Ανάλυση και έλεγχος δικτύου με χρήση του εργαλείου Wireshark

Version 1.01

Επιμέλεια Σημειώσεων: Πουλίζος Μίλτος
Τσεβάς Σπύρος
Πατρικάκης Χαράλαμπος

Πίνακας περιεχομένων

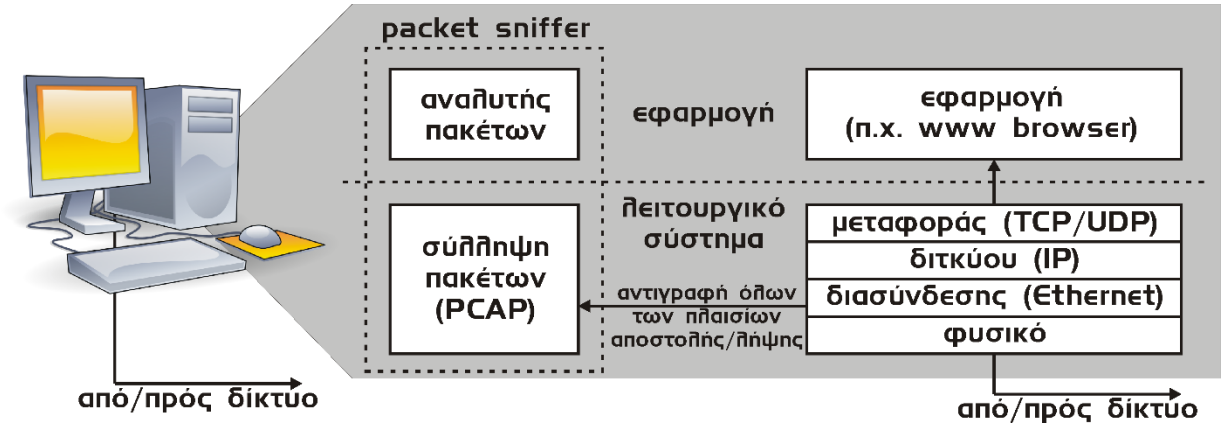
Εισαγωγικές έννοιες: ανίχνευση, σύλληψη και ανάλυση πακέτων

Η ανάλυση του δικτύου (network analysis ή traffic analysis ή protocol analysis ή packet analysis ή eavesdropping …) είναι η διαδικασία κατά την οποία αφού συλλαμβάνουμε (packet capture ή packet sniffing) όλα τα μηνύματα που κυκλοφορούν στο δίκτυο (την κυκλοφορία του δικτύου δηλαδή), την αναλύσουμε με σκοπό να αντιληφθούμε τι συμβαίνει στο δίκτυο ή να ορίσουμε κανόνες στη κυκλοφορία εντός του. Για το σκοπό αυτό χρησιμοποιούνται δύο εργαλεία:

1. Ένας ανιχνευτής πακέτων, ο οποίος αναλαμβάνει να διαβάσει και καταγράψει την πληροφορία η οποία διακινείται στο δίκτυο (όχι υποχρεωτικά από και προς τον υπολογιστή μας). Ο ανιχνευτής πακέτων, που ονομάζεται και sniffer, συνήθως έχει τη δυνατότητα να αποθηκεύει και να 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
2. Ένας αναλυτής πρωτοκόλλων, οποίος αναλαμβάνει να αποκωδικοποιήσει τα πακέτα δεδομένων που ανταλλάσσονται μεταξύ των γνωστών πρωτοκόλλων και να αποδίδει την κίνηση στο δίκτυο σε μια μορφή που είναι αναγνώσιμη.

Αν και τα δύο εργαλεία είναι διαφορετικά μεταξύ τους, συνήθως τα συναντάμε σε ένα ενιαίο πακέτο λογισμικού (γεγονός ο οποίο οδηγεί αρκετούς στο να αναφέρονται στα δύο εργαλεία συχνά ως ένα, το οποίο δεν είναι σωστό, μια και ένας sniffer μπορεί να εκτελεστεί ανεξάρτητα, δημιουργώντας ένα αρχείο κίνησης το οποίο να διοχετευθεί σε ένα διαφορετικό σύστημα για ανάλυση). Στη συνέχεια των σημειώσεων, και με δεδομένο ότι αναφερόμαστε στο wireshark το οποίο ενσωματώνει τις δυνατότητες και των δύο εργαλείων, οποιαδήποτε αναφορά σε ανιχνευτή ή αναλυτή πακέτων θα αναφέρεται σε έναν ολοκληρωμένο ανιχνευτή-αναλυτή.

Στο σχήμα που ακολουθεί φαίνεται η δομή ενός -ανιχνευτή – αναλυτή πακέτων.



Εικόνα 1: Σχεδιάγραμμα ενός ανιχνευτή-αναλυτή πακέτων

Στο προηγούμενο σχήμα βλέπουμε τη στοίβα πρωτοκόλλων TCP/IP, καθώς επίσης, και διάφορες συνήθεις δικτυακές εφαρμογές που εκτελούνται σε ένα υπολογιστή, όπως ένας πλοηγός ιστού ή πελάτης FTP. Ο ανιχνευτής πακέτων, που παριστάνεται με το διαγραμμισμένο πλαίσιο στο σχήμα, είναι μια προσθήκη στο λογισμικό του συστήματος όπου εκτελείται και αποτελείται από δύο τμήματα: α) την ανάλυσης πακέτων και β) τη βιβλιοθήκη σύλληψης πακέτων.

Η βιβλιοθήκη σύλληψης πακέτων λαμβάνει ένα αντίγραφο κάθε πλαισίου που στέλνεται ή λαμβάνεται από την κάρτα δικτύωσης. Τα πλαίσια αυτά ανήκουν στο επίπεδο ζεύξης δεδομένων του προτύπου OSI/TCP-IP και περιέχουν ενθυλακωμένα τα διάφορα μηνύματα που ανταλλάσσονται μεταξύ των πρωτοκόλλων ανώτερων στρωμάτων. Το παραπάνω σχήμα αφορά την περίπτωση του Ethernet όπου το φυσικό επίπεδο μετάδοσης των πλαισίων είναι το καλώδιο Ethernet. Αντίστοιχη είναι η περίπτωση ενός ασύρματου δικτύου, όπου το ρόλο του καλωδίου τον παίζει ο αέρας, αν και εδώ υπάρχουν κάποιες διαφορές και περιορισμοί. Το δεύτερο τμήμα του ανιχνευτή πακέτων, δηλαδή, ο αναλυτής πακέτων, εμφανίζει τα περιεχόμενα όλων των πεδίων που περιέχονται σε ένα μήνυμα. Για το σκοπό αυτό, πρέπει να γνωρίζει τη δομή των μηνυμάτων όλων των πρωτοκόλλων. Για παράδειγμα, στην περίπτωση ενός μηνύματος HTTP, απαιτείται, κατ' αρχήν, γνώση της δομής των πλαισίων Ethernet (Ethernet Frames), ώστε ο αναλυτής πρωτοκόλλων να είναι σε θέση να αναγνωρίσει το πακέτο IP (IP datagram) που έχει ενθυλακωθεί στο πλαίσιο Ethernet. Επιπλέον, δεδομένης της δομής ενός πακέτου IP, μπορεί να αναλυθεί το τεμάχιο TCP (TCP segment) που εμπεριέχεται μέσα στο IP. Ομοίως, η δομή του τεμαχίου TCP επιτρέπει την αποκωδικοποίηση του μηνύματος HTTP (HTTP message), ενώ περαιτέρω ανάλυση οδηγεί στο συγκεκριμένο τύπο του μηνύματος HTTP, δηλαδή HTTP GET, HTTP POST κ.ά.

Ο ανιχνευτής-αναλυτής πακέτων Wireshark

Στη συνέχεια θα προχωρήσουμε στην εισαγωγή στη χρήση του αναλυτή πρωτοκόλλων Wireshark του οποίου οι βασικές λειτουργίες είναι: (α) καταγραφή και σύλληψη (capture) καθώς και (β) ανάλυση της δικτυακής κίνησης του υπολογιστή. Το Wireshark αποτελεί εξέλιξη του ευρέως γνωστού sniffer Ethereal και διατίθεται ως ανοιχτό λογισμικό διαθέσιμο σε πληθώρα λειτουργικών συστημάτων. Η παρουσίαση συνοδεύεται από ερωτήσεις οι οποίες έχουν σκοπο να σας βοηθήσουν στην εξοικείωση με το εργαλείο.

Πληροφορίες για το πακέτο καθώς και τις πλέον ενημερωμένες εκδόσεις των απαραίτητων εκτελέσιμων αρχείων για εγκατάσταση στον υπολογιστή σας μπορείτε να τα βρείτε στο

http:/www.wireshark.org

και

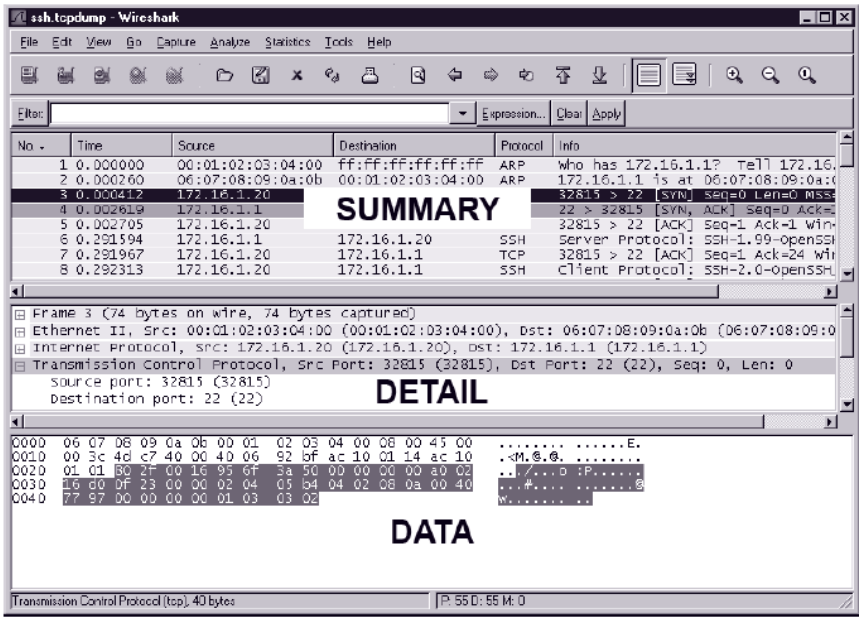
http://www.wireshark.org/download.html

Για να λειτουργήσει το Wireshark απαιτείται η ύπαρξη της βιβλιοθήκης σύλληψης πακέτων libpcap. Για τα συστήματα Windows η βιβλιοθήκη ονομάζεται WinPcap και εγκαθίσταται μαζί με το πρόγραμμα. Εναλλακτικά, μπορείτε να την κατεβάσετε από την ιστοσελίδα http://www.winpcap.org/. Περισσότερες πληροφορίες σχετικά με τον αναλυτή πρωτοκόλλων Wireshark μπορείτε να βρείτε στη σελίδα http://www.wireshark.org/docs/ όπου υπάρχουν σύνδεσμοι για το εγχειρίδιο χρήσης σε διάφορες μορφές (html, pdf, κλπ) καθώς και στην http://www.wireshark.org/faq.html για την περίπτωση που συναντήσετε δυσκολίες.

Στην παρακάτω εικόνα αποδίδεται η κεντρική οθόνη του sniffer, η οποία μπορεί να διαιρεθεί σε τρία τμήματα:

- **Summary**: εδώ συνοψίζεται η κίνηση του δικτύου σε μια λίστα καταγεγραμμένων πακέτων με συνοπτικές πληροφορίες για το καθένα όπως ο αύξων αριθμός τους, ημέρα (date) και ώρα (time) καταγραφής, διεύθυνση προέλευσης (source address), δ/νση προορισμού (destination address) καθώς και το όνομα του πρωτοκόλλου ανώτατου στρώματος (highest layer protocol) και οι σχετικές με αυτό πληροφορίες.

- **Detail**: Εδώ παρέχονται όλες οι σχετικές πληροφορίες (σε δενδροειδή δομή) με το πακέτο που μας ενδιαφέρει (λεπτομέρειες επικεφαλίδας – header details). Οι πληροφορίες εκτείνονται σε όλα τα επίπεδα (layers) τα οποία περιέχονται στο εκάστοτε πακέτο.
- **Data**: Εδώ εμφανίζονται τα αμιγή (raw) δεδομένα όπως αυτά συνελήφθηκαν (captured) σε δεκαεξαδική μορφή αλλά και ως κείμενο (ASCII).



Εικόνα 2: Παρουσίαση των κεντρικών οθονών χρήσης του wireshark

Επιπλέον, ακριβώς πάνω από το Summary και κάτω από το βασικό μενού, βρίσκεται το πεδίο όπου μπορούν να οριστούν τα φίλτρα ανάλυσης (packet display filter field). Στο πεδίο αυτό μπορούμε να εισάγουμε το όνομα ενός πρωτοκόλλου ή άλλη πληροφορία έτσι ώστε να φιλτράρουμε την πληροφορία που παρουσιάζεται στη λίστα του Summary (το wireshark μας δίνει επιπλέον τη δυνατότητα να ορίσουμε και το είδος των πακέτων που θα συλλαμβάνονται).

Τα φίλτρα που αναλαμβάνουν το φιλτράρισμα των πακέτων που έχουν ήδη καταγραφεί (display filters), ακολουθούν μια ειδική σύνταξη που επιτρέπει την ταξινόμηση των πακέτων με τον επιθυμητό, κάθε φορά, τρόπο. Το Wireshark υποστηρίζει πλειάδα πρωτοκόλλων καθώς και αντίστοιχων display filters τα οποία πληθαίνουν καθώς το πακέτο ωριμάζει και όλο και περισσότεροι χρήστες εμπλέκονται στην ανάπτυξη και τον εμπλουτισμό του. Στον πίνακα που ακολουθεί δίνονται παραδείγματα πρωτοκόλλων και των αντίστοιχων display filters.

Internet Protocol (IP) Field	Name	Type
ip.addr	Source or Destination Address	IPv4 address
ip.checksum	Header checksum	Unsigned 16-bit integer
ip.checksum_bad	Bad Header checksum	Boolean
ip.dsfield	Differentiated Services field	Unsigned 8-bit integer
ip.dsfield.ce	ECN-CE, Explicit Congestion Notification: Congestion Experienced	Unsigned 8-bit integer
ip.dsfield.dscp	Differentiated Services Codepoint	Unsigned 8-bit integer

ip.dsfield.ect	ECN-Capable Transport (ECT)	Unsigned 8-bit integer
ip.dst	Destination	IPv4 address
ip.flags	Flags	Unsigned 8-bit integer
ip.flags.df	Don't fragment	Boolean
ip.flags.mf	More fragments	Boolean
ip.frag_offset	Fragment offset	Unsigned 16-bit integer
ip.fragment	IP Fragment	Frame number
ip.fragment.error	Defragmentation error	Frame number
ip.fragment.multipletails	Multiple tail fragments found	Boolean
ip.fragment.overlap	Fragment overlap	Boolean
ip.fragment.overlap.conflict	Conflicting data in fragment overlap	Boolean
ip.fragment.toolongfragment	Fragment too long	Boolean
ip.fragments	IP fragments	No value
ip.hdr_len	Header length	Unsigned 8-bit integer
ip.id	Identification	Unsigned 16-bit integer
ip.len	Total length	Unsigned 16-bit integer
ip.proto	Protocol	Unsigned 8-bit integer
ip.reassembled_in	Reassembled IP in frame	Frame number
ip.src	Source	IPv4 address
ip.tos	Type of service	Unsigned 8-bit integer
ip.tos.cost	Cost	Boolean
ip.tos.delay	Delay	Boolean
ip.tos.precedence	Precedence	Unsigned 8-bit integer
ip.tos.reliability	Reliability	Boolean
ip.tos.throughput	Throughput	Boolean
ip.ttl	Time-to-live	Unsigned 8-bit integer
ip.version	Version	Unsigned 8-bit integer

Εικόνα 3: Παραδείγματα πρωτοκόλλων και display filters

Τα display filters μπορούν επίσης να χρησιμοποιηθούν για τη σύγκριση των πεδίων ενός πρωτοκόλλου με μια δεδομένη τιμή ή την τιμή ενός άλλου πεδίου. Όπως για παράδειγμα οι εντολές:

```
ip.src == 192.168.1.1
```

```
ip.src == ip.dst
```

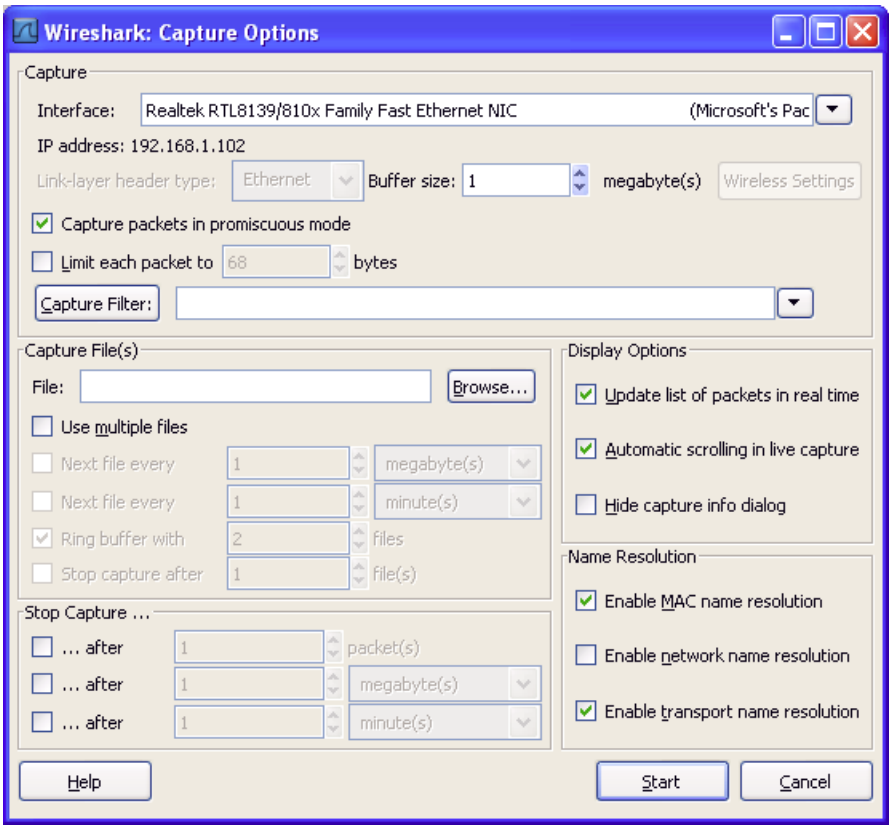
Η πρώτη εντολή αναλαμβάνει την προβολή στο πεδίο Summary εκείνων των πακέτων των οποίο η διεύθυνση προέλευσης είναι η 192.168.1.1, ενώ η δεύτερη προβάλλει τα πακέτα εκείνα για τα οποία η διεύθυνση προέλευσης ταυτίζεται με τη δ/νση αποστολής. Οι τελεστές σύγκρισης που χρησιμοποιούνται για το φιλτράρισμα είναι οι παρακάτω:

Ίσο	:	`eq`	ή	`==`
Διάφορο	:	`ne`	ή	`!=`
Μεγαλύτερο από	:	`gt`	ή	`>`
Μικρότερο από	:	`lt`	ή	`<`
Μεγαλύτερο ή ίσο	:	`ge`	ή	`>=`
Μικρότερο ή ίσο	:	`le`	ή	`<=`

Εξοικείωση με το περιβάλλον του Wireshark

Ως εισαγωγικό παράδειγμα πρόκειται να παρατηρήσετε την κίνηση που προκύπτει από την επίσκεψη σε μια ιστοσελίδα.

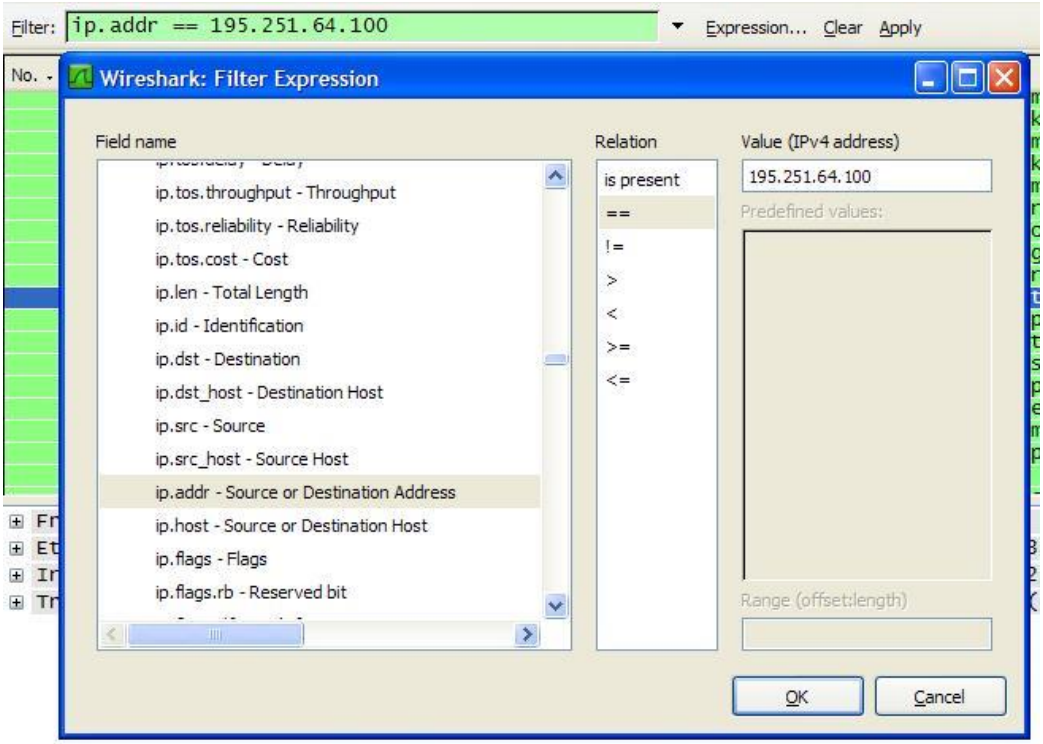
Αφού ξεκινήσετε το Wireshark, οι διάφορες επιλογές που αφορούν τη λειτουργία της καταγραφής ρυθμίζονται ακολουθώντας από το μενού επιλογών τη διαδρομή Capture → Options…. Στο παράθυρο που εμφανίζεται βεβαιωθείτε ότι στο πεδίο Interface αναφέρεται το όνομα της κάρτας δικτύου του υπολογιστή σας και επιπλέον ότι η επιλογή Enable network name resolution είναι ενεργοποιημένη. Το παράθυρο θα μοιάζει με αυτό της επόμενης εικόνας:



Εικόνα 4: Οθόνη επιλογών καταγραφής

Πατώντας το Start θα αρχίσει η σύλληψη των μηνυμάτων τα οποία θα εμφανίζονται στην οθόνη μας.

Ενώ το Wireshark είναι ενεργοποιημένο, επισκεφτείτε τη σελίδα http://www.teipir.gr και μόλις φορτωθεί πλήρως πατήστε το Stop ώστε να σταματήσει η καταγραφή. Ενδέχεται στο κύριο παράθυρο του Wireshark (Summary) να παρατηρήσετε κίνηση που να μη σχετίζεται με την ιστοσελίδα που φορτώσατε πριν από λίγο. Η ζητούμενη κίνηση μπορεί να απομονωθεί με την εφαρμογή φίλτρου παρατήρησης (display filter) ως εξής: Από την μπάρα εργαλείων Filter πατήστε το πλήκτρο Expression. Από το πεδίο Field Name βρείτε την επιλογή IP και αφού αναπτύξετε τις υποεπιλογές πατώντας το πλήκτρο + επιλέξτε `ip.addr – Source or Destination Address`. Στη συνέχεια από το πεδίο Relation επιλέξτε == , πληκτρολογήστε στο πεδίο Value(IPv4 address) `195.251.64.100` και πατήστε OK. Το πλήκτρο ενεργοποιείται πατώντας Apply. Η διαδικασία φαίνεται και στην επόμενη εικόνα:

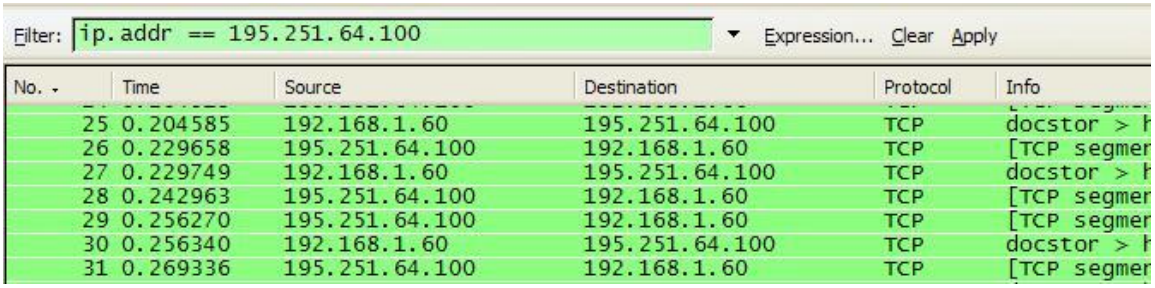


Εικόνα 5: Εφαρμογή φίλτρων παρατήρησης

Εναλλακτικά, θα μπορούσατε κατευθείαν να δώσετε την εντολή:

```
ip.addr == 195.251.64.100
```

στο πεδίο Filter και να πατήσετε Apply, όπως στην επόμενη εικόνα:



Εικόνα 6: Εφαρμογή φίλτρου παρατήρησης

Έπειτα από την παραπάνω διαδικασία, το πιθανότερο είναι να διαπιστώσετε ότι η κίνηση είναι ενδεχομένως περιορισμένη σε σχέση με την παρατήρηση χωρίς φίλτρο. Στη λίστα των καταγεγραμμένων πακέτων, και κάτω από την επικεφαλίδα Protocol, εμφανίζεται το εκάστοτε πρωτόκολλο υψηλότερου στρώματος που περιέχει το πλαίσιο. Επιλέξτε το πρώτο μήνυμα HTTP που εμφανίζεται. Αυτό θα είναι και το πρώτο μήνυμα `HTTP GET` που έστειλε ο υπολογιστής σας στον HTTP server (εξυπηρετητή) του ΤΕΙ για να κατεβάσει τη σελίδα, και την αντίστοιχη απόκριση HTTP του εξυπηρετητή. Εναλλακτικά μπορείτε να απομονώσετε τα HTTP μηνύματα πληκτρολογώντας στο πεδίο filter: `HTTP` και πατώντας Apply. 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 εμφανιστούν στο παράθυρο των Details. Κλείστε τις λεπτομέρειες στα παράθυρο Details (να είναι όλα + και όχι –) ώστε να φαίνονται οι επικεφαλίδες όλων των πρωτοκόλλων (Ethernet, IP, TCP).

Ερώτηση 1: Καταγράψτε τις προαναφερόμενες επικεφαλίδες όπως εμφανίζονται στην οθόνη.

Ερώτηση 2: Κάνοντας διπλό κλικ στη γραμμή Frame του παραθύρου λεπτομερειών μπορείτε να δείτε στο πεδίο `Protocols in frame` όλα τα πρωτόκολλα που περιλαμβάνει το πλαίσιο καθώς και τη σειρά ενθυλάκωσής τους στο πλαίσιο Ethernet. Αναφέρατε το επίπεδο στο οποίο ανήκει το κάθε ένα σύμφωνα με το πρότυπο OSI.

Στη συνέχεια αφού τακτοποιήσετε τα πλαίσια σε αύξουσα αριθμητική σειρά (κάνοντας κλικ στην επικεφαλίδα No του παραθύρου με τη λίστα καταγεγραμμένων πακέτων (Summary)). Κατόπιν επιλέξτε το πρώτο πλαίσιο που περιέχει τεμάχιο TCP και επιλέξτε Follow TCP stream. Στην οθόνη που θα εμφανισθεί βλέπετε το περιεχόμενο της συγκεκριμένης ροής TCP, δηλαδή, την ανταλλαγή μηνυμάτων μεταξύ του πλοηγού (browser) και του εξυπηρετητή ιστού (server) . Τα μηνύματα (εντολές) του πλοηγού εμφανίζονται με ροζ γράμματα (πρώτο μπλοκ δεδομένων), ενώ τα μηνύματα (αποκρίσεις) του εξυπηρετητή εμφανίζονται με γαλάζια γράμματα (δεύτερο μπλοκ δεδομένων), όπως στο ακόλουθο παράδειγμα:

```
GET / HTTP/1.1
Host: www.in.gr
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.3) Gecko/20070309
Firefox/2.0.0.3
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
X-Powered-By: ASP.NET
Content-Location: http://www.in.gr/default_rendered.htm
Set-Cookie: SITESERVER=ID=ac7cdc2854e2a76030ded808986d9029; expires=Monday, 01-Jan-2035
00:00:00 GMT; path=/
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Date: Tue, 17 Apr 2007 19:27:12 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 17 Apr 2007 19:25:02 GMT
ETag: "ccce4182681c71:8d6"
Content-Length: 44876
```

Εικόνα 7: Παρακολούθηση TCP stream

Ερώτηση 3: Με βάση τα αποτελέσματα της προηγούμενης καταγραφής, βρείτε (α) τον τύπο του server που φιλοξενεί τη σελίδα που επισκεφτήκατε και (β) την ακριβή έκδοση του browser που χρησιμοποιήσατε.

Ερώτηση 4: Ποιά είναι η σύνταξη του φίλτρου που εμφανίζεται τώρα στο κεντρικό παράθυρο; Περιγράψτε τη με λόγια.