Εργαστήριο Δικτύων Υπολογιστών

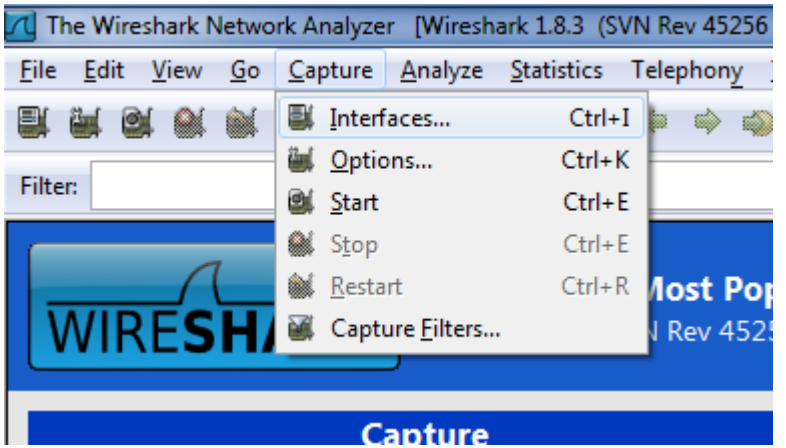
Wireshark by example

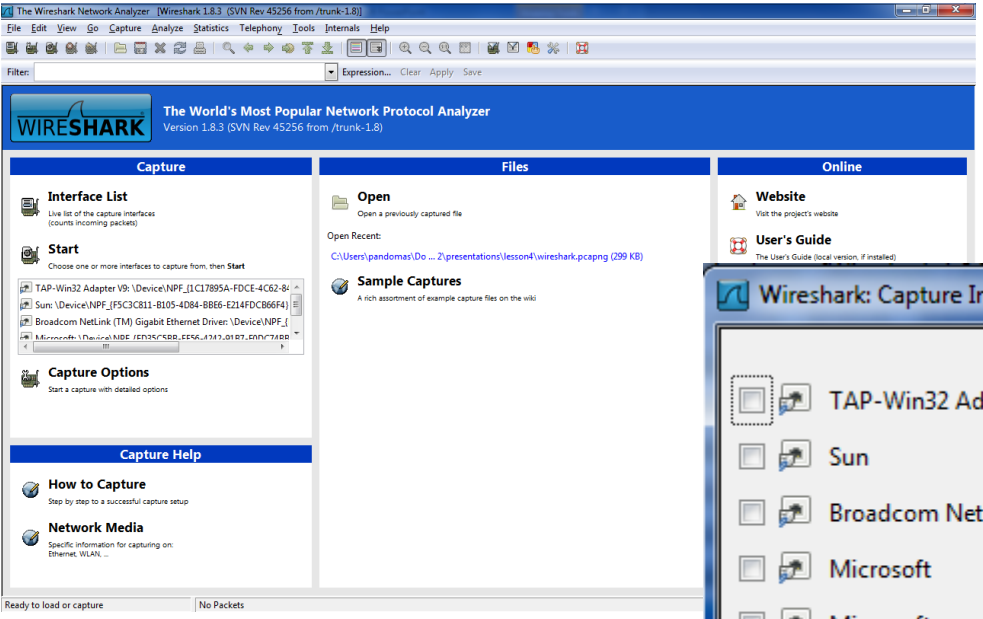
Wireshark

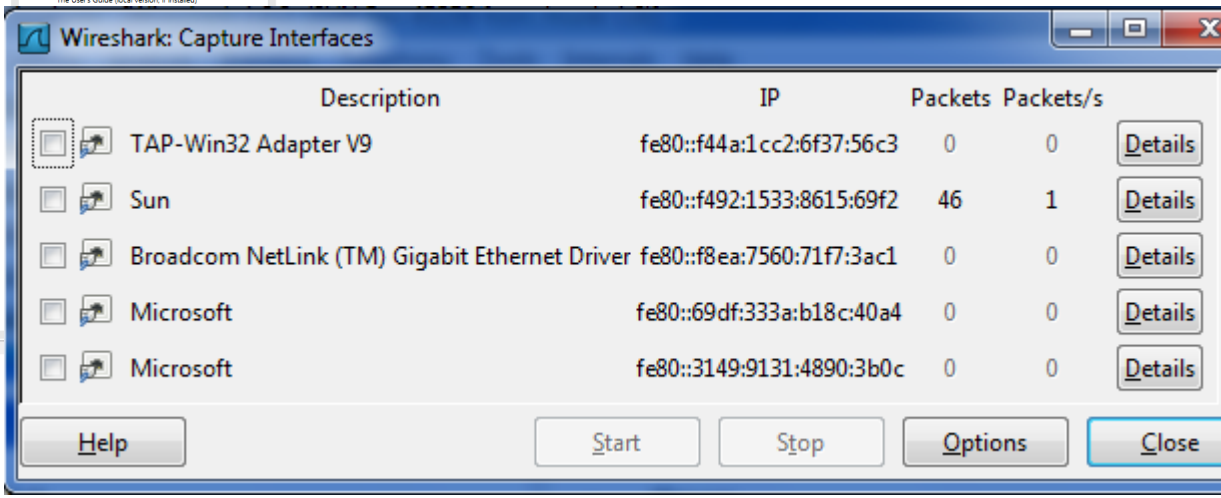
- Packet sniffer
- Network protocol analyzer
- Παλιότερα γνωστό με το όνομα Ethereal

Καταγραφή μίας HTTP συνόδου

- Καθαρισμός cache του φυλλομετρητή
- Άνοιγμα Wireshark
- Επιλογή διεπαφής καταγραφής

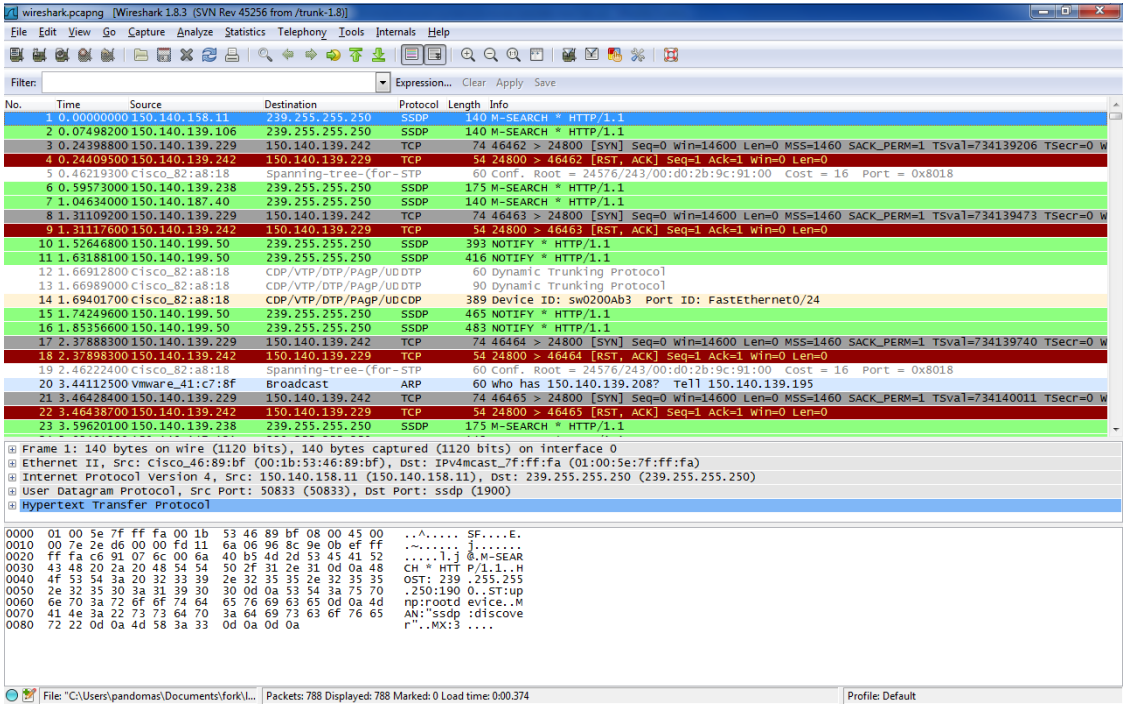






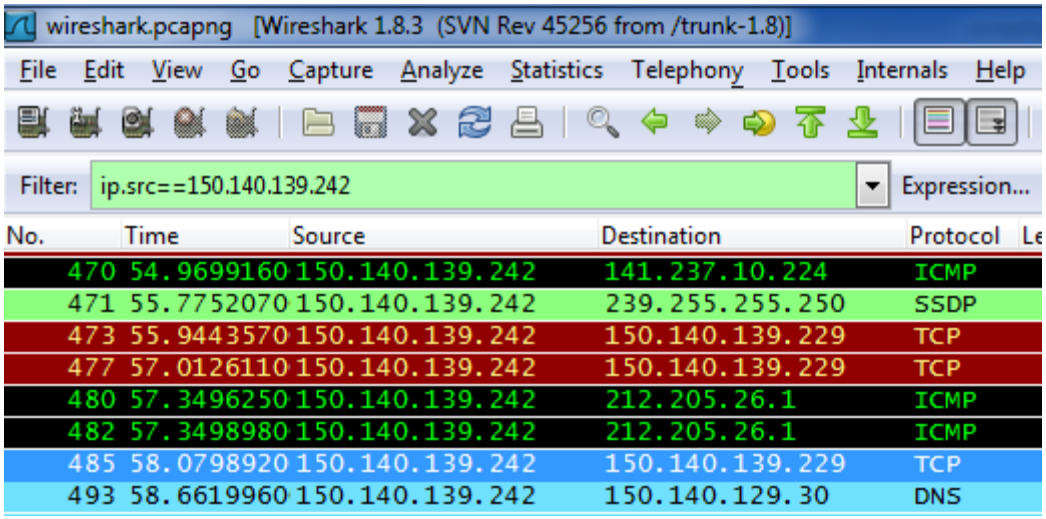
Καταγραφή μίας HTTP συνόδου

- Εκκίνηση καταγραφής
- Επίσκεψη στην σελίδα μέσω του φυλλομετρητή
- Κλείσιμο του φυλλομετρητή και διακοπή καταγραφής



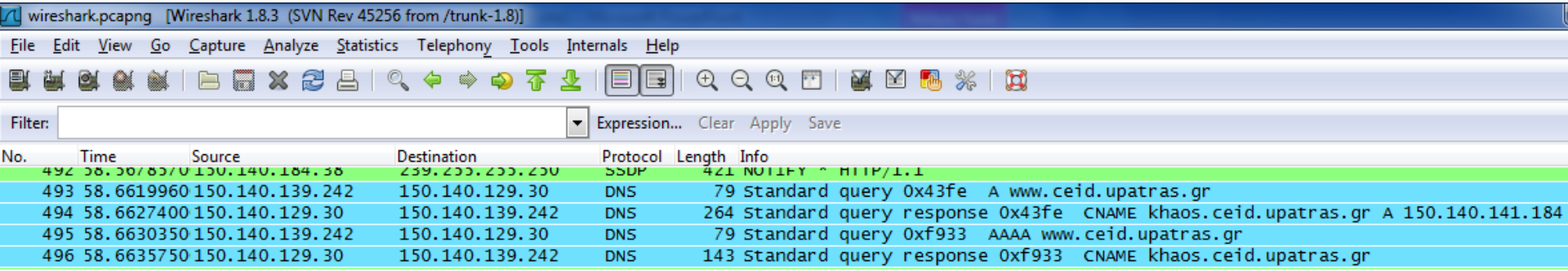
Ανάλυση Δεδομένων

- Επιλογή φίλτρου: ip.src==150.140.xxx.xxx



Ανάλυση Δεδομένων

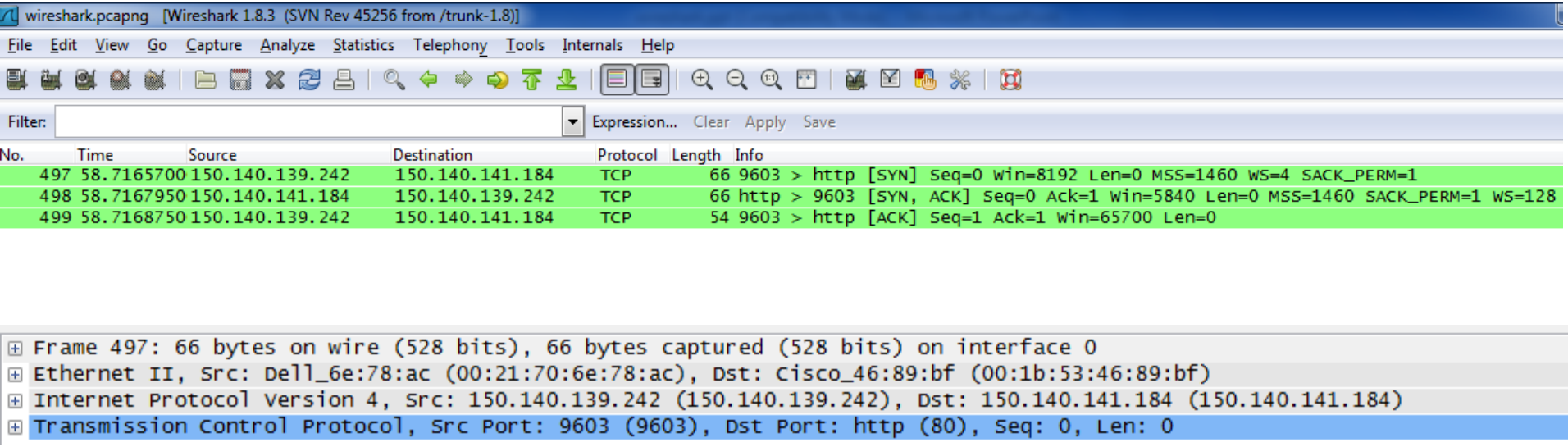
- DNS αίτηση




```
Frame 493: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: Dell_6e:78:ac (00:21:70:6e:78:ac), Dst: Cisco_46:89:bf (00:1b:53:46:89:bf)
Internet Protocol Version 4, Src: 150.140.139.242 (150.140.139.242), Dst: 150.140.129.30 (150.140.129.30)
User Datagram Protocol, Src Port: 59779 (59779), Dst Port: domain (53)
Domain Name System (query)
```

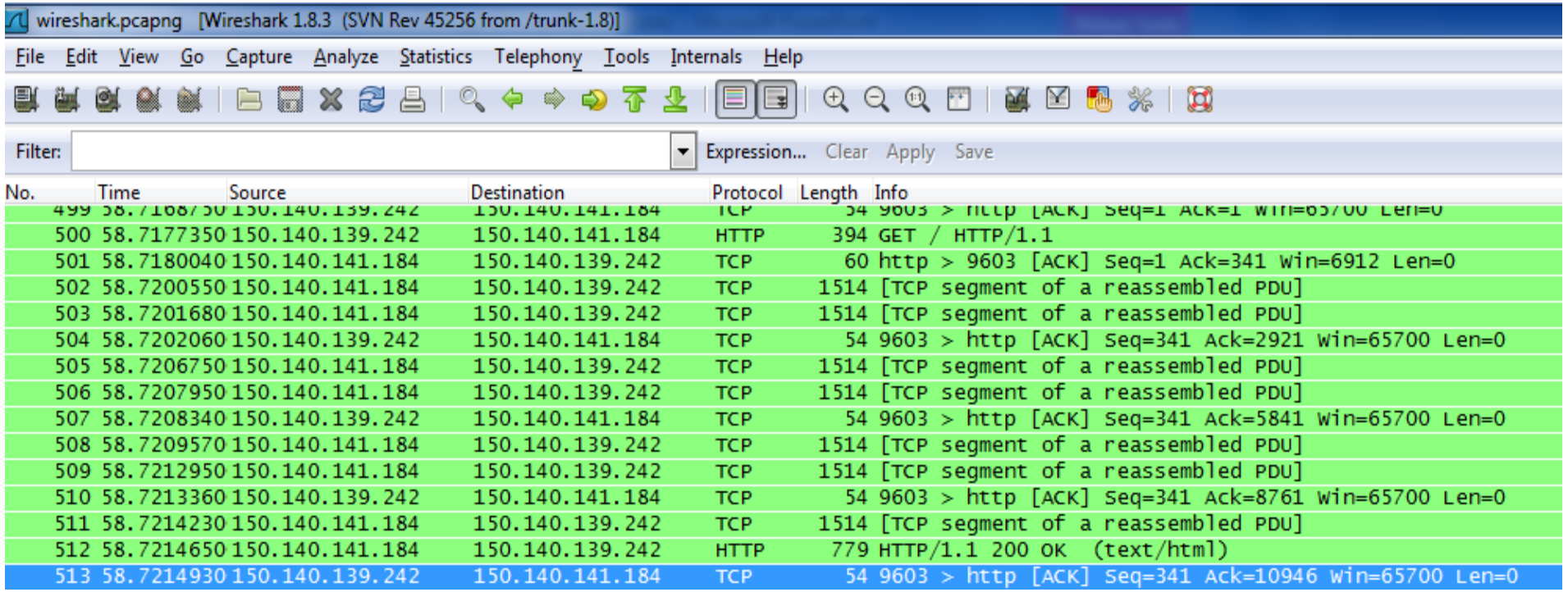
Ανάλυση Δεδομένων

- Δημιουργία TCP σύνδεσης



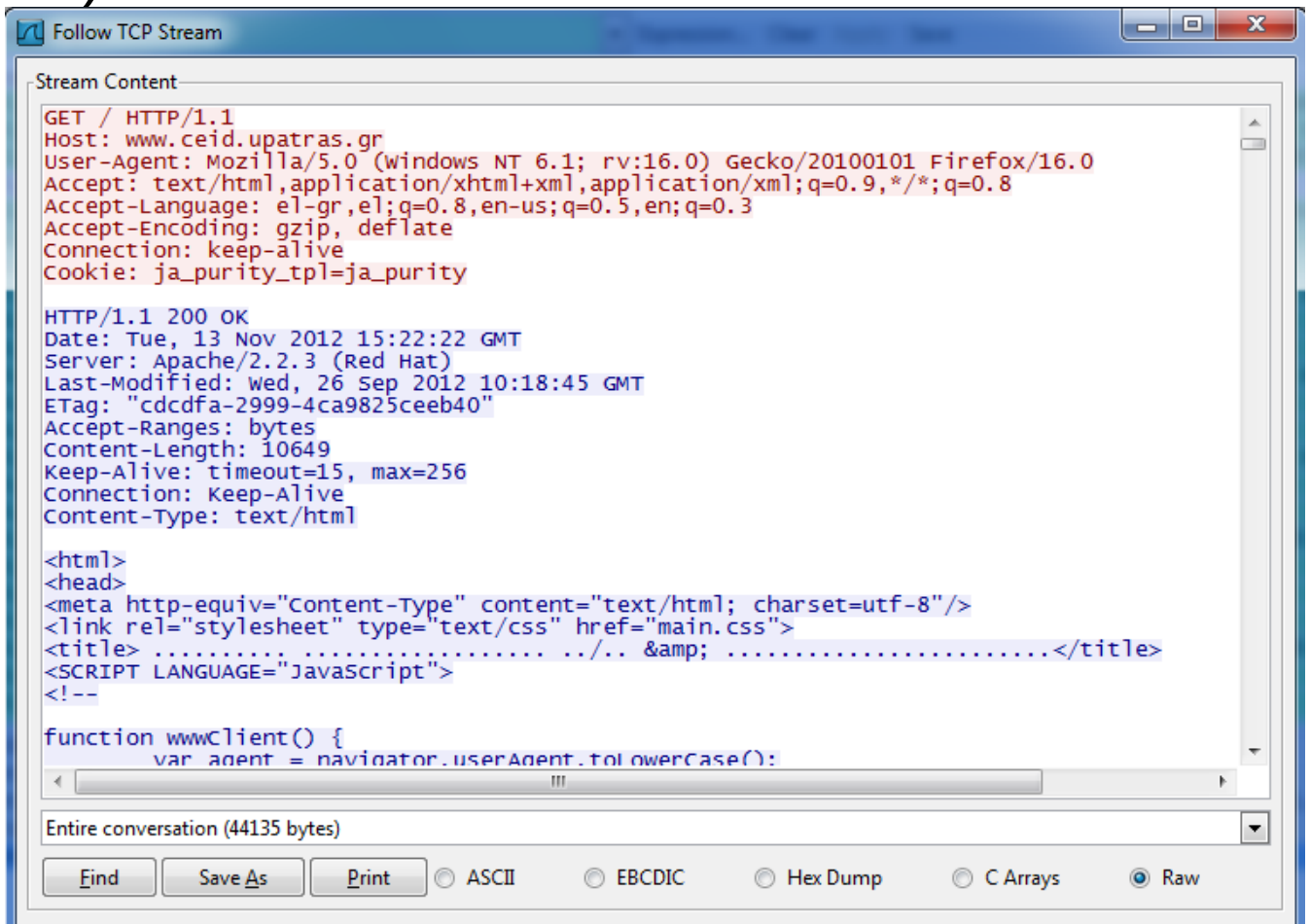
Ανάλυση Δεδομένων

- Μεταφορά δεδομένων



Ανάλυση Δεδομένων

- Μεταφορά δεδομένων (δεξί κλικ και “Follow TCP stream”)



Ανάλυση Δεδομένων

- Ολοκλήρωση σύνδεσης
- Ενώ νέες συνδέσεις δημιουργούνται για την μεταφορά των υπόλοιπων δεδομένων