Πρωτόκολλα και επικοινωνίες δικτύων
Εργαστήριο 1

Τμήμα Πληροφορικής και τηλεπικοινωνιών
Πανεπιστήμιο Ιωαννίνων, Άρτα

2023-03-01

Περιεχόμενα

1 Εισαγωγή

1.1 Εισαγωγικές έννοιες

Διευθύνσεις IP: Σχεδιάστηκαν για να επικοινωνούν οι συσκευές μεταξύ τους σε ένα τοπικό δίκτυο ή μέσω του Διαδικτύου. Χρησιμοποιούνται για την αναγνώριση του κεντρικού υπολογιστή ή της διεπαφής δικτύου. Παρέχουν τη θέση του κεντρικού υπολογιστή και την ικανότητα δημιουργίας της διαδρομής προς τον κεντρικό υπολογιστή στο εν λόγω δίκτυο. **Πρωτόκολλο Διαδικτύου** είναι το σύνολο των προκαθορισμένων κανόνων ή όρων βάσει των οποίων πρέπει να διεξάγεται η επικοινωνία. Οι τύποι διευθύνσεων IP είναι οι IPv4 και IPv6.

- Το IPv4 είναι μια διεύθυνση 32 bit στην οποία κάθε ομάδα αντιπροσωπεύει 8 bit που κυμαίνονται από 0 έως 255.
- Η διεύθυνση IPv6 είναι 128-bit.

Οι διευθύνσεις IP εκχωρούνται στον κεντρικό υπολογιστή είτε δυναμικά είτε με στατική διεύθυνση IP. Οι περισσότεροι από τους ιδιώτες χρήστες έχουν δυναμική διεύθυνση IP, ενώ οι επιχειρηματικοί χρήστες ή οι διακομιστές έχουν στατική διεύθυνση IP. Η δυναμική διεύθυνση αλλάζει κάθε φορά που η συσκευή συνδέεται στο Διαδίκτυο.

Θύρες υπολογιστή: Οι θύρες υπολογιστή λειτουργούν σε συνδυασμό με τη διεύθυνση IP κατευθύνοντας όλα τα εξερχόμενα και εισερχόμενα πακέτα στις κατάλληλες θέσεις. Υπάρχουν γνωστές θύρες με τις οποίες μπορείτε να συνεργαστείτε, όπως το FTP (File Transfer Protocol), το οποίο έχει θύρα με αριθμό 21, κ.λπ. Όλες οι θύρες έχουν σκοπό να κατευθύνουν όλα τα πακέτα προς την προκαθορισμένη κατεύθυνση.

Πρωτόκολλο: Το πρωτόκολλο είναι ένα σύνολο προκαθορισμένων κανόνων. Θεωρούνται ως ο τυποποιημένος τρόπος επικοινωνίας. Ένα από τα πλέον χρησιμοποιούμενα πρωτόκολλα είναι το TCP/IP. Σημαίνει Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου.

Μοντέλο OSI: Το μοντέλο OSI σημαίνει Open System Interconnect (Διασύνδεση ανοικτών συστημάτων). Το μοντέλο OSI έχει επτά επίπεδα, δηλαδή, επίπεδο εφαρμογής, επίπεδο παρουσίασης, επίπεδο συνόδου, επίπεδο μεταφοράς, επίπεδο δικτύου, επίπεδο σύνδεσης δεδομένων και το φυσικό επίπεδο. Το μοντέλο OSI παρέχει μια λεπτομερή αναπαράσταση και επεξήγηση της μετάδοσης και λήψης δεδομένων μέσω των επιπέδων. Το μοντέλο OSI υποστηρίζει τόσο τον τρόπο επικοινωνίας χωρίς σύνδεση όσο και τον τρόπο επικοινωνίας με προσανατολισμό στη σύνδεση μέσω του στρώματος δικτύου. Το μοντέλο OSI αναπτύχθηκε από τον ISO (Διεθνής Οργανισμός Τυποποίησης).

1.2 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:

- 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.
- 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.

1.3 Ανιχνευτής Πακέτων

Ο **packet sniffer (ανιχνευτής πακέτων)** αποτελεί το βασικό εργαλείο για την παρατήρηση των μηνυμάτων που ανταλλάσσονται μεταξύ των εκτελούμενων οντοτήτων πρωτοκόλλων. Συγκεκριμένα:

- Όπως υπονοεί και το όνομα, ο packet sniffer συλλαμβάνει ("sniffs") τα μηνύματα τα οποία στέλνονται ή λαμβάνονται από τον υπολογιστή μας.
- Συνήθως, ο packet sniffer αποθηκεύει και απεικονίζει τα περιεχόμενα διαφόρων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνονται.
- Ενώ αυτός παραμένει παθητικός.
- Δεν στέλνει ποτέ πακέτα αλλά παρατηρεί τα μηνύματα που στέλνονται και λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που τρέχουν στον υπολογιστή μας.
- Τα πακέτα που λαμβάνονται 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.
- Οι packet sniffers μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, συμπεριλαμβανομένης της δικτυακής αντιμετώπισης προβλημάτων(network troubleshooting), την ανάλυση ασφάλειας και βελτιστοποίηση επιδόσεων.

1.4 Αναλυτής πακέτων

Ο **αναλυτής πακέτων (packet analyzer)** είναι ένα εργαλείο που χρησιμοποιείται για την ανάλυση των συλλεχθέντων πακέτων(captured packets) και την παροχή πληροφοριών σχετικά με την κυκλοφορία του δικτύου(network traffic). Συγκεκριμένα:

- Εμφανίζει τα περιεχόμενα όλων των πεδίων που περιέχονται σε ένα μήνυμα.
- Για τον σκοπό αυτό, πρέπει να γνωρίζει τη δομή των μηνυμάτων όλων των πρωτοκόλλων.
  - Π.χ., στην περίπτωση ενός μηνύματος HTTP, απαιτείται, κατ' αρχήν, γνώση της δομής των πλαισίων Ethernet.
  - Ώστε ο αναλυτής πρωτοκόλλων να είναι σε θέση να αναγνωρίσει το πακέτο IP που έχει ενθυλακωθεί στο πλαίσιο Ethernet.
- Επιπλέον, δεδομένης της δομής ενός πακέτου IP, μπορεί να αναλυθεί το τμήμα (segment) TCP που εμπεριέχεται μέσα στο IP.
- Ομοίως, η δομή του τμήματος TCP επιτρέπει την αποκωδικοποίηση του μηνύματος HTTP, ενώ περαιτέρω ανάλυση οδηγεί στο συγκεκριμένο τύπο του μηνύματος HTTP.

Για παράδειγμα, έστω ότι ενδιαφερόμαστε να απεικονίσουμε τα διάφορα πεδία των μηνυμάτων που ανταλλάσσονται από το πρωτόκολλο HTTP σε ένα δίκτυο Ethernet. Ο αναλυτής πακέτων καταλαβαίνει τα πλαίσια Ethernet με αποτέλεσμα να 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. Έτσι, γνωρίζει ότι τα πρώτα bytes ενός μηνύματος HTTP θα περιέχουν τις ακολουθίες χαρακτήρων "GET", "POST", κ.ά..

2 Πρόγραμμα ανάλυσης Πρωτοκόλλων Wireshark

Πρόκειται για πρόγραμμα ανάλυσης πρωτοκόλλων του οποίου οι βασικές λειτουργίες είναι **η Καταγραφή – σύλληψη (capture) πακέτων** και **η Ανάλυση της δικτυακής κίνησης του υπολογιστή**. Το πρόγραμμα Wireshark διατίθεται ως ανοικτό λογισμικό(www.wireshark.org) για πληθώρα λειτουργικών συστημάτων. Η βασική του λειτουργία έγκειται στη σύλληψη των μηνυμάτων που στέλνονται ή λαμβάνονται από την κάρτα δικτύωσης και παρέχει τη δυνατότητα να απεικονίσουμε τα περιεχόμενα των μηνυμάτων, που στέλνονται ή λαμβάνονται από τα πρωτόκολλα σε διαφορετικά επίπεδα της στοίβας πρωτοκόλλων. Επίσης Είναι πλούσιος σε λειτουργίες που περιλαμβάνουν τη ικανότητα να αναλύει περισσότερα από 500 πρωτόκολλα και έχει μία καλά σχεδιασμένη διεπαφή χρήστη (user interface).

2.1 Εγκατάσταση του Wireshark

Αρχικά κατεβάστε το πρόγραμμα εγκατάστασης από το download. Για να εγκαταστήσετε και να χρησιμοποιήσετε το Wireshark στα Windows, δεν χρειάζεστε εξωτερικές βιβλιοθήκες, επειδή το πακέτο εγκατάστασης περιλαμβάνει όλες τις απαιτούμενες βιβλιοθήκες. Ωστόσο, κατά τη διάρκεια της διαδικασίας εγκατάστασης, το πρόγραμμα εγκατάστασης του Wireshark ενδέχεται να σας ζητήσει να εγκαταστήσετε πρόσθετο λογισμικό ή προγράμματα οδήγησης, όπως το WinPcap ή το Npcap, τα οποία απαιτούνται για τη λήψη της δικτυακής κίνησης στα Windows. Αυτά τα προγράμματα είναι απαραίτητα για να μπορέσει το Wireshark να συλλάβει και να αναλύσει την κυκλοφορία δικτύου στο μηχάνημα με Windows. Το WinPcap και το Npcap είναι και τα δύο βιβλιοθήκες σύλληψης πακέτων που επιτρέπουν στο Wireshark να συλλαμβάνει την κυκλοφορία δικτύου. Το WinPcap είναι μια παλαιότερη βιβλιοθήκη που δεν συντηρείται πλέον, ενώ το Npcap είναι μια νεότερη και πιο ενεργά αναπτυγμένη βιβλιοθήκη που συνιστάται για τις νεότερες εκδόσεις των Windows. Εάν χρησιμοποιείτε Windows 10, συνιστάται η εγκατάσταση του Npcap, το οποίο περιλαμβάνεται στο πακέτο εγκατάστασης του Wireshark από προεπιλογή. Εάν χρησιμοποιείτε παλαιότερη έκδοση των Windows, όπως τα Windows 7 ή τα Windows 8, ενδέχεται να χρειαστεί να εγκαταστήσετε ξεχωριστά το WinPcap πριν από την εγκατάσταση του Wireshark. Αναλυτικές οδηγίες εγκατάστασης μπορείτε να βρείτε στο instructions.

Αν η εγκατάσταση έχει ολοκληρωθεί σωστά θα πρέπει να εμφανίζεται το παράθυρο της εικόνας 1.

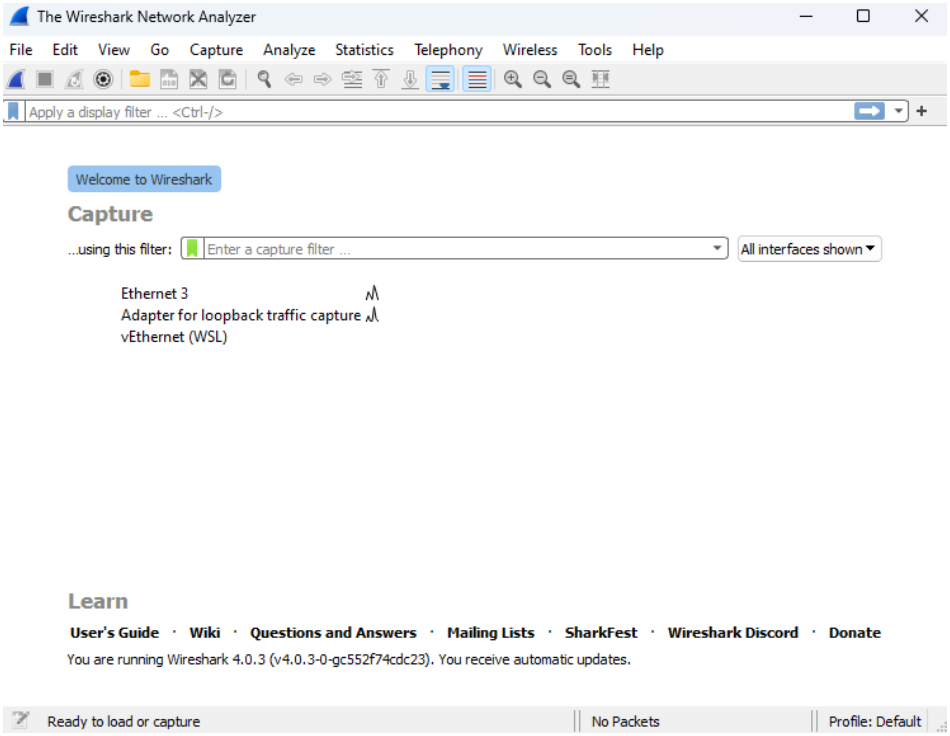


Figure 1: Διεπαφή Wireshark

2.2 Μενού Capture

Το μενού Capture στο Wireshark(Εικόνα 2) χρησιμοποιείται για τη σύλληψη της δικτυακής κίνησης και την επιλογή των κατάλληλων επιλογών σύλληψης. Αποτελεί βασικό μέρος του Wireshark και παρέχει διάφορες επιλογές για τη λήψη και την ανάλυση της δικτυακής κίνησης. Χρησιμοποιώντας το μενού καταγραφής, οι διαχειριστές δικτύων(network managers) και οι επαγγελματίες ασφαλείας(security experts) μπορούν να επιλύουν προβλήματα δικτύου, να εντοπίζουν απειλές ασφαλείας και να βελτιστοποιούν την απόδοση του δικτύου. Το μενού Capture παρέχει διάφορες επιλογές για την έναρξη, τη διακοπή και τη διαχείριση των συλλήψεων πακέτων. **Ορισμένες από τις λειτουργίες του μενού είναι:**

- **Start:** Αυτή η επιλογή ξεκινά τη διαδικασία καταγραφής, επιτρέποντάς σας να καταγράψετε και να αναλύσετε την κυκλοφορία του δικτύου.
- **Stop:** Αυτή η επιλογή σταματά τη διαδικασία καταγραφής πακέτων, επιτρέποντάς σας να αποθηκεύσετε και να αναλύσετε τα καταγεγραμμένα πακέτα.
- **Options:** Αυτή η επιλογή ανοίγει το παράθυρο διαλόγου επιλογών σύλληψης, το οποίο σας επιτρέπει να διαμορφώσετε τις ρυθμίσεις σύλληψης, όπως η διασύνδεση από την οποία θα γίνει η σύλληψη, το φίλτρο σύλληψης και η μορφή εξόδου αρχείου.
- **Interfaces:** Αυτή η επιλογή εμφανίζει μια λίστα με τις διαθέσιμες διασυνδέσεις δικτύου στο σύστημά σας από τις οποίες μπορείτε να συλλάβετε πακέτα.
- **Capture Filters:** Αυτή η επιλογή εμφανίζει μια λίστα με φίλτρα σύλληψης που μπορείτε να χρησιμοποιήσετε για να περιορίσετε τα πακέτα που συλλαμβάνονται μόνο σε εκείνα που πληρούν συγκεκριμένα κριτήρια, όπως η διεύθυνση IP πηγής ή προορισμού ή ο αριθμός θύρας.
- **Display Filters:** Αυτή η επιλογή ανοίγει το παράθυρο διαλόγου φίλτρων εμφάνισης, το οποίο σας επιτρέπει να φιλτράρετε και να εμφανίζετε μόνο τα πακέτα που ανταποκρίνονται σε συγκεκριμένα κριτήρια, όπως πρωτόκολλο, διεύθυνση IP πηγής ή προορισμού ή περιεχόμενο πακέτου.

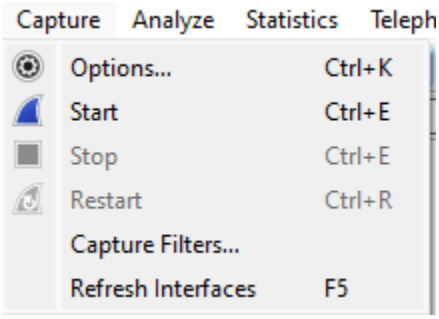


Figure 2: Μενού Capture στο wireshark

Πραγματοποιώντας εκκίνηση σύλληψης πακέτων από το μενού Capture, εμφανίζεται το παράθυρο με τη λίστα καταγεγραμμένων πακέτων (packet-listing window) και περιληπτικές πληροφορίες για το καθένα όπως:

- Τον αύξοντα αριθμό πλαισίου κατά την καταγραφή.
- Την διεύθυνση αποστολέα(Source)
- Την διεύθυνση παραλήπτη(Destination)
- Τον χρόνο σύλληψης του πακέτου(Time)
- Το είδος του πρωτοκόλλου(Protocol)
- Πληροφορία σχετική με το πρωτόκολλο η οποία περιέχεται στο πακέτο(Info)

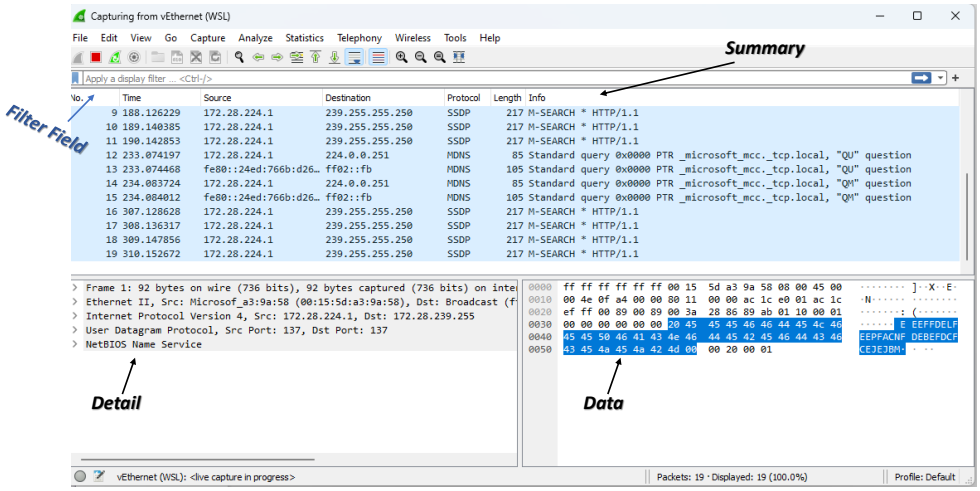


Figure 3: Κεντρική οθόνη sniffer

Στην εικόνα 3 παρουσιάζεται η κεντρική οθόνη του sniffer, η οποία μπορεί να διαιρεθεί σε τρία τμήματα:

- **Summary:** Σε αυτό το πεδίο 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:** Σε αυτό το πεδίο, 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:** Σε αυτό το πεδίο εμφανίζονται τα αμιγή (raw) δεδομένα όπως αυτά συνελήφθηκαν (captured) σε δεκαεξαδική μορφή αλλά και ως κείμενο (ASCII).

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).

2.3 Φίλτρα στο Wireshark

Τα φίλτρα χρησιμοποιούνται για την εμφάνιση πακετών που ικανοποιούν συγκεκριμένα κριτήρια. Στον πίνακα 1, παρουσιάζονται τα display filters ανά πρωτόκολλο.

Internet Protocol Field	Name	Type
ip.addr	Source or Destination Address	IPv4
ip.checksum	Header Checksum	Unsigned 16-bit Integer Boolean
ip.checksum_bad	Bad Header checksum	Boolean
ip.dsfield	ECN-CE	Unsigned 8-bit Integer
ip.dsfield.dscp	Differentianed 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.overleap	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	Reassembled IP in a frame	Frame number
ip.src	Source	IPv4
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

Table 1: Display Filters

Οι τελεστές σύγκρισης που μπορούν να χρησιμοποιηθούν στο πεδίο φιλτραρίσματος παρουσιάζονται στο πίνακα 2.

Operator	Mean
eq ή ==	Ίσο
ne ή !=	Διάφορο
gt ή >	Μεγαλύτερο από
lt ή <	Μικρότερο από
ge ή ≥	Μεγαλύτερο ή ίσο
le ή ≤	Μικρότερο ή ίσο

Table 2: Τελεστές φίλτρων

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. Στην εικόνα 4 παρουσιάζεται το παράθυρο που θα εμφανιστεί για να ρυθμίσετε τις επιλογές φίλτρων.

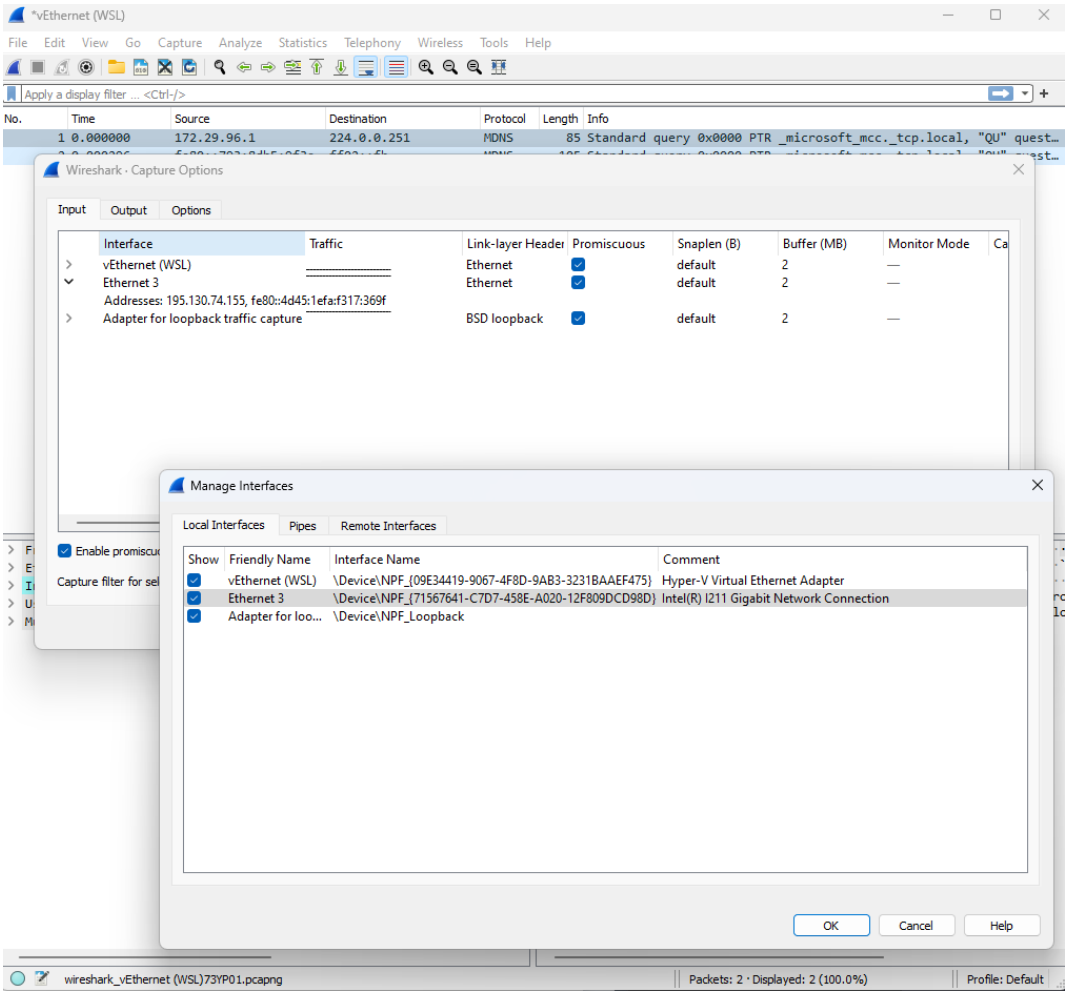


Figure 4: Capture options

2.4 Κανόνες χρωματισμού

Ενώ τα φίλτρα σύλληψης και εμφάνισης του Wireshark περιορίζουν τα πακέτα που καταγράφονται ή εμφανίζονται στην οθόνη, η λειτουργία χρωματισμού του πηγαίνει τα πράγματα ένα βήμα παραπέρα: Μπορεί να διακρίνει μεταξύ διαφορετικών τύπων πακέτων με βάση την απόχρωσή τους. Έτσι, εντοπίζονται γρήγορα ορισμένα πακέτα μέσα σε ένα αποθηκευμένο σύνολο με βάση το χρώμα της γραμμής τους στο παράθυρο λίστας πακέτων. Το Wireshark έρχεται με περίπου 20 προεπιλεγμένους κανόνες χρωματισμού, ο καθένας από τους οποίους μπορεί να επεξεργαστεί, να απενεργοποιηθεί ή να διαγραφεί. Επιλέξτε **View → Coloring Rules** χρωματισμού για μια επισκόπηση του τι σημαίνει κάθε χρώμα. Μπορείτε επίσης να προσθέσετε τα δικά σας φίλτρα με βάση το χρώμα.

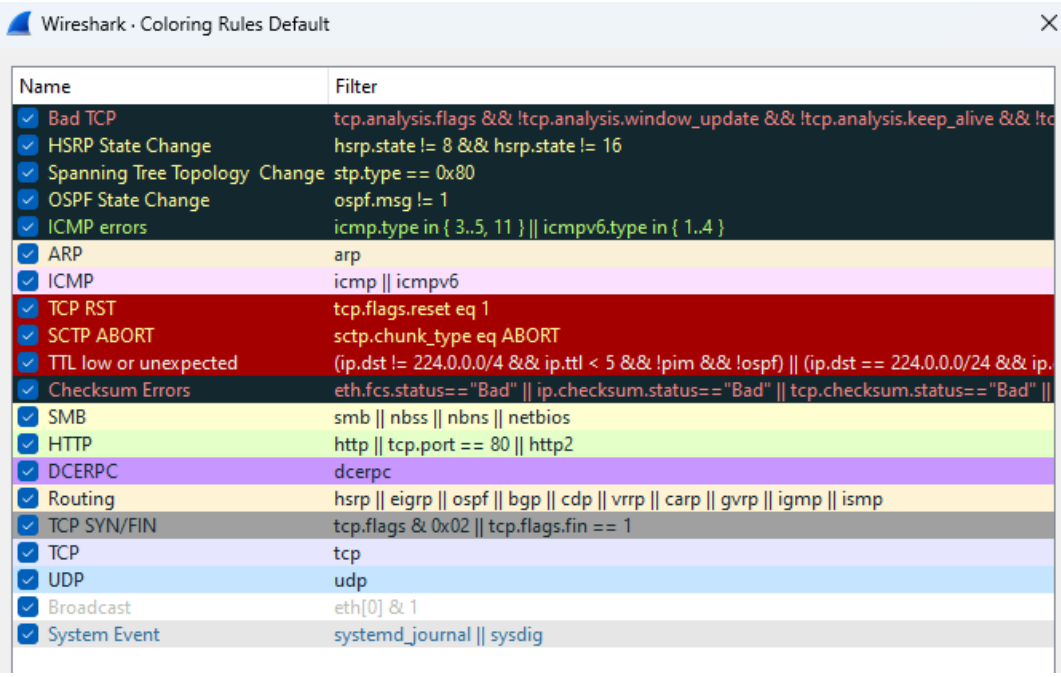
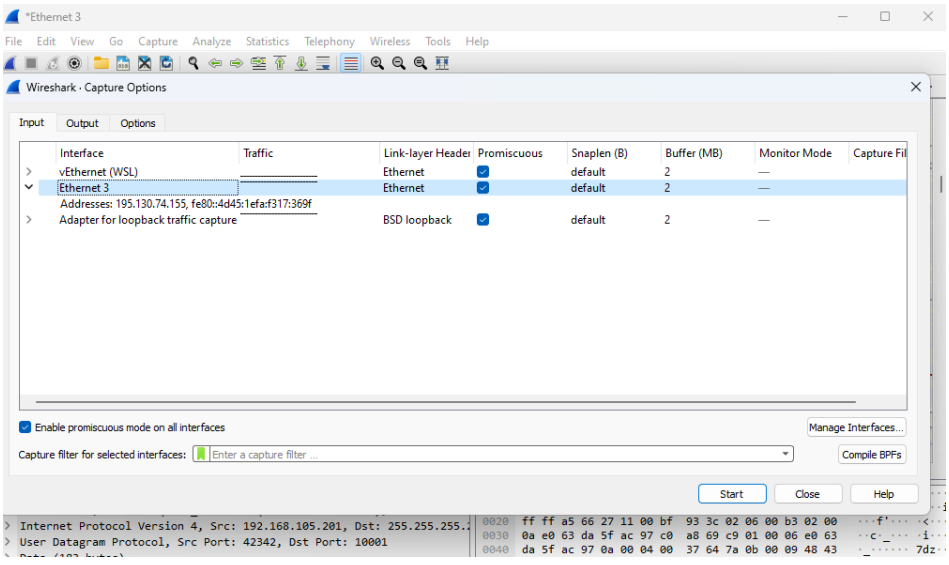


Figure 5: Wireshark-κανόνες χρωματισμού

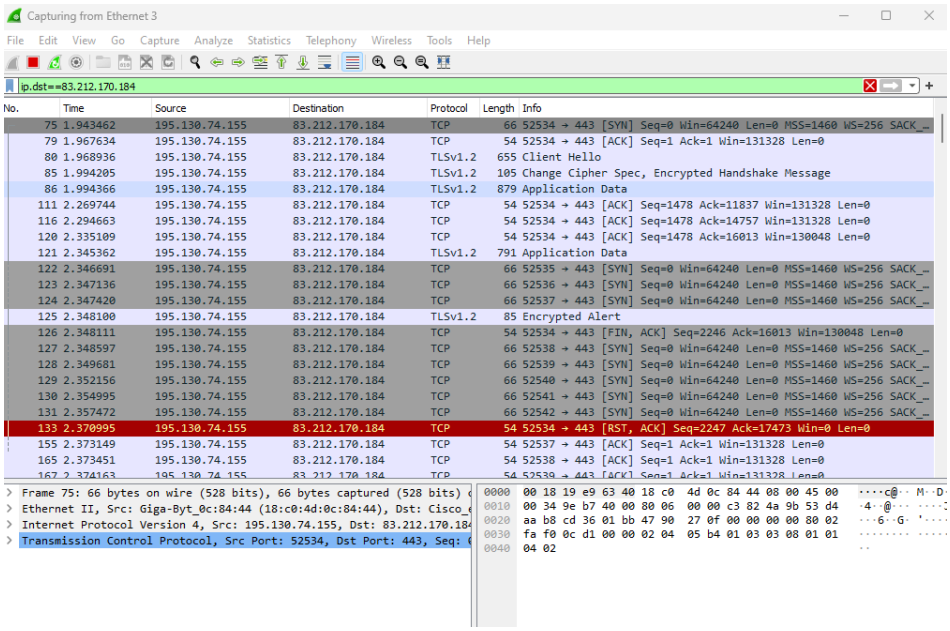
3 Παραδείγματα

1. Ως πρώτο εισαγωγικό παράδειγμα πρόκειται να παρατηρήσετε την κίνηση που προκύπτει από την επίσκεψη του τμήματος πληρεοφορικής και τηλεπικοινωνιών. Για να εκτελέσετε το παράγειγμα πραγματοποιήστε τα εξής βήματα:

   - Επιλέξτε capture→Capture Options και βεβαιωθείται ότι έχει επιλεγεί το κατάλληλο interface(Εικόνα 1).



   - Στο πεδίο εισαγωγής φίλτρων πληκτρολογίστε το query που παρουσιάζεται στην εικόνα(Filter:**ip.dst**==83.212.170.184) και εισάγεται το φίλτρο στον αναλυτή.
   - Επισκεφτείτε την ιστοσελίδα του τμήματος https://www.dit.uoi.gr/(Εικόνα 1).



- Διακόψετε την ανάλυση επιλέγοντας **Capture** → **Stop**. Στην συνέχεια επιλέξτε **Statistics**→**Capture** File Properties και δείτε τα αντίστοιχα στατιστικά.

Details

File

Name:	C:\Users\VASILE~1\AppData\Local\Temp\wireshark_Ethernet 3A01Z01.pcapng
Length:	10 MB
Hash (SHA256):	96504136f45fe71bb153540b494871411b9f38d10ff4707e07362042911c7691
Hash (RIPEMD160):	2cd88791fc0f6fe8831f263a59d2d64a75e2e640
Hash (SHA1):	13948be2b79ba932443731ebf8df20af9ba0960d
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2023-02-28 13:06:36
Last packet:	2023-02-28 13:14:55
Elapsed:	00:08:18

Capture

Hardware:	AMD Ryzen 7 5700G with Radeon Graphics (with SSE4.2)
OS:	64-bit Windows (22H2), build 22621
Application:	Dumpcap (Wireshark) 4.0.3 (v4.0.3-0-gc552f74cdc23)

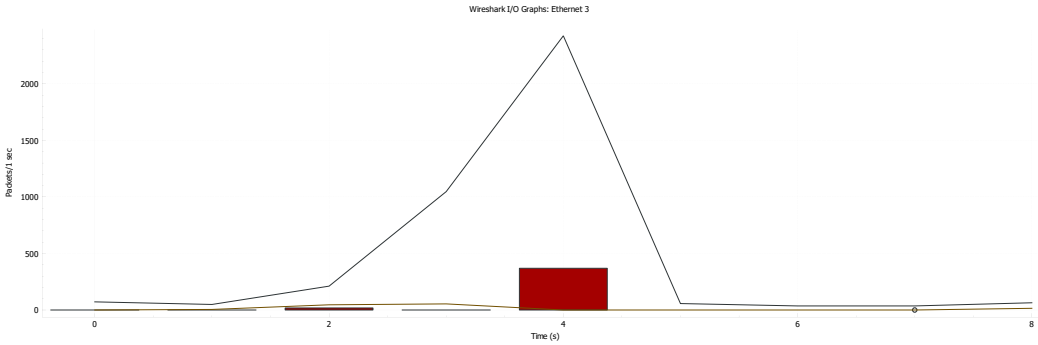
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet 3	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	31143	129 (0.4%)	—
Time span, s	498.743	7.325	—
Average pps	62.4	17.6	—
Average packet size, B	306	380	—
Bytes	9542725	48991 (0.5%)	0
Average bytes/s	19 k	6688	—
Average bits/s	153 k	53 k	—

- Τέλος επιλέγοντας από το μενού Statistics → I/O Graph εμφανίστε το ακόλουθο γράφημα



4 Appendix

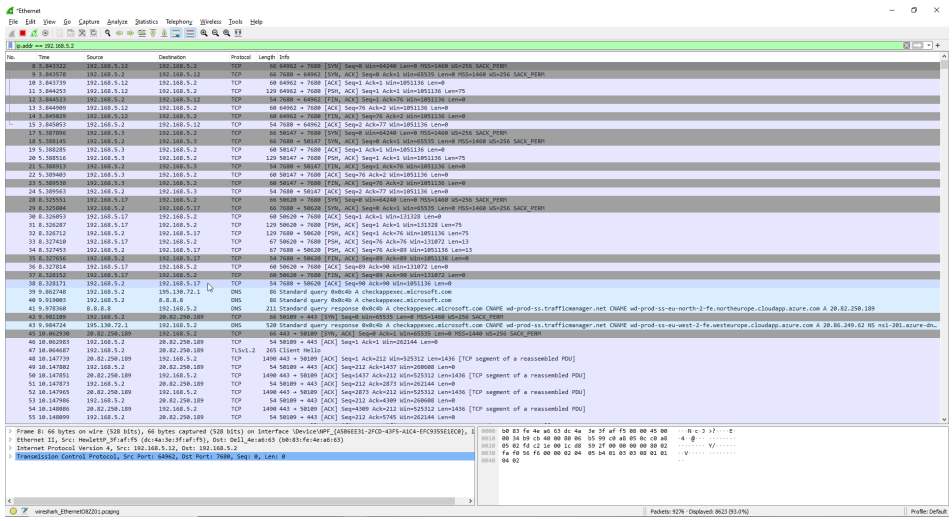


Figure 6: Παράδειγμα εκτέλεσης ip.addr

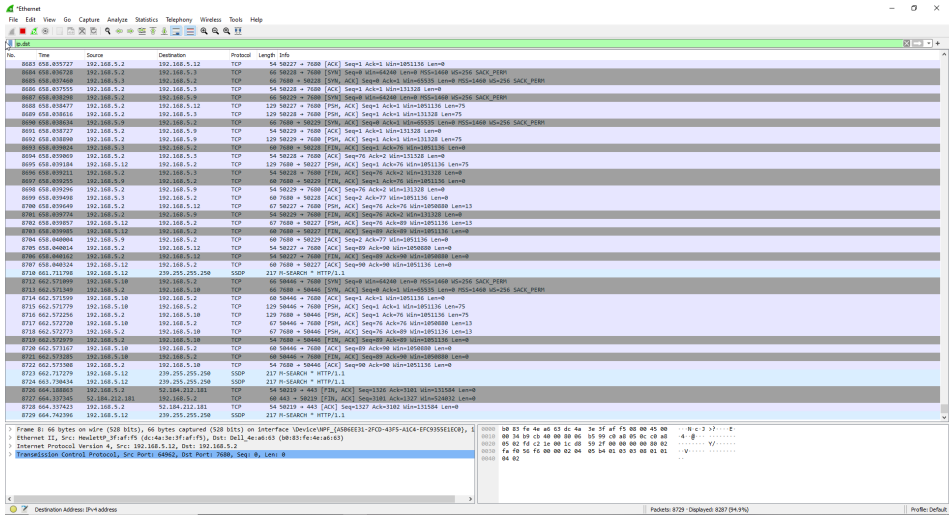


Figure 7: Παράδειγμα εκτέλεσης ip.dst

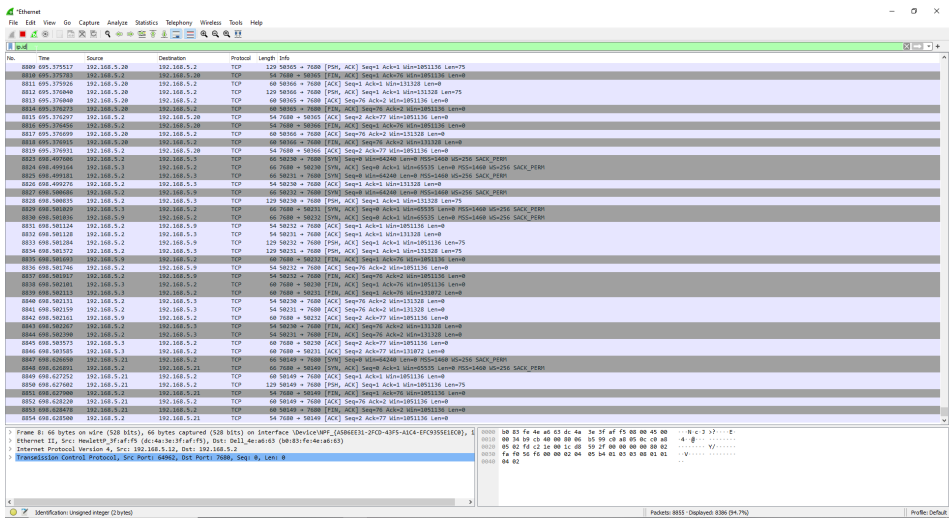


Figure 8: Παράδειγμα εκτέλεσης ip.id

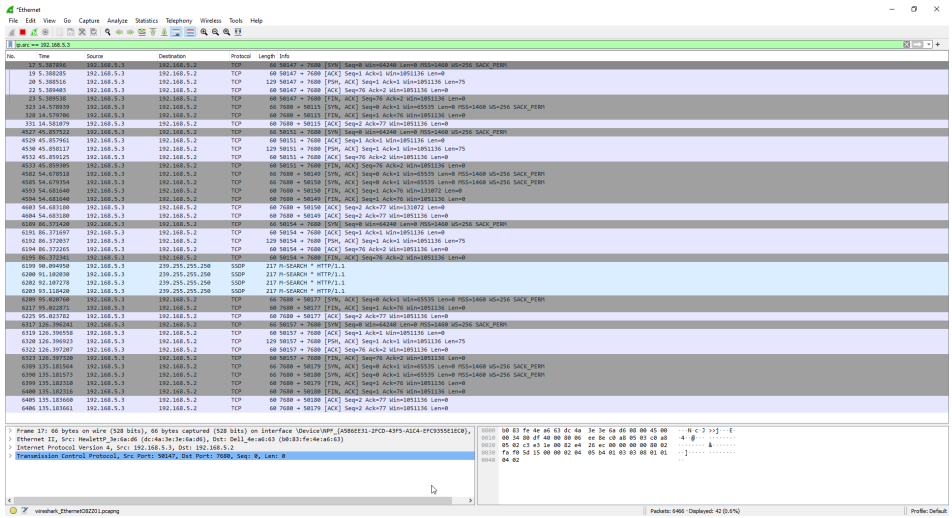


Figure 9: Παράδειγμα εκτέλεσης ip.src_equal

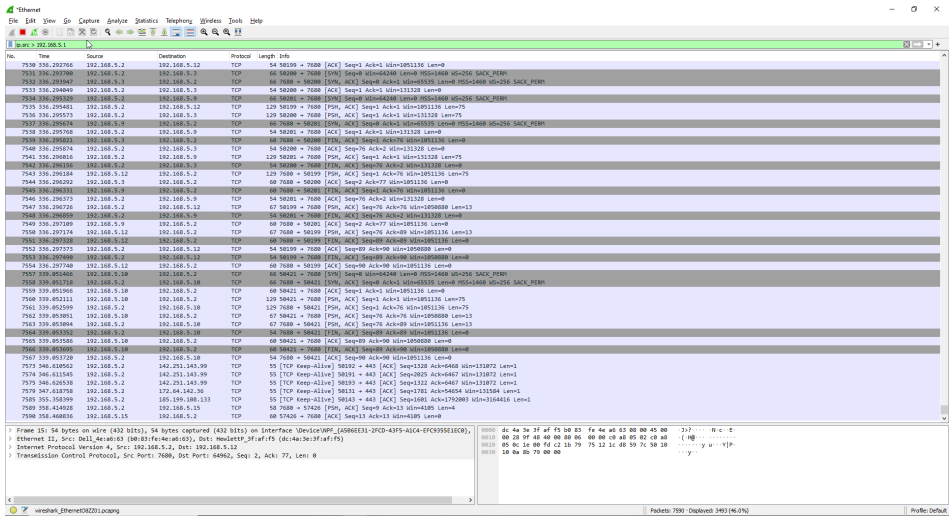


Figure 10: Παράδειγμα εκτέλεσης ip.src_greater

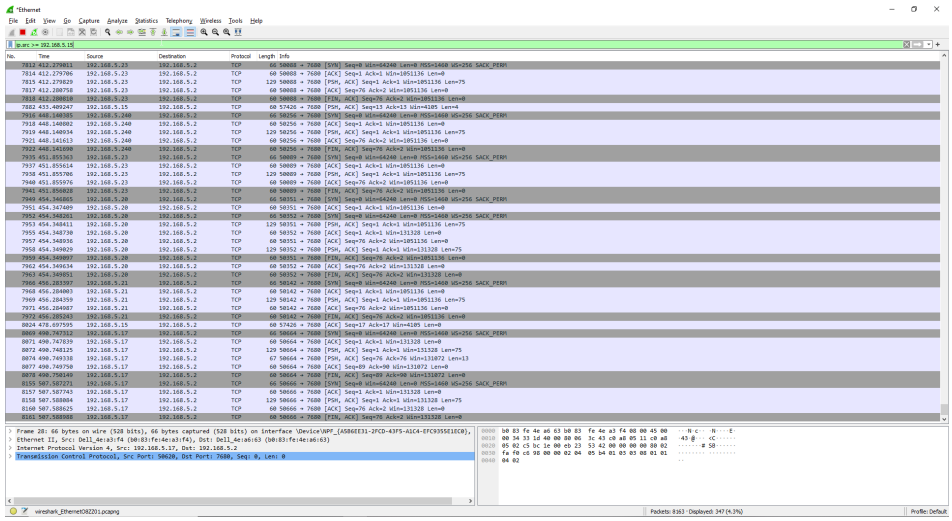


Figure 11: Παράδειγμα εκτέλεσης ip.src_greater_equal

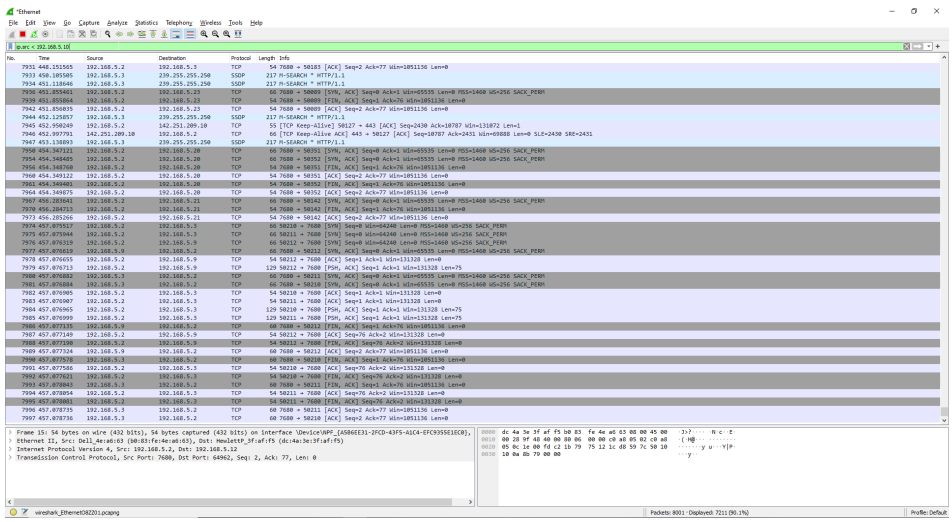


Figure 12: Παράδειγμα εκτέλεσης ip.src_less

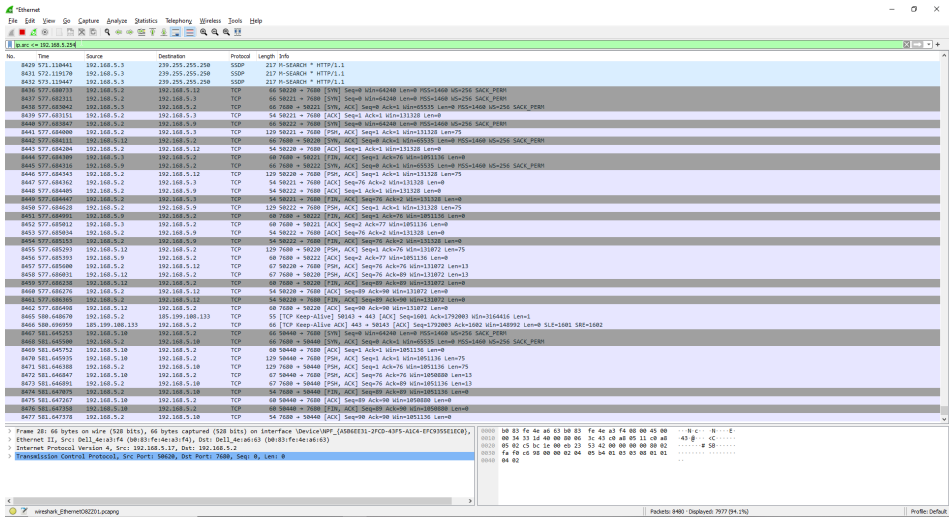


Figure 13: Παράδειγμα εκτέλεσης ip.src_less_equal

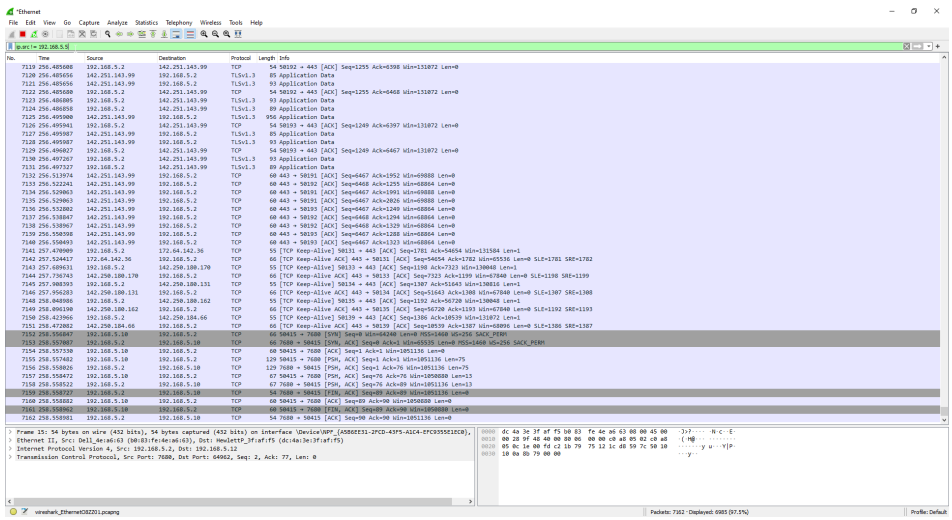


Figure 14: Παράδειγμα εκτέλεσης ip.src_not_equal

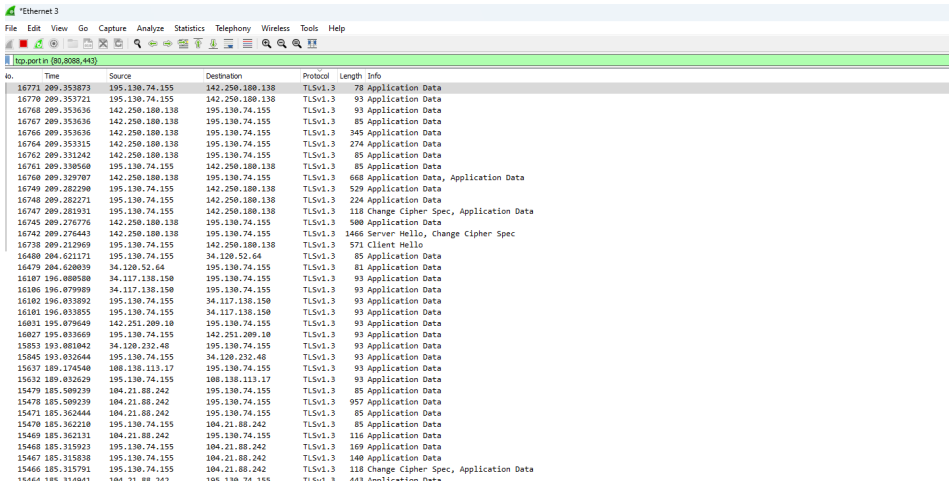


Figure 15: Παράδειγμα εκτέλεσης tcp_port

References

[1] *SecNews*, https://www.secnews.gr/202495/wireshark-xrisimopoihsete-kalitero-network-sniffer/

[2] *Lifewire* https://www.lifewire.com/wireshark-tutorial-4143298

[3] *University_of_Oregen* https://nsrc.org/workshops/2014/pacnog15-netsecurity/raw-attachment/wiki/Track2Agenda/0-2-9-Wireshark_Lab.pdf

[4] *eecs.yorku.ca* https://www.eecs.yorku.ca/course_archive/2011-12/F/3213/Project/exercises.pdf

[5] *solarwinds* https://www.solarwinds.com/network-performance-monitor/use-cases/packet-analyzer

[6] *Npcap* https://npcap.com/

[7] Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. Forensic Science International: Digital Investigation, 32, 200892.

[8] Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, 40, 307-324.

[9] Bagyalakshmi, G., Rajkumar, G., Arunkumar, N., Easwaran, M., Narasimhan, K., Elamaran, V., ... Ramirez-Gonzalez, G. (2018). Network vulnerability analysis on brain signal/image databases using Nmap and Wireshark tools. Ieee Access, 6, 57144-57151.

[10] *Wireshark* https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html