεί ή το άνοιγμα ενός αρχείου που περιέχει δεδομένα πακέτων που είχαν συλληφθεί προηγουμένως και την έξοδο από το Wireshark. Το μενού Capture σας επιτρέπει να ξεκινήσετε τη σύλληψη πακέτων.
- Το **παράθυρο καταλόγου πακέτων** (**packet-listing window**) παρουσιάζει μία περίληψη της μιας γραμμής για κάθε πακέτο που συλλαμβάνεται η οποία περιλαμβάνει τον αριθμό πακέτου (πρόκειται για αριθμό που απονέμεται από το

Wireshark και *όχι* για έναν αριθμό πακέτου που περιέχεται στην επικεφαλίδα οποιουδήποτε πρωτοκόλλου), τον χρόνο σύλληψης του πακέτου, τις διευθύνσεις πηγής και προορισμού του πακέτου, το είδος του πρωτοκόλλου και πληροφορία σχετική με το πρωτόκολλο η οποία περιέχεται στο πακέτο. Ο κατάλογος των πακέτων μπορεί να ταξινομηθεί σύμφωνα με οποιαδήποτε από αυτές τις κατηγορίες κάνοντας κλικ στο όνομα της αντίστοιχης στήλης. Στο πεδίο είδος πρωτοκόλλου (protocol type) αναφέρεται το ανωτάτου επιπέδου πρωτόκολλο το οποίο έστειλε ή έλαβε ένα πακέτο, δηλαδή, το πρωτόκολλο που είναι η πηγή ή ο τελικός αποδέκτης αυτού του πακέτου.

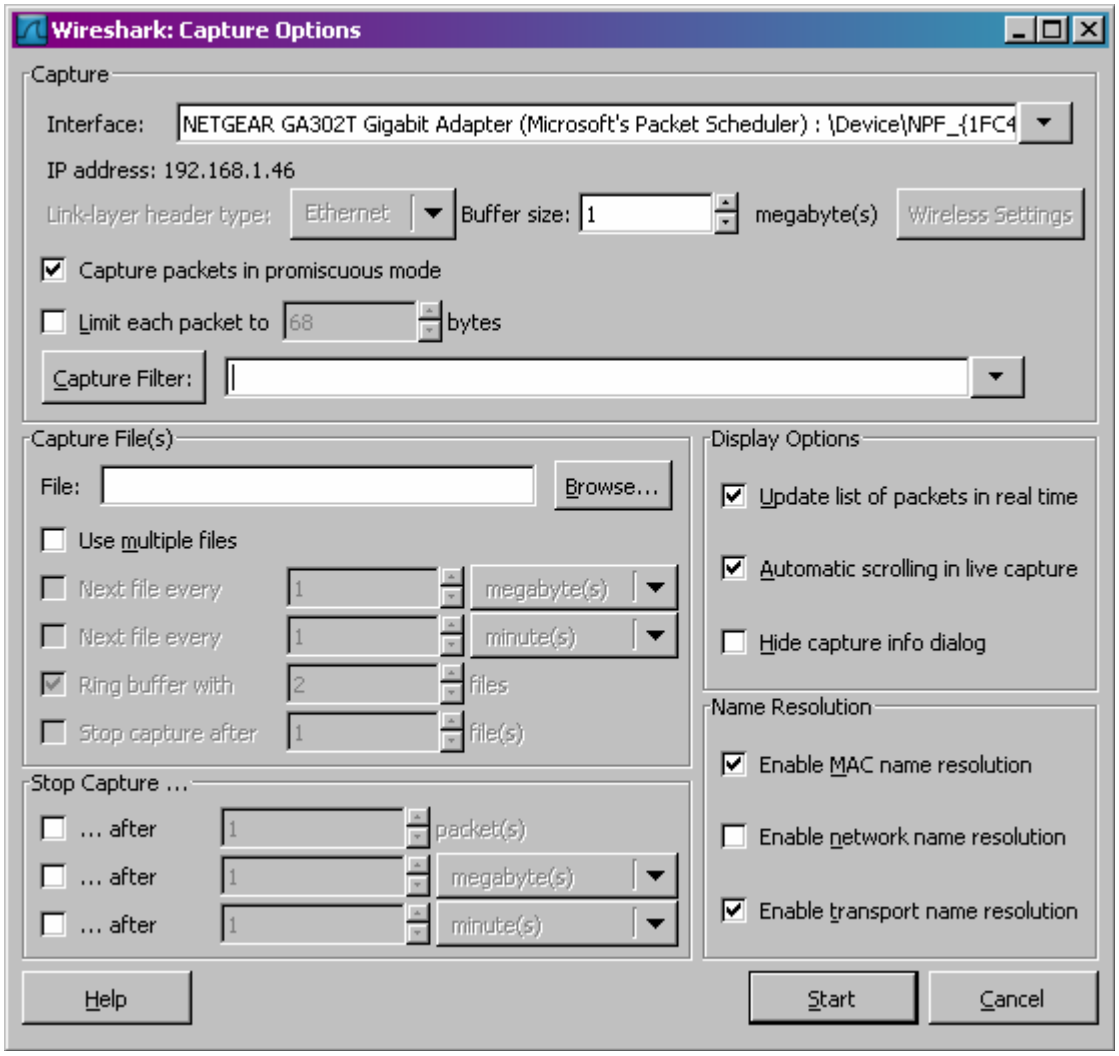
- Το **παράθυρο λεπτομερειών επικεφαλίδας πακέτου** (**packet-header details window**) παρέχει λεπτομέρειες σχετικά με το επιλεγμένο στο παράθυρο packet-listing πακέτο. (Για να επιλέξετε ένα από τα πακέτα του παραθύρου packet-listing, τοποθετείστε τον cursor πάνω από την μιας-γραμμής περίληψη του πακέτου στο παράθυρο packet-listing και κάντε αριστερό κλικ.) Οι λεπτομέρειες αυτές περιλαμβάνουν πληροφορίες σχετικά με το πλαίσιο Ethernet και το IP datagram που περιέχουν αυτό το πακέτο. Το ποσό των λεπτομερειών που παρουσιάζεται για το Ethernet και το επίπεδο IP μπορεί να επεκταθεί ή να ελαχιστοποιηθεί κάνοντας κλικ στο βέλος που δείχνει δεξιά ή προς τα κάτω και βρίσκεται στα αριστερά της γραμμής του πλαισίου Ethernet ή του IP datagram στο παράθυρο packet-header details. Εάν το πακέτο έχει μεταφερθεί με TCP ή UDP, θα παρουσιαστούν και οι λεπτομέρειες που αφορούν το TCP ή το UDP, οι οποίες μπορούν να επεκταθούν ή να ελαχιστοποιηθούν με παρόμοιο τρόπο. Τέλος, λεπτομέρειες παρέχονται επίσης για το ανωτάτου επιπέδου πρωτόκολλο το οποίο έστειλε ή έλαβε αυτό το πακέτο.
- Το **παράθυρο περιεχομένων πακέτου** (**packet-contents window**) παρουσιάζει ολόκληρο το περιεχόμενο ενός συλλαμβανόμενου πλαισίου και σε μορφή ASCII και σε δεκαεξαδική μορφή.
- Προς το επάνω μέρος της διεπαφής Wireshark βρίσκεται το **πεδίο του φίλτρου παρουσίασης πακέτων** (**packet display filter field**) στο οποίο μπορούμε να εισάγουμε το όνομα ενός πρωτοκόλλου ή άλλη πληροφορία έτσι ώστε να φιλτράρουμε την πληροφορία που παρουσιάζεται στο παράθυρο packet-listing (και επομένως στα παράθυρα packet-header και packet-contents). Στο παράδειγμα που ακολουθεί θα χρησιμοποιήσουμε το πεδίο packet display filter ώστε να κάνουμε το Wireshark να κρύψει (να μην παρουσιάσει) όλα τα πακέτα εκτός από εκείνα που αντιστοιχούν σε μηνύματα HTTP.

Δοκιμαστική εκτέλεση του Wireshark

Ο καλύτερος τρόπος για να εξοικειωθεί κανείς με ένα νέο κομμάτι λογισμικού είναι η δοκιμή. Υποθέτουμε ότι ο υπολογιστής σας συνδέεται στο Διαδίκτυο μέσω μίας ενσύρματης διεπαφής Ethernet. Ακολουθήστε τα παρακάτω βήματα:

1. Ξεκινήστε τον web browser της αρεσκείας σας, ο οποίος θα εμφανίσει την αρχική σελίδα που έχετε επιλέξει.

2. Ξεκινήστε το λογισμικό Wireshark. Θα δείτε αρχικά ένα παράθυρο παρόμοιο με αυτό του Σχήματος 2 με τη διαφορά ότι δε θα εμφανίζονται πακέτα στα παράθυρα packet-listing, packet-header, ή packet-contents, αφού το Wireshark δεν έχει αρχίσει ακόμη να συλλαμβάνει πακέτα.
3. Για να αρχίσει η σύλληψη πακέτων, επιλέξτε *Options* στο μενού Capture. Αυτό θα έχει ως αποτέλεσμα την εμφάνιση του παραθύρου "Wireshark: Capture Options" όπως φαίνεται στο Σχήμα 3.

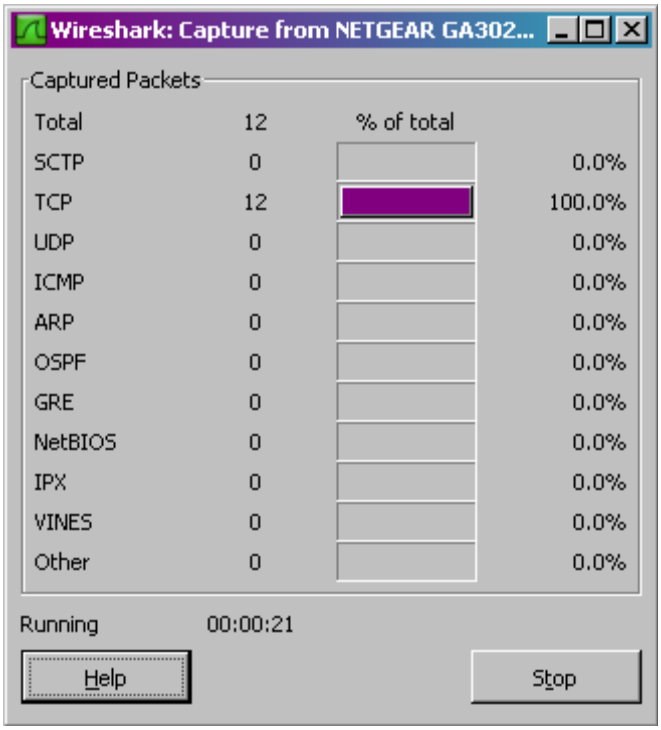


Σχήμα 3: Παράθυρο Capture Options του Wireshark

4. Μπορείτε να χρησιμοποιήσετε όλες τις προεπιλεγμένες τιμές αυτού του παραθύρου. Οι διεπαφές δικτύου (δηλαδή οι φυσικές συνδέσεις) του υπολογιστή σας με το δίκτυο θα εμφανίζονται στο μενού Interface στο επάνω μέρος του παραθύρου Capture Options. Σε περίπτωση που ο υπολογιστής σας έχει περισσότερες από μία ενεργές διεπαφές δικτύου (π.χ. εάν έχετε αμφότερες

μία ασύρματη και μία ενσύρματη σύνδεση Ethernet), θα χρειαστεί να επιλέξετε μία διεπαφή την οποία θα χρησιμοποιήσετε για να στέλνετε και να λαμβάνετε πακέτα (το πιθανότερο την ενσύρματη διεπαφή). Αφού επιλέξετε τη διεπαφή δικτύου (ή χρησιμοποιήσετε την προεπιλεγμένη διεπαφή που επιλέγει το Wireshark), κάντε κλικ στο Start. Στο σημείο αυτό αρχίζει η σύλληψη των πακέτων: όλα τα πακέτα που στέλνονται ή λαμβάνονται από τον υπολογιστή σας συλλαμβάνονται από το Wireshark.

5. Μόλις αρχίσει η σύλληψη πακέτων θα εμφανισθεί ένα παράθυρο περίληψης σύλληψης πακέτων (packet capture summary window) όπως φαίνεται στο Σχήμα 4. Το παράθυρο αυτό συνοψίζει τον αριθμό των διαφόρων ειδών πακέτων που συλλαμβάνονται και περιέχει το κουμπί *Stop* το οποίο θα σας επιτρέψει να διακόψετε τη σύλληψη πακέτων. Μην σταματήσετε τη σύλληψη πακέτων ακόμη.



Σχήμα 4: Παράθυρο Packet Capture του Wireshark

6. Ενώ το Wireshark τρέχει, εισάγετε το URL:
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
   ώστε ο browser να παρουσιάσει αυτήν την ιστοσελίδα. Για να παρουσιάσει αυτή τη σελίδα, ο browser σας θα επικοινωνήσει με τον HTTP server στο gaia.cs.umass.edu και θα ανταλλάξει μηνύματα HTTP με τον server όπως συζητήθηκε στην Ενότητα 2.2 του βιβλίου. Τα πλαίσια Ethernet που περιέχουν αυτά τα μηνύματα HTTP θα συλληφθούν από το Wireshark.
7. Αφού ο browser σας παρουσιάσει τη σελίδα INTRO-wireshark-file1.html, σταματήστε τη σύλληψη πακέτων επιλέγοντας stop στο παράθυρο capture του

Wireshark. Αυτό θα έχει ως αποτέλεσμα να εξαφανισθεί το παράθυρο capture του Wireshark και το κύριο παράθυρο του Wireshark να εμφανίζει όλα τα πακέτα που συνελήφθησαν από τότε που αρχίσατε τη σύλληψη πακέτων. Το κύριο παράθυρο του Wireshark θα πρέπει τώρα να μοιάζει με αυτό του Σχήματος 2. Έχετε τώρα στη διάθεσή σας "ζωντανά" δεδομένα πακέτων τα οποία περιέχουν όλα τα μηνύματα πρωτοκόλλων που ανταλλάχθηκαν μεταξύ του υπολογιστή σας και άλλων δικτυακών οντοτήτων. Οι ανταλλαγές μηνυμάτων HTTP με τον web server gaia.cs.umass.edu θα πρέπει να εμφανίζονται κάπου στον κατάλογο πακέτων που συνελήφθησαν. Όμως θα εμφανίζονται επίσης και πολλά άλλα είδη πακέτων (προσέξτε, για παράδειγμα, το μεγάλο αριθμό διαφορετικών ειδών πρωτοκόλλων που φαίνονται στη στήλη *Protocol* του Σχήματος 2). Αν και η μόνη δική σας ενέργεια ήταν να φορτώσετε μία ιστοσελίδα, προφανώς στον υπολογιστή σας έτρεχαν πολλά άλλα πρωτόκολλα χωρίς να τα αντιλαμβάνεται ο χρήστης. Θα μάθετε πολλά περισσότερα για τα πρωτόκολλα αυτά καθώς προχωρούμε στο βιβλίο.

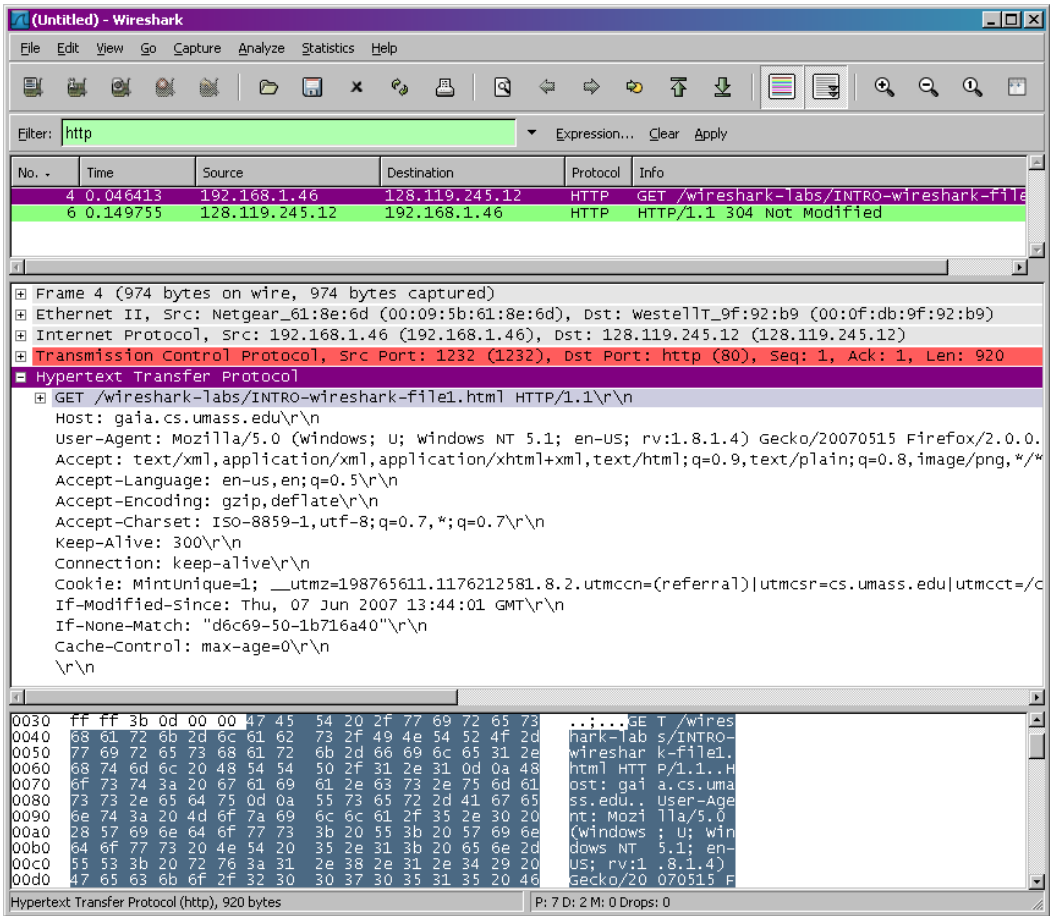
8. Πληκτρολογήστε "http" (χωρίς τα εισαγωγικά και με μικρά γράμματα - στο Wireshark όλα τα ονόματα πρωτοκόλλων είναι με μικρά γράμματα) στο παράθυρο προσδιορισμού του φίλτρου παρουσίασης, στο επάνω μέρος του κυρίου παραθύρου του Wireshark. Στη συνέχεια επιλέξτε *Apply* (δεξιά από εκεί όπου εισάγατε "http"). Αυτό θα έχει ως αποτέλεσμα στο παράθυρο packet-listing να εμφανίζονται μόνο τα μηνύματα HTTP.
9. Επιλέξτε το πρώτο μήνυμα HTTP που εμφανίζεται στο παράθυρο packet-listing. Αυτό θα πρέπει να είναι το μήνυμα HTTP GET το οποίο στάλθηκε από τον υπολογιστή σας στον HTTP server gaia.cs.umass.edu. Όταν επιλέξετε το μήνυμα HTTP GET, οι πληροφορίες για το πλαίσιο Ethernet, το IP datagram, το TCP segment και την επικεφαλίδα του μηνύματος HTTP θα εμφανισθούν στο παράθυρο packet header[2]. Κάνοντας κλικ στα κουτάκια με τα σύμβολα συν (+) και πλην (-) στην αριστερή πλευρά του παραθύρου packet-header details, *ελαχιστοποιείστε* την πληροφορία που εμφανίζεται για το πλαίσιο, το Ethernet, το πρωτόκολλο Internet και το πρωτόκολλο TCP. *Μεγιστοποιείστε* την πληροφορία που εμφανίζεται για το πρωτόκολλο HTTP. Το κύριο παράθυρο του Wireshark θα πρέπει τώρα να μοιάζει σε γενικές γραμμές με αυτό που φαίνεται στο Σχήμα 5. (Δώστε ιδιαίτερη προσοχή στο ελαχιστοποιημένο ποσό πληροφοριών πρωτοκόλλου για όλα τα πρωτόκολλα εκτός από το HTTP και το μεγιστοποιημένο ποσό πληροφοριών πρωτοκόλλου για το HTTP στο παράθυρο packet-header details.)
10. Έξοδος από το Wireshark

Στο σημείο αυτό έχετε ολοκληρώσει το πρώτο εργαστήριο.

Τι θα παραδώσετε

[2] Υπενθυμίζεται ότι το μήνυμα HTTP GET που στέλνεται στον web server gaia.cs.umass.edu περιέχεται μέσα σε ένα TCP segment, το οποίο περιέχεται μέσα σε ένα IP datagram, το οποίο είναι ενθυλακωμένο μέσα σε ένα πλαίσιο Ethernet.

Ο πρωταρχικός στόχος αυτού του πρώτου εργαστηρίου ήταν η εισαγωγή στο Wireshark. Οι ακόλουθες ερωτήσεις θα δείξουν ότι ήσασταν σε θέση να εγκαταστήσετε και να τρέξετε το Wireshark και ότι έχετε εξερευνήσει μερικές από τις δυνατότητές του. Βασιζόμενοι στον πειραματισμό σας με το Wireshark, απαντήστε στις ακόλουθες ερωτήσεις:



Σχήμα 5: Το παράθυρο του Wireshark μετά το βήμα 9

1. Αναφέρατε έως 10 διάφορα πρωτόκολλα που εμφανίζονται στη στήλη *Protocol* στο αφιλτράριστο παράθυρο packet-listing στο βήμα 7 παραπάνω.
2. Πόσος χρόνος πέρασε από τότε που στάλθηκε το μήνυμα HTTP GET μέχρι να ληφθεί η απόκριση HTTP OK; (Η τιμή της στήλης *Time* στο παράθυρο packet-listing είναι, εκ προεπιλογής, το χρονικό διάστημα από την έναρξη σύλληψης πακέτων σε δευτερόλεπτα. Για να δείτε το πεδίο Time με τη μορφή ώρα της ημέρας (time-of-day), επιλέξτε το μενού *View*, μετά επιλέξτε *Time Display Format* και μετά επιλέξτε *Time-of-day*.)
3. Ποια η διεύθυνση IP του gaia.cs.umass.edu (επίσης γνωστού ως www-net.cs.umass.edu); Ποια η διεύθυνση IP του υπολογιστή σας;

4. Εξάγετε τα δύο μηνύματα HTTP που απεικονίζονται στο βήμα 9 παραπάνω. Για να το κάνετε αυτό, επιλέξτε *Export Packet Disssections* από το menu εντολών *File* του Wireshark, επιλέξτε "*Selected Packet Only"* και *"As plain text"* και μετά κάντε κλικ στο OK.