εργασία για το μάθημα

Διαχείρισης Δικτύων

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Τσαούσης Λεωνίδας
Α.Μ.: 1115201200184
Εαρινό εξάμηνο 2015-’16

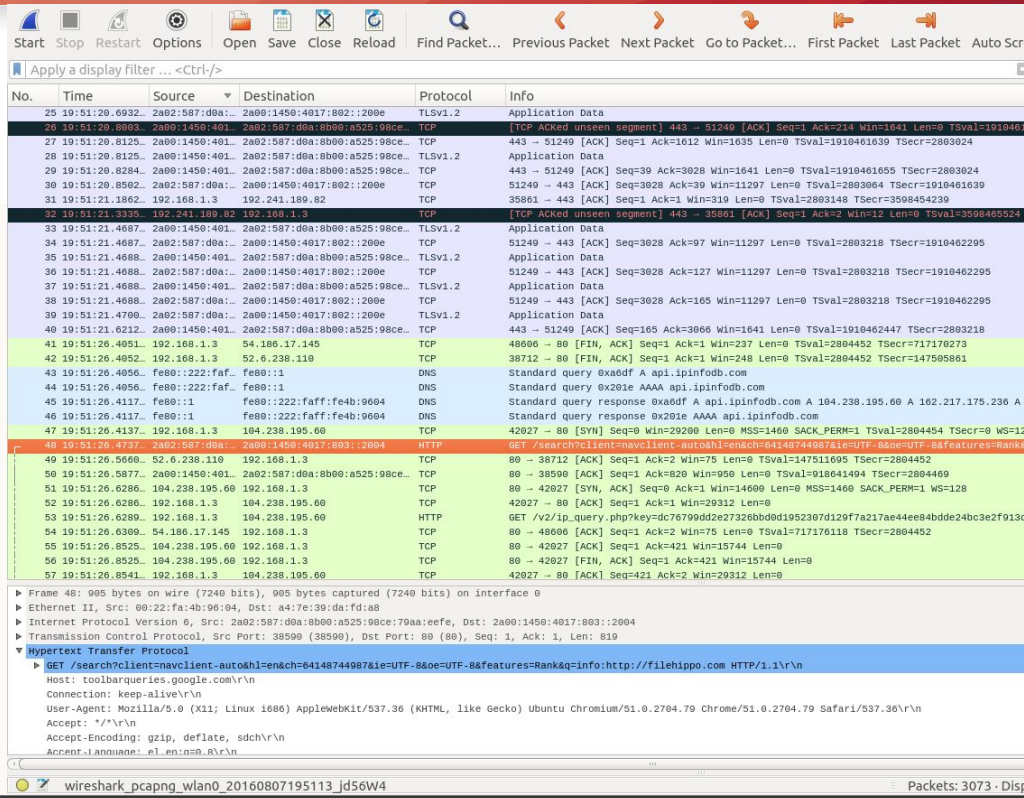
Αντικείμενο της εργασίας

- **Εκτέλεση** εργαλείων παρακολοήθησης δικτύων και ανίχνευσης πακέτων (sniffers).
- **Καταγραφή** δεδομένων για την ύπαρξη και χρήση ασύρματων δικτύων αλλα και των υπολογιστών/εφαρμογών που είναι συνδεδεμένοι στα τοπικά αυτά δίκτυα. Παρακολούθηση:
  - της χρήσης καναλιών, ισχύς σήματος, κάλυψης κτλ. των ασύρματων δικτύων
  - πρωτόκολλα που χρησιμοποιήθηκαν για την πρόσβαση στον ιστό, υπηρεσίες και στατιστικά
  - συσκευές που συνδέθηκαν, user agents
- Δημιουργία **βάσης δεδομένων** και εισαγωγή των παραπάνω καταγεγραμμένων στοιχείων σ'αυτην.
- **Σχεδιασμός εφαρμογής** για την παρουσίαση, επεξεργασία και λήψη αποφάσεων.
- Συσχέτιση των δράσεων αυτών/ευθυγράμμιση τους με το **θεωρητικό υπόβαθρο** (π. χ. μοντέλο *FCAPS)* της διαχείρισης δικτύων

Καταγραφή δεδομένων

Με το λογισμικό
Wireshark

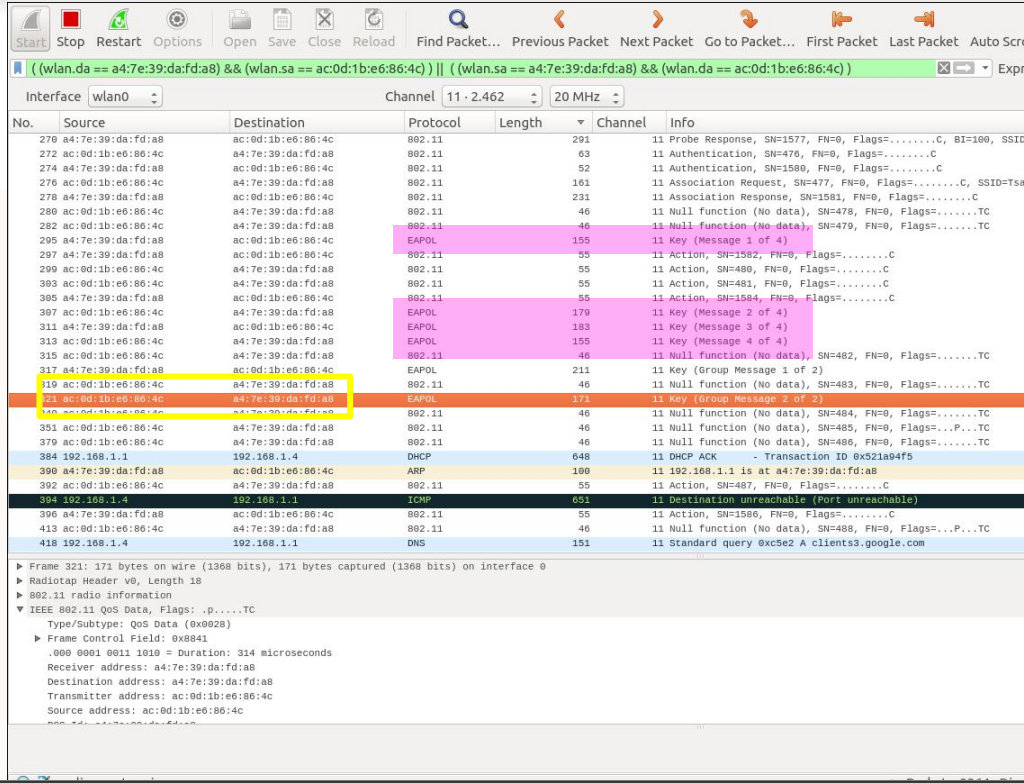
Ενεργοποίηση του monitor mode/promiscuous mode στις κάρτες δικτύου



Απο το οικιακό δίτκυο...

- view/capture filters, configuration profiles για 802.11 κινηση

  https://wiki.wireshark.org/CaptureSetup/WLAN



...αλλα και απο γειτονικά

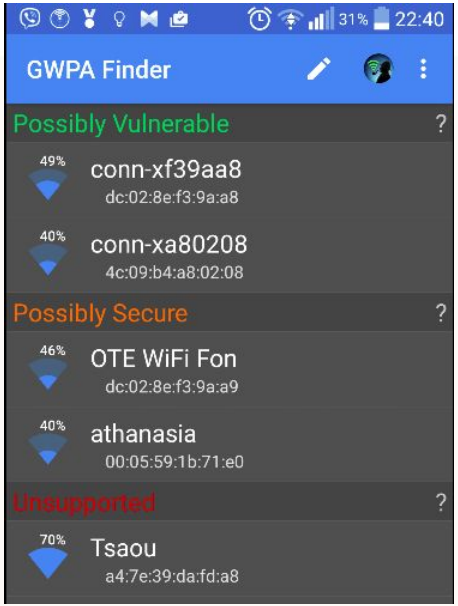
- Channel Hopping

```
#!/bin/bash

IFACE=wlan0
SEC=0.5

IEEE80211bg="1 2 3 4 5 6 7 8 9 10 11"
IEEE80211bg_intl="$IEEE80211bg 12 13 14"
IEEE80211bg_eu="$IEEE80211bg 12 13"

IEEE80211a="36 40 44 48 52 56 60 64 149 153 157 161"
IEEE80211bga="$IEEE80211bg $IEEE80211a"
IEEE80211bga_intl="$IEEE80211bg_intl $IEEE80211a"

ifconfig $IFACE down
iwconfig $IFACE mode monitor
ifconfig $IFACE up

while true ; do
    for CHAN in $IEEE80211bg_eu ; do
        echo "Switching to channel $CHAN"
        iwconfig $IFACE channel  $CHAN
        sleep $SEC
    done
done
```

~/chanho2.sh [sh] enH row:17/24 col:001 [+] All
-- INSERT --

+

- WiFi keys



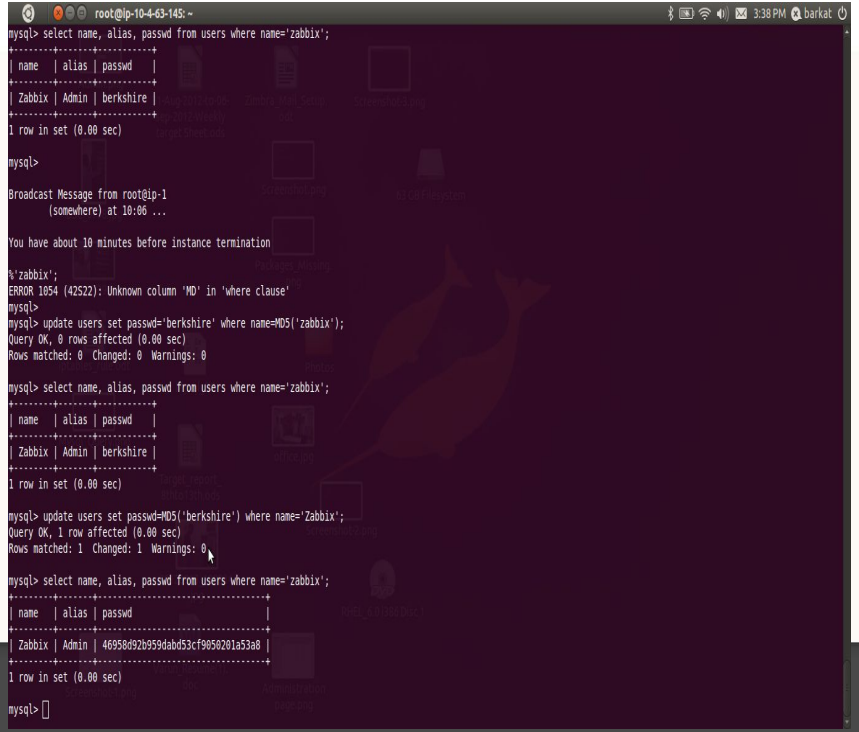
=

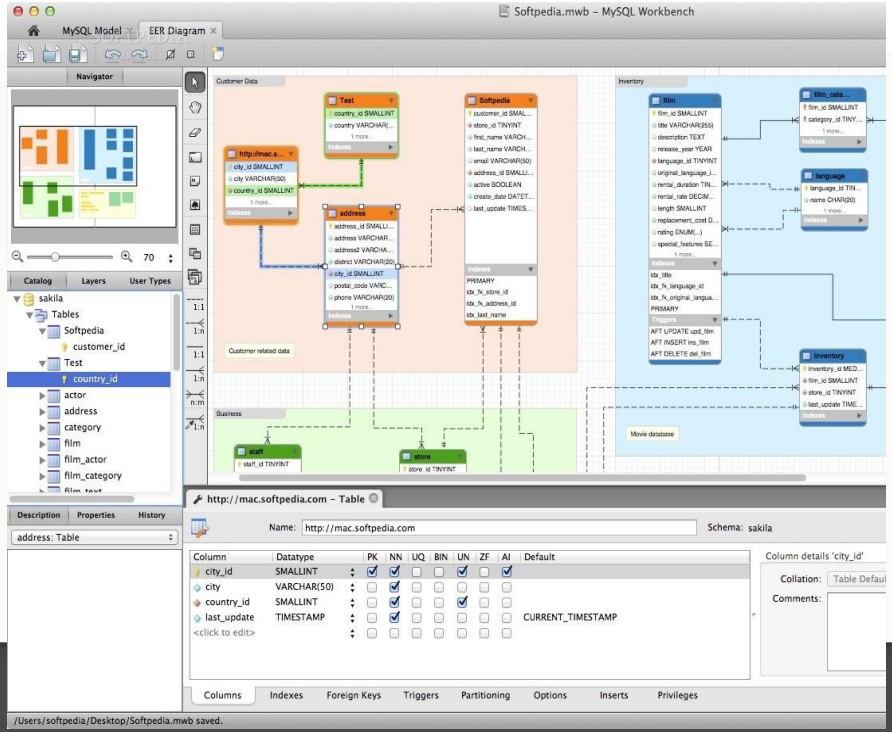
Βάση δεδομένων

MySQL server / client

+

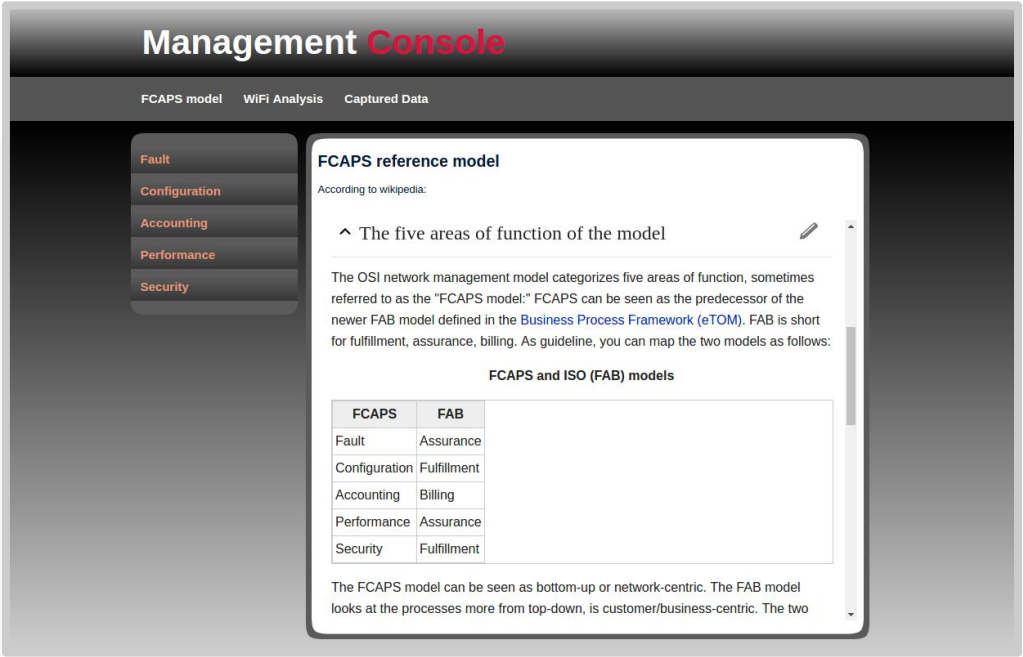
MySQL Workbench για τον σχεδιασμό του μοντέλου





Management Console

- LAMP server
- Automates DB population
- Some DB operations (e.g. ‘Empty’)
- Visualizes information
- Ease-of-use



Live Demo

1. Open MySQL Workbench > `quick_queries.sql + mib.mwb`
2. Open Management Console (look around > Index)
3. FCAPS > Fault > Analyze
   - Tsaou
   - tasoswaterski
4. Empty DB
5. Show .xml, Populate DB (ether.xml)
6. FCAPS > Conf > Analyze
   - Tsaou
   - Vergis

   ...

7. Show Code (PHP + CSS + HTML + SQL)
8. Take a closer look!

Συλλογή δεδομένων

Εκτέλεση Wireshark (λάπτοπ = “router”) σε

- διάφορα δίκτυα
  a. σπιτιού μου
  b. σπίτια φίλων
  c. δίκτυο καφετέριας

- τρέχωντας στο λάπτοπ μου διάφορες διεργασίες
  a. browsing
  b. torrents
  c. streaming (internet radio)
  d. χρήση εκτυπωτών
  e. pings

- κάνοντας σε αλλες συνδεδεμένες συσκευες (smartphones) διάφορες διεργασίες

Capturing configurations: 2 είδη

1. στην wlan0 με monitor mode και link-layer header: *802.11+radiotap*
2. στην wlan0 χωρις monitor mode και link-layer header: ethernet (pseudo)

Αλλαζοντας το channel κάθε 5 λεπτά μεχρι να τα καλύψω ολα

Για να πιάσω 802.11 Headers με info οπως:

- signal strength
- SSIDs
- data rates
- encryption types