Δρ. Άννα Κεφάλα

WireShark (a network protocol analyser)

WireShark

About Packet Sniffing

Κατανόηση Δικτυακών Πρωτοκόλλων

- Παρατήρηση ακολουθίας ανταλλασσόμενων μηνυμάτων
- Λεπτομέρειες λειτουργίας πρωτοκόλλων
- Δύο δυνατότητες
  - Προσομοίωση λειτουργίας δικτύου
  - «Παρακολούθηση» πραγματικής λειτουργίας δικτύου

Τί είναι Packet Sniffer?

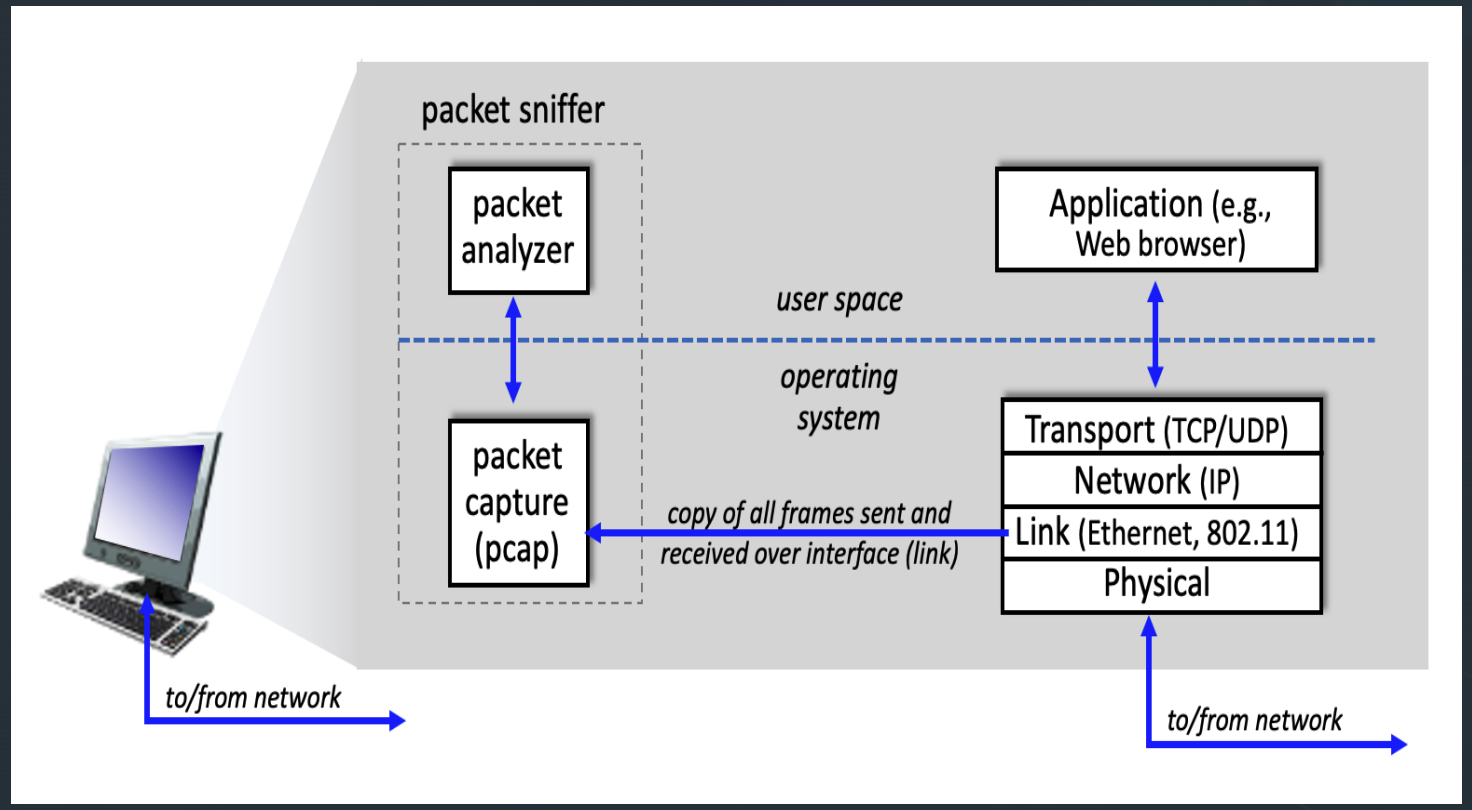
Packet analyzer, network analyzer, protocol analyzer ή packet sniffer

- captures (αιχμαλωτίζει) τα δικτυακά μηνύματα (πακέτα) *υποκλοπή και καταγραφή κίνησης*
- καθώς οι ροές επικοινωνίας δεδομένων κινούνται στο δίκτυο, ο sniffer αιχμαλωτίζει (captures) τα πακέτα, αποκωδικοποιεί (decodes) τα ανεπεξέργαστα δεδομένα (πεδία πρωτοκόλλων πακέτου) και τα αναλύει (analyzes) σύμφωνα με RFC ή άλλα specifications

Τί είναι Packet Sniffer? (συν.)

- Passive, μόνο λαμβάνει αντίγραφα των πακέτων
  - η επεξεργασία των πακέτων συνεχίζεται κανονικά
- Αποτελείται από δύο μέρη:
  - Packet Capture Library: όλα τα πρωτόκολλα ενσωματώνονται στο πλαίσιο (frame) του επιπέδου σύνδεσης (π.χ. Ethernet)
  - Packet Analyzer: headers από Ethernet frame, IP datagram, TCP/UDP segment, application message

Packet Sniffer Structure



Application Message

TCP/UDP Segment

IP Datagram

Ethernet Frame

WireShark

WireShark: Network Protocol Analyzer

- Κάνει capture και εμφανίζει αλληλεπιδραστικά την κίνηση στο δίκτυο σε πραγματικό χρόνο
- Δεν αποκωδικοποιεί μόνο τα bits & bytes αλλά και τις συσχετίσεις μεταξύ πακέτων και πρωτοκόλλων και την αλληλουχία μηνυμάτων των πρωτοκόλλων
- Τρέχει σε Windows, MacOS, Linux, Unix
- Open source, GNU General Public License Ver. 2
- Ξεκίνησε και έγινε γνωστό ως Ethereal

WireShark Packet Sniffer

http://www.wireshark.org/

Γιατί αυτό το εργαλείο;

- Stable
- Μεγάλη βάση χρηστών
- Καλή τεκμηρίωση
- Πλούσια λειτουργικότητα (αναλύει εκατοντάδες πρωτόκολλα)
- Καλή σχεδίαση του user interface

WireShark: ποιοι το χρησιμοποιούν…

- Network administrators: troubleshoot προβλήματα δικτύου
- Network security engineers: διερεύνηση προβλημάτων ασφάλειας
- Quality Assurance engineers: επικύρωση δικτυακών εφαρμογών
- Developers: debug υλοποίηση πρωτοκόλλων
- οποιοσδήποτε: εκμάθηση λειτουργίας πρωτοκόλλων δικτύου

Τί μπορούμε να κάνουμε με το WireShark

- capture κίνηση πακέτων σε πραγματικό χρόνο σε μία δικτυακή διεπαφή
- ανάλυση δεδομένων πακέτων από αρχεία που έχουν δημιουργηθεί με tcpdump/WinDump, Wireshark ή κάποιο άλλο πρόγραμμα capturing
- εμφάνιση πακέτων και λεπτομερή πληροφορία πρωτοκόλλων
- δυνατότητα αποθήκευσης των δεδομένων για offline ανάλυση
- φιλτράρισμα/αναζήτηση πακέτων βάση κριτηρίων
- συγκέντρωση και εμφάνιση στατιστικών στοιχείων

Installing

- https://www.wireshark.org/download.html

- Documentation
  - https://www.wireshark.org/docs/
- User's guide
  - https://www.wireshark.org/docs/wsug_html_chunked/

Υποστηριζόμενα Πρωτόκολλα

- Οργανώνει τα πρωτόκολλα βάση της ιεραρχίας με την οποία εμφανίζονται στο trace
- Εκατοντάδες τα υποστηριζόμενα πρωτόκολλα (π.χ. tcp), πεδία πρωτοκόλλων (π.χ. tcp.port) και μέσα

Υποστηριζόμενες συσκευές/διεπαφές

- Φυσικές διεπαφές
  - Ethernet, serial (PPP), 802.11 (WiFi) wireless LANs, Bluetooth, IrDA, USB
- Εικονικές διεπαφές
  - Loopback
  - VLANs

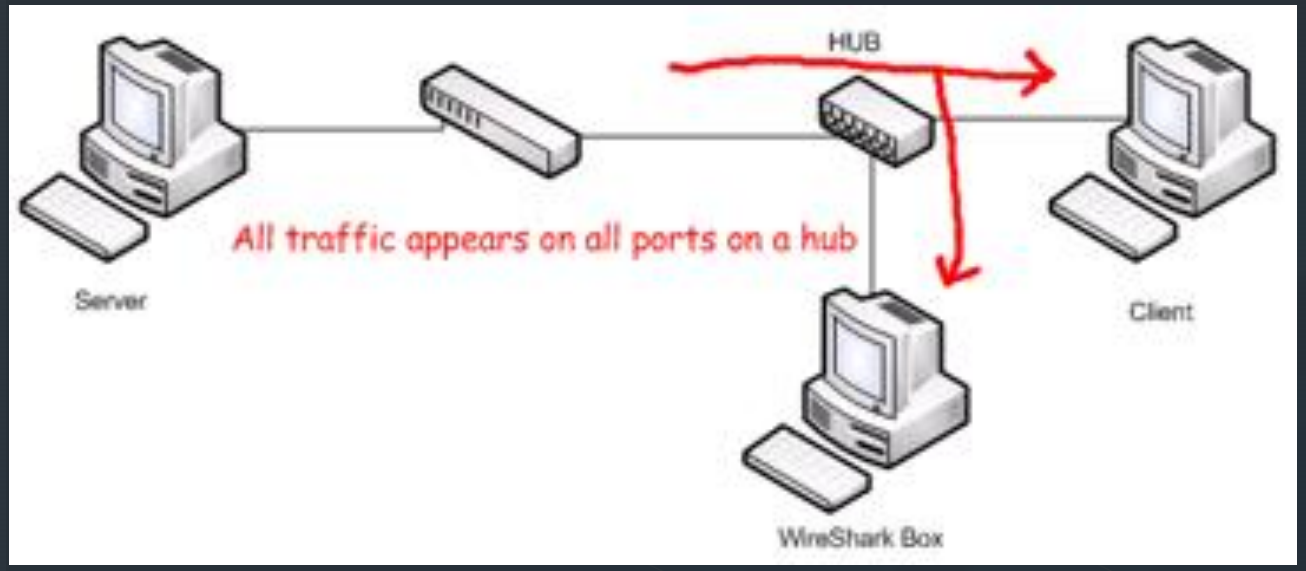
Υποστηριζόμενα interfaces ανά πλατφόρμα

Interface	AIX	FreeBSD	HP-UX	Irix	Linux	macOS	NetBSD	OpenBSD	Solaris	Tru64 UNIX	Windows
ATM	?	?	?	?	✓	✗	?	?	✓	?	?
Bluetooth	✗	✗	✗	✗	✓[1]	✗	✗	✗	✗	✗	✗
CiscoHDLC	?	✓	?	?	✓	?	✓	✓	?	?	?
Ethernet	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FDDI	?	?	?	?	✓	✗	?	?	✓	?	?
FrameRelay	?	?	✗	✗	✓	✗	?	?	✗	✗	✗
IrDA	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
ppp[2]	?	?	?	?	✓	✓	?	?	✗	?	✓
TokenRing	✓	✓	?	✗	✓	✗	✓	✓	✓	?	✓
USB	✗	✗	✗	✗	✓[3]	✗	✗	✗	✗	✗	✗
WLAN[4]	?	✓	?	?	✓	✓	✓	✓	?	?	✓
Loopback (virtual)	?	✓	✗	?	✓	✓	✓	✓	✗	✓	N/A[5]
VLAN Tags (virtual)	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓

Μπορώ να δω όλη την κίνηση?

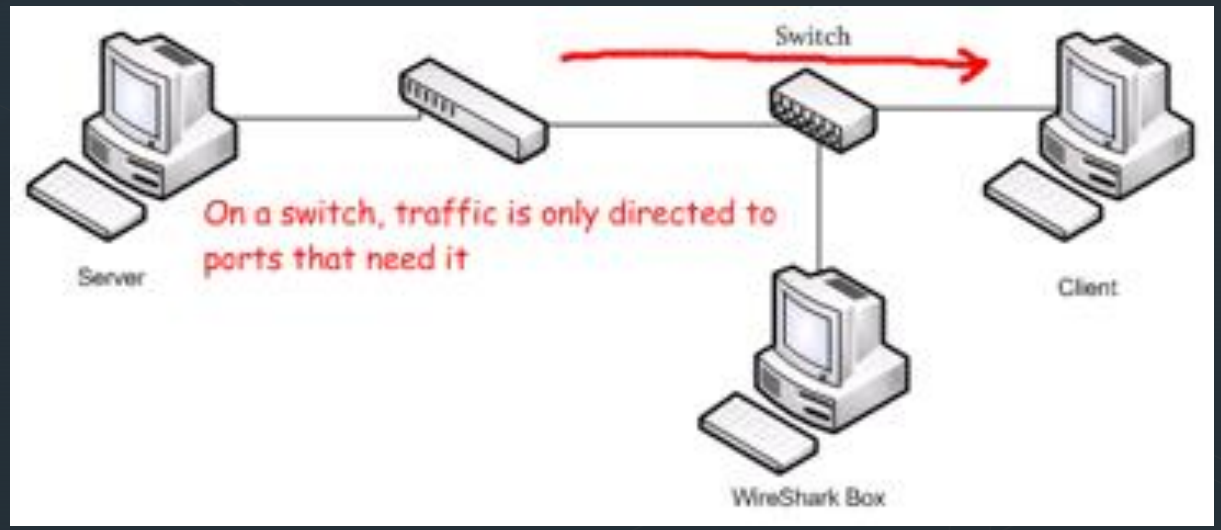
- Μόνο πακέτα από ή προς το μηχάνημά μου
- Η unicast κίνηση δεν στέλνεται παντού σε ένα switched network
- Broadcast και multicast κίνηση

Πού «τρέχω» το WireShark?



HUB

SWITCH



Ας το δούμε στην πράξη...