LAB 1

ΣΤΑΥΡΟΥΛΑ ΣΙΑΧΑΛΟΥ

ΣΠΥΡΟΣ ΜΕΓΑΛΟΥ

ΒΑΣΙΚΕΣ ΕΝΤΟΛΕΣ ΔΙΚΤΥΩΝ

Ip config: Μία από τις πιο βασικές εντολές. Επιστρέφει ένα overview των ρυθμίσεων δικτύου του υπολογιστή.

Ip config/all: Παρόμοια εντολή με την ipconfig. Παρέχει λίγες παραπάνω πληροφορίες για τις ρυθμίσεις δικτύου του υπολογιστή.

Ping: Χρησιμοποιεί το ICMP (Internet Control Message Protocol) για να στείλει πακέτα ECHO_REQUEST με στόχο την πρόκληση ECHO_REPLY. Το ping χρησιμοποιείται για να γίνει έλεγχος της λειτουργίας μιας άλλης δικτυακής συσκευής συνδεδεμένης στο δίκτυο.

Tracert: Η εντολή αυτή παρέχει στο χρήστη ένα overview του μονοπατιού(route) από τον υπολογιστή μας μέχρι τον destination host, αναφέρει κάθε δρομολογητή ή πύλη που συναντά ένα πακέτο στη διαδρομή προς άλλον κεντρικό υπολογιστή.

Nslookup: Η εντολή αυτή μας επιτρέπει να εισάγουμε ένα όνομα host για να ανακαλύψουμε την IP διεύθυνση του και το αντίστροφο.

Pathping: Με το Pathping μπορείτε να λάβετε πληροφορίες σχετικά με την καθυστέρηση σε ένα δίκτυο και επίσης να καταλάβετε σε ποια στάδια της μετάδοσης των πακέτων, υπάρχουν απώλειες ή καθυστερήσεις.

ΒΑΣΙΚΕΣ ΕΝΤΟΛΕΣ ΔΙΚΤΥΩΝ

Route: Χρησιμοποιείται για την εμφάνιση και διαχείριση του πίνακα δρομολόγησης σε έναν υπολογιστή και κυρίως για τον ορισμό στατικών δρομολογίων προς συγκεκριμένα δίκτυα και υπολογιστές μέσω μιας δικτυακής διασύνδεσης (κάρτας δικτύου) αμέσως μετά τη ρύθμιση και ενεργοποίησή της. Στα windows η εμφάνιση του πίνακα δρομολόγησης γίνεται με τη συνοδεία της διαταγής **print.**

Netstat: Η εντολή **netstat** εμφανίζει πληροφορίες για τις τρέχουσες συνδέσεις TCP/IP και στατιστικά για την δικτυακή κίνηση.

ARP: Η εντολή arp χρησιμοποιείται για την διαχείριση του πίνακα (cache) ARP που υποστηρίζει το πρωτόκολλο ARP (Address Resolution Protocol) για αντιστοίχιση Λογικών Διευθύνσεων σε Φυσικές Διευθύνσεων (MAC) σε. Με άλλα λόγια βοηθά κάποιον υπολογιστή που θέλει να στείλει ένα μήνυμα σε κάποια IP διεύθυνση μιας συσκευής που βρίσκεται στο ίδιο τοπικό δίκτυο να εντοπίζει την αντίστοιχη φυσική διεύθυνση για να την τοποθετήσει στο πλαίσιο του επιπέδου 2.

Systeminfo: Αυτή η εντολή μας παρέχει μια ολοκληρωμένη επισκόπηση των πληροφοριών του συστήματος

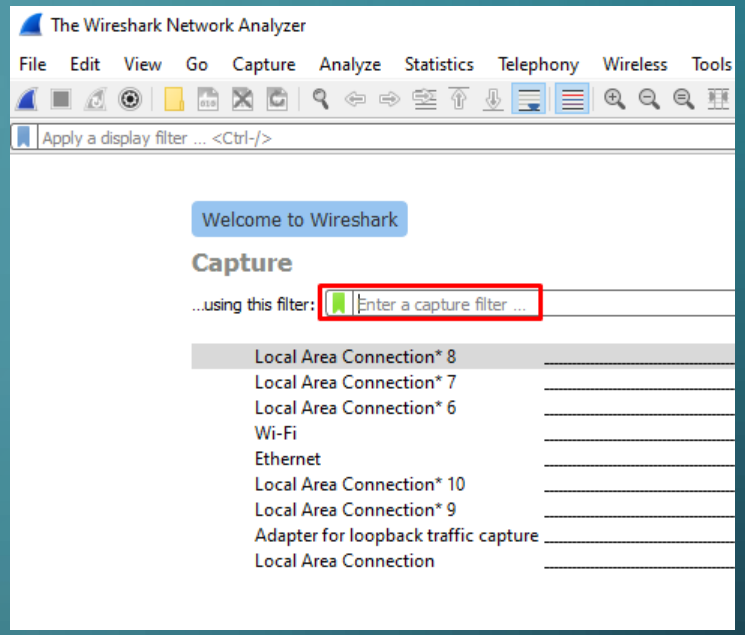
ΑΝΑΛΥΤΗΣ ΠΡΩΤΟΚΟΛΛΩΝ: WIRESHARK (GNU GPL)

- Λογισμικό που παρακολουθεί και εξετάζει το trace των πακέτων, καθώς και χρησιμοποιείται ευρέως για την αντιμετώπιση προβλημάτων δικτύων.
- Συμβατό με Windows, Mac, Linux, κ.α.
- Γραφική διεπαφή χρήστη που δείχνει την ακολουθία των πακέτων και τη σημασία των bit όταν ερμηνεύονται ως header ή δεδομένα.
- Χρωματίζει τους κωδικούς των πακέτων με βάση τον τύπο τους, και έχει διάφορους τρόπους για να φιλτράρει και να αναλύσει τα πακέτα για να σας επιτρέψει να διερευνήσετε τη συμπεριφορά των πρωτοκόλλων δικτύου.

ΦΙΛΤΡΑ

- Φίλτρα σύλληψης: Χρησιμοποιούνται για την επιλογή των δεδομένων που θα καταγραφούν στα αρχεία καταγραφής. Καθορίζονται πριν την εκκίνηση της σύλληψης.

- Φίλτρα απεικόνισης: Χρησιμοποιούνται για την αναζήτηση μέσα στα αρχεία καταγραφών. Μπορούν να τροποποιηθούν ενόσω τα δεδομένα συλλαμβάνονται.



ΦΙΛΤΡΑ ΣΥΛΛΗΨΗΣ

Σύνταξη:	Πρωτόκολλο	Κατεύθυνση	Host(s)	Τιμή	Λογικές Πράξεις	Άλλες εκφράσεις

Τιμές πεδίων:

Πρωτόκολλο: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. Εάν δεν δηλωθεί κανένα πρωτόκολλο, χρησιμοποιούνται όλα τα πρωτόκολλα.

Κατεύθυνση: src, dst, src and dst, src or dst. Εάν δεν δηλωθεί ούτε πηγή ούτε προορισμός, οι λέξεις κλειδιά "src ή dst" εφαρμόζονται. Για παράδειγμα, το "host 10.2.2.2" είναι ίσο με το "src ή dst host 10.2.2.2".

Host(s): net, port, host, portrange. Εάν δεν δηλωθεί host(s), χρησιμοποιείται η λέξη κλειδί "host". Για παράδειγμα, το "src 10.1.1.1" είναι ίσο με το "src host 10.1.1.1".

Λογικές Πράξεις: not, and, or. Η άρνηση ("not") έχει μεγαλύτερη προτεραιότητα. Η εναλλαγή ("or") και η αλληλουχία ("and") έχουν ίση προτεραιότητα και συνδέουν τα αριστερά με τα δεξιά. Για παράδειγμα, το "not tcp port 3128 and tcp port 23" είναι ίσο με το "(not tcp port 3128) and tcp port 23". ΔΕΝ είναι ίσο με το "not (tcp port 3128 and tcp port 23)".

ΦΙΛΤΡΑ ΣΥΛΛΗΨΗΣ – ΠΑΡΑΔΕΙΓΜΑΤΑ

tcp dst port 3128 Δείχνει τα πακέτα με προορισμό την θύρα TCP 3128.

ip src host 10.1.1.1 Δείχνει τα πακέτα με τη διεύθυνση πηγής IP που ισούται με το 10.1.1.1.

host 10.1.2.3 Δείχνει τα πακέτα με πηγή ή προορισμό τη διεύθυνση IP η οποία είναι ίση με το 10.1.2.3.

src portrange 2000-2500 Δείχνει τα πακέτα με θύρες πηγής UDP ή TCP μεταξύ του εύρους 2000-2500.

not icmp Δείχνει τα πάντα εκτός από τα πακέτα του icmp (το icmp χρησιμοποιείται τυπικά από το εργαλείο ping).

src host 10.7.2.12 and not dst net 10.200.0.0/16 Δείχνει τα πακέτα με τη διεύθυνση IP πηγής η οποία ισούται με το 10.7.2.12 και την ίδια στιγμή όχι με τη διεύθυνση IP προορισμού του δικτύου 10.200.0.0/16.

(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000 and dst net 10.0.0.0/8 Δείχνει τα πακέτα με τη διεύθυνση IP πηγής 10.4.1.12 ή το δίκτυο πηγής 10.6.0.0/16, το αποτέλεσμα είναι η αλυσιδωτή σύνδεση των πακέτων τα οποία έχουν προορισμό το εύρος θυρών TCP από 200 έως 10000 και διεύθυνση IP του δικτύου προορισμού 10.0.0.0/8.

ΦΙΛΤΡΑ ΑΠΕΙΚΟΝΙΣΗΣ

- Για αναζήτηση μέσα σε δεδομένα τα οποία έχουν ληφθεί με κάποιο φίλτρο σύλληψης. Οι δυνατότητες αναζήτησης μπορούν να είναι μεγαλύτερες από εκείνες ενός φίλτρου σύλληψης και δεν είναι απαραίτητο να γίνει η επανεκκίνηση της σύλληψης όταν επιθυμήσουμε την αλλαγή του φίλτρου μας.
- Πρωτόκολλο: Ένας μεγάλος αριθμός πρωτοκόλλων, τα οποία βρίσκονται μεταξύ του 2ου και του 7ου του μοντέλου OSI, είναι διαθέσιμος. Μπορείτε να τα δείτε όταν πατήσετε πάνω στο κουμπί "Expression..." στο κυρίως παράθυρο. Μερικά παραδείγματα : IP, TCP, DNS, SSH
- Case sensitive

ΠΡΑΞΕΙΣ ΣΥΓΚΡΙΣΗΣ

```
ip.src==10.0.0.5

ip.src!=10.0.0.5

frame.len > 10

frame.len < 128

frame.len ge 0x100

frame.len <= 0x20
```

Αγγλική μορφή:	Μορφή γλώσσας C:	Σημασία:
eq	==	Ίσο
ne	!=	Διάφορο
gt	>	Μεγαλύτερο από
lt	<	Μικρότερο από
ge	>=	Μεγαλύτερο ή ίσο
le	<=	Μικρότερο ή ίσο

ΛΟΓΙΚΕΣ ΕΚΦΡΑΣΕΙΣ

- `ip.src==10.0.0.5 and tcp.flags.fin`
- `ip.src==10.0.0.5 or ip.src==192.1.1.1`
- `tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29`
- `not llc`

Αγγλική μορφή:	Μορφή γλώσσας C:	Σημασία:
and	&&	Λογικό AND
or	||	Λογικό OR
xor	^^	Λογικό XOR
not	!	Λογικό NOT

ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΠΕΙΚΟΝΙΣΗΣ

ip.addr == 10.1.1.1 Εμφανίζει τα πακέτα με διεύθυνση IP πηγής ή προορισμού η οποία ισούται με 10.1.1.1.

ip.src != 10.1.2.3 or ip.dst != 10.4.5.6 Εμφανίζει τα πακέτα με διεύθυνση IP πηγής διαφορετική της 10.1.2.3 ή με διεύθυνση IP προορισμού διαφορετική της 10.4.5.6.

ip.src != 10.1.2.3 and ip.dst != 10.4.5.6 Εμφανίζει τα πακέτα με διεύθυνση IP πηγής διαφορετική από την 10.1.2.3 και την ίδια στιγμή με διεύθυνση IP προορισμού διαφορετική της 10.4.5.6

tcp.port == 25 Εμφανίζει τα πακέτα πηγής TCP ή προορισμό την θύρα 25.

tcp.flags Εμφανίζει τα πακέτα με σημαία TCP.

tcp.flags.syn == 0x02 Εμφανίζει τα πακέτα με σημαία TCP SYN.

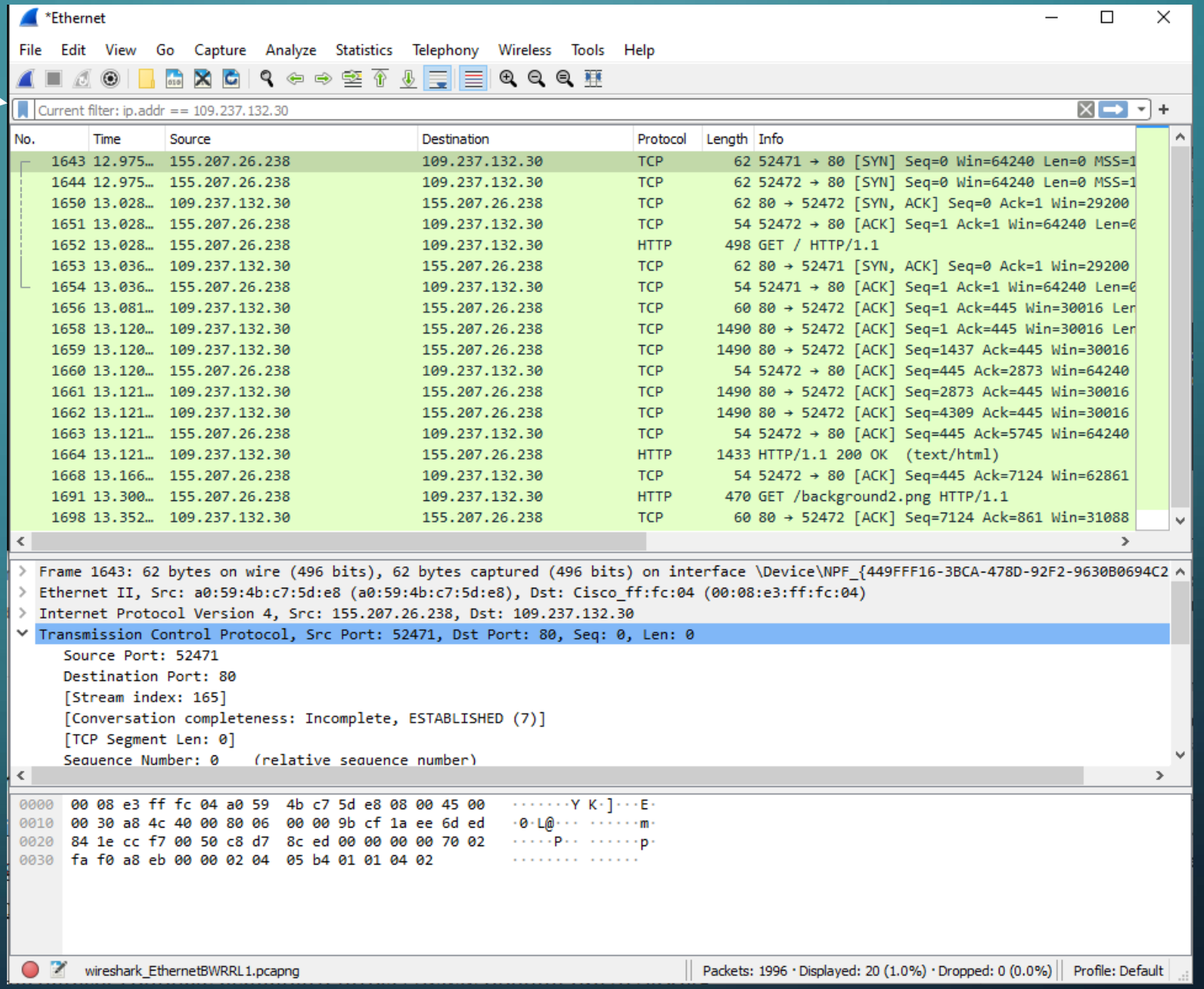
Εάν η σύνταξη του φίλτρου είναι σωστή, θα υπογραμμιστεί με πράσινο χρώμα, ειδάλλως εάν υπάρχει λάθος στην σύνταξή του θα υπογραμμιστεί με κόκκινο χρώμα

Display Filter

Packet List Pane

Packet Details Pane

Packet Bytes Pane




First packet in a conversation.

Part of the selected conversation.

Not part of the selected conversation.


Last packet in a conversation.


Request.


Response.


The selected packet acknowledges this packet.


The selected packet is a duplicate acknowledgement of this packet.


The selected packet is related to this packet in some other way, e.g. as part of reassembly.